Protección de datos y recuperación ante desastres

ONTAP 9

NetApp
March 05, 2026

This PDF was generated from https://docs.netapp.com/es-es/ontap/peering/index.html on March 05, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Protección de datos y recuperación ante desastres . . . 1
- Relaciones entre iguales de clústeres y SVM . . . 1
  - Obtenga más información sobre la paridad de clústeres de ONTAP y SVM . . . 1
  - Prepare la relación entre iguales de clústeres y SVM . . . 1
  - Configure las LIF de interconexión de clústeres . . . 5
  - Configure las relaciones de paridad . . . 19
  - Habilite el cifrado de clústeres entre iguales de ONTAP en relaciones entre iguales . . . 29
  - Quite el cifrado de clústeres de paridad de ONTAP de las relaciones entre iguales . . . 29
- Permite gestionar snapshots locales . . . 31
  - Obtenga más información sobre la gestión de snapshots locales de ONTAP . . . 31
  - Obtenga más información sobre las instantáneas de retención a largo plazo de ONTAP . . . 31
  - Configurar políticas de snapshots personalizadas . . . 31
  - Administrar instantáneas manualmente . . . 35
  - Gestione la reserva de snapshot . . . 38
  - Restaurar archivos desde instantáneas . . . 42
- Replicación de volúmenes de SnapMirror . . . 48
  - Obtenga más información sobre la replicación de volúmenes de SnapMirror . . . 49
  - Configure la replicación de volumen de SnapMirror . . . 82
  - Gestione la replicación de volúmenes de SnapMirror . . . 103
- Gestione la replicación de SVM de SnapMirror . . . 134
  - Obtenga más información sobre la replicación de SVM de ONTAP SnapMirror . . . 134
  - Replicar las configuraciones de SVM . . . 143
  - Sirva datos desde un destino de recuperación ante desastres de SVM de SnapMirror . . . 156
  - Vuelva a activar la SVM de origen de SnapMirror . . . 161
  - Convertir una relación de recuperación ante desastres de volúmenes de ONTAP SnapMirror en una relación de recuperación ante desastres de Storage Virtual Machine . . . 174
  - Elimine una relación de replicación de SVM de ONTAP SnapMirror . . . 175
- Gestionar la replicación de volúmenes raíz de SnapMirror . . . 176
  - Obtenga más información sobre la replicación de volúmenes raíz de ONTAP SnapMirror . . . 177
  - Crear e inicializar relaciones de reflejos de uso compartido de carga de ONTAP . . . 177
  - Actualizar una relación de reflejo de uso compartido de carga de ONTAP . . . 179
  - Promocione un reflejo de uso compartido de carga de ONTAP . . . 179
- Backup en el cloud . . . 181
  - Instalar una licencia en la nube de ONTAP SnapMirror . . . 181
  - Realice backups de los datos en el cloud con ONTAP SnapMirror . . . 182
  - Realice copias de seguridad de datos con NetApp Backup and Recovery . . . 184
- Archivado y cumplimiento de normativas con tecnología SnapLock . . . 188
  - Obtenga más información sobre ONTAP SnapLock . . . 188
  - Configure SnapLock . . . 194
  - Gestione los archivos WORM . . . 209
  - Mover un volumen SnapLock de ONTAP . . . 225
  - Bloquear una instantánea de ONTAP para protegerse contra ataques de ransomware . . . 226
- Grupos de consistencia . . . 235

Obtenga más información sobre los grupos de consistencia de ONTAP . . . 235
Obtenga información sobre los límites del grupo de consistencia de ONTAP . . . 241
Configurar un único grupo de consistencia de ONTAP . . . 242
Configurar un grupo de consistencia ONTAP jerárquico . . . 248
Proteger los grupos de consistencia de ONTAP . . . 252
Modificar volúmenes de miembros en un grupo de consistencia de ONTAP . . . 260
Modificar la geometría del grupo de consistencia de ONTAP . . . 266
Modificar las etiquetas de aplicaciones y componentes del grupo de consistencia de ONTAP . . . 272
Clonar un grupo de consistencia de ONTAP . . . 273
Eliminar un grupo de consistencia de ONTAP . . . 276
SnapMirror síncrono activo . . . 276
Introducción . . . 276
Planificación . . . 290
Configurar . . . 300
Gestione la sincronización activa de SnapMirror y proteja los datos . . . 344
Solucionar problemas . . . 362
Mediador de ONTAP para la sincronización activa de MetroCluster y SnapMirror . . . 372
Más información sobre ONTAP Mediator . . . 372
Nuevas funciones en ONTAP Mediator . . . 374
Instale o actualice . . . 379
Gestionar Mediador ONTAP . . . 423
Mantenga el SO del host para ONTAP Mediator . . . 454
Obtenga más información sobre la administración de sitios IP de MetroCluster con ONTAP System Manager . . . 458
Protección de datos mediante backup en cinta . . . 459
Obtenga información sobre la copia de seguridad en cinta de los volúmenes ONTAP FlexVol . . . 459
Flujo de trabajo de copia de seguridad y restauración de cintas de ONTAP . . . 459
Casos de uso para motores de copia de seguridad de volcado y SMTape de ONTAP . . . 460
Gestión de unidades de cinta . . . 461
Acerca de las unidades de cinta . . . 467
Transferir datos entre sistemas de almacenamiento . . . 476
NDMP para volúmenes FlexVol . . . 480
Obtenga información sobre la compatibilidad de NDMP con volúmenes ONTAP FlexGroup . . . 506
Obtenga información sobre NDMP con volúmenes SnapLock de ONTAP . . . 506
Gestione el modo NDMP de ámbito del nodo para volúmenes FlexVol . . . 506
Gestione el modo NDMP de ámbito SVM para volúmenes FlexVol . . . 508
Acerca del motor de volcado para volúmenes FlexVol . . . 515
Acerca del motor SMTape para volúmenes de FlexVol . . . 528
Supervisar las operaciones de backup y restauración a cinta para volúmenes de FlexVol . . . 533
Mensajes de error para backup y restauración a cinta de volúmenes de FlexVol . . . 537
Configuración de NDMP . . . 557
Obtenga más información sobre la configuración de NDMP de ONTAP . . . 558
Obtenga más información sobre el flujo de trabajo de configuración de NDMP de ONTAP . . . 558
Preparar configuraciones NDMP de ONTAP . . . 559
Verificar las conexiones del dispositivo de cinta NDMP de ONTAP . . . 562

Habilitar reservas de cinta para operaciones de respaldo NDMP de ONTAP 563
Configure NDMP con ámbito SVM 564
Configure el NDMP de ámbito del nodo 574
Configurar aplicaciones de respaldo para la configuración NDMP de ONTAP 580
Replicación entre software de NetApp Element y información general de ONTAP 580

Protección de datos y recuperación ante desastres

Relaciones entre iguales de clústeres y SVM

Obtenga más información sobre la paridad de clústeres de ONTAP y SVM

Puede crear una relación entre iguales de clústeres de origen y de destino, y entre máquinas virtuales de almacenamiento (SVM) de origen y de destino. Debe crear relaciones entre iguales entre estas entidades para poder replicar las snapshots con SnapMirror.

ONTAP 9.3 ofrece mejoras que simplifican la forma de configurar relaciones entre iguales entre clústeres y SVM. Los procedimientos de paridad de clústeres y SVM están disponibles para todas las versiones de ONTAP 9. Debe utilizar el procedimiento adecuado para su versión de ONTAP.

Los procedimientos se realizan mediante la interfaz de línea de comandos (CLI), no con System Manager ni con una herramienta de secuencias de comandos automatizadas.

Prepare la relación entre iguales de clústeres y SVM

Conceptos básicos de relación de paridad de ONTAP

Debe crear relaciones *entre iguales* entre los clústeres de origen y de destino, y entre SVM de origen y de destino antes de poder replicar snapshots mediante SnapMirror. Una relación de paridad define las conexiones de red que permiten que clústeres y SVM intercambien datos de forma segura.

Los clústeres y las SVM en relaciones entre iguales se comunican a través de la red de interconexión de clústeres mediante las interfaces lógicas de interconexión de clústeres (LIF)._ una LIF de interconexión de clústeres es una LIF compatible con el servicio de interfaz de red «núcleo entre clústeres» y normalmente se crea mediante la política de servicio de interfaz de red de «interconexión de clústeres predeterminada». Debe crear LIF de interconexión de clústeres en cada nodo en los clústeres que se van a establecer una relación entre iguales.

Las LIF de interconexión de clústeres utilizan las rutas que pertenecen a la SVM del sistema a la que se han asignado. ONTAP crea automáticamente una SVM del sistema para las comunicaciones a nivel de clúster dentro de un espacio IP.

Se admiten topologías en cascada y distribución ramificada. En una topología en cascada, solo necesita crear redes de interconexión de clústeres entre los clústeres principal y secundario, y entre los clústeres secundario y terciario. No es necesario crear una red de interconexión de clústeres entre el clúster principal y el terciario.

Es posible (pero no aconsejable) que un administrador elimine el servicio interclúster-core de la directiva de servicio de interconexión de clústeres predeterminada. Si esto sucede, las LIF creadas con «interconexión de clústeres predeterminada» no serán realmente LIF de interconexión de clústeres. Para confirmar que la política de servicio de interconexión de clústeres predeterminada contiene el servicio principal entre clústeres, utilice el siguiente comando:

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

Obtenga más información sobre `network interface service-policy show` en el "Referencia de comandos del ONTAP".

Requisitos previos de paridad de ONTAP

Antes de configurar cluster peering, debe confirmar que la conectividad, el puerto, la dirección IP, subred, firewall, y se cumplen los requisitos de nomenclatura de los clústeres.

A partir de ONTAP 9,6, Cluster peering proporciona compatibilidad de cifrado TLS 1,2 AES-256 GCM para la replicación de datos de forma predeterminada. Los cifrados de seguridad predeterminados («PSK-AES256-GCM-SHA384») son necesarios para que el emparejamiento de clústeres funcione incluso si el cifrado está desactivado.

A partir de ONTAP 9.11.1, los cifrados de seguridad DHE-PSK están disponibles por defecto.

A partir de ONTAP 9.15.1, Cluster peering proporciona compatibilidad de cifrado TLS 1,3 para la replicación de datos de forma predeterminada.

Requisitos de conectividad

Todas las LIF de interconexión de clústeres del clúster local deben poder comunicarse con todas las LIF de interconexión de clústeres del clúster remoto.

Aunque no es necesario, generalmente es más fácil configurar las direcciones IP que se usan para las LIF de interconexión de clústeres de la misma subred. Las direcciones IP pueden residir en la misma subred que las LIF de datos, o en una subred diferente. La subred que se utiliza en cada clúster debe cumplir los siguientes requisitos:

- La subred debe pertenecer al dominio de retransmisión que contenga los puertos que se utilizan para la comunicación entre clústeres.
- La subred debe tener suficientes direcciones IP disponibles para asignar a una LIF de interconexión de clústeres por nodo.

  Por ejemplo, en un clúster de cuatro nodos, la subred que se usa para la comunicación entre clústeres debe tener cuatro direcciones IP disponibles.

Cada nodo debe tener una LIF de interconexión de clústeres con una dirección IP en la red de interconexión de clústeres.

Las LIF entre clústeres pueden tener una dirección IPv4 o IPv6.

ONTAP le permite migrar sus redes entre iguales de IPv4 a IPv6 si, de manera opcional, permite que ambos protocolos estén presentes simultáneamente en las LIF de interconexión de clústeres. En las versiones anteriores, todas las relaciones de interconexión de clústeres de todo un clúster eran IPv4 o IPv6. Esto significaba que el cambio de protocolos era un evento que podía provocar interrupciones.

Requisitos de puertos

Se pueden usar puertos dedicados para la comunicación entre clústeres o para compartir puertos que usa la red de datos. Los puertos deben cumplir con los siguientes requisitos:

- Todos los puertos que se utilizan para comunicarse con un clúster remoto determinado deben estar en el mismo espacio IP.

  Se pueden utilizar varios espacios IP para establecer la misma relación entre iguales con varios clústeres. La conectividad de malla completa en par sólo se requiere dentro de un espacio IP.

- El dominio de retransmisión que se usa para la comunicación entre clústeres debe incluir al menos dos puertos por nodo para que la comunicación entre clústeres pueda conmutar por error de un puerto a otro.

  Los puertos que se añaden a un dominio de retransmisión pueden ser puertos de red físicos, VLAN o grupos de interfaces (ifgrps).

- Todos los puertos deben estar cableadas.
- Todos los puertos deben estar en buen estado.
- La configuración de MTU de los puertos debe ser coherente.

Requisitos del firewall

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".

Los firewalls y la política de firewall de interconexión de clústeres deben permitir los siguientes protocolos:

- Tráfico ICMP bidireccional
- Tráfico TCP iniciado bidireccional hacia las direcciones IP de todas las LIF de interconexión de clústeres a través de los puertos 11104 y 11105
- HTTPS bidireccional entre las LIF de interconexión de clústeres

  Aunque HTTPS no es necesario cuando se configura una relación de clústeres entre iguales con la CLI, se requiere HTTPS más adelante si se utiliza System Manager para configurar la protección de datos.

La `intercluster` política de firewall predeterminada permite el acceso a través del protocolo HTTPS y desde todas las direcciones IP (0,0.0,0/0). Puede modificar o reemplazar la política si es necesario.

Requisitos del clúster

Los clústeres deben cumplir los siguientes requisitos:

- No puede haber un clúster en una relación de paridad con más de 255 clústeres.

Utilice puertos ONTAP compartidos o dedicados

Se pueden usar puertos dedicados para la comunicación entre clústeres o para compartir puertos que usa la red de datos. Para decidir si se comparten puertos, debe tener en cuenta el ancho de banda de la red, el intervalo de replicación y la disponibilidad del puerto.

Es posible compartir puertos en un clúster con una relación entre iguales mientras se usan puertos dedicados en el otro.

Ancho de banda de red

Si tiene una red de alta velocidad, como 10 GbE, es posible que tenga suficiente ancho de banda LAN local para realizar la replicación con los mismos puertos de 10 GbE que se utilizan para el acceso a datos.

Incluso entonces, debería comparar su ancho de banda WAN disponible con su ancho de banda LAN. Si el ancho de banda WAN disponible es significativamente inferior a 10 GbE, es posible que deba utilizar puertos dedicados.

La única excepción a esta regla podría ser cuando todos los nodos del clúster replican los datos, en cuyo caso la utilización de ancho de banda suele extenderse por todos los nodos.

Si no utiliza puertos dedicados, el tamaño máximo de unidad de transmisión (MTU) de la red de replicación debe ser, por lo general, el mismo tamaño de MTU de la red de datos.

El intervalo de replicación

Si la replicación se realiza en horas de menor actividad, debería poder utilizar puertos de datos para la replicación incluso sin conexión LAN de 10 GbE.

Si la replicación se realiza durante el horario laboral normal, debe tener en cuenta la cantidad de datos que se replicarán y si se requiere tanto ancho de banda como para provocar la contención con protocolos de datos. Si el uso de la red por protocolos de datos (SMB, NFS e iSCSI) supera el 50%, debe usar puertos dedicados para la comunicación entre clústeres con el fin de no degradar el rendimiento en caso de producirse una conmutación por error de nodo.

Disponibilidad de puertos

Si determina que el tráfico de replicación interfiere con el tráfico de datos, puede migrar las LIF de interconexión de clústeres a cualquier otro puerto compartido compatible con la interconexión de clústeres en el mismo nodo.

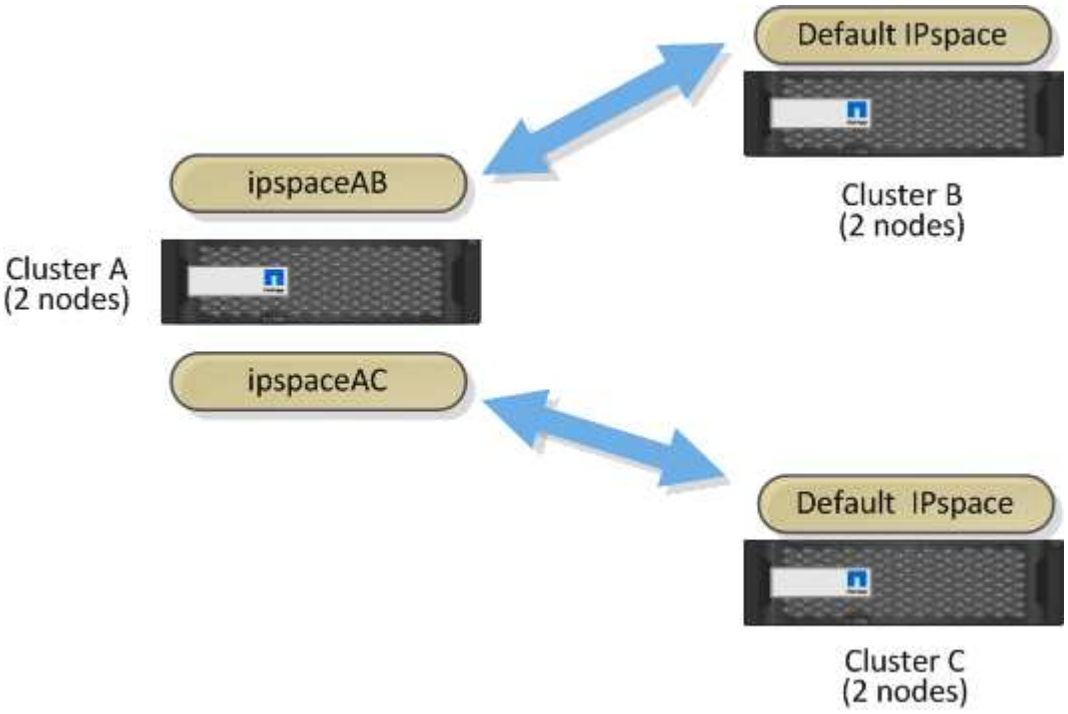
También puede dedicar puertos VLAN para la replicación. El ancho de banda del puerto se comparte entre todas las VLAN y el puerto base.

Utilice espacios IP de ONTAP personalizados para aislar el tráfico de replicación

Puede utilizar espacios IP personalizados para separar las interacciones que tiene un clúster con sus iguales. Esta configuración, denominada conectividad entre clústeres designada_, permite a los proveedores de servicios aislar el tráfico de replicación en entornos multi-tenant.

Suponga, por ejemplo, que desea que el tráfico de replicación entre el clúster A y el clúster B se separe del tráfico de replicación entre el clúster A y el clúster C. Para lograr esto, puede crear dos espacios IP en el clúster A.

Un espacio IP contiene las LIF de interconexión de clústeres que se usan para comunicarse con el clúster B. El otro contiene las LIF de interconexión de clústeres que se usan para comunicarse con el clúster C, como se muestra en la ilustración siguiente.



Información relacionada

- "Obtenga más información sobre la configuración del espacio IP de ONTAP"

Configure las LIF de interconexión de clústeres

Configure LIF de interconexión de clústeres de ONTAP en puertos de datos compartidos

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.

Pasos

1. Enumere los puertos del clúster:

   `network port show`

   Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

   El siguiente ejemplo muestra 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. Cree LIF de interconexión de clústeres en una SVM de administrador (espacio IP predeterminado) o una SVM de sistema (espacio IP personalizado):

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*
En ONTAP 9.5 y anteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

Obtenga más información sobre `network interface create` en el "Referencia de comandos del ONTAP".

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

```
cluster01::> network interface create -vserver cluster01 -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 cluster01 -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:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster`

Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

```
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:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster -failover`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster -failover`

Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

El ejemplo siguiente muestra que las LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02` del `e0c` puerto conmutarán al `e0d` puerto tras una conmutación al nodo de respaldo.

```
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
```

Configurar LIF de interconexión de clústeres de ONTAP en puertos dedicados

Puede configurar LIF de interconexión de clústeres en puertos dedicados. Al hacerlo, normalmente aumenta el ancho de banda disponible para el tráfico de replicación.

Pasos

1. Enumere los puertos del clúster:

   `network port show`

   Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

   El siguiente ejemplo muestra 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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Determine qué puertos están disponibles para dedicar a la comunicación entre clústeres:

   `network interface show -fields home-port,curr-port`

   Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

   El ejemplo siguiente muestra que se `e0e` `e0f` han asignado puertos y no se han asignado LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. Cree un grupo de recuperación tras fallos para los puertos dedicados:

`network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical _or_logical_ports`

En el siguiente ejemplo se asignan puertos `e0e` y `e0f` al grupo de conmutación por error `intercluster01` en la SVM del sistema `cluster01`:

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. Compruebe que el grupo de recuperación tras fallos se ha creado:

   `network interface failover-groups show`

   Obtenga más información sobre `network interface failover-groups show` en el "Referencia de comandos del ONTAP".

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. Cree LIF de interconexión de clústeres en la SVM del sistema y asígnelas al grupo de recuperación tras fallos.

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group`
En ONTAP 9.5 y anteriores:	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group`

Obtenga más información sobre `network interface create` en el "Referencia de comandos del ONTAP".

En el siguiente ejemplo se crean LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02` en el grupo de recuperación tras fallos `intercluster01`:

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

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

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster`

Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

```
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  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

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

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster -failover`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster -failover`

Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

El ejemplo siguiente muestra que las LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02` del puerto SVM`e0e` conmutarán al `e0f` puerto tras una conmutación al nodo de respaldo.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configurar LIF de interconexión de clústeres de ONTAP en espacios IP personalizados

Puede configurar LIF de interconexión de clústeres en espacios IP personalizados. Al hacerlo, puede aislar el tráfico de replicación en entornos multi-tenant.

Cuando crea un espacio IP personalizado, el sistema crea una máquina virtual de almacenamiento (SVM) del sistema para que actúe como contenedor de los objetos del sistema en ese espacio IP. Puede usar la nueva SVM como contenedor de cualquier LIF entre clústeres del nuevo espacio IP. La nueva SVM tiene el mismo nombre que el espacio IP personalizado.

Pasos

1. Enumere los puertos del clúster:

   `network port show`

   Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

   El siguiente ejemplo muestra 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
       e0e       Default      Default          up     1500   auto/1000
       e0f       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
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. Cree espacios IP personalizados en el clúster:

   `network ipspace create -ipspace` *`ipspace`*

   El siguiente ejemplo crea el espacio IP personalizado `ipspace-IC1` :

   ```
   cluster01::> network ipspace create -ipspace ipspace-IC1
   ```

   Obtenga más información sobre `network ipspace create` en el "Referencia de comandos del ONTAP".

3. Determine qué puertos están disponibles para dedicar a la comunicación entre clústeres:

   `network interface show -fields home-port,curr-port`

   Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

   El ejemplo siguiente muestra que se `e0e` `e0f` han asignado puertos y no se han asignado LIF:

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01_clus1   e0a       e0a
Cluster cluster01_clus2   e0b       e0b
Cluster cluster02_clus1   e0a       e0a
Cluster cluster02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

4. Elimine los puertos disponibles del dominio de difusión predeterminado:

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   Un puerto no puede estar en más de un dominio de retransmisión a la vez. Obtenga más información sobre `network port broadcast-domain remove-ports` en el "Referencia de comandos del ONTAP".

   En el ejemplo siguiente se quitan los puertos `e0e` y `e0f` del dominio de retransmisión predeterminado:

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. Compruebe que los puertos se han eliminado del dominio de retransmisión predeterminado:

   `network port show`

   Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

   En el ejemplo siguiente se muestra que los puertos `e0e` y `e0f` se han eliminado del dominio de retransmisión predeterminado:

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU     Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. Cree un dominio de retransmisión en el espacio IP personalizado:

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   En el siguiente ejemplo, se crea el dominio de retransmisión `ipspace-IC1-bd` en el espacio IP `ipspace-IC1`:

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. Compruebe que se ha creado el dominio de retransmisión:

   `network port broadcast-domain show`

   Obtenga más información sobre `network port broadcast-domain show` en el "Referencia de comandos del ONTAP".

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                       Update
Name    Domain Name    MTU  Port List                   Status Details
------- ----------- ------  --------------------------- --------------
Cluster Cluster       9000
                            cluster01-01:e0a            complete
                            cluster01-01:e0b            complete
                            cluster01-02:e0a            complete
                            cluster01-02:e0b            complete
Default Default       1500
                            cluster01-01:e0c            complete
                            cluster01-01:e0d            complete
                            cluster01-01:e0f            complete
                            cluster01-01:e0g            complete
                            cluster01-02:e0c            complete
                            cluster01-02:e0d            complete
                            cluster01-02:e0f            complete
                            cluster01-02:e0g            complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e            complete
                            cluster01-01:e0f            complete
                            cluster01-02:e0e            complete
                            cluster01-02:e0f            complete
```

8. Cree LIF de interconexión de clústeres en la SVM del sistema y asígnelas al dominio de retransmisión:

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
En ONTAP 9.5 y anteriores:	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

La LIF se crea en el dominio de retransmisión al que está asignado el puerto inicial. El dominio de difusión tiene un grupo de conmutación por error predeterminado con el mismo nombre que el dominio de difusión. Obtenga más información sobre `network interface create` en el "Referencia de comandos del ONTAP".

En el ejemplo siguiente se crean LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02` en el dominio de retransmisión `ipspace-IC1-bd`:

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

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

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster`

Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0f
true
```

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

Opción	Descripción
En ONTAP 9.6 y posterior:	`network interface show -service-policy default-intercluster -failover`
En ONTAP 9.5 y anteriores:	`network interface show -role intercluster -failover`

Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

El ejemplo siguiente muestra que las LIF de interconexión de clústeres `cluster01_icl01` y `cluster01_icl02` del puerto SVM `e0e` conmutan al «e0f» puerto:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

Configure las relaciones de paridad

Crear relaciones de paridad entre clústeres de ONTAP

Para poder proteger sus datos replicándolos en un clúster remoto con fines de backup de datos y recuperación ante desastres, debe crear una relación de paridad de clústeres entre el clúster local y el remoto.

Acerca de esta tarea

Este procedimiento se aplica a los sistemas FAS, AFF y ASA. Si tiene un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 o ASA C30), siga "estos pasos" para crear y configurar la replicación de instantáneas. Los sistemas R2 de ASA ofrecen una experiencia de ONTAP simplificada específica para clientes de SAN.

Existen varias políticas de protección predeterminadas disponibles. Debe haber creado las políticas de protección si desea usar políticas personalizadas.

Antes de empezar

Si utiliza la CLI de ONTAP, debe haber creado LIF de interconexión de clústeres en cada nodo de los clústeres en relación de paridad usando uno de los siguientes métodos:

- "Configure las LIF de interconexión de clústeres en puertos de datos compartidos"
- "Configure LIF de interconexión de clústeres en puertos de datos dedicados"
- "Configure las LIF de interconexión de clústeres en espacios IP personalizados"

Pasos

Lleve a cabo esta tarea mediante System Manager de ONTAP o la interfaz de línea de comandos de ONTAP.

System Manager

1. En el clúster local, haga clic en **Clúster > Configuración**.
2. En la sección **Intercluster Settings**, haga clic en **Add Network Interfaces** e introduzca la dirección IP y la máscara de subred para agregar interfaces de red de interconexión de clústeres para el cluster.

   Repita este paso en el clúster remoto.
3. En el clúster remoto, haga clic en **Clúster > Configuración**.
4. Haga clic en ⋮ la sección **Peones de clúster** y seleccione **Generar contraseña**.
5. Seleccione la versión del clúster de ONTAP remoto.
6. Copie la clave de acceso generada.
7. En el clúster local, en **Cluster peers**, haga clic ⋮ y seleccione **Peer cluster**.
8. En la ventana **Peer cluster**, pega la frase de acceso y haz clic en **Iniciar interconexión de clústeres**.

CLI

1. En el clúster de destino, cree una relación entre iguales con el clúster de origen:

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addrs
   <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ipspace
   <ipspace>
   ```

   Si especifica tanto `-generate-passphrase` como `-peer-addrs`, solo el clúster cuyas LIF entre clústeres se especifican en `-peer-addrs` puede usar la contraseña generada.

   Puede ignorar `-ipspace` la opción si no está utilizando un espacio IP personalizado. Obtenga más información sobre `cluster peer create` en el "Referencia de comandos del ONTAP".

   Si está creando la relación entre iguales en ONTAP 9.6 o posterior y no desea que las comunicaciones entre pares entre clústeres se cifren, debe utilizar la `-encryption-protocol -proposed none` opción para desactivar el cifrado.

   En el siguiente ejemplo, se crea una relación de paridad de clústeres con un clúster remoto sin especificar y se autorizan previamente las relaciones entre iguales con las SVM `vs1` y `vs2` en el clúster local:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

En el siguiente ejemplo se crea una relación entre iguales de clústeres con el clúster remoto en las direcciones IP de LIF entre clústeres 192.140.112.103 y 192.140.112.104, y se autoriza previamente una relación entre iguales con cualquier SVM del clúster local:

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

En el siguiente ejemplo, se crea una relación de paridad de clústeres con un clúster remoto sin especificar y se autorizan previamente las relaciones entre iguales con las SVM`vs1` y `vs2` en el clúster local:

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. En el clúster de origen, autentique el clúster de origen al clúster de destino:

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

Obtenga más información sobre `cluster peer create` en el "Referencia de comandos del ONTAP".

En el siguiente ejemplo se autentica el clúster local en el clúster remoto en las direcciones IP de LIF entre clústeres 192.140.112.101 y 192.140.112.102:

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

Introduzca la frase de acceso para la relación entre iguales cuando se le solicite.

3. Compruebe que se ha creado la relación de paridad entre clústeres:

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
               Availability of the Remote Cluster: Available
                              Remote Cluster Name: cluster2
                              Active IP Addresses: 192.140.112.101,
192.140.112.102
                            Cluster Serial Number: 1-80-123456
                   Address Family of Relationship: ipv4
             Authentication Status Administrative: no-authentication
                Authentication Status Operational: absent
                                  Last Update Time: 02/05 21:05:41
                     IPspace for the Relationship: Default
```

4. Compruebe la conectividad y el estado de los nodos en la relación de paridad:

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general de preparación para la recuperación ante desastres de volúmenes"

Crear relaciones entre iguales de SVM entre clústeres de ONTAP

Puede utilizar el `vserver peer create` comando para crear una relación entre iguales entre SVM en clústeres locales y remotos.

Antes de empezar

- Los clústeres de origen y destino deben tener una relación entre iguales.
- Debe tener relaciones entre iguales "preautorizadas" para las SVM en el clúster remoto.

  Para obtener más información, consulte "Creación de una relación de paridad entre clústeres".

Acerca de esta tarea

Puede "autorizar previamente" relaciones entre pares para múltiples SVM enumerando los SVM en el

`-initial-allowed-vserver` Opción al crear una relación de pares de clúster. Para obtener más información, consulte "Creación de una relación de paridad entre clústeres".

Pasos

1. En el clúster de destino de protección de datos, muestre las SVM que están autorizadas previamente para la paridad:

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. En el clúster de origen de protección de datos, cree una relación entre iguales con una SVM preautorizada en el clúster de destino de protección de datos:

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Obtenga más información sobre `vserver peer create` en el "Referencia de comandos del ONTAP".

   En el siguiente ejemplo se crea una relación entre iguales entre la SVM local `pvs1` y la SVM remota preautorizada `vs1`:

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   ```

3. Compruebe las relaciones entre iguales de SVM:

   `vserver peer show`

   ```
   cluster01::> vserver peer show
               Peer        Peer                           Peering
   Remote
   Vserver     Vserver     State        Peer Cluster      Applications
   Vserver
   ----------- ----------- ------------ ----------------- --------------
   ---------
   pvs1        vs1         peered       cluster02         snapmirror
   vs1
   ```

Añada relaciones entre iguales de SVM entre clústeres de ONTAP

Si crea una SVM después de configurar una relación de paridad de clústeres, deberá añadir una relación de paridad para la SVM manualmente. Puede usar el `vserver peer create` comando para crear una relación entre iguales entre SVM. Una vez

creada la relación de iguales, se puede ejecutar `vserver peer accept` en el clúster remoto para autorizar la relación de iguales.

Antes de empezar

Los clústeres de origen y destino deben tener una relación entre iguales.

Acerca de esta tarea

Puede crear relaciones entre iguales entre SVM en el mismo clúster para el backup de datos local. Obtenga más información sobre `vserver peer create` en el "Referencia de comandos del ONTAP".

En ocasiones, los administradores usan `vserver peer reject` el comando para rechazar una relación entre iguales de SVM propuesta. Si la relación entre las SVM está en el `rejected` estado, debe eliminar esa relación para poder crear una nueva. Obtenga más información sobre `vserver peer reject` en el "Referencia de comandos del ONTAP".

Pasos

1. En el clúster de origen de protección de datos, cree una relación entre iguales con una SVM en el clúster de destino de protección de datos:

   `vserver peer create -vserver local_SVM -peer-vserver remote_SVM -applications snapmirror|file-copy|lun-copy -peer-cluster remote_cluster`

   En el siguiente ejemplo se crea una relación entre iguales entre la SVM local`pvs1` y la SVM remota`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   Si las SVM locales y remotas tienen los mismos nombres, debe usar un *local name* para crear la relación entre iguales de SVM:

   ```
   cluster01::> vserver peer create -vserver vs1 -peer-vserver
   vs1 -applications snapmirror -peer-cluster cluster01
   -local-name cluster1vs1LocallyUniqueName
   ```

2. En el clúster de origen de protección de datos, compruebe que se ha iniciado la relación de paridad:

   `vserver peer show-all`

   Obtenga más información sobre `vserver peer show-all` en el "Referencia de comandos del ONTAP".

   En el ejemplo siguiente se muestra que se`pvs1vs1` ha iniciado la relación entre iguales entre SVM y SVM:

```
cluster01::> vserver peer show-all
            Peer        Peer                         Peering
Vserver     Vserver     State      Peer Cluster      Applications
--------    --------    ---------  -------------     ------------
pvs1        vs1         initiated   Cluster02          snapmirror
```

3. En el clúster de destino de la protección de datos, muestre la relación entre iguales de SVM pendiente:

   `vserver peer show`

   Obtenga más información sobre `vserver peer show` en el "Referencia de comandos del ONTAP".

   El siguiente ejemplo muestra las relaciones entre iguales pendientes para `cluster02`:

```
cluster02::> vserver peer show

                  Peer               Peer
Vserver           Vserver            State
-----------       -----------        ------------
vs1               pvs1               pending
```

4. En el clúster de destino de la protección de datos, autorice la relación entre iguales pendiente:

   `vserver peer accept -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   Obtenga más información sobre `vserver peer accept` en el "Referencia de comandos del ONTAP".

   En el siguiente ejemplo se autoriza la relación entre iguales entre la SVM local `vs1` y la SVM remota `pvs1`:

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. Compruebe las relaciones entre iguales de SVM:

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                           Peering
Remote
Vserver     Vserver     State        Peer Cluster      Applications
Vserver
----------- ----------- ------------ ----------------- --------------
---------
pvs1        vs1         peered       cluster02         snapmirror
vs1
```

Habilite el cifrado de clústeres entre iguales de ONTAP en relaciones entre iguales

A partir de ONTAP 9.6, el cifrado de paridad de clústeres está habilitado de forma predeterminada en todas las relaciones de paridad de clústeres que haya creado recientemente. El cifrado de interconexión de clústeres utiliza una clave precompartida (PSK) y la capa de seguridad de transporte (TLS) para proteger las comunicaciones de interconexión entre clústeres. Esto añade una capa adicional de seguridad entre los clústeres con una relación entre iguales.

Acerca de esta tarea

Si va a actualizar clústeres con una relación entre iguales a ONTAP 9.6 o posterior y la relación de paridad se creó en ONTAP 9.5 o versiones anteriores, el cifrado de paridad de clústeres se debe habilitar manualmente después de la actualización. Ambos clústeres de la relación de paridad deben ejecutar ONTAP 9.6 o una versión posterior para habilitar el cifrado de paridad de clústeres.

Pasos

1. En el clúster de destino, habilite el cifrado para las comunicaciones con el clúster de origen:

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. Cuando se le solicite, introduzca una frase de contraseña.
3. En el clúster de origen de la protección de datos, habilite el cifrado para la comunicación con el clúster de destino de la protección de datos:

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. Cuando se le solicite, escriba la misma clave de acceso introducida en el clúster de destino.

Obtenga más información sobre `cluster peer modify` en el "Referencia de comandos del ONTAP".

Quite el cifrado de clústeres de paridad de ONTAP de las relaciones entre iguales

De forma predeterminada, el cifrado de paridad de clústeres está habilitado en todas las relaciones entre iguales creadas en ONTAP 9.6 o posterior. Si no desea utilizar el cifrado para las comunicaciones entre clústeres entre iguales, puede deshabilitarlo.

Pasos

1. En el clúster de destino, modifique las comunicaciones con el clúster de origen para interrumpir el uso del cifrado de interconexión de clústeres:
   - Para eliminar el cifrado, pero mantener la autenticación, introduzca:

     ```
     cluster peer modify <source_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Para eliminar el cifrado y la autenticación:
     i. Modifique la política de interconexión de clústeres para permitir el acceso sin autenticar:

        ```
        cluster peer policy modify -is-unauthenticated-access-permitted
        true
        ```

     ii. Modificar cifrado y acceso de autenticación:

        ```
        cluster peer modify <source_cluster> -auth-status no-
        authentication
        ```

2. Cuando se le solicite, introduzca la frase de acceso.
3. Vuelva a introducirla para confirmar la frase de acceso.
4. En el clúster de origen, deshabilite el cifrado para la comunicación con el clúster de destino:
   - Para eliminar el cifrado, pero mantener la autenticación, introduzca:

     ```
     cluster peer modify <destination_cluster> -auth-status-admin use-
     authentication -encryption-protocol-proposed none
     ```

   - Para eliminar el cifrado y la autenticación:
     i. Modifique la política de interconexión de clústeres para permitir el acceso sin autenticar:

        ```
        cluster peer policy modify -is-unauthenticated-access-permitted
        true
        ```

     ii. Modificar cifrado y acceso de autenticación:

        ```
        cluster peer modify <destination_cluster> -auth-status no-
        authentication
        ```

5. Cuando se le solicite, introduzca y vuelva a introducir la misma clave de acceso que utilizó en el clúster de destino.

Permite gestionar snapshots locales

Obtenga más información sobre la gestión de snapshots locales de ONTAP

Una *snapshot* es una imagen puntual de solo lectura de un volumen. La imagen consume un espacio de almacenamiento mínimo y apenas supone una sobrecarga de rendimiento, ya que sólo registra los cambios realizados en los archivos desde la última copia Snapshot.

Puede utilizar una instantánea para restaurar todo el contenido de un volumen o para recuperar archivos o LUN individuales. Las instantáneas se almacenan en el directorio del volumen. `.snapshot`

En ONTAP 9.4 y versiones posteriores, un FlexVol volume puede contener hasta 1023 instantáneas. En ONTAP 9.3 y versiones anteriores, un volumen puede contener hasta 255 instantáneas.

A partir de ONTAP 9,8, los volúmenes FlexGroup pueden contener 1023 snapshots. Para obtener más información, consulte "Proteger los volúmenes de FlexGroup mediante snapshots".

Obtenga más información sobre las instantáneas de retención a largo plazo de ONTAP

Las relaciones de SnapMirror con un tipo de política "bóveda" o "espejo-bóveda" permiten la creación de instantáneas directamente en el volumen secundario de la relación SnapMirror . Estas instantáneas se conservan en el destino como copias de seguridad. Estas instantáneas a menudo se crean para la retención a largo plazo y se denominan instantáneas de retención a largo plazo.

Para crear una instantánea de retención a largo plazo, especifique un programa de creación de instantáneas en la regla de política de SnapMirror , el prefijo del nombre de la instantánea, la etiqueta de SnapMirror y el recuento de retención. Esta instantánea se conserva en el volumen de destino de SnapMirror independientemente de las reglas de retención en el origen.

Las instantáneas de retención a largo plazo solo están disponibles para configuraciones de FlexVol SnapMirror . No se pueden crear instantáneas de retención a largo plazo para configuraciones de FlexGroup SnapMirror .

En una relación en cascada de SnapMirror , las instantáneas de retención a largo plazo solo se pueden crear en el último volumen de la cascada.

Información relacionada

- "Obtenga más información sobre cómo funcionan las implementaciones en cascada"
- "Defina una programación de ONTAP SnapMirror para crear una copia local en el destino"

Configurar políticas de snapshots personalizadas

Obtenga información sobre la configuración de políticas Snapshot de ONTAP personalizadas

A *snapshot policy* define la forma en que el sistema crea instantáneas. La política especifica cuándo crear snapshots, cuántas copias se conservan y cómo asignarles un

nombre. Por ejemplo, un sistema puede crear una copia Snapshot todos los días a las 12:10 a.m., conservar las dos copias más recientes y asignar el nombre a las copias «daaily.`timestamp`».

La política predeterminada para un volumen crea automáticamente Snapshot en la siguiente programación, con las copias de Snapshot más antiguas eliminadas para dejar espacio para copias más recientes:

- Un máximo de seis instantáneas cada hora tomadas cinco minutos más allá de la hora.
- Un máximo de dos instantáneas diarias tomadas de lunes a sábado a las 10 minutos después de la medianoche.
- Un máximo de dos instantáneas semanales tomadas cada domingo a las 15 minutos después de la medianoche.

A menos que se especifique una política de snapshot al crear un volumen, el volumen hereda la política de Snapshot asociada con la SVM que contiene la máquina virtual de almacenamiento (SVM).

Cuándo configurar una política de snapshots de ONTAP personalizada

Si la política de snapshots predeterminada no es adecuada para un volumen, se puede configurar una política personalizada que modifique la frecuencia, la retención y el nombre de snapshots. La programación estará dictada principalmente por la tasa de cambio del sistema de archivos activo.

Puede ser recomendable realizar el backup de un sistema de archivos muy utilizado, como una base de datos, cada hora, mientras que el backup de archivos de uso poco frecuente una vez al día. Incluso en el caso de una base de datos, suele ejecutar un backup completo una o dos veces al día, mientras realiza el backup de los registros de transacciones cada hora.

Otros factores son la importancia de los archivos para la organización, el SLA, el RPO y el RTO. En términos generales, sólo deberá conservar tantas instantáneas como sea necesario.

Crear una programación de tareas de Snapshot de ONTAP

Una política de Snapshot requiere al menos una programación de trabajo de Snapshot. Puede usar System Manager o `job schedule cron create` el comando para crear una programación de trabajo. Obtenga más información sobre `job schedule cron create` en el "Referencia de comandos del ONTAP".

Acerca de esta tarea

Este procedimiento se aplica a los sistemas FAS, AFF y ASA. Si tiene un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 o ASA C30), siga "estos pasos" para crear una programación de trabajos de instantáneas. Los sistemas R2 de ASA ofrecen una experiencia de ONTAP simplificada específica para clientes de SAN.

De forma predeterminada, ONTAP forma los nombres de las instantáneas agregando una marca de tiempo al nombre de la programación del trabajo.

Si especifica valores para el día del mes y el día de la semana, los valores se consideran independientes. Por ejemplo, un programa cron con la especificación de día `Friday` y el día del mes `13` se ejecuta todos los viernes y el día 13th de cada mes, no solo los viernes 13th.

Ejemplo 1. Pasos

System Manager

1. Vaya a **Protección > Descripción general** y expanda **Configuración de política local**.
2. En el panel **Schedules**, haga clic en →.
3. En la ventana **Schedules**, haga clic en + Add .
4. En la ventana **Agregar horario**, ingrese el nombre del horario y elija el contexto y el tipo de horario.
5. Haga clic en **Guardar**.

CLI

1. Crear un programa de trabajo:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Para `-month` `-dayofweek` , y `-hour`, puede especificar `all` que se ejecute el trabajo cada mes, día de la semana y hora, respectivamente.

A partir de ONTAP 9.10.1, puede incluir Vserver para su programación de trabajo:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

El siguiente ejemplo crea una programación de trabajo llamada `myweekly` que se ejecuta los sábados a las 3:00 a.m.:

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

En el siguiente ejemplo se crea una programación llamada `myweeklymulti` que especifica varios días, horas y minutos:

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

Cree una política de snapshots de ONTAP

Una política de Snapshot especifica cuándo crear snapshots, cuántas copias se retendrán y cómo asignarles un nombre. Por ejemplo, un sistema puede crear una copia Snapshot todos los días a las 12:10:00, conservar las dos copias más recientes y

llamarlas «daaily.*timestamp*.» Una política de Snapshot puede contener hasta cinco programaciones de trabajos.

Acerca de esta tarea

Este procedimiento se aplica a los sistemas FAS, AFF y ASA. Si tiene un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 o ASA C30), siga "estos pasos" para crear una política de instantáneas. Los sistemas R2 de ASA ofrecen una experiencia de ONTAP simplificada específica para clientes de SAN.

De forma predeterminada, ONTAP forma los nombres de las instantáneas agregando una marca de tiempo al nombre del programa de trabajo:

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Si lo prefiere, puede sustituir un prefijo por el nombre del programa de trabajo.

```
`snapmirror-label`La opción es para la replicación de SnapMirror. Para
obtener más información, consulte xref:{relative_path}define-rule-policy-
task.html["Definición de una regla para una política"].
```

Pasos

Puede crear una política de Snapshot mediante System Manager o la interfaz de línea de comandos de ONTAP. El procedimiento crea una política de Snapshot únicamente en el clúster local.

System Manager

1. Vaya a **Protección > Descripción general** y expanda **Configuración de política local**.
2. En el panel **Políticas de instantánea**, haga clic en →.
3. En la pestaña **Políticas de instantánea**, haga clic en + Add .
4. En la ventana **Add snapshot policy**, introduzca el nombre de la política y elija el ámbito.
5. Haga clic en + Add .
6. Para seleccionar una planificación, haga clic en el nombre de la programación que se muestra actualmente, haga clic en ⌄ y seleccione una programación diferente.
7. Introduzca las copias máximas de Snapshot que se retendrán y, si es necesario, introduzca la etiqueta de SnapMirror y el período de retención de SnapLock.
8. Haga clic en **Guardar**.

CLI

1. Cree una política de Snapshot:

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

En el siguiente ejemplo se crea una política de Snapshot llamada `snap_policy_daily` que se ejecuta en una `daily` programación. La política tiene un máximo de cinco snapshots, cada una con el nombre `daily.`*`timestamp`* y la etiqueta SnapMirror `daily` :

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

Administrar instantáneas manualmente

Crear y eliminar copias Snapshot manualmente

Las Snapshot se pueden crear manualmente cuando no se puede esperar a que se cree una snapshot programada y se pueden eliminar cuando ya no son necesarias.

Acerca de esta tarea

Este procedimiento se aplica a los sistemas FAS, AFF y ASA. Si tiene un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 o ASA C30), siga "estos pasos" para crear una instantánea a pedido. Los sistemas R2 de ASA ofrecen una experiencia de ONTAP simplificada específica para clientes de SAN.

Cree una instantánea manualmente

Puede crear manualmente una copia de Snapshot mediante System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

Pasos

1. Vaya a **Almacenamiento > Volúmenes** y seleccione la pestaña **Instantáneas**.
2. Haga clic en + Add .
3. En la ventana **Agregar una instantánea**, acepte el nombre predeterminado de la instantánea o edítela si lo desea.
4. **Opcional**: Añade una etiqueta de SnapMirror.
5. Haga clic en **Agregar**.

CLI

1. Cree una instantánea:

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

Elimine las instantáneas manualmente

Puede eliminar manualmente una copia de Snapshot mediante System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

Pasos

1. Vaya a **Almacenamiento > Volúmenes** y seleccione la pestaña **Copias de instantánea**.
2. Localice la instantánea que desea eliminar, haga clic en ⋮ y seleccione **Eliminar**.
3. En la ventana **Eliminar instantánea**, selecciona **Eliminar instantánea**.
4. Haga clic en **Eliminar**.

CLI

1. Utilice `volume snapshot show` el comando para verificar las copias Snapshot que desea eliminar.

```
volume snapshot show -vserver <SVM> -volume <volume>
```

En este ejemplo, el comando muestra las copias Snapshot del volumen vol3 en la SVM VS3.

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                  Size   Total% Used%
-------- ------- ------------------------ -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB    0%    32%
                 snap2.2013-05-09_0010   76KB    0%    32%
                 snap2.2013-05-10_0010   76KB    0%    32%
                 snap3.2013-05-10_1005   72KB    0%    31%
                 snap3.2013-05-10_1105   72KB    0%    31%
                 snap3.2013-05-10_1205   72KB    0%    31%
                 snap3.2013-05-10_1305   72KB    0%    31%
                 snap3.2013-05-10_1405   72KB    0%    31%
                 snap3.2013-05-10_1505   72KB    0%    31%
10 entries were displayed.
```

2. Eliminar una instantánea:

Si desea…	Introduzca este comando…
Elimine una sola copia de Snapshot	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name_`

Si desea…	Introduzca este comando…
Elimine varias copias Snapshot	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name1_[,_snapshot_name2_,...]`
Elimine todas las snapshots	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot *`

Calcule el espacio reclamado antes de eliminar instantáneas

A partir de ONTAP 9.10.1, puede usar System Manager para seleccionar las copias Snapshot que desea eliminar y calcular el espacio reclamante antes de eliminarlas.

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione el volumen del cual desea eliminar copias de Snapshot.
3. Haga clic en **Instantáneas**.
4. Seleccione una o más copias de Snapshot.
5. Haga clic en **calcular espacio recuperable**.

Gestione la reserva de snapshot

Infórmese sobre la gestión de la reserva de snapshot de ONTAP

Snapshot reserve reserva un porcentaje de espacio en disco para las instantáneas, cinco por ciento por defecto. Dado que las instantáneas utilizan espacio en el sistema de archivos activo cuando se agota la reserva de instantáneas, es posible que desee aumentar la reserva de instantáneas según sea necesario. También puede eliminar automáticamente las instantáneas cuando la reserva esté llena.

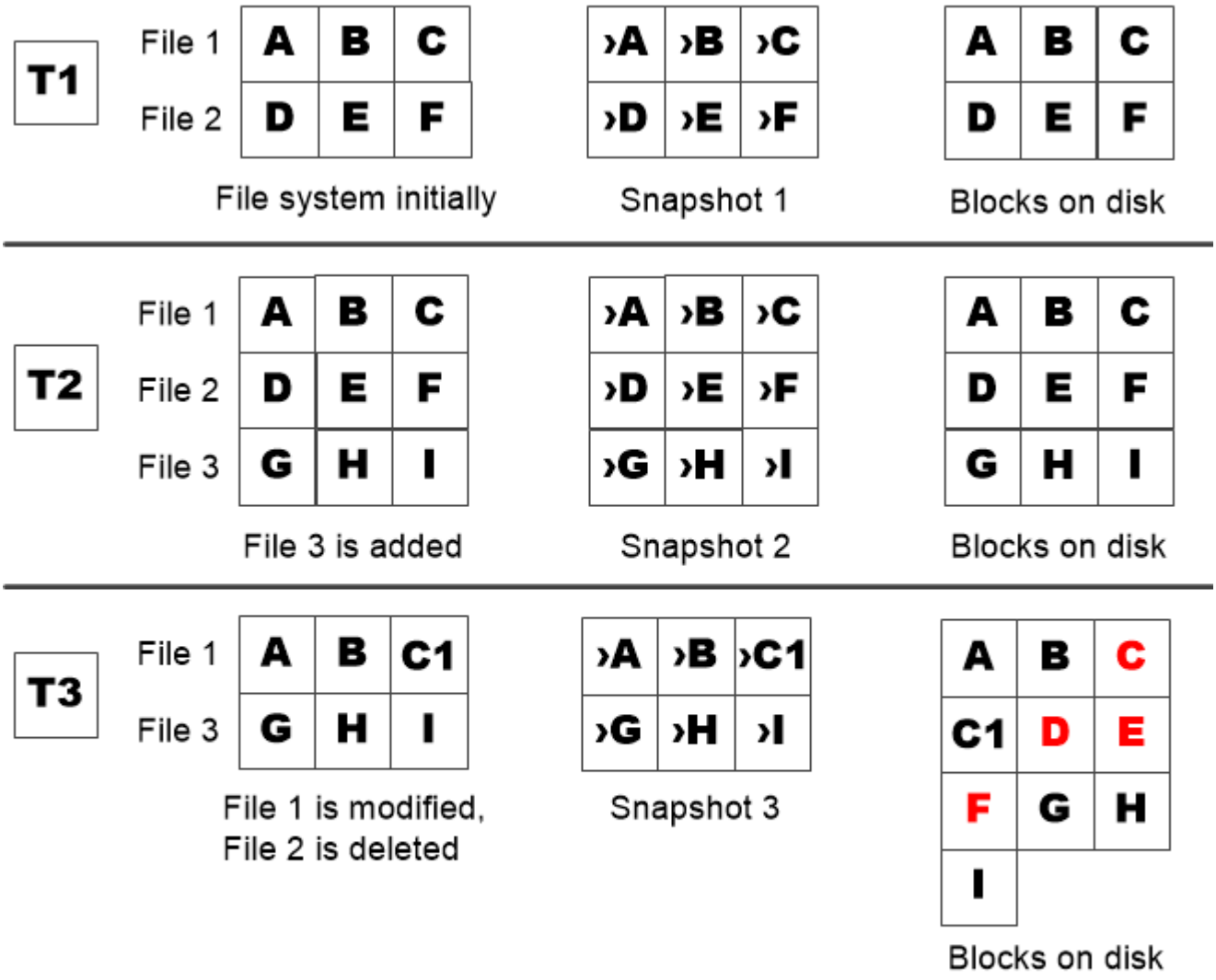
Cuándo aumentar la reserva de instantáneas

Al decidir si desea aumentar la reserva de instantáneas, es importante recordar que una instantánea sólo registra los cambios en los archivos desde que se realizó la última instantánea. Consume espacio en disco solo si se modifican o eliminan bloques del sistema de archivos activo.

Esto significa que la tasa de cambio del sistema de archivos es el factor clave para determinar la cantidad de espacio en disco utilizado por las instantáneas. No importa cuántas instantáneas cree, no consumirán espacio en disco si el sistema de archivos activo no ha cambiado.

Un FlexVol volume que contenga registros de transacciones de base de datos, por ejemplo, puede tener una reserva de snapshots de hasta un 20 % para justificar su mayor tasa de cambios. No solo querrá crear más instantáneas para capturar las actualizaciones más frecuentes de la base de datos, sino que también querrá tener una reserva de instantáneas más grande para manejar el espacio en disco adicional que consumen las instantáneas.

Una snapshot consta de punteros a bloques en lugar de copias de bloques. Puede pensar que un puntero es una «reclamación» en un bloque: ONTAP «retiene» el bloque hasta que se elimina la copia snapshot.



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

La eliminación de archivos protegidos puede reducir el espacio de archivos de lo esperado

Una instantánea apunta a un bloque incluso después de eliminar el archivo que utilizó el bloque. Esto explica por qué una reserva de instantáneas agotada podría conducir a un resultado contraintuitivo en el que la eliminación de un sistema de archivos completo da como resultado menos espacio disponible que el sistema de archivos ocupado.

Observe el siguiente ejemplo. Antes de eliminar cualquier archivo, el `df` resultado del comando es el siguiente:

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

Después de eliminar todo el sistema de archivos y hacer una instantánea del volumen, `df` el comando genera la siguiente salida:

```
Filesystem          kbytes  used    avail  capacity
/vol/vol0/          3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

Como se muestra en la salida, los 3 GB completos utilizados anteriormente por el sistema de archivos activo ahora están siendo utilizados por las instantáneas, además de los 0,5 GB utilizados antes de la eliminación.

Debido a que el espacio en disco utilizado por las instantáneas ahora excede la reserva de instantáneas, el desbordamiento de 2,5 GB “pastillas” en el espacio reservado para los archivos activos, dejándole con 0,5 GB de espacio libre para los archivos donde razonablemente podría haber esperado 3 GB.

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Supervisar el consumo de disco de instantáneas de ONTAP

Puede supervisar el consumo de disco Snapshot con `df` el comando. El comando muestra la cantidad de espacio libre en el sistema de archivos activo y la reserva de instantáneas.

Paso

1. Mostrar consumo de disco de instantánea: `df`

   En el siguiente ejemplo se muestra el consumo de disco Snapshot:

   ```
   cluster1::> df
   Filesystem          kbytes  used    avail  capacity
   /vol/vol0/          3000000 3000000 0       100%
   /vol/vol0/.snapshot 1000000 500000  500000   50%
   ```

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Compruebe la reserva de snapshots de ONTAP disponible en un volumen

Se recomienda comprobar la cantidad de reserva de snapshots disponible en un

volumen mediante el `snapshot-reserve-available` parámetro con `volume show` el comando. Obtenga más información sobre `volume show` en el "Referencia de comandos del ONTAP".

Paso

1. Compruebe la reserva de snapshots disponible en un volumen:

   `vol show -vserver SVM -volume volume -fields snapshot-reserve-available`

   El siguiente ejemplo muestra la reserva de instantáneas disponible para `vol1`:

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ --------------------------
vs0     vol1   4.84GB
```

Modifique la reserva de snapshot de ONTAP

Es posible que desee configurar una reserva de instantáneas más grande para evitar que las instantáneas utilicen el espacio reservado para el sistema de archivos activo. Es posible reducir la reserva de snapshot cuando ya no se necesita tanto espacio para las Snapshot.

Paso

1. Modifique la reserva de snapshot:

   `volume modify -vserver SVM -volume volume -percent-snapshot-space snap_reserve`

   Obtenga más información sobre `volume modify` en el "Referencia de comandos del ONTAP".

   En el siguiente ejemplo se define la reserva de instantáneas `vol1` en un 10%:

```
cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
-space 10
```

Eliminar automáticamente snapshots de ONTAP

Puede usar el `volume snapshot autodelete modify` comando para activar la eliminación automática de snapshots cuando se supera la reserva de Snapshot. De forma predeterminada, las snapshots más antiguas se eliminan primero. Obtenga más información sobre `volume snapshot autodelete modify` en el "Referencia de comandos del ONTAP".

Acerca de esta tarea

La LUN y los clones de archivos se eliminan cuando no hay más instantáneas que eliminar.

Paso

1. Eliminar instantáneas automáticamente:

   `volume snapshot autodelete modify -vserver` *SVM* `-volume` *volume* `-enabled true|false -trigger volume|snap_reserve`

   En el siguiente ejemplo, se eliminan automáticamente las instantáneas para `vol1` cuando se agota la reserva de instantáneas:

```
cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
-enabled true -trigger snap_reserve
```

Restaurar archivos desde instantáneas

Restaure un archivo desde una snapshot de ONTAP en un cliente de NFS o SMB

Un usuario en un cliente de NFS o SMB puede restaurar un archivo directamente desde una snapshot sin la intervención de un administrador del sistema de almacenamiento.

Todos los directorios del sistema de archivos contienen un subdirectorio denominado `.snapshot` accesible para los usuarios de NFS y SMB. El `.snapshot` subdirectorio contiene subdirectorios correspondientes a las instantáneas del volumen:

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

Cada subdirectorio contiene los archivos a los que hace referencia la instantánea. Si los usuarios eliminan o sobrescriben accidentalmente un archivo, pueden restaurarlo en el directorio principal de lectura y escritura copiando el archivo del subdirectorio de instantáneas al directorio de lectura y escritura:

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

Habilitar y deshabilitar el acceso de clientes NFS y SMB al directorio Snapshot de ONTAP

Es posible habilitar y deshabilitar el acceso al directorio Snapshot mediante la opción de interfaz de línea de comandos de ONTAP `-snapdir-access` del `volume modify` comando, y a partir de ONTAP 9.10.1, puede usar System Manager para habilitar o deshabilitar los sistemas cliente a fin de acceder a un directorio de snapshots en un volumen. Al habilitar el acceso, el directorio Snapshot podrá ser visible para los clientes y los clientes Windows pueden asignar una unidad al directorio Snapshot para ver y acceder a su contenido. Los clientes de NFS y SMB pueden restaurar un archivo o LUN desde una copia de Snapshot.

Puede habilitar o deshabilitar el acceso al directorio Snapshot de un volumen mediante la edición de la configuración del volumen o la configuración de recursos compartidos del volumen.

Habilite o deshabilite el acceso de clientes al directorio Snapshot mediante la edición de un volumen

Pasos

Puede habilitar y deshabilitar el acceso al directorio Snapshot de cliente mediante ONTAP System Manager o la interfaz de línea de comandos de ONTAP. De forma predeterminada, los clientes pueden acceder al directorio de snapshots en un volumen.

System Manager

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione el volumen que contiene el directorio de snapshots que desea mostrar u ocultar.
3. Haga clic ⋮ y seleccione **Editar**.
4. En la sección **Configuración de instantáneas (locales)**, seleccione o desmarque **Mostrar el directorio de instantáneas a los clientes**.
5. Haga clic en **Guardar**.

CLI

1. Compruebe el estado de acceso al directorio de instantáneas:

   ```
   volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-
   access
   ```

   Ejemplo:

   ```
   clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
   access
   vserver volume snapdir-access
   ------- ------ --------------
   vs0     vol1   false
   ```

   Obtenga más información sobre `volume show` en el "Referencia de comandos del ONTAP".

2. Habilitar o deshabilitar el acceso al directorio de snapshots:

   ```
   volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access
   <true|false>
   ```

   En el siguiente ejemplo, se habilita el acceso al directorio Snapshot en vol1:

   ```
   clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access
   true
   Volume modify successful on volume vol1 of Vserver vs0.
   ```

   Obtenga más información sobre `volume modify` en el "Referencia de comandos del ONTAP".

Habilite o deshabilite el acceso del cliente al directorio de instantáneas editando un recurso compartido

De forma predeterminada, los clientes pueden acceder al directorio de snapshots en un volumen.

Pasos

1. Haga clic en **almacenamiento > Recursos compartidos**.
2. Seleccione el volumen que contiene el directorio de snapshots que desea mostrar u ocultar.
3. Haga clic ⋮ y seleccione **Editar**.
4. En la sección **Compartir Propiedades**, seleccione o anule la selección de **Permitir que los clientes accedan al directorio de instantáneas**.
5. Haga clic en **Guardar**.

Restaurar un solo archivo desde una copia Snapshot de ONTAP

Puede usar el `volume snapshot restore-file` comando para restaurar un solo archivo o LUN desde una copia de Snapshot. Es posible restaurar el archivo a otra ubicación en el volumen primario de lectura y escritura si no desea reemplazar un archivo existente.

Acerca de esta tarea

Si va a restaurar una LUN existente, se crea un clon LUN y se realiza un backup en forma de copia de Snapshot. Durante la operación de restauración, puede leer la LUN y escribir en ella.

Los archivos con flujos se restauran de forma predeterminada.

Pasos

1. Enumere las snapshots en un volumen:

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

   Obtenga más información sobre `volume snapshot show` en el "Referencia de comandos del ONTAP".

   En el siguiente ejemplo se muestran las instantáneas en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaurar un archivo desde una instantánea:

   `volume snapshot restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`*

`-path file_path -restore-path destination_path`

Obtenga más información sobre `volume snapshot restore-file` en el "Referencia de comandos del ONTAP".

El siguiente ejemplo restaura el archivo `myfile.txt`:

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

Restaurar parte de un archivo a partir de una instantánea de ONTAP

Puede utilizar `volume snapshot partial-restore-file` el comando para restaurar un rango de datos desde una snapshot a una LUN o a un archivo de contenedor NFS o SMB, suponiendo que se conoce el desplazamiento de bytes de inicio de los datos y el número de bytes. Este comando puede usarse para restaurar una de las bases de datos en un host que almacena varias bases de datos en el mismo LUN.

A partir de ONTAP 9.12.1, está disponible la restauración parcial para los volúmenes que usan SnapMirror síncrono activo.

Pasos

1. Enumere las snapshots en un volumen:

   `volume snapshot show -vserver SVM -volume volume`

   Obtenga más información sobre `volume snapshot show` en el "Referencia de comandos del ONTAP".

   En el siguiente ejemplo se muestran las instantáneas en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaurar parte de un archivo a partir de una instantánea:

`volume snapshot partial-restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-start-byte` *`starting_byte`* `-byte-count` *`byte_count`*

El desplazamiento de bytes de inicio y el número de bytes deben ser múltiplos de 4,096.

El siguiente ejemplo restaura los primeros 4.096 bytes del archivo `myfile.txt`:

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

Restaure el contenido de un volumen a partir de una copia de Snapshot de ONTAP

Es posible recuperar un volumen a un momento específico anterior mediante la restauración a partir de una copia de Snapshot. Puede usar System Manager o `volume snapshot restore` el comando para restaurar el contenido de un volumen a partir de una copia de Snapshot. Obtenga más información sobre `volume snapshot restore` en el "Referencia de comandos del ONTAP".

Acerca de esta tarea

Si el volumen tiene relaciones de SnapMirror, replique manualmente todas las copias reflejadas del volumen inmediatamente después de la restauración desde una copia de Snapshot. Si no lo hace, puede provocar copias reflejadas inutilizables que se deban eliminar y volver a crear.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para restaurar a partir de una copia de Snapshot anterior.

System Manager

1. Haga clic en **almacenamiento** y seleccione un volumen.
2. En **Copias de instantánea**, haz clic ⋮ junto a la instantánea que deseas restaurar y selecciona **Restaurar**.

CLI

1. Enumere las snapshots en un volumen:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

El siguiente ejemplo muestra la snapshot en `vol1`:

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. Restaure el contenido de un volumen a partir de una copia de Snapshot:

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

El siguiente ejemplo restaura el contenido de `vol1` :

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

Replicación de volúmenes de SnapMirror

Obtenga más información sobre la replicación de volúmenes de SnapMirror

Obtenga más información sobre la recuperación ante desastres asíncrona de ONTAP SnapMirror

SnapMirror es la tecnología de recuperación ante desastres diseñada para la conmutación al nodo de respaldo del almacenamiento principal al secundario en un sitio geográficamente remoto. Como su nombre indica, SnapMirror crea una réplica, o *mirror,* de sus datos de trabajo en el almacenamiento secundario desde el cual puede continuar proporcionando datos en caso de catástrofe en el sitio principal.

Si el sitio primario sigue disponible para servir datos, sólo tiene que transferir cualquier dato que necesite y no facilitar el servicio a los clientes del espejo. Como se indica en el caso de uso de conmutación por error, las controladoras del sistema secundario deben ser equivalentes o casi equivalentes a las controladoras del sistema primario para servir datos de forma eficiente desde el almacenamiento reflejado.

Relaciones de protección de datos

Los datos se reflejan en el nivel de volumen. La relación entre el volumen de origen en el almacenamiento primario y el volumen de destino en el almacenamiento secundario se denomina una relación de protección de datos._ Los clústeres en los que residen los volúmenes y las SVM que sirven datos de los volúmenes deben estar "con relaciones entre iguales". Una relación de paridad permite que los clústeres y las SVM intercambien datos de forma segura.

En esta figura, se ilustran las relaciones de protección de datos de SnapMirror:

A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.

Ámbito de las relaciones de protección de datos

Puede crear una relación de protección de datos directamente entre los volúmenes o entre las SVM que poseen los volúmenes. En una relación de protección de datos _SVM, se replica toda la configuración de SVM o parte de ella, desde las exportaciones NFS y los recursos compartidos de SMB a RBAC, así como los datos de los volúmenes que posee la SVM.

También puede utilizar SnapMirror para aplicaciones especiales de protección de datos:

- Una copia *mirror* de uso compartido de la carga del volumen raíz de la SVM garantiza que los datos permanecen accesibles en caso de interrupción del servicio o conmutación por error de un nodo.
- Una relación de protección de datos entre *SnapLock Volumes* permite replicar los archivos WORM en el almacenamiento secundario.

  "Archivado y cumplimiento de normativas con tecnología SnapLock"

- A partir de ONTAP 9.13,1, se puede usar SnapMirror Asynchronous para proteger grupos de consistencia. A partir de ONTAP 9.14.1, se puede usar SnapMirror asíncrono para replicar copias Snapshot granulares de volúmenes en el clúster de destino mediante la relación del grupo de coherencia. Para obtener más información, consulte Configurar la protección asíncrona de SnapMirror.

Cómo se inicializan las relaciones de protección de datos de SnapMirror

La primera vez que se invoca SnapMirror, se realiza una transferencia *baseline* del volumen de origen al volumen de destino. La directiva *SnapMirror* de la relación define el contenido de la línea base y las actualizaciones.

Una transferencia completa bajo la política SnapMirror predeterminada `MirrorAllSnapshots` implica los siguientes pasos:

- Realice una copia Snapshot del volumen de origen.
- Transferir la instantánea y todos los bloques de datos con los que se hace referencia al volumen de destino.
- Transfiera las snapshots restantes y menos recientes del volumen de origen al volumen de destino para su uso en caso de que el duplicado «`activo » esté dañado.

Cómo se actualizan las relaciones de protección de datos de SnapMirror

Las actualizaciones son asíncronas, según la programación configurada. La retención refleja la política de snapshots en el origen.

En cada actualización de la `MirrorAllSnapshots` política, SnapMirror crea una instantánea del volumen de origen y transfiere esa instantánea y cualquier instantánea realizada desde la última actualización. En el siguiente resultado del `snapmirror policy show` comando para la `MirrorAllSnapshots` política, tenga en cuenta lo siguiente:

- `Create Snapshot` Es "`verdadero", lo que indica que `MirrorAllSnapshots` crea una instantánea cuando SnapMirror actualiza la relación.
- `MirrorAllSnapshots` Tiene las reglas «sm_created» y ««all_source_snapshots»», lo que indica que tanto la instantánea creada por SnapMirror como las instantáneas que se han realizado desde la última actualización se transfieren cuando SnapMirror actualiza la relación.

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                    Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
            Create Snapshot: true
                    Comment: SnapMirror asynchronous policy for mirroring
all snapshots
                             and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

Política de MirrorLatest

La política preconfigurada `MirrorLatest` funciona exactamente de la misma manera que `MirrorAllSnapshots`, excepto que sólo la instantánea creada por SnapMirror se transfiere en el momento de la inicialización y la actualización.

```
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
```

Información relacionada

- "Mostrar política de Snapmirror"

Obtenga información sobre la recuperación ante desastres síncrona de ONTAP SnapMirror

A partir de la versión ONTAP 9.5, la tecnología síncrona de SnapMirror (SM-S) es

compatible con todas las plataformas FAS y AFF que tengan al menos 16 GB de memoria y en todas las plataformas ONTAP Select. La tecnología síncrona de SnapMirror es una función con licencia por nodo que proporciona replicación de datos síncrona a nivel de volumen.

Esta funcionalidad aborda las normativas regulatorias y nacionales para la replicación síncrona en sectores financieros, sanitarios y otros regulados, en los que no es necesaria una pérdida de datos nula.

Operaciones síncronas de SnapMirror permitidas

El límite del número de operaciones de replicación síncrona de SnapMirror por par de alta disponibilidad depende del modelo de controladora.

En la tabla siguiente se enumera el número de operaciones síncronas de SnapMirror que se permiten por pareja de alta disponibilidad según el tipo de plataforma y la versión de ONTAP.

Plataforma	ONTAP 9.14.1 a ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	Versiones anteriores a ONTAP 9.9.1
AFF	400	200	160	80
ASA	400	200	160	80
FAS	80	80	80	40
ONTAP Select	40	40	40	20

Funciones admitidas

La siguiente tabla indica las funciones compatibles con SnapMirror Synchronous y las versiones ONTAP que admiten.

Función	Se admite la primera versión	Información adicional
Antivirus en el volumen principal de la relación síncrona de SnapMirror	ONTAP 9,6	
Replicación de snapshots creada por aplicaciones	ONTAP 9,7	Si una instantánea está etiquetada con la etiqueta apropiada en el momento de la `snapshot create` operación, utilizando la CLI o la API de ONTAP , SnapMirror replica de manera sincrónica las instantáneas, tanto las creadas por el usuario como las creadas con scripts externos, después de inactivar las aplicaciones. Las instantáneas programadas creadas mediante una política de instantáneas no se replican. Para obtener más información sobre cómo replicar instantáneas creadas por la aplicación, consulte la"Base de conocimientos de NetApp : Cómo replicar snapshots creados por aplicaciones con SnapMirror sincrónico" .

Clonar eliminación automática	ONTAP 9,6	
Los agregados de FabricPool con política de organización en niveles de Ninguna, Snapshot o Automática son compatibles con el origen y el destino de SnapMirror síncronos.	ONTAP 9,5	El volumen de destino de un agregado de FabricPool no se puede establecer en la política de organización en niveles All.
FC	ONTAP 9,5	En todas las redes para las que la latencia no supere los 10ms ms
FC-NVMe	ONTAP 9,7	
Clones de archivo	ONTAP 9,7	
FPolicy en el volumen principal de la relación síncrona de SnapMirror	ONTAP 9,6	
Cuotas duras y flexibles en el volumen principal de la relación síncrona de SnapMirror	ONTAP 9,6	Las reglas de cuota no se replican en el destino; por lo tanto, la base de datos de cuotas no se replica en el destino.
Relaciones síncronas dentro del clúster	ONTAP 9.14.1	La alta disponibilidad se proporciona cuando los volúmenes de origen y de destino se encuentran en diferentes pares de alta disponibilidad. Si se desactiva todo el clúster, no será posible el acceso a los volúmenes hasta que se recupere el clúster. Las relaciones síncronas de SnapMirror dentro del clúster contribuirán al límite general de Relaciones por pareja de alta disponibilidad.
iSCSI	ONTAP 9,5	
Clones LUN y clones de espacio de nombres NVMe	ONTAP 9,7	
Clones LUN respaldados por copias Snapshot creadas por aplicación	ONTAP 9,7	
Acceso de protocolo mixto (NFS v3 y SMB)	ONTAP 9,6	
Restauración de NDMP/NDMP	ONTAP 9.13.1	El clúster de origen y de destino deben ejecutar ONTAP 9.13.1 o versiones posteriores para usar NDMP con SnapMirror síncrono. Para obtener más información, consulte Transferencia de datos mediante la copia ndmp.
Operaciones síncronas de SnapMirror (NDO) sin interrupciones solo en plataformas AFF/ASA.	ONTAP 9.12.1	La compatibilidad con operaciones no disruptivas le permite realizar muchas tareas de mantenimiento comunes sin necesidad de programar un tiempo de inactividad. Las operaciones admitidas incluyen la toma de control y el retorno al nodo primario, y el movimiento de volúmenes, siempre y cuando haya un solo nodo superviviente entre cada uno de los dos clústeres.
NFS v4,2	ONTAP 9.10.1	

NFS v4,0	ONTAP 9,6	
NFS v4,1	ONTAP 9,6	
NVMe/TCP	9.10.1	
Eliminación de una limitación elevada de la frecuencia de funcionamiento de metadatos	ONTAP 9,6	
Seguridad para datos confidenciales en tránsito con cifrado TLS 1.2	ONTAP 9,6	
Restauración parcial de archivos y archivos individuales	ONTAP 9.13.1	
SMB 2,0 o posterior	ONTAP 9,6	
Cascada de reflejos síncronos SnapMirror	ONTAP 9,6	La relación del volumen de destino de la relación síncrona de SnapMirror debe ser una relación de SnapMirror asíncrono.
Recuperación ante desastres de SVM	ONTAP 9,6	* Una fuente síncrona de SnapMirror también puede ser una fuente de recuperación ante desastres de SVM, por ejemplo, una configuración de fan-out con SnapMirror síncrono como una pierna y la recuperación ante desastres de SVM como la otra. * Una fuente síncrona de SnapMirror no puede ser un destino de recuperación ante desastres de SVM porque SnapMirror Synchronous no admite la configuración en cascada de una fuente de protección de datos. Debe liberar la relación síncrona antes de ejecutar un cambio de sincronización de recuperación ante desastres de SVM en el clúster de destino. * Un destino síncrono de SnapMirror no puede ser una fuente de recuperación de desastres de SVM porque la recuperación de desastres de SVM no admite la replicación de volúmenes de DP. Una resincronización flip del origen síncrono provocaría la recuperación ante desastres de SVM excepto el volumen DP en el clúster de destino.
Restauración basada en cinta al volumen de origen	ONTAP 9.13.1	
Paridad de marca de hora entre los volúmenes de origen y destino para NAS	ONTAP 9,6	Si se actualizó de ONTAP 9,5 a ONTAP 9,6, la marca de tiempo se replica solo para todos los archivos nuevos y modificados en el volumen de origen. La Marca de hora de los archivos existentes en el volumen de origen no está sincronizada.

Funciones no admitidas

Las siguientes funciones no se admiten con las relaciones síncronas de SnapMirror:

- Protección autónoma de ransomware
- Grupos de consistencia

- Sistemas DPO optimizados para DP
- Volúmenes de FlexGroup
- Volúmenes de FlexCache
- Limitación global
- En una configuración ramificada, solo una relación puede ser una relación síncrona de SnapMirror; todas las demás relaciones del volumen de origen deben ser relaciones asíncronas de SnapMirror.
- Movimiento de LUN
- Configuraciones de MetroCluster
- No se admiten las LUN de acceso SAN y NVMe combinadas ni los espacios de nombres NVMe en el mismo volumen o SVM.
- SnapCenter
- Volúmenes de SnapLock
- Snapshots a prueba de manipulación
- Backup a cinta o restauración con volcado y SMTape en el volumen de destino
- Piso de rendimiento (QoS mín.) para volúmenes de origen
- SnapRestore de volumen
- VVol

Modos de funcionamiento

SnapMirror Synchronous tiene dos modos de funcionamiento según el tipo de política de SnapMirror utilizada:

- **Modo de sincronización** en modo de sincronización, las operaciones de E/S de la aplicación se envían en paralelo a los sistemas de almacenamiento primario y secundario. Si la escritura en el almacenamiento secundario no se realiza por ningún motivo, se permite que la aplicación continúe escribiendo en el almacenamiento principal. Cuando se corrige la condición de error, la tecnología síncrona de SnapMirror se vuelve a sincronizar automáticamente con el almacenamiento secundario y reanuda la replicación del almacenamiento principal al secundario en modo síncrono. En el modo síncrono, RPO=0 y RTO son muy bajos hasta que se produce un fallo de replicación secundaria en el momento en el que el objetivo de punto de recuperación y el objetivo de tiempo de recuperación se vuelven indeterminados, pero igual que el tiempo para reparar el problema que provocó un error en la replicación secundaria y para finalizar la resincronización.
- **Modo StrictSync** SnapMirror synchronous puede operar opcionalmente en modo StrictSync. Si la escritura en el almacenamiento secundario no se completa por ningún motivo, las operaciones de I/o de la aplicación fallan y, por lo tanto, se garantiza que el almacenamiento primario y secundario sean idénticos. La I/O de la aplicación al primario se reanuda únicamente cuando la relación de SnapMirror vuelve al `InSync` estado. Si falla el almacenamiento primario, se pueden reanudar las operaciones de I/o de la aplicación en el almacenamiento secundario después de la conmutación por error, sin pérdida de datos. En el modo StrictSync, el objetivo de punto de recuperación es siempre cero y el objetivo de tiempo de recuperación es muy bajo.

Estado de la relación

El estado de una relación síncrona SnapMirror es siempre en el `InSync` estado durante un funcionamiento normal. Si la transferencia SnapMirror falla por cualquier motivo, el destino no está sincronizado con el origen y puede pasar al `OutofSync` estado.

En el caso de las relaciones síncronas de SnapMirror, el sistema comprueba automáticamente el estado de la

relación `InSync`o `OutofSync`) a un intervalo fijo. Si el estado de la relación es `OutofSync`, ONTAP activa automáticamente el proceso de resincronización automática para restablecer la relación con `InSync` el estado. La resincronización automática se activa solo si la transferencia falla debido a alguna operación, como la conmutación por error no planificada del almacenamiento en el origen o en el destino, o una interrupción del servicio de red. Operaciones iniciadas por el usuario, `snapmirror quiesce` como y `snapmirror break` no activan la resincronización automática.

Si el estado de la relación es `OutofSync` para una relación síncrona de SnapMirror en el modo StrictSync, se detienen todas las operaciones de I/O del volumen primario. `OutofSync`El estado en la relación síncrona de SnapMirror en el modo de sincronización no interrumpe el funcionamiento del volumen primario y las operaciones de I/O en el volumen primario.

Información relacionada

- "Informe técnico de NetApp 4733: Prácticas recomendadas y configuración síncrona de SnapMirror"
- "rotura de snapmirror"
- "Snapmirror en reposo"

Políticas de protección de datos predeterminadas de ONTAP

ONTAP incluye varias políticas de protección predeterminadas que puede utilizar en las relaciones de protección de datos. La política que use depende del tipo de relación de protección.

Si las políticas predeterminadas no satisfacen sus necesidades de relaciones de protección de datos, "crear una política personalizada"puede .

Lista de políticas de protección predeterminadas y descripciones

A continuación se describen las políticas de protección predeterminadas y sus tipos de políticas asociados.

Nombre	Descripción	Tipo de política
Asíncrona	Una política de almacén y asíncrona de SnapMirror unificada para reflejar el último sistema de archivos activo y copias snapshot diarias y semanales con un programa de transferencia por hora.	Asíncrona
Fallo de AutomatedOver	Política para SnapMirror síncrono con garantía de objetivo de tiempo de recuperación cero en la que las I/O del cliente no se verán interrumpidas en el fallo de replicación.	Síncrona
AutomatedFailOverDuplex	Política para SnapMirror síncrono con garantía de objetivo de tiempo de recuperación cero y replicación síncrona bidireccional.	Síncrona
CloudBackuppredeterminado	Política de almacén con regla diaria.	Asíncrona
Continuo	Política de mirroring de bloques S3.	Continuo
DailyBackup	Política de almacén con una regla diaria y un programa de transferencia diario.	Asíncrona

Nombre	Descripción	Tipo de política
DPPredeterminado	Política asíncrona de SnapMirror para mirroring de todas las instantáneas y el sistema de archivos activo más reciente.	Asíncrona
MirrorAllSnapshots	Política asíncrona de SnapMirror para mirroring de todas las instantáneas y el sistema de archivos activo más reciente.	Asíncrona
MirrorAllSnapshotsDiscardNetwork	Política asíncrona de SnapMirror para reflejar todas las instantáneas y el sistema de archivos activo más reciente, excepto las configuraciones de red.	Asíncrona
Reflejo de AndVault	Una política de almacén y asíncrona de SnapMirror unificada para reflejar el sistema de archivos activo más reciente e instantáneas diarias y semanales.	Asíncrona
MirrorAndVaultDiscardNetwork	Una directiva de almacén y asíncrona de SnapMirror unificada para reflejar el sistema de archivos activo más reciente y las instantáneas diarias y semanales excluyendo las configuraciones de red.	Asíncrona
MirrorÚltimas	Política asíncrona de SnapMirror para reflejar el sistema de archivos activo más reciente.	Asíncrona
SnapCenterSync	Política para la configuración de snapshot síncrona de SnapMirror para SnapCenter con aplicación creada.	Síncrona
StrictSync	Política de SnapMirror síncrono en la que el acceso del cliente se interrumpirá en caso de fallo de replicación.	Síncrona
Síncrona	Política de SnapMirror síncrono en la que el acceso del cliente no se interrumpirá en caso de fallo de replicación.	Síncrona
Unified7year	Política de Unified SnapMirror con retención de 7 años.	Asíncrona
XDPDefault	De vault con reglas diarias y semanales.	Asíncrona

Obtenga información sobre las cargas de trabajo admitidas por las políticas StrictSync y Sync de ONTAP

Las políticas de StrictSync y Sync admiten todas las aplicaciones basadas en LUN con los protocolos FC, iSCSI y FC-NVMe, así como los protocolos NFSv3 y NFSv4 para aplicaciones empresariales como bases de datos, VMware, Quota, SMB, etc. A partir de ONTAP 9.6, SnapMirror síncrono se puede usar para servicios de archivos empresariales, como la automatización de diseño electrónico (EDA), los directorios iniciales y las cargas de trabajo de la compilación de software.

En ONTAP 9.5, para una política de sincronización, debe tener en cuenta algunos aspectos importantes a la vez que selecciona las cargas de trabajo NFSv3 o NFSv4. No se tiene en cuenta la cantidad de datos que realizan las operaciones de lectura o escritura por parte de las cargas de trabajo, ya que la política de sincronización puede gestionar cargas de trabajo de lectura o escritura elevadas. En ONTAP 9.5, las cargas

de trabajo que tienen una creación de archivos, una creación de directorios, cambios de permisos de archivos o cambios de permisos de directorio pueden no ser adecuadas (estas se denominan cargas de trabajo con metadatos elevados). Un ejemplo típico de una carga de trabajo con metadatos altos es una carga de trabajo de DevOps en la que se crean varios archivos de prueba, se ejecuta la automatización y se eliminan los archivos. Otro ejemplo es la carga de trabajo de compilación paralela que genera varios archivos temporales durante la compilación. El impacto de una tasa alta de la actividad de metadatos de escritura es que puede provocar que la sincronización entre los reflejos se rompa temporalmente, lo que bloquea la I/o de lectura y escritura del cliente.

A partir de ONTAP 9.6, estas limitaciones se eliminan y SnapMirror síncrono puede usarse para cargas de trabajo de servicios de archivos empresariales que incluyen entornos multiusuario, como directorios iniciales y cargas de trabajo de creación de software.

Información relacionada

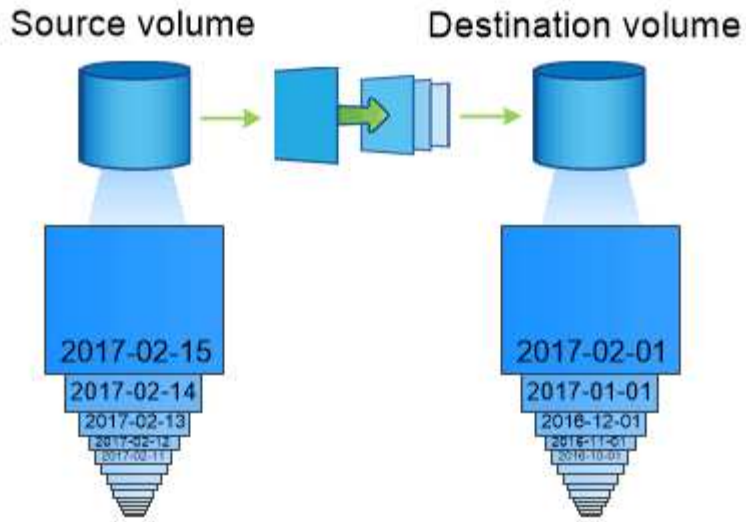
"Configuración síncrona y prácticas recomendadas de SnapMirror"

Obtenga más información sobre el archivado de almacenes mediante la tecnología ONTAP SnapMirror

Las políticas de almacén de SnapMirror sustituyen a la tecnología SnapVault en ONTAP 9.3 y versiones posteriores. Se utiliza una política de almacén de SnapMirror para realizar replicaciones con snapshots disco a disco para el cumplimiento de normativas y otros fines relacionados con la gobernanza. A diferencia de una relación de SnapMirror, en la que el destino generalmente contiene solo las copias Snapshot actualmente en el volumen de origen, un destino de almacén normalmente conserva las copias Snapshot de un momento específico creadas durante un período mucho más largo.

Es posible que desee conservar snapshots mensuales de los datos en un plazo de 20 años, por ejemplo, para cumplir con las normativas de contabilidad gubernamental para su empresa. Como no hay necesidad de servir datos desde un almacenamiento de almacén, puede utilizar discos más lentos y menos costosos en el sistema de destino.

La siguiente figura muestra las relaciones de protección de datos de SnapMirror Vault.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Cómo se inicializan las relaciones de protección de datos del almacén

La política de SnapMirror para la relación define el contenido de la línea de base y cualquier actualización.

Una transferencia básica con la política de almacén predeterminada `XDPDefault` crea una copia Snapshot del volumen de origen y, a continuación, transfiere esa copia y los bloques de datos a los que hace referencia al volumen de destino. A diferencia de las relaciones con SnapMirror, un backup de almacén no incluye las Snapshot más antiguas en la base.

Cómo se actualizan las relaciones de protección de datos de almacén

Las actualizaciones son asíncronas, según la programación configurada. Las reglas que defina en la política para la relación identifican qué snapshots nuevas deben incluirse en las actualizaciones y cuántas copias se retendrán. Las etiquetas definidas en la política («por ejemplo, «en orden») deben coincidir con una o más etiquetas definidas en la política de instantáneas del origen. De lo contrario, la replicación falla.

En cada actualización de la `XDPDefault` directiva, SnapMirror transfiere instantáneas que se han realizado desde la última actualización, siempre que tengan etiquetas que coincidan con las definidas en las reglas de política. En el siguiente resultado del `snapmirror policy show` comando para la `XDPDefault` política, tenga en cuenta lo siguiente:

- `Create Snapshot` Es «`false`», lo que indica `XDPDefault` que no crea una instantánea cuando SnapMirror actualiza la relación.
- `XDPDefault` Tiene reglas “daily” y “weekly”, lo que indica que todas las instantáneas con etiquetas coincidentes en el origen se transfieren cuando SnapMirror actualiza la relación.

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                     Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Información relacionada

- "Mostrar política de Snapmirror"

Obtenga más información sobre la replicación unificada de ONTAP SnapMirror

SnapMirror *Unified replication* permite configurar la recuperación ante desastres y el archivado en el mismo volumen de destino. Cuando la replicación unificada es apropiada, ofrece ventajas en la reducción de la cantidad de almacenamiento secundario que se necesita, lo que limita el número de transferencias básicas y reduce el tráfico de red.

Cómo se inicializan las relaciones de protección de datos unificadas

Al igual que sucede con SnapMirror, la protección de datos unificada realiza una transferencia de referencia la primera vez que se invoca. La política de SnapMirror para la relación define el contenido de la línea de base y cualquier actualización.

Una transferencia completa con la política de protección de datos unificada predeterminada `MirrorAndVault` realiza una copia Snapshot del volumen de origen y, a continuación, transfiere dicha copia y los bloques de datos a los que hace referencia al volumen de destino. Al igual que el archivado de almacenes, la protección de datos unificada no incluye copias Snapshot más antiguas como referencia.

Cómo se actualizan las relaciones de protección de datos unificadas

En cada actualización de la `MirrorAndVault` política, SnapMirror crea una instantánea del volumen de origen y transfiere esa instantánea y cualquier instantánea que se haya realizado desde la última actualización, siempre y cuando tengan etiquetas que coincidan con las definidas en las reglas de política de instantáneas. En el siguiente resultado del `snapmirror policy show` comando para la `MirrorAndVault` política, tenga en cuenta lo siguiente:

- `Create Snapshot` Es ``verdadero", lo que indica que `MirrorAndVault` crea una instantánea cuando SnapMirror actualiza la relación.
- `MirrorAndVault` Tiene reglas “sm_created”, “daaily” y “weekly”, que indican que tanto la instantánea creada por SnapMirror como las instantáneas con etiquetas coincidentes en el origen se transfieren cuando SnapMirror actualiza la relación.

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                    Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified SnapMirror synchronous and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Unified7year

La política preconfigurada `Unified7year` funciona exactamente de la misma manera que `MirrorAndVault`, excepto que una cuarta regla transfiere instantáneas mensuales y las conserva durante

siete años.

```
                        Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                               ----------------     ----  -------- ----
--------- ------
                               sm_created              1  false       0 -
-
                               daily                   7  false       0 -
-
                               weekly                 52  false       0 -
-
                               monthly                84  false       0 -
-
```

Proporcionar protección frente a una posible corrupción de datos

La replicación unificada limita el contenido de la transferencia completa a la snapshot creada por SnapMirror durante la inicialización. En cada actualización, SnapMirror crea otra instantánea del origen y transfiere esa instantánea y cualquier instantánea nueva que tenga etiquetas que coincidan con las etiquetas definidas en las reglas de política de instantáneas.

Puede protegerse contra la posibilidad de que una snapshot actualizada esté dañada creando una copia de la última snapshot transferida en el destino. Esta «copia local» se conserva con independencia de las reglas de retención en el origen, de modo que incluso si la instantánea originalmente transferida por SnapMirror ya no está disponible en el origen, una copia de ella estará disponible en el destino.

Cuándo utilizar la replicación de datos unificada

Debe sopesar las ventajas que supone mantener una copia completa frente a las ventajas que ofrece la replicación unificada para reducir la cantidad de almacenamiento secundario, limitar el número de transferencias básicas y reducir el tráfico de red.

El factor clave para determinar la idoneidad de la replicación unificada es la tasa de cambio del sistema de archivos activo. Un reflejo tradicional es posible que resulte más adecuado para un volumen que contiene instantáneas cada hora de registros de transacciones de base de datos, por ejemplo.

Información relacionada

- "Mostrar política de Snapmirror"

Cuando un volumen de destino de la protección de datos de ONTAP aumenta automáticamente

Durante una transferencia de mirroring para la protección de datos, el volumen de destino aumenta automáticamente su tamaño si se ha incrementado el volumen de origen, siempre y cuando haya espacio disponible en el agregado que contiene el volumen.

Este comportamiento se produce independientemente de cualquier configuración de crecimiento automático en el destino. No es posible limitar el crecimiento del volumen ni evitar que ONTAP lo haga.

De forma predeterminada, los volúmenes de protección de datos se establecen en `grow_shrink` el modo autosize, lo que permite que el volumen aumente o se reduzca en respuesta a la cantidad de espacio utilizado. El tamaño máximo automático de los volúmenes de protección de datos es igual al tamaño máximo de FlexVol y depende de la plataforma. Por ejemplo:

- FAS8200, volumen DP predeterminado máx.-autosize = 100 TB

Para obtener más información, consulte "NetApp Hardware Universe".

Obtenga más información sobre las distribuciones ramificadas y las puestas en marcha en cascada de la protección de datos de ONTAP

Puede utilizar una implementación de *fan-out* para ampliar la protección de datos a varios sistemas secundarios. Puede utilizar una implementación *Cascade* para ampliar la protección de datos a sistemas terciarios.

Tanto las puestas en marcha ramificadas como aquellas en cascada son compatibles con cualquier combinación de recuperación ante desastres de SnapMirror, SnapVault o replicación unificada. A partir de ONTAP 9.5, las relaciones síncronas de SnapMirror permiten puestas en marcha ramificadas con una o más relaciones asíncronas de SnapMirror. Solo una relación en la configuración ramificada puede ser una relación síncrona de SnapMirror; todas las demás relaciones del volumen de origen deben ser relaciones asíncronas de SnapMirror. Las relaciones síncronas de SnapMirror también admiten las puestas en marcha en cascada (a partir de ONTAP 9.6); no obstante, la relación con el volumen de destino de la relación síncrona de SnapMirror debe ser una relación asíncrona de SnapMirror. SnapMirror síncrono activo (Compatible a partir de ONTAP 9.13,1) también admite configuraciones de distribución ramificada.

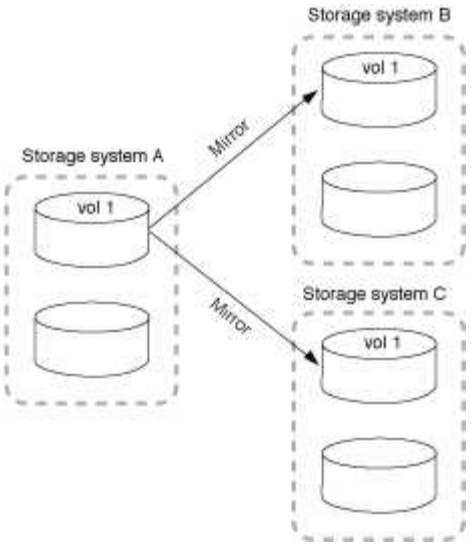
Puede utilizar una implementación *fan-in* para crear relaciones de protección de datos entre varios sistemas principales y un único sistema secundario. Cada relación debe usar un volumen diferente en el sistema secundario.

Debe tener en cuenta que los volúmenes que forman parte de una configuración en cascada o en distribución ramificada pueden tardar más en volver a sincronizar. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.

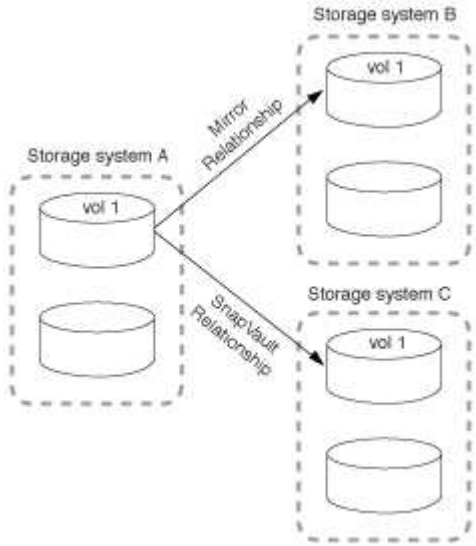
Cómo funcionan las implementaciones de dispersión

SnapMirror admite la puesta en marcha de «varios duplicados_ y de «mirror-vault» con «fan-out».

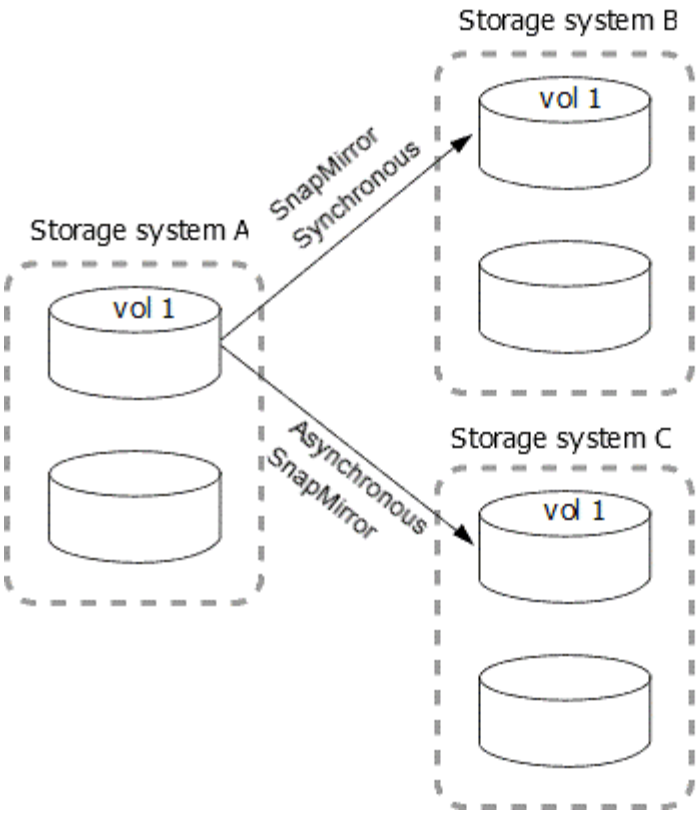
Una puesta en marcha de «fan-out» de varios reflejos consiste en un volumen de origen que tiene una relación de reflejo con varios volúmenes secundarios.



Una implementación de «fan-out» de reflejo-almacén consta de un volumen de origen que tiene una relación de mirroring con un volumen secundario y una relación de SnapVault con otro volumen secundario.



A partir de ONTAP 9.5, puede tener puestas en marcha ramificadas con relaciones síncronas de SnapMirror; sin embargo, solo una relación en la configuración ramificada puede ser una relación síncrona de SnapMirror; todas las demás relaciones del volumen de origen deben ser relaciones asíncronas de SnapMirror.



Cómo funcionan las implementaciones en cascada

SnapMirror admite puestas en marcha en cascada de *mirror-mirror*, *mirror-vault*, *vault-mirror* y *vault-vault*.

Una puesta en marcha en cascada de reflejos consiste en una cadena de relaciones en las que un volumen de origen se refleja en un volumen secundario, mientras que el volumen secundario se duplica en un volumen terciario. Si el volumen secundario deja de estar disponible, puede sincronizar la relación entre los volúmenes primario y terciario sin necesidad de realizar una nueva transferencia de base de referencia.

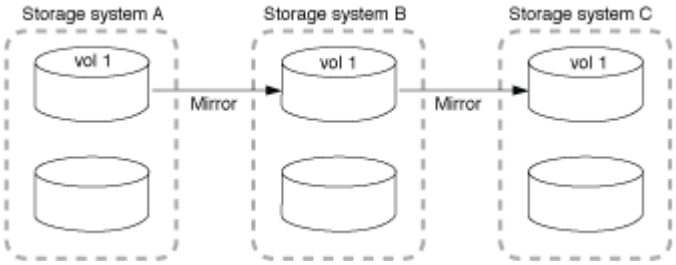
En una relación de volúmenes en cascada, las instantáneas de retención a largo plazo solo se admiten en el volumen de destino SnapMirror final de la cascada en todas las versiones de ONTAP 9. Si se habilitan instantáneas de retención a largo plazo en cualquier volumen intermedio de la cascada, se pierden copias de seguridad e instantáneas. Si tiene una configuración no compatible en la que se han habilitado instantáneas de retención a largo plazo en cualquier volumen intermedio de una cascada, comuníquese con el soporte técnico y consulte la "Base de conocimientos de NetApp : No se admite la conexión en cascada de un volumen con instantáneas de retención a largo plazo (LTR) habilitadas" para obtener ayuda.

Las siguientes versiones de ONTAP no le permiten habilitar instantáneas de retención a largo plazo en ningún volumen en cascada, excepto el volumen de destino final de SnapMirror .

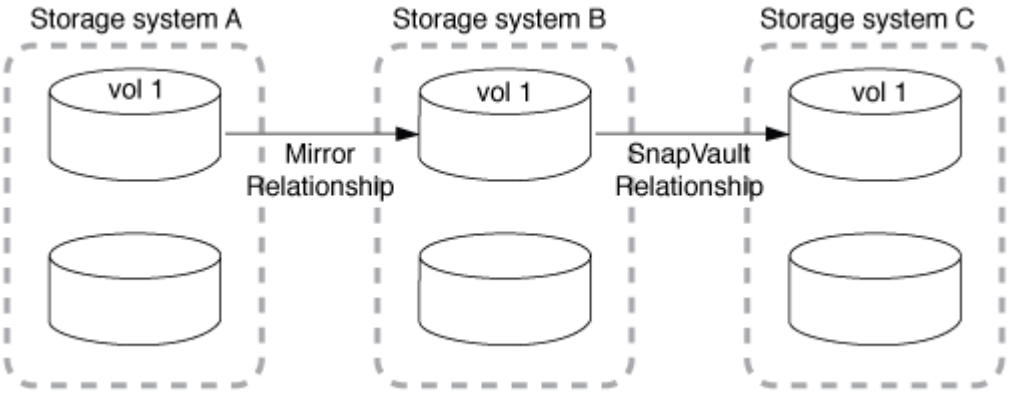
- 9.15.1 y posteriores
- 9.14.1P2 y P4 a P14
- 9.13.1P9 a P17
- 9.12.1 P12 a P19
- 9.11.1P15 a P20
- 9.10.1P18 a P20
- 9.9.1P20

Obtenga más información sobre"instantáneas de retención a largo plazo" .

A partir de ONTAP 9.6, las relaciones síncronas de SnapMirror se admiten en una puesta en marcha en cascada de reflejo-reflejo. Solo los volúmenes primario y secundario pueden estar en una relación síncrona de SnapMirror. La relación entre los volúmenes secundarios y los volúmenes terciarios debe ser asíncrona.



Una puesta en marcha en cascada de copias-vault consta de una cadena de relaciones en las que un volumen de origen se refleja en un volumen secundario y el volumen secundario se realiza en un volumen terciario.



También se admiten implementaciones en cascada de Vault-mirror y Vault-Vault:

- Una puesta en marcha en cascada de reflejos de almacén consta de una cadena de relaciones en las que se realiza un volumen de origen en un volumen secundario, mientras que el volumen secundario se duplica en un volumen terciario.
- Una implementación en cascada de bóveda a bóveda consta de una cadena de relaciones en la que un volumen de origen se aboveda en un volumen secundario, y el volumen secundario se aboveda en un volumen terciario.

Información relacionada

- Reanude la protección en una configuración ramificada con SnapMirror Active Sync

Obtenga más información sobre las licencias de ONTAP SnapMirror

A partir de ONTAP 9.3, se ha simplificado la licencia para la replicación entre instancias de ONTAP. En las versiones ONTAP 9, la licencia de SnapMirror admite tanto relaciones de almacén como de mirroring. Puede usar una licencia de SnapMirror para admitir la replicación de ONTAP tanto en casos prácticos de backup como de recuperación ante desastres.

Antes de la versión de ONTAP 9,3, se necesitaba una licencia de SnapVault independiente para configurar las

relaciones *vault* entre las instancias de ONTAP, donde la instancia de DP podía retener un mayor número de snapshots para admitir casos prácticos de backup con tiempos de retención más largos, y era necesaria una licencia de SnapMirror para configurar las relaciones *mirror* entre las instancias de ONTAP, donde cada instancia de ONTAP mantendría el mismo número de snapshots (es decir, una imagen *mirror*) para admitir casos de uso de recuperación tras fallos de clúster para permitir que se hicieran posibles. Las licencias de SnapMirror y SnapVault siguen usándose y son compatibles con las versiones de ONTAP 8.x y 9.x.

Aunque las licencias de SnapVault siguen funcionando y son compatibles con las versiones ONTAP 8.x y 9.x, la licencia de SnapMirror puede usarse en lugar de una licencia de SnapVault y puede usarse para configuraciones de mirroring y almacén.

Para la replicación asíncrona de ONTAP, a partir de ONTAP 9.3, se usa un único motor de replicación unificado para configurar las políticas de modo de protección de datos ampliado (XDP), donde la licencia de SnapMirror se puede configurar para una política de mirroring, una normativa de almacén o una política de mirroring-almacén. Se requiere una licencia de SnapMirror en los clústeres de origen y destino. Una licencia de SnapVault no es necesaria si ya se ha instalado una licencia de SnapMirror. La licencia perpetua asíncrona de SnapMirror se incluye en la suite de software ONTAP One que está instalada en los nuevos sistemas AFF y FAS.

Los límites de configuración de protección de datos se determinan por varios factores, como la versión de ONTAP, la plataforma de hardware y las licencias instaladas. Para obtener más información, consulte "Hardware Universe".

Licencia síncrona de SnapMirror

A partir de ONTAP 9.5, se admiten las relaciones síncronas de SnapMirror. Requiere las siguientes licencias para crear una relación síncrona de SnapMirror:

- La licencia síncrona de SnapMirror se requiere en el clúster de origen y el de destino.

  La licencia síncrona de SnapMirror forma parte de la "Suite de licencia ONTAP ONE".

  Si su sistema se adquirió antes de junio de 2019 con un paquete Premium o Flash, puede descargar una clave maestra NetApp para obtener la licencia síncrona de SnapMirror necesaria desde el sitio de soporte de NetApp: "Claves de licencia principal".

- Se requiere la licencia de SnapMirror en los clústeres de origen y destino.

Licencia de cloud de SnapMirror

A partir de ONTAP 9,8, la licencia de cloud de SnapMirror proporciona replicación asíncrona de snapshots desde instancias de ONTAP a extremos de almacenamiento de objetos. Los destinos de replicación se pueden configurar usando almacenes de objetos locales, así como servicios de almacenamiento de objetos en cloud público compatibles con S3 y S3. Las relaciones de cloud de SnapMirror son compatibles con los sistemas ONTAP a los destinos de almacenamiento de objetos calificados previamente.

SnapMirror Cloud no está disponible como licencia independiente. Solo se necesita una licencia por clúster ONTAP. Además de la licencia cloud de SnapMirror, también se necesita la licencia asíncrona de SnapMirror.

Requiere las siguientes licencias para crear una relación cloud de SnapMirror:

- Tanto una licencia de SnapMirror como una licencia de cloud de SnapMirror para replicar directamente en el extremo del almacén de objetos.
- Cuando se configura un flujo de trabajo de replicación de varias políticas (por ejemplo, de disco a disco a cloud), se requiere una licencia de SnapMirror en todas las instancias de ONTAP, mientras que la licencia

de cloud de SnapMirror solo se necesita para el clúster de origen que se replica directamente en el extremo de almacenamiento de objetos.

Comenzando con ONTAP 9.9,1, usted puede "Utilice System Manager para la replicación en cloud de SnapMirror".

En el sitio web de NetApp se publica una lista de aplicaciones autorizadas de terceros en cloud de SnapMirror.

Licencia optimizada de Data Protection

Las licencias de protección de datos optimizada (DPO) ya no se venden y DPO no es compatible con las plataformas actuales; sin embargo, si tiene una licencia DPO instalada en una plataforma compatible, NetApp sigue ofreciendo soporte hasta el fin de la disponibilidad de dicha plataforma.

DPO no se incluye con el paquete de licencia ONTAP One y no se puede actualizar al paquete de licencia ONTAP One si la licencia DPO está instalada en un sistema.

Para obtener información sobre las plataformas compatibles, consulte "Hardware Universe".

Mejoras en las funciones de los sistemas DPO de ONTAP

A partir de ONTAP 9.6, el número máximo de volúmenes FlexVol admitidos aumenta cuando se instala la licencia DP_Optimized (DPO). A partir de la versión 9,4 de ONTAP, los sistemas con licencia DPO admiten el respaldo de SnapMirror, la deduplicación en segundo plano entre volúmenes, el uso de bloques de instantáneas como donantes y la compactación.

A partir de ONTAP 9.6, se ha incrementado el número máximo admitido de volúmenes FlexVol en sistemas secundarios o de protección de datos, lo que permite escalar hasta 2,500 volúmenes FlexVol por nodo o hasta 5,000 en modo de conmutación por error. El aumento de volúmenes de FlexVol se habilita con la "Licencia DP_Optimized (DPO)". "Licencia de SnapMirror"También se requiere A en los nodos de origen y destino.

A partir de ONTAP 9.4, se realizan las siguientes mejoras en las funciones de los sistemas DPO:

- Backoff de SnapMirror: En sistemas DPO, el tráfico de replicación tiene la misma prioridad que se da a las cargas de trabajo del cliente.

  La funcionalidad de backup de SnapMirror está deshabilitada de forma predeterminada en los sistemas DPO.

- Deduplicación en segundo plano de volumen y deduplicación en segundo plano entre volúmenes: Se habilitan la deduplicación en segundo plano de volúmenes y la deduplicación en segundo plano entre volúmenes en sistemas DPO.

  Puede ejecutar `storage aggregate efficiency cross-volume-dedupe start -aggregate` *`aggregate_name`* `-scan-old-data true` el comando para deduplicar los datos existentes. La práctica recomendada es ejecutar el comando durante las horas de menor actividad para reducir el impacto en el rendimiento.

  Obtenga más información sobre `storage aggregate efficiency cross-volume-dedupe start` en el "Referencia de comandos del ONTAP".

- Mayor ahorro al utilizar bloques de instantáneas como donadores: Los bloques de datos que no están disponibles en el sistema de archivos activos, pero atrapados en snapshots se usan como donadores para

la deduplicación de volumen.

Los nuevos datos se pueden deduplicar con los datos atrapados en las copias snapshot, lo que también comparte eficazmente los bloques de copias snapshot. El mayor espacio donante permite un mayor ahorro, especialmente cuando el volumen tiene un gran número de instantáneas.

- Compactación: La compactación de datos está habilitada de forma predeterminada en los volúmenes DPO.

Obtenga información acerca de la coincidencia de patrones de nombres de ruta en comandos ONTAP SnapMirror

Puede utilizar la coincidencia de patrones para especificar las rutas de origen y destino en `snapmirror` los comandos.

```
`snapmirror` los comandos utilizan nombres de ruta de acceso completos en el siguiente formato `vserver:volume`: . No se puede introducir el nombre de la SVM para abreviar el nombre de la ruta de acceso. Si hace esto, el `snapmirror` comando asume el contexto de SVM local del usuario.
```

Suponiendo que la SVM se llama "`vserver1`" y el volumen se llama "`vol1`", el nombre de la ruta completamente cualificado es `vserver1:vol1`.

Puede utilizar el asterisco (*) en las rutas de acceso como comodín para seleccionar nombres de ruta de acceso coincidentes y completos. En la siguiente tabla, se proporcionan ejemplos del uso del comodín para seleccionar un rango de volúmenes.

`*`	Coincide con todas las rutas.
`vs*`	Coincide con todas las SVM y los volúmenes con nombres SVM que comienzan por `vs`.
`:*src`	Coincide con todas las SVM con los nombres de los volúmenes que contienen `src` el texto.
`:vol`	Coincide con todas las SVM con los nombres de los volúmenes que comienzan por `vol`.

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------ ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                Snapmirrored  Idle           -
true    -
```

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

Obtenga información sobre las consultas ampliadas para las operaciones de relaciones de ONTAP SnapMirror

Puede utilizar *extended queries* para realizar operaciones de SnapMirror en varias relaciones de SnapMirror a la vez. Por ejemplo, es posible que tenga varias relaciones SnapMirror no inicializarse que desea inicializar con un comando.

Acerca de esta tarea

Puede aplicar consultas ampliadas a las siguientes operaciones de SnapMirror:

- Inicializando relaciones no iniciadas
- Reanude relaciones en modo inactivo
- Resincronizando relaciones rotas
- Actualizando relaciones de inactividad
- Anulación de transferencias de datos de relaciones

Paso

1. Realice una operación de SnapMirror en varias relaciones:

   `snapmirror command` `{-state state } *`

   El siguiente comando inicializa las relaciones de SnapMirror que están en un `Uninitialized` estado:

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

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

Versiones de ONTAP compatibles para relaciones de SnapMirror

Los volúmenes de origen y destino deben ejecutar versiones de ONTAP compatibles antes de crear una relación de protección de datos de SnapMirror. Antes de actualizar ONTAP, debe comprobar que la versión actual de ONTAP sea compatible con la versión de ONTAP de destino para las relaciones de SnapMirror.

Relaciones de replicación unificadas

En lo que respecta a las relaciones de SnapMirror del tipo «'XDP», utilizando las versiones locales o de Cloud Volumes ONTAP:

A partir de ONTAP 9,9.0:

- Las versiones ONTAP 9.x,0 son versiones de solo cloud y son compatibles con los sistemas Cloud Volumes ONTAP. El asterisco (*) después de la versión indica una versión de sólo nube.

> ONTAP 9.16.0 es una excepción a la regla de solo nube porque proporciona soporte para"Sistemas ASA r2" . El signo más (+) después de la versión de lanzamiento indica una versión compatible tanto con ASA r2 como con la nube. Los sistemas ASA r2 admiten relaciones SnapMirror únicamente con otros sistemas ASA r2.

- Las versiones ONTAP 9.x,1 son versiones generales y son compatibles tanto con los sistemas locales como con los sistemas Cloud Volumes ONTAP.

> Si "equilibrado de capacidad avanzado" se habilita en volúmenes de clústeres que ejecutan ONTAP 9.16.1 o posterior, las transferencias de SnapMirror no se admiten para los clústeres que ejecutan versiones de ONTAP anteriores a ONTAP 9.16.1.

> La interoperabilidad es bidireccional.

Interoperabilidad para ONTAP versión 9.4 y posteriores

Versión ONTAP…	Interactúa con estas versiones anteriores de ONTAP…																					
	9.18.1	9.17.1	9.16.1	9.16.0 o posterior	9.15.1	9.15.0*	9.14.1	9.14.0*	9.13.1	9.13.0*	9.12.1	9.12.0*	9.11.1	9.11.0*	9.10.1	9.10.0*	9.9.1	9.9.0*	9,8	9,7	9,6	9,5
9.18.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	**Sí**	No	No	No	No	No	No	No	No	No	No	No	No
9.17.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No	No	No	No	No	No	No

9.16.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No	No	No	No	No
9.16.0 o posterior	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	No	No	No	No	No	No	No
9.15.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No	No
9.15.0 *	No	**Sí**	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	No	No	No	No	No
9.14.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No
9.14.0 *	No	**Sí**	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	No	No	No	No	No
9.13.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No
9.13.0 *	No	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	No	No	No
9.12.1	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9.12.0 *	No	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	No	No	No
9.11.1	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No
9.11.0 *	No	No	No	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	**Sí**	No
9.10.1	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9.10.0 *	No	No	No	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9.9.1	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9.9.0*	No	No	No	No	No	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9,8	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9,7	No	No	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**

9,6	No	No	No	No	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9,5	No	No	No	No	No	No	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**

Relaciones síncronas de SnapMirror

SnapMirror Synchronous no es compatible con las instancias de cloud de ONTAP.

Versión ONTAP…	Interactúa con estas versiones anteriores de ONTAP…													
	9.18.1	9.17.1	9.16.1	9.15.1	9.14.1	9.13.1	9.12.1	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5
9.18.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No	No	No
9.17.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No	No	No
9.16.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No	No
9.15.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No
9.14.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No
9.13.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9.12.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9.11.1	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No
9.10.1	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No
9.9.1	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9,8	No	No	No	No	**Sí**	**Sí**	**Sí**	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No
9,7	No	No	No	No	No	**Sí**	**Sí**	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9,6	No	No	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**
9,5	No	No	No	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**

Relaciones de recuperación ante desastres de SVM de SnapMirror

- Esta matriz se aplica a la función de migración de movilidad de datos de SVM a partir de ONTAP 9.10.1.
- Puede utilizar SVM DR para migrar un SVM que no cumpla con las restricciones indicadas para "Migración de SVM (movilidad de datos de SVM)".
- En ambos casos, un máximo de 2 versiones **más nuevas** de ONTAP principales pueden separar los clústeres de origen y destino, con el requisito de que el destino sea la misma versión o más nueva que la versión de ONTAP de origen.

Para los datos de recuperación ante desastres de SVM y la protección de SVM:

La recuperación ante desastres de SVM solo se admite entre clústeres que ejecutan la misma versión de ONTAP. **La independencia de versiones no es compatible con la replicación de SVM**.

Para la recuperación ante desastres de SVM para la migración de SVM:

- La replicación es compatible en una sola dirección de una versión anterior de ONTAP en origen para que la misma versión de ONTAP o una posterior en el destino.
- La versión de ONTAP en el clúster de destino no debe tener más de dos versiones en las instalaciones principales más recientes o dos versiones de cloud principales más recientes (a partir de ONTAP 9,9.0), tal como se muestra en la tabla a continuación.
    - La replicación no es compatible con los casos de uso de protección de datos a largo plazo.

El asterisco (*) después de la versión indica una versión de sólo nube.

Para determinar la compatibilidad, busque la versión de origen en la columna de la tabla izquierda y, a continuación, busque la versión de destino en la fila superior (DR/Migración para versiones similares y Migración sólo para versiones más recientes).

Si está utilizando ONTAP 9.10.1 o posterior, puede utilizar el "Movilidad de datos de SVM" función en lugar de SVM DR para migrar SVM de un clúster a otro.

Origen	Destino																				
	9,5	9,6	9,7	9,8	9.9.0*	9.9.1	9.10.0*	9.10.1	9.11.0*	9.11.1	9.12.0*	9.12.1	9.13.0*	9.13.1	9.14.0*	9.14.1	9.15.0*	9.15.1	9.16.0	9.16.1	9.17.1	9.18.1
9,5	Recuperación ante desastres/Migración	Migración	Migración																		
9,6		Recuperación ante desastres/Migración	Migración	Migración																	

9,7			Recuperación ante desastres/Migración	Migración	Migración																
9,8				Recuperación ante desastres/Migración	Migración	Migración		Migración														
9.9.0*					Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración	Migración												

9.9.1						Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración											
9.10.0*							Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración	Migración									
9.10.1								Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración									

9.11.0*									Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración	Migración						
9.11.1										Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración						
9.12.0*											Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración	Migración				

9.12.1												Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración					
9.13.0*													Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración	Migración				
9.13.1														Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración				

9.14.0*															Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración	Migración		
9.14.1																Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración		
9.15.0*																	Recuperación ante desastres/Migración	Migración	Migración	Migración	Migración	

9.15.1																		Recuperación ante desastres/Migración	Migración	Migración	Migración
9.16.0																			Recuperación ante desastres/Migración	Migración	Migración	Migración
9.16.1																				Recuperación ante desastres/Migración	Migración	Migración

9.17.1																				Recuperación ante desastres/Migración	Migración
9.18.1																					Recuperación ante desastres/Migración

Relaciones de recuperación ante desastres de SnapMirror

Para relaciones de SnapMirror del tipo «DP» y del tipo de política «duplicación asíncrona»:

Los reflejos de tipo DP no se pueden inicializar comenzando con ONTAP 9.11.1 y están completamente obsoletos en ONTAP 9.12.1. Para obtener más información, consulte "Amortización de las relaciones de SnapMirror para la protección de datos".

En la siguiente tabla, la columna de la izquierda indica la versión de ONTAP en el volumen de origen y la fila superior indica las versiones de ONTAP que se pueden tener en el volumen de destino.

Origen	Destino								
	9.11.1	9.10.1	9.9.1	9,8	9,7	9,6	9,5	9,4	9,3
9.11.1	Sí	No	No	No	No	No	No	No	No
9.10.1	Sí	Sí	No	No	No	No	No	No	No
9.9.1	Sí	Sí	Sí	No	No	No	No	No	No
9,8	No	Sí	Sí	Sí	No	No	No	No	No
9,7	No	No	Sí	Sí	Sí	No	No	No	No

9,6	No	No	No	Sí	Sí	Sí	No	No	No
9,5	No	No	No	No	Sí	Sí	Sí	No	No
9,4	No	No	No	No	No	Sí	Sí	Sí	No
9,3	No	No	No	No	No	No	Sí	Sí	Sí

La interoperabilidad no es bidireccional.

Obtenga información sobre las limitaciones de ONTAP SnapMirror

Debe conocer las limitaciones básicas de SnapMirror antes de crear una relación de protección de datos.

- Un volumen de destino solo puede tener un volumen de origen.

  Un volumen de origen puede tener varios volúmenes de destino. El volumen de destino puede ser el volumen de origen de cualquier tipo de relación de replicación de SnapMirror.

- Según el modelo de cabinas, se pueden distribuir de forma ramificada un máximo de ocho o dieciséis volúmenes de destino de un único volumen de origen. Consulte la "Hardware Universe" para obtener más información sobre su configuración específica.
- No puede restaurar archivos en el destino de una relación de recuperación ante desastres de SnapMirror.
- Los volúmenes de SnapVault de origen o destino no pueden tener 32 bits.
- El volumen de origen de una relación de SnapVault no debe ser un volumen FlexClone.

  La relación funcionará, pero no se conservará la eficiencia que ofrecen los volúmenes FlexClone.

Configure la replicación de volumen de SnapMirror

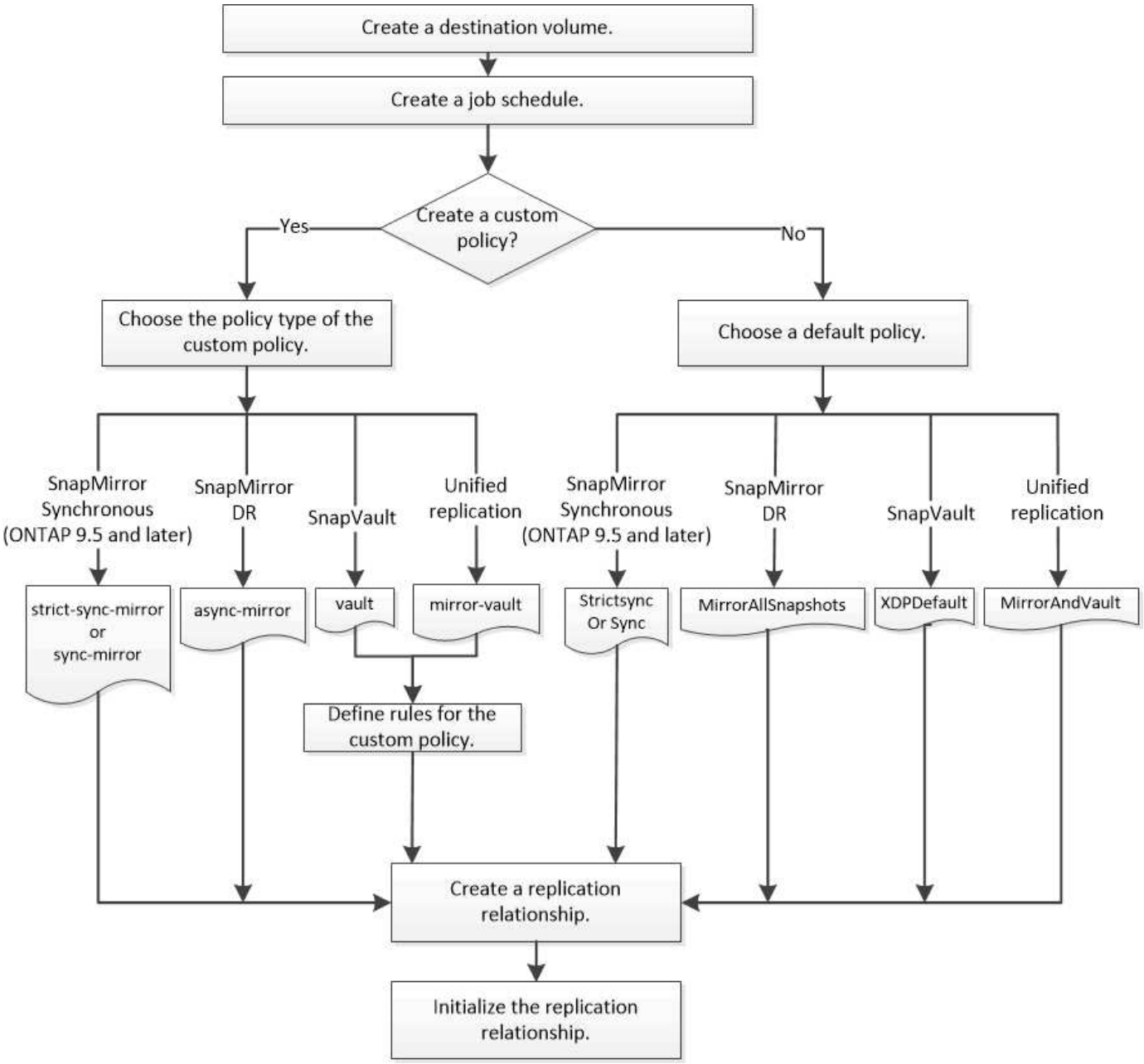
Flujo de trabajo de replicación de ONTAP SnapMirror

SnapMirror ofrece tres tipos de relación de protección de datos: Recuperación ante desastres de SnapMirror, archivado (anteriormente conocido como SnapVault) y replicación unificada. Puede seguir el mismo flujo de trabajo básico para configurar cada tipo de relación.

Comenzando con la disponibilidad general en ONTAP 9.9,1, "SnapMirror síncrono activo" proporciona un objetivo de tiempo de recuperación cero (objetivo de tiempo de recuperación cero) o conmutación al respaldo transparente (TAF) para permitir la conmutación automática al respaldo de aplicaciones críticas para el negocio en entornos SAN.

Para cada tipo de relación de protección de datos de SnapMirror, el flujo de trabajo es el mismo: Crear un volumen de destino, crear una programación de trabajos, especificar una política, crear e inicializar la relación.

A partir de ONTAP 9.3, puede utilizar `snapmirror protect` el comando para configurar una relación de protección de datos en un único paso. Incluso si utiliza `snapmirror protect`, debe comprender cada paso del flujo de trabajo.



Información relacionada

- "protección de SnapMirror"

Configure una relación de replicación de ONTAP SnapMirror en un paso

A partir de ONTAP 9.3, puede utilizar el `snapmirror protect` Comando para configurar una relación de protección de datos en un solo paso. Debe especificar una lista de volúmenes que se replicarán, una SVM en el clúster de destino, una programación de trabajos y una política SnapMirror . `snapmirror protect` hace el resto

Antes de empezar

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

"Relaciones entre iguales de clústeres y SVM"

- El idioma del volumen de destino debe ser el mismo que el del volumen de origen.

Acerca de esta tarea

El `snapmirror protect` comando elige un agregado asociado con la SVM especificada. Si no hay ningún agregado asociado con la SVM, elige de todos los agregados del clúster. La elección del agregado se basa en la cantidad de espacio libre y el número de volúmenes del agregado.

`snapmirror protect`A continuación, el comando realiza los siguientes pasos:

- Crea un volumen de destino con un tipo adecuado y la cantidad de espacio reservado para cada volumen de la lista de volúmenes que se van a replicar.
- Configura una relación de replicación adecuada para la directiva que usted especifique.
- Inicializa la relación.

El nombre del volumen de destino tiene el formato *source_volume_name_dst*. En caso de un conflicto con un nombre existente, el comando añade un número al nombre del volumen. Puede especificar un prefijo o sufijo en las opciones del comando. El sufijo sustituye al `dst` sufijo proporcionado por el sistema.

En ONTAP 9.4 y versiones posteriores, un volumen de destino puede contener hasta 1019 instantáneas. En ONTAP 9.3 y versiones anteriores, un volumen de destino puede contener hasta 251 instantáneas.

La inicialización puede requerir mucho tiempo. `snapmirror protect` no espera a que se complete la inicialización antes de que finalice el trabajo. Por este motivo, debe utilizar `snapmirror show` el comando en lugar `job show` del comando para determinar cuándo se ha completado la inicialización.

A partir de ONTAP 9.5, se pueden crear relaciones síncronas de SnapMirror mediante `snapmirror protect` el comando.

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

Paso

1. Cree e inicialice una relación de replicación en un paso:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. `-auto -initialize`La opción por defecto es «`verdadero».

En el siguiente ejemplo, se crea e inicializa una relación de recuperación ante desastres de SnapMirror utilizando la `MirrorAllSnapshots` política predeterminada:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```

Puede utilizar una directiva personalizada si lo prefiere. Para obtener más información, consulte "Creación de una política de replicación personalizada".

En el siguiente ejemplo, se crea e inicializa una relación de SnapVault utilizando la `XDPDefault` política predeterminada:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

En el siguiente ejemplo, se crea e inicializa una relación de replicación unificada mediante la `MirrorAndVault` política predeterminada:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

En el siguiente ejemplo, se crea e inicializa una relación síncrona de SnapMirror utilizando la `Sync` política predeterminada:

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

Para las políticas de replicación unificada y de SnapVault, puede resultarle útil definir una programación para crear una copia de la última snapshot transferida en el destino. Para obtener más información, consulte "Definir una programación para crear una copia local en el destino".

Después de terminar

Utilice `snapmirror show` el comando para verificar que la relación de SnapMirror se ha creado.

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

Información relacionada

- "exposición de trabajos"

Configure una relación de replicación paso a paso

Cree un volumen de destino de ONTAP SnapMirror

Puede usar `volume create` el comando en el destino para crear un volumen de destino. El volumen de destino debe tener el mismo tamaño o más que el volumen de origen. Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

Paso

1. Cree un volumen de destino:

   `volume create -vserver` *`SVM`* `-volume volume -aggregate` *`aggregate`* `-type DP -size` *`size`*

   En el ejemplo siguiente se crea un volumen de destino de 2 GB llamado `volA_dst`:

   ```
   cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
   -aggregate node01_aggr -type DP -size 2GB
   ```

Cree una programación de trabajos de replicación de ONTAP SnapMirror

La programación de tareas determina el momento en que SnapMirror actualiza automáticamente la relación de protección de datos a la que se asigna la programación. Puede usar System Manager o `job schedule cron create` el comando para crear una programación de trabajos de replicación. Obtenga más información sobre `job schedule cron create` en el "Referencia de comandos del ONTAP".

Acerca de esta tarea

Debe asignar una programación de tareas cuando crea una relación de protección de datos. Si no asigna una programación de trabajo, debe actualizar la relación manualmente.

Pasos

Puede crear una programación de tareas de replicación con System Manager o la CLI de ONTAP.

System Manager

1. Vaya a **Protección > Descripción general** y expanda **Configuración de política local**.
2. En el panel **Schedules**, haga clic en →.
3. En la ventana **Schedules**, haga clic en + Add .
4. En la ventana **Agregar horario**, ingrese el nombre del horario y elija el contexto y el tipo de horario.
5. Haga clic en **Guardar**.

CLI

1. Crear un programa de trabajo:

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

Para `-month` `-dayofweek` , y `-hour`, puede especificar `all` que se ejecute el trabajo cada mes, día de la semana y hora, respectivamente.

A partir de ONTAP 9.10.1, puede incluir Vserver para su programación de trabajo:

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

ⓘ La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror para volúmenes es de 5 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror para volúmenes es de 30 minutos.

El siguiente ejemplo crea una programación de trabajo llamada `my_weekly` que se ejecuta los sábados a las 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Personalizar una política de replicación de SnapMirror

Cree una política de replicación de ONTAP SnapMirror personalizada

Puede crear una directiva de replicación personalizada si la directiva predeterminada para una relación no es adecuada. Por ejemplo, se pueden comprimir datos en una transferencia de red, o modificar el número de intentos que realiza SnapMirror para transferir snapshots.

Puede usar una directiva predeterminada o personalizada al crear una relación de replicación. Para un archivo personalizado (anteriormente SnapVault) o una política de replicación unificada, debe definir una o más *rules* que determinen las instantáneas que se transfieren durante la inicialización y la actualización. También se recomienda definir una programación para crear Snapshot locales en el destino.

El *policy type* de la directiva de replicación determina el tipo de relación que admite. En la siguiente tabla se muestran los tipos de directivas disponibles.

Tipo de política	Tipo de relación
reflejo asíncrono	Recuperación ante desastres de SnapMirror
almacén	SnapVault
mirror-vault	Replicación unificada
estricto-síncrono-mirror	SnapMirror síncrono en el modo StrictSync (admitido a partir de ONTAP 9.5)
reflejo síncrono	SnapMirror síncrono en el modo Sincronización (se admite a partir de ONTAP 9.5)

Al crear una directiva de replicación personalizada, es una buena idea modelar la directiva después de una directiva predeterminada.

Pasos

Puede crear políticas de protección de datos personalizadas con System Manager o la interfaz de línea de comandos de ONTAP. A partir de ONTAP 9.11.1, puede usar System Manager para crear políticas de mirroring y almacén personalizadas, y para mostrar y seleccionar políticas heredadas. Esta función también está disponible en ONTAP 9.8P12 y en parches posteriores de ONTAP 9.8.

Cree políticas de protección personalizadas en los clústeres de origen y destino.

System Manager

1. Haga clic en **Protección > Descripción general > Configuración de directivas locales**.
2. En **Políticas de protección**, haga clic en →.
3. En el panel **Políticas de protección**, haga clic en + Add .
4. Escriba el nombre de la nueva política y seleccione el alcance de la misma.
5. Elija un tipo de política. Para agregar una directiva sólo de almacén o sólo de duplicación, seleccione **asíncrona** y haga clic en **utilizar un tipo de directiva heredada**.
6. Complete los campos obligatorios.
7. Haga clic en **Guardar**.
8. Repita estos pasos en el otro clúster.

CLI

1. Cree una política de replicación personalizada:

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

A partir de ONTAP 9,5, puede especificar la programación para crear una programación Snapshot común para relaciones síncronas de SnapMirror mediante `-common-snapshot-schedule` el parámetro. De forma predeterminada, la programación de Snapshot común para las relaciones síncronas de SnapMirror es de una hora. Es posible especificar un valor entre 30 minutos y dos horas para la programación de Snapshot para las relaciones síncronas de SnapMirror.

En el ejemplo siguiente se crea una política de replicación personalizada para la recuperación ante desastres de SnapMirror que permite la compresión de red para las transferencias de datos:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

En el ejemplo siguiente se crea una política de replicación personalizada para SnapVault:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

En el ejemplo siguiente se crea una política de replicación personalizada para la replicación unificada:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

En el siguiente ejemplo se crea una política de replicación personalizada para la relación síncrona de SnapMirror en el modo StrictSync:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

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

Después de terminar

Para los tipos de políticas «`vault`» y ««marror-vault»», debe definir reglas que determinen qué instantáneas se transfieren durante la inicialización y la actualización.

Utilice el `snapmirror policy show` Comando para verificar que se creó la política SnapMirror .

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

Defina una regla para una política de ONTAP SnapMirror

Para las políticas personalizadas con el `vault` tipo de política OR `mirror-vault`, debe definir al menos una regla que determine qué instantáneas se transfieren durante la inicialización y actualización. También puede definir reglas para políticas predeterminadas con el `vault` tipo de política o. `mirror-vault`

Acerca de esta tarea

Cada política con el `vault` tipo de política OR `mirror-vault` debe tener una regla que especifique las instantáneas que se van a replicar. La regla `bi-monthly`, por ejemplo, indica que sólo se deben replicar las instantáneas asignadas a la etiqueta SnapMirror `bi-monthly`. La etiqueta de SnapMirror se especifica al configurar la política de Snapshot en el origen.

Cada tipo de política está asociado a una o más reglas definidas por el sistema. Estas reglas se asignan automáticamente a una directiva cuando se especifica su tipo de directiva. La siguiente tabla muestra las reglas definidas por el sistema.

Regla definida por el sistema	Se utiliza en tipos de políticas	Resultado
sm_creado	Reflejo asíncrono, reflejo-almacén, sincronización, StrictSync	Una instantánea creada por SnapMirror se transfiere en el momento de la inicialización y la actualización.

all_source_snapshots	reflejo asíncrono	Las nuevas instantáneas del origen se transfieren durante la inicialización y la actualización.
todos los días	almacén, reflejo-almacén	Las nuevas instantáneas en el origen con la etiqueta SnapMirror `daily` se transfieren durante la inicialización y la actualización.
semanal	almacén, reflejo-almacén	Las nuevas instantáneas en el origen con la etiqueta SnapMirror `weekly` se transfieren durante la inicialización y la actualización.
mensual	mirror-vault	Las nuevas instantáneas en el origen con la etiqueta SnapMirror `monthly` se transfieren durante la inicialización y la actualización.
coherente con la aplicación	Sync, StrictSync	Las copias Snapshot que tienen la etiqueta SnapMirror `app_consistent` en el origen se replican de forma síncrona en el destino. Compatible a partir de ONTAP 9,7.

Excepto para el tipo de política «'duplicación asíncrona'», puede especificar reglas adicionales según sea necesario, para directivas predeterminadas o personalizadas. Por ejemplo:

- Para la política predeterminada `MirrorAndVault`, puede crear una regla llamada `bi-monthly` para que coincida con las instantáneas en el origen con `bi-monthly` la etiqueta SnapMirror.
- Para una política personalizada con el `mirror-vault` tipo de política, puede crear una regla llamada `bi-weekly` para hacer coincidir las instantáneas en el origen con `bi-weekly` la etiqueta SnapMirror.

Paso

1. Definir una regla para una directiva:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-keep` *`retention_count`*

   En el siguiente ejemplo, se agrega una regla con la etiqueta SnapMirror `bi-monthly` a la `MirrorAndVault` política predeterminada:

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   En el siguiente ejemplo, se agrega una regla con la etiqueta SnapMirror `bi-weekly` a la `my_snapvault` política personalizada:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_snapvault -snapmirror-label bi-weekly -keep 26
```

En el siguiente ejemplo, se agrega una regla con la etiqueta SnapMirror `app_consistent` a la `Sync` política personalizada:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
-snapmirror-label app_consistent -keep 1
```

Obtenga más información sobre `snapmirror policy add-rule` en el "Referencia de comandos del ONTAP".

Luego, es posible replicar copias de Snapshot del clúster de origen que coincidan con la siguiente etiqueta de SnapMirror:

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
snapshot1 -snapmirror-label app_consistent
```

Defina una programación de ONTAP SnapMirror para crear una copia local en el destino

Para las relaciones de SnapVault y de replicación unificada, se puede proteger contra la posibilidad de que una snapshot actualizada esté dañada mediante la creación de una copia de la última snapshot transferida en el destino. Esta «copia local» se conserva independientemente de las reglas de retención en el origen, de modo que aunque la instantánea transferida originalmente por SnapMirror ya no esté disponible en el origen, habrá disponible una copia en el destino.

Acerca de esta tarea

Usted especifica la programación para crear una copia local en el `-schedule` opción de la `snapmirror policy add-rule` dominio.

Paso

1. Definir una programación para crear una copia local en el destino:

   `snapmirror policy add-rule -vserver` *`SVM`* `-policy` *`policy_for_rule`* `-snapmirror -label` *`snapmirror-label`* `-schedule` *`schedule`*

   Para ver un ejemplo de cómo crear un programa de trabajo, consulte "Crear una programación de trabajo de replicación".

   En el ejemplo siguiente se agrega una programación para crear una copia local a la `MirrorAndVault` política predeterminada:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
```

En el siguiente ejemplo, se agrega una programación para crear una copia local a la `my_unified` política personalizada:

```
cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
my_unified -snapmirror-label my_monthly -schedule my_monthly
```

Obtenga más información sobre `snapmirror policy add-rule` en el "Referencia de comandos del ONTAP".

Cree una relación de replicación de ONTAP SnapMirror

La relación entre el volumen de origen en el almacenamiento primario y el volumen de destino en el almacenamiento secundario se denomina relación de protección de datos._ Se puede utilizar `snapmirror create` el comando para crear relaciones de protección de datos de replicación unificada, DR o SnapVault de SnapMirror.

> Este procedimiento se aplica a los sistemas FAS, AFF y ASA. Si tiene un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 o ASA C30), siga "estos pasos" para crear una relación de replicación. Los sistemas R2 de ASA ofrecen una experiencia de ONTAP simplificada específica para clientes de SAN.

A partir de ONTAP 9.11.1, se puede usar System Manager para seleccionar políticas de mirroring y almacén predefinidas y personalizadas, para mostrar y seleccionar políticas heredadas, y para anular las programaciones de transferencia definidas en una política de protección al proteger volúmenes y máquinas virtuales de almacenamiento. Esta función también está disponible en ONTAP 9.8P12 y en parches posteriores de ONTAP 9.8.

> Si utiliza la versión de revisión de ONTAP 9.8P12 o posterior de ONTAP 9.8 y configuró SnapMirror con System Manager, debe utilizar ONTAP 9.9.1P13 o posterior y ONTAP 9.10.1P10 o versiones de revisión posteriores si tiene pensado actualizar a las versiones de ONTAP 9.9.1 o ONTAP 9.10.1.

Antes de empezar

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

  "Relaciones entre iguales de clústeres y SVM"

- El idioma del volumen de destino debe ser el mismo que el del volumen de origen.

Acerca de esta tarea

Hasta ONTAP 9.3, SnapMirror invocado en modo DP y SnapMirror invocado en modo XDP utilizaba distintos motores de replicación, con distintos enfoques respecto a la dependencia de versión:

- SnapMirror que se invoca en el modo DP utilizaba un motor de replicación *version-dependent* en el que la versión de ONTAP debía ser la misma en el almacenamiento primario y secundario:

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- SnapMirror, al que se invocó en el modo XDP, utilizó un motor de replicación de *version-flexible* que admitía diferentes versiones de ONTAP en el almacenamiento primario y secundario:

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

Las importantes ventajas de SnapMirror, que ofrece una versión flexible, superan la ligera ventaja del rendimiento de la replicación obtenido con el modo basado en la versión. Por este motivo, a partir de ONTAP 9.3, se ha creado el modo XDP como nuevo valor predeterminado, y cualquier invocación del modo DP en la línea de comandos o en scripts nuevos o existentes se convierte automáticamente al modo XDP.

Las relaciones existentes no se ven afectadas. Si una relación ya es del tipo DP, seguirá siendo del tipo DP. La siguiente tabla muestra el comportamiento que puede esperar.

Si especifica…	El tipo es…	La política predeterminada (si no se especifica una política) es…
PROTECCIÓN DE DATOS	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)
Nada	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)
XDP	XDP	XDPDefault (SnapVault)

Consulte también los ejemplos del procedimiento siguiente.

Las únicas excepciones a la conversión son las siguientes:

- Las relaciones de protección de datos de SVM siguen siendo las predeterminadas en el modo DP.

  Especifique XDP explícitamente para obtener el modo XDP con la `MirrorAllSnapshots` política predeterminada.

- Las relaciones de protección de datos con uso compartido de carga siguen siendo las predeterminadas en el modo DP.
- Las relaciones de protección de datos de SnapLock siguen siendo las predeterminadas en el modo DP.
- Las invocaciones explícitas de DP siguen en el modo DP de forma predeterminada si establece la siguiente opción para todo el clúster:

```
options replication.create_data_protection_rels.enable on
```

  Esta opción se ignora si no invoca explícitamente DP.

A partir de ONTAP 9.14.1, la `-backoff-level` opción se agrega a los `snapmirror create`comandos , `snapmirror modify`y `snapmirror restore` para permitirle especificar el nivel de interrupción por relación. La opción solo se admite con las relaciones SnapMirror de FlexVol. El comando opcional especifica el nivel de backup de SnapMirror debido a las operaciones del cliente. Los valores de retroceso pueden ser altos, medios o ninguno. El valor predeterminado es high.

A partir de ONTAP 9.5, se admiten las relaciones síncronas de SnapMirror.

En ONTAP 9.4 y versiones posteriores, un volumen de destino puede contener hasta 1019 instantáneas. En ONTAP 9.3 y versiones anteriores, un volumen de destino puede contener hasta 251 instantáneas.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para crear una relación de replicación.

System Manager

1. Seleccione el volumen o LUN que desea proteger: Haga clic en **almacenamiento > volúmenes** o **almacenamiento > LUN** y, a continuación, haga clic en el volumen o nombre de LUN que desee.
2. Haga clic en Protect.
3. Seleccione el clúster de destino y la máquina virtual de almacenamiento.
4. De forma predeterminada, la política asíncrona está seleccionada. Para seleccionar una directiva síncrona, haga clic en **más opciones**.
5. Haga clic en **proteger**.
6. Haga clic en la ficha **SnapMirror (local o remoto)** del volumen o LUN seleccionados para verificar que la protección está configurada correctamente.

CLI

1. En el clúster de destino, cree una relación de replicación:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   `schedule`El parámetro no es aplicable al crear relaciones síncronas de SnapMirror.

   En el ejemplo siguiente se crea una relación de recuperación ante desastres de SnapMirror con la `MirrorLatest` política predeterminada:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   En el ejemplo siguiente se crea una relación de SnapVault a través de la `XDPDefault` política predeterminada:

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   En el siguiente ejemplo, se crea una relación de replicación unificada mediante la `MirrorAndVault` política predeterminada:

   ```
   cluster_dst:> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorAndVault
   ```

En el siguiente ejemplo, se crea una relación de replicación unificada mediante la `my_unified` política personalizada:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

En el ejemplo siguiente se crea una relación de SnapMirror síncrona con la `Sync` política predeterminada:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

En el ejemplo siguiente se crea una relación de SnapMirror síncrona con la `StrictSync` política predeterminada:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. Cuando el tipo DP se convierte automáticamente a XDP y sin especificar ninguna política, la política se establece por defecto en la `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. Si no se ha especificado ningún tipo o política, la política se establece por defecto en la `MirrorAllSnapshots` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror. Si no se ha especificado ninguna política, la política se establece por defecto en la `XDPDefault` política:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

En el siguiente ejemplo, se crea una relación síncrona de SnapMirror con la política predefinida `SnapCenterSync`:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

La política predefinida `SnapCenterSync` es de tipo `Sync`. Esta política replica cualquier snapshot que se cree con el `snapmirror-label` «APP_CONFORTABLE».

Después de terminar

Utilice `snapmirror show` el comando para verificar que la relación de SnapMirror se ha creado.

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

Información relacionada

- "Crear y eliminar volúmenes de prueba de conmutación al nodo de respaldo de SnapMirror".

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general sobre backup de volúmenes mediante SnapVault"

Información relacionada

- "snapmirror create"

Inicialice una relación de replicación de ONTAP SnapMirror

Para todos los tipos de relaciones, la inicialización realiza una transferencia *baseline*: Crea una instantánea del volumen de origen y luego transfiere esa copia y todos los bloques de datos a los que hace referencia al volumen de destino. De lo contrario, el contenido de la transferencia depende de la política.

Antes de empezar

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

"Relaciones entre iguales de clústeres y SVM"

Acerca de esta tarea

La inicialización puede requerir mucho tiempo. Puede ser conveniente ejecutar la transferencia básica en horas de menor actividad.

A partir de ONTAP 9.5, se admiten las relaciones síncronas de SnapMirror.

Debe tener en cuenta que si un sistema de archivos se reinicia por cualquier motivo, como un reinicio de nodo, una toma de control/devolución o un pánico, la inicialización no se reanudará automáticamente y deberá reiniciarse manualmente.

Paso

1. Inicializar una relación de replicación:

```
snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el ejemplo siguiente, se inicializa la relación entre el volumen `volA` `svm1` de origen en y el volumen de destino `volA_dst` en `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

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

Asegúrese de una instantánea común en una implementación de mirror-vault de ONTAP

Puedes utilizar el `snapmirror snapshot-owner create` Comando para conservar una instantánea etiquetada en el almacén secundario en una implementación de bóveda reflejada. Esto garantiza que exista una instantánea común para la actualización de la relación entre bóvedas.

Acerca de esta tarea

Si utiliza una combinación de replicación ramificada entre reflejo y almacén o implementación en cascada, debe tener en cuenta que las actualizaciones generarán errores si no existe una snapshot común en los volúmenes de origen y de destino.

Esto nunca es un problema de la relación de reflejo en una implementación ramificada reflejo-almacén o en cascada, ya que SnapMirror siempre crea una copia Snapshot del volumen de origen antes de llevar a cabo la actualización.

Sin embargo, puede ser un problema para la relación de almacén, ya que SnapMirror no crea una copia Snapshot del volumen de origen cuando actualiza una relación de almacén. Debe utilizar `snapmirror snapshot-owner create` para asegurarse de que hay al menos una instantánea común tanto en el origen como en el destino de la relación de almacén. "Obtenga más información sobre la distribución ramificada y las puestas en marcha en cascada de la protección de datos".

Pasos

1. En el volumen de origen, asigne un propietario a la snapshot etiquetada que desea conservar:

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   En el siguiente ejemplo se asigna `ApplicationA` como propietario de `snap1` la copia de Snapshot:

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   Obtenga más información sobre `snapmirror snapshot-owner create` en el "Referencia de

comandos del ONTAP" .

2. Actualice la relación de reflejo, tal como se describe en "Actualizar manualmente una relación de replicación".

   También puede esperar a la actualización programada de la relación de reflejo.

3. Transfiera la instantánea etiquetada al destino del almacén:

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot
   ```

   En el siguiente ejemplo se transfiere la `snap1` copia de Snapshot

   ```
   clust1::> snapmirror update -vserver vs1 -volume vol1
   -source-snapshot snap1
   ```

   La instantánea etiquetada se conservará cuando se actualice la relación de almacén.

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

4. En el volumen de origen, quite el propietario de la snapshot etiquetada:

   ```
   snapmirror snapshot-owner delete -vserver SVM -volume volume -snapshot
   snapshot -owner owner
   ```

   Los siguientes ejemplos eliminan `ApplicationA` como propietario de `snap1` la instantánea:

   ```
   clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   Obtenga más información sobre `snapmirror snapshot-owner delete` en el "Referencia de comandos del ONTAP".

Ejemplo: Configurar una cascada de almacén-almacén de ONTAP SnapMirror

Un ejemplo mostrará en términos concretos cómo puede configurar las relaciones de replicación paso a paso. Puede utilizar el despliegue en cascada vault-vault configurado en el ejemplo para retener más de 251 instantáneas etiquetadas `my-weekly`.

Antes de empezar

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

Acerca de esta tarea

En el ejemplo se dan por hechos los siguientes elementos:

- Ha configurado las instantáneas en el clúster de origen con las etiquetas SnapMirror `my-daily` , `my-weekly` y `my-monthly`.

- Configuró los volúmenes de destino denominados `volA` en los clústeres de destino secundario y terciario.
- Ha configurado las programaciones de trabajos de replicación denominadas `my_snapvault` en los clústeres de destino secundarios y terciarios.

El ejemplo muestra cómo crear relaciones de replicación basadas en dos políticas personalizadas:

- `snapvault_secondary`La política retiene 7 copias Snapshot diarias, 52 semanales y 180 mensuales en el clúster de destino secundario.
- El `snapvault_tertiary policy` retiene 250 copias de Snapshot semanales en el clúster de destino terciario.

Pasos

1. En el clúster de destino secundario, cree la `snapvault_secondary` política:

   ```
   cluster_secondary::> snapmirror policy create -policy snapvault_secondary
   -type vault -comment "Policy on secondary for vault to vault cascade" -vserver
   svm_secondary
   ```

2. En el clúster de destino secundario, defina `my-daily` la regla para la política:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-daily -keep 7 -vserver svm_secondary
   ```

3. En el clúster de destino secundario, defina `my-weekly` la regla para la política:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-weekly -keep 52 -vserver svm_secondary
   ```

4. En el clúster de destino secundario, defina `my-monthly` la regla para la política:

   ```
   cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
   -snapmirror-label my-monthly -keep 180 -vserver svm_secondary
   ```

5. En el clúster de destino secundario, compruebe la política:

   ```
   cluster_secondary::> snapmirror policy show snapvault_secondary -instance
   ```

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily                7  false       0 -
-
                              my-weekly              52  false       0 -
-
                              my-monthly            180  false       0 -
-
```

6. En el clúster de destino secundario, cree la relación con el clúster de origen:

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
snapvault_secondary
```

7. En el clúster de destino secundario, inicialice la relación con el clúster de origen:

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. En el clúster de destino terciario, cree la `snapvault_tertiary` política:

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. En el clúster de destino terciario, defina `my-weekly` la regla para la política:

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. En el clúster de destino terciario, compruebe la política:

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                    Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. En el clúster de destino terciario, cree la relación con el clúster secundario:

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. En el clúster de destino terciario, inicialice la relación con el clúster secundario:

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

Información relacionada

- "snapmirror create"
- "inicializar snapmirror"
- "regla de adición de política de SnapMirror"
- "Crear política de SnapMirror"
- "Mostrar política de Snapmirror"

Gestione la replicación de volúmenes de SnapMirror

Convertir una relación de tipo DP de ONTAP SnapMirror existente a XDP

Si actualiza a ONTAP 9.12.1 o una versión posterior, debe convertir las relaciones de tipo

DP a XDP antes de realizar la actualización. ONTAP 9.12.1 y las versiones posteriores no admiten relaciones de tipo DP. Puede convertir fácilmente una relación de tipo de DP existente a XDP para poder aprovechar las ventajas de la flexibilidad de versión de SnapMirror.

Antes de actualizar a ONTAP 9.12.1, debe convertir las relaciones de tipo DP existentes a XDP antes de poder actualizar a ONTAP 9.12.1 y versiones posteriores.

Acerca de esta tarea

- SnapMirror no convierte automáticamente las relaciones de tipo DP existentes a XDP. Para convertir la relación, debe romper y eliminar la relación existente, crear una nueva relación XDP y volver a sincronizar la relación.
- Al planificar la conversión, tenga en cuenta que la preparación en segundo plano y la fase de almacenamiento de datos de una relación de SnapMirror para XDP pueden llevar mucho tiempo. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.

> Después de convertir un tipo de relación de SnapMirror de DP a XDP, las configuraciones relacionadas con el espacio, como la configuración automática de tamaño y la garantía de espacio, ya no se replican en el destino.

Pasos

1. En el clúster de destino, compruebe que la relación SnapMirror sea del tipo DP, que el estado de mirroring sea en SnapMirror, que el estado de la relación sea inactivo y que la relación esté en buen estado:

   ```
   snapmirror show -destination-path <SVM:volume>
   ```

   En el ejemplo siguiente se muestra el resultado del `snapmirror show` comando:

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

Puede resultarle útil conservar una copia `snapmirror show` del resultado del comando para realizar un seguimiento de la existencia de la configuración de relaciones. Obtenga más información sobre `snapmirror show` en el "Referencia de comandos del ONTAP".

2. Desde los volúmenes de origen y destino, debe asegurarse de que ambos volúmenes tengan una snapshot común:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

En el ejemplo siguiente, se muestra `volume snapshot show` el resultado de los volúmenes de origen y destino:

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. Para garantizar que las actualizaciones programadas no se ejecuten durante la conversión, desactive la relación de tipo DP existente:

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

El ejemplo siguiente pone en modo inactivo la relación entre el volumen `volA` `svm1` de origen en y el de destino `volA_dst` en `svm_backup`:

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

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

4. Rompa la relación de tipo de DP existente:

```
snapmirror break -destination-path <SVM:volume>
```

Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el ejemplo siguiente, se interrumpe la relación entre el volumen de origen `volA` `svm1` `volA_dst` en y el de destino en `svm_backup`:

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

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

5. Si la eliminación automática de Snapshot está habilitada en el volumen de destino, deshabilite este elemento:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

En el ejemplo siguiente se deshabilita la eliminación automática de Snapshot en el volumen de destino `volA_dst` :

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. Elimine la relación de tipo de DP existente:

```
snapmirror delete -destination-path <SVM:volume>
```

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

> Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el ejemplo siguiente se elimina la relación entre el volumen de origen `volA` en `svm1` y el volumen de destino `volA_dst` en `svm_backup`:

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. Libere la relación de recuperación ante desastres de la SVM de origen en el origen:

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

En el ejemplo siguiente se libera la relación de recuperación de desastres de SVM:

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

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

8. Puede utilizar la salida que conservó del `snapmirror show` comando para crear la nueva relación de tipo XDP:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

La nueva relación debe usar el mismo volumen de origen y destino. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

> Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el ejemplo siguiente se crea una relación de recuperación de desastres de SnapMirror entre el volumen de origen `volA` en `svm1` y el volumen de destino `volA_dst` cuando `svm_backup` se utiliza `MirrorAllSnapshots` la política predeterminada:

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. Resincronización de los volúmenes de origen y destino:

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

Para mejorar el tiempo de resincronización, puede utilizar el `-quick-resync` opción, pero debe tener en cuenta que se pueden perder ahorros en eficiencia de almacenamiento.

> Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

En el siguiente ejemplo, se vuelve a sincronizar la relación entre el volumen `volA` `svm1` de origen en y el de destino `volA_dst` en `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

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

10. Si deshabilitó la eliminación automática de snapshots, vuelva a habilitarla:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Después de terminar

1. Utilice `snapmirror show` el comando para verificar que la relación de SnapMirror se ha creado.

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

2. Una vez que el volumen de destino de SnapMirror XDP comience a actualizar las instantáneas tal como se define en la política de SnapMirror, utilice el comando de salida `snapmirror list-destinations` del clúster de origen para mostrar la nueva relación de SnapMirror XDP.

Información adicional sobre las relaciones de tipo DP

A partir de ONTAP 9,3, el modo XDP es el valor predeterminado, y cualquier invocación del modo DP en la línea de comandos o en scripts nuevos o existentes se convierte automáticamente al modo XDP.

Las relaciones existentes no se ven afectadas. Si una relación ya es del tipo DP, seguirá siendo del tipo DP. A partir de ONTAP 9,5, MirrorAndVault es la política predeterminada cuando no se especifica ningún modo de protección de datos o cuando se especifica el modo XDP como tipo de relación. La siguiente tabla muestra el comportamiento esperado.

Si especifica…	El tipo es…	La política predeterminada (si no se especifica una política) es…
PROTECCIÓN DE DATOS	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)

Nada	XDP	MirrorAndVault (replicación unificada)
XDP	XDP	MirrorAndVault (replicación unificada)

Como se muestra en la tabla, las políticas predeterminadas asignadas a XDP en diferentes circunstancias garantizan que la conversión mantenga la equivalencia funcional de los tipos anteriores. Por supuesto, puede utilizar diferentes políticas según sea necesario, incluidas las políticas para la replicación unificada:

Si especifica…	Y la política es…	El resultado es…
PROTECCIÓN DE DATOS	MirrorAllSnapshots	Recuperación ante desastres de SnapMirror
XDPDefault	SnapVault	Reflejo de AndVault
Replicación unificada	XDP	MirrorAllSnapshots
Recuperación ante desastres de SnapMirror	XDPDefault	SnapVault

Las únicas excepciones a la conversión son las siguientes:

- Las relaciones de protección de datos de SVM siguen siendo las predeterminadas para el modo DP en ONTAP 9.3 y versiones anteriores.

  A partir de ONTAP 9.4, las relaciones de protección de datos de la SVM se establecen en el modo XDP de manera predeterminada.

- Las relaciones de protección de datos con uso compartido de carga de volumen raíz continúan hasta los valores predeterminados en el modo DP.
- Las relaciones de protección de datos de SnapLock continúan en el modo DP de ONTAP 9.4 y versiones anteriores.

  A partir de ONTAP 9.5, las relaciones de protección de datos de SnapLock se establecen en el modo XDP de manera predeterminada.

- Las invocaciones explícitas de DP siguen en el modo DP de forma predeterminada si establece la siguiente opción para todo el clúster:

  ```
  options replication.create_data_protection_rels.enable on
  ```

  Esta opción se ignora si no invoca explícitamente DP.

Información relacionada

- "snapmirror create"

- "snapmirror elimina"
- "Snapmirror en reposo"
- "versión de snapmirror"
- "resincronización de SnapMirror"

Convertir el tipo de una relación de ONTAP SnapMirror

A partir de ONTAP 9.5, se admite SnapMirror síncrono. Es posible convertir una relación asíncrona de SnapMirror en una relación síncrona de SnapMirror o viceversa sin realizar una transferencia completa.

Acerca de esta tarea

No se puede convertir una relación asíncrona de SnapMirror en una relación síncrona de SnapMirror o viceversa cambiando la política de SnapMirror.

Pasos

- **Convertir una relación asíncrona de SnapMirror a una relación síncrona de SnapMirror**

  a. Desde el clúster de destino, elimine la relación asíncrona de SnapMirror:

  ```
  snapmirror delete -destination-path <SVM:volume>
  ```

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  b. En el clúster de origen, libere la relación de SnapMirror sin eliminar las copias de Snapshot comunes:

  ```
  snapmirror release -relationship-info-only true -destination-path
  <destination_SVM>:<destination_volume>
  ```

  ```
  cluster1::>snapmirror release -relationship-info-only true
  -destination-path vs1_dr:vol1
  ```

  c. Desde el clúster de destino, cree una relación síncrona de SnapMirror:

  ```
  snapmirror create -source-path src_SVM:src_volume -destination-path
  <destination_SVM>:<destination_volume> -policy sync-mirror
  ```

  ```
  cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
  vs1_dr:vol1 -policy sync
  ```

  d. Resincronice la relación síncrona de SnapMirror:

  ```
  snapmirror resync -destination-path <destination_SVM:destination_volume>
  ```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- **Convertir una relación síncrona de SnapMirror a una relación asíncrona de SnapMirror**

  a. Desde el clúster de destino, desactive la relación síncrona de SnapMirror existente:

  `snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>`

  ```
  cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
  ```

  b. Desde el clúster de destino, elimine la relación asíncrona de SnapMirror:

  `snapmirror delete -destination-path <SVM:volume>`

  ```
  cluster2::>snapmirror delete -destination-path vs1_dr:vol1
  ```

  c. En el clúster de origen, libere la relación de SnapMirror sin eliminar las copias de Snapshot comunes:

  `snapmirror release -relationship-info-only true -destination-path <destination_SVM:destination_volume>`

  ```
  cluster1::>snapmirror release -relationship-info-only true
  -destination-path vs1_dr:vol1
  ```

  d. Desde el clúster de destino, cree una relación asíncrona de SnapMirror:

  `snapmirror create -source-path` *`src_SVM:src_volume`* `-destination-path <destination_SVM:destination_volume> -policy MirrorAllSnapshots`

  ```
  cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
  vs1_dr:vol1 -policy sync
  ```

  e. Resincronice la relación síncrona de SnapMirror:

  `snapmirror resync -destination-path <destination_SVM:destination_volume>`

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

Información relacionada

- "snapmirror create"
- "snapmirror elimina"

- "Snapmirror en reposo"
- "versión de snapmirror"
- "resincronización de SnapMirror"

Convierta el modo de una relación síncrona de ONTAP SnapMirror

A partir de ONTAP 9.5, se admiten las relaciones síncronas de SnapMirror. Puede convertir el modo de una relación síncrona de SnapMirror de StrictSync a Sync o viceversa.

Acerca de esta tarea

No puede modificar la política de una relación síncrona de SnapMirror para convertir su modo.

Pasos

1. Desde el clúster de destino, desactive la relación síncrona de SnapMirror existente:

   `snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
   ```

2. Desde el clúster de destino, elimine la relación síncrona de SnapMirror existente:

   `snapmirror delete -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster2::> snapmirror delete -destination-path vs1_dr:vol1
   ```

3. En el clúster de origen, libere la relación de SnapMirror sin eliminar las copias de Snapshot comunes:

   `snapmirror release -relationship-info-only true -destination-path <destination_SVM>:<destination_volume>`

   ```
   cluster1::> snapmirror release -relationship-info-only true -destination
   -path vs1_dr:vol1
   ```

4. Desde el clúster de destino, cree una relación síncrona de SnapMirror especificando el modo en el que desea convertir la relación síncrona de SnapMirror:

   `snapmirror create -source-path vs1:vol1 -destination-path <destination_SVM>:<destination_volume> -policy Sync|StrictSync`

   ```
   cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
   vs1_dr:vol1 -policy Sync
   ```

5. En el clúster de destino, resincronice la relación SnapMirror:

```
snapmirror resync -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

Información relacionada

- "snapmirror create"
- "snapmirror elimina"
- "Snapmirror en reposo"
- "versión de snapmirror"
- "resincronización de SnapMirror"

Crear y eliminar volúmenes de prueba de conmutación al nodo de respaldo de ONTAP SnapMirror

A partir de ONTAP 9.14.1, puede usar System Manager para crear un clon de volumen a fin de probar la conmutación por error y la recuperación ante desastres de SnapMirror sin interrumpir la relación de SnapMirror activa. Cuando termine la prueba, puede limpiar los datos asociados y eliminar el volumen de prueba.

Crear un volumen de prueba de conmutación por error de SnapMirror

Acerca de esta tarea

- Puede realizar pruebas de conmutación al nodo de respaldo en relaciones síncronas y asíncronas de SnapMirror.
- Se crea un clon de volumen para realizar la prueba de recuperación ante desastres.
- El volumen clonado se crea en la misma máquina virtual de almacenamiento que el destino de SnapMirror.
- Se pueden usar las relaciones de SnapMirror de FlexVol y FlexGroup.
- Si ya existe un clon de prueba para la relación seleccionada, no puede crear otro clon para esa relación.
- No se admiten las relaciones de almacén de SnapLock.

Antes de empezar

- Debe ser un administrador de clústeres.
- La licencia de SnapMirror debe instalarse en los clústeres de origen y de destino.

Pasos

1. En el clúster de destino, seleccione **Protección > Relaciones**.
2. Seleccione ⋮ junto al origen de la relación y elija **Test Failover**.
3. En la ventana **Test Failover**, selecciona **Test Failover**.
4. Seleccione **Almacenamiento > Volúmenes** y compruebe que el volumen de conmutación por error de prueba aparece en la lista.
5. Selecciona **Almacenamiento > Acciones**.
6. Selecciona + Add y elige **Compartir**.
7. En la ventana **Agregar recurso compartido**, escriba un nombre para el recurso compartido en el campo

Compartir nombre.

8. En el campo **Carpeta**, seleccione **Examinar**, seleccione el volumen de clonación de prueba y **Guardar**.
9. En la parte inferior de la ventana **Agregar Compartir**, selecciona **Guardar**.
10. En el panel **Almacenamiento > Recursos compartidos**, localice el recurso compartido que ha creado y seleccione para ver la información del recurso compartido.
11. En **Acceso SMB/CIFS**, copia o toma nota de la ruta de acceso para el recurso compartido; por ejemplo, `\\123.456.7.890\failover_test`.
12. Utilice la ruta de acceso de SMB para abrir el recurso compartido en el cliente y verificar que el volumen de prueba tenga capacidades de lectura y escritura.

Limpie los datos de conmutación por error y elimine el volumen de prueba

Después de completar las pruebas de conmutación al nodo de respaldo, puede borrar todos los datos asociados al volumen de prueba y eliminarlos.

Pasos

1. En el clúster de destino, seleccione **Protección > Relaciones**.
2. Seleccione junto al origen de la relación y elija **Limpiar prueba de failover**.
3. En la ventana **Limpiar prueba de failover**, selecciona **Limpiar**.
4. Seleccione **Almacenamiento > Volúmenes** y compruebe que se ha eliminado el volumen de prueba.

Proporcione datos desde un volumen de destino de recuperación ante desastres de SnapMirror

Permita que se pueda escribir el volumen de destino de ONTAP SnapMirror

Debe hacer que el volumen de destino sea editable, para poder proporcionar datos del volumen a los clientes. Para servir datos desde un destino de mirroring cuando un origen deja de estar disponible, detenga las transferencias programadas hacia el destino y, a continuación, rompa la relación de SnapMirror para hacer que el destino sea editable.

Acerca de esta tarea

Debe realizar esta tarea desde la SVM de destino o el clúster de destino.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para que un volumen de destino pueda escribirse.

System Manager

1. Seleccione la relación de protección: Haga clic en **Protección > Relaciones** y, a continuación, haga clic en el nombre del volumen deseado.
2. Haga clic en ⋮.
3. Detener transferencias programadas : haga clic en **Pausa**.
4. Haga que el destino sea editable: Haga clic en **romper**.
5. Vaya a la página principal **Relaciones** para verificar que el estado de la relación se muestra como "roto".

Siguientes pasos

Debe hacerlo "resincronice reverso la relación de replicación" después de hacer que un volumen de destino se pueda escribir.

Cuando el volumen de origen deshabilitado vuelve a estar disponible, es necesario revertir la relación de nuevo para copiar los datos actuales en el volumen de origen original.

CLI

1. Detenga las transferencias programadas al destino:

```
snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

En el ejemplo siguiente se detienen las transferencias programadas entre el volumen de origen `volA` en `svm1` y el volumen de destino `volA_dst` `svm_backup` en :

```
cluster_dst::> snapmirror quiesce -source-path svm1:volA
-destination-path svm_backup:volA_dst
```

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

2. Detenga las transferencias continuas al destino:

```
snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

> Este paso no es necesario para las relaciones síncronas de SnapMirror (se admite a partir de ONTAP 9.5).

El ejemplo siguiente detiene las transferencias en curso entre el volumen de origen `volA` en `svm1` y el volumen de destino `volA_dst` en `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

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

3. Rompa la relación de recuperación ante desastres de SnapMirror:

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

En el ejemplo siguiente, se interrumpe la relación entre el volumen de origen `volA` `svm1` `volA_dst` en y el de destino en `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

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

Siguientes pasos

Debe hacerlo "resincronice la relación de replicación" después de hacer que un volumen de destino se pueda escribir.

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general sobre la recuperación ante desastres de volúmenes"

Configure el volumen de destino de ONTAP SnapMirror para acceder a los datos

Tras hacer que el volumen de destino sea editable, debe configurar el volumen para el acceso a los datos. Los clientes NAS, el subsistema NVMe y hosts SAN pueden acceder a los datos desde el volumen de destino hasta que se reactive el volumen de origen.

Entorno NAS:

1. Monte el volumen NAS en el espacio de nombres mediante la misma ruta de unión en la que se montó el volumen de origen en la SVM de origen.
2. Aplique las ACL adecuadas para los recursos compartidos de SMB en el volumen de destino.
3. Asigne las políticas de exportación de NFS al volumen de destino.
4. Aplique las reglas de cuota al volumen de destino.
5. Redirija a los clientes al volumen de destino.

6. Vuelva a montar los recursos compartidos de NFS y SMB en los clientes.

ENTORNO SAN:

1. Asigne las LUN del volumen al iGroup correspondiente.
2. Para iSCSI, cree sesiones iSCSI desde los iniciadores de host SAN hasta las LIF DE SAN.
3. En el cliente SAN, realice una nueva exploración del almacenamiento para detectar las LUN conectadas.

Para obtener más información sobre el entorno NVMe, consulte "Administración de SAN".

Reactivar el volumen de origen original de ONTAP SnapMirror

Puede restablecer la relación de protección de datos original entre los volúmenes de origen y destino cuando ya no necesite servir datos desde el destino.

Acerca de esta tarea

- En el siguiente procedimiento se asume que la línea base del volumen de origen original está intacta. Si la base de referencia no está intacta, debe crear e inicializar la relación entre el volumen desde el que se sirven datos y el volumen de origen original antes de realizar el procedimiento.
- La preparación en segundo plano y la fase de almacenamiento de datos de una relación de SnapMirror para XDP pueden llevar mucho tiempo. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.

Pasos

1. Invierta la relación de protección de datos original:

   `snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

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

   > Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original. Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad. El comando genera un error si no existe una snapshot común en el origen y el destino. Se utiliza `snapmirror initialize` para reinicializar la relación. Obtenga más información sobre `snapmirror initialize` en el "Referencia de comandos del ONTAP".

   En el siguiente ejemplo se revierte la relación entre el volumen de origen original, `volA` `svm1` en y el volumen desde el que sirve datos, `volA_dst` en `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. Una vez que esté listo para restablecer el acceso a los datos en el origen original, detenga el acceso al volumen de destino original. Una manera de hacerlo es detener la SVM de destino original:

   `vserver stop -vserver` *`SVM`*

Debe ejecutar este comando desde la SVM de destino original o desde el clúster de destino original. Este comando detiene el acceso del usuario a la SVM original completa de destino. Puede que desee detener el acceso al volumen de destino original mediante otros métodos.

En el ejemplo siguiente se detiene la SVM de destino original:

```
cluster_dst::> vserver stop svm_backup
```

Obtenga más información sobre `vserver stop` en el "Referencia de comandos del ONTAP".

3. Actualice la relación de inversión:

`snapmirror update -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

En el ejemplo siguiente se actualiza la relación entre el volumen desde `volA_dst` `svm_backup` el que se sirven datos, en , y el volumen de origen original, `volA` en `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

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

4. Desde la SVM de origen original o el clúster de origen original, detenga las transferencias programadas para la relación inversa:

`snapmirror quiesce -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

En el ejemplo siguiente se detienen las transferencias programadas entre el volumen de destino original, `volA_dst` `svm_backup` el y el volumen de origen original, `volA` el `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

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

5. Cuando la actualización final se completa y la relación indica "Quiesced" para el estado de la relación, ejecute el siguiente comando desde la SVM de origen original o el clúster de origen original para romper la relación inversa:

`snapmirror break -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen.

En el ejemplo siguiente, se interrumpe la relación entre el volumen de destino original, `volA_dst` por `svm_backup` y el volumen de origen original, `volA` en `svm1`:

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

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

6. En la SVM de origen original o en el clúster de origen original, elimine la relación de protección de datos inversa:

`snapmirror delete -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

En el ejemplo siguiente se elimina la relación invertida entre el volumen de origen original, `volA` `svm1` en y el volumen del que sirve datos, `volA_dst` en `svm_backup`:

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

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

7. Libere la relación inversa de la SVM de destino original o el clúster de destino original.

`snapmirror release -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

Debe ejecutar este comando desde la SVM de destino original o desde el clúster de destino original.

En el ejemplo siguiente se libera la relación inversa entre el volumen de destino original, `volA_dst` `svm_backup` el y el volumen de origen original, `volA` el `svm1`:

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

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

8. Restablezca la relación de protección de datos original desde el destino original:

`snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

En el ejemplo siguiente se restablece la relación entre el volumen de origen, `volA svm1` en y el volumen de destino original, `volA_dst` en `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

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

9. Si es necesario, inicie la SVM de destino original:

   `vserver start -vserver` *SVM*

   En el ejemplo siguiente se inicia la SVM de destino original:

   ```
   cluster_dst::> vserver start svm_backup
   ```

   Obtenga más información sobre `vserver start` en el "Referencia de comandos del ONTAP".

Después de terminar

Utilice `snapmirror show` el comando para verificar que la relación de SnapMirror se ha creado.

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

Restaurar los archivos de un volumen de destino de SnapMirror

Restaure un espacio de nombres de archivos, LUN o NVMe desde un destino de ONTAP SnapMirror

Es posible restaurar un único archivo, LUN, un conjunto de archivos o LUN desde una copia Snapshot o un espacio de nombres NVMe desde un volumen de destino de SnapMirror. A partir de ONTAP 9.7, también se pueden restaurar espacios de nombres NVMe desde un destino síncrono de SnapMirror. Es posible restaurar archivos en el volumen de origen original o en otro volumen.

Antes de empezar

Para restaurar un archivo o un LUN desde un destino síncrono de SnapMirror (compatible a partir de ONTAP 9.5), primero debe eliminar y liberar la relación.

Acerca de esta tarea

El volumen al que va a restaurar archivos o LUN (el volumen de destino) debe ser un volumen de lectura y escritura:

- SnapMirror realiza una restauración *incremental* si los volúmenes de origen y destino tienen una snapshot común (como suele suceder cuando se restaura al volumen de origen original).
- De lo contrario, SnapMirror realizará una restauración *baseline*, en la que la snapshot especificada y todos los bloques de datos a los que hace referencia se transferirán al volumen de destino.

Pasos

1. Enumere las copias Snapshot en el volumen de destino:

   `volume snapshot show -vserver <SVM> -volume volume`

   Obtenga más información sobre `volume snapshot show` en el "Referencia de comandos del ONTAP".

   En el ejemplo siguiente se muestran las copias de Snapshot en el `vserverB:secondary1` destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaure un único archivo o LUN o un conjunto de archivos o LUN desde una copia Snapshot en un volumen de destino de SnapMirror:

   `snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, … -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot snapshot -file-list <source_file_path,@destination_file_path>`

   Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

   El siguiente comando restaura los archivos `file1` y `file2` de la instantánea `daily.2013-01-25_0010` en el volumen de destino original `secondary1` , en la misma ubicación en el sistema de archivos activo del volumen de origen original `primary1` :

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

El siguiente comando restaura los archivos `file1` y `file2` de la instantánea `daily.2013-01-25_0010` en el volumen de destino original `secondary1` , en una ubicación diferente en el sistema de archivos activo del volumen de origen original `primary1` .

La ruta del archivo de destino comienza con el símbolo @ seguido por la ruta del archivo desde la raíz del volumen de origen original. En este ejemplo, `file1` se restaura en `/dir1/file1.new` y file2 se restaura en `/dir2.new/file2` el `primary1`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

El siguiente comando restaura los archivos `file1` y `file3` de la instantánea `daily.2013-01-25_0010` en el volumen de destino original `secondary1` , en distintas ubicaciones del sistema de archivos activo del volumen de origen original `primary1` y restaura `file2` desde `snap1` a la misma ubicación en el sistema de archivos activo de `primary1`.

En este ejemplo, el archivo `file1` se restaura en `/dir1/file1.new` y `file3` se restaura en `/dir3.new/file3`:

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

Información relacionada

- "restauración de snapmirror"

Restaurar el contenido de los volúmenes desde un destino de ONTAP SnapMirror

Se puede restaurar el contenido de un volumen completo desde una copia de Snapshot en un volumen de destino de SnapMirror. Es posible restaurar el contenido del volumen en el volumen de origen original o en otro volumen.

Acerca de esta tarea

Este procedimiento se aplica a los sistemas FAS, AFF y ASA. Si tiene un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30, ASA A20 o ASA C30), siga "estos pasos" para restaurar datos. Los sistemas R2 de ASA ofrecen una experiencia de ONTAP simplificada específica para clientes de SAN.

El volumen de destino de la operación de restauración debe ser uno de los siguientes:

- Un volumen de lectura y escritura, en cuyo caso SnapMirror realiza una restauración *incremental*, siempre y cuando los volúmenes de origen y de destino tengan una snapshot común (como suele ocurrir cuando se restaura el volumen de origen original).

  El comando falla si no hay una snapshot común. No es posible restaurar el contenido de un volumen en un volumen vacío de lectura/escritura.

- Un volumen de protección de datos vacío, en cuyo caso SnapMirror ejecuta una *baseline restore*, en la que la instantánea especificada y todos los bloques de datos a los que hace referencia se transfieren al volumen de origen.

La restauración del contenido de un volumen es una operación disruptiva. No debe ejecutarse el tráfico de SMB en el volumen primario de SnapVault cuando se ejecuta una operación de restauración.

Si el volumen de destino de la operación de restauración tiene la compresión habilitada y el volumen de origen no tiene la compresión habilitada, se debe deshabilitar la compresión en el volumen de destino. Es necesario volver a habilitar la compresión una vez que se completa la operación de restauración.

Las reglas de cuota definidas para el volumen de destino se desactivan antes de ejecutar la restauración. Puede usar `volume quota modify` el comando para reactivar las reglas de cuota una vez finalizada la operación de restauración.

Cuando se pierden o dañan datos de un volumen, la restauración a partir de una copia de Snapshot anterior se puede revertir los datos.

Este procedimiento reemplaza los datos actuales del volumen de origen con datos de una versión Snapshot anterior. Debe realizar esta tarea en el clúster de destino.

Pasos

Es posible restaurar el contenido de un volumen mediante System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

1. Haga clic en **Protección > Relaciones** y, a continuación, haga clic en el nombre del volumen de origen.
2. Haga clic ⋮ y luego seleccione **Restaurar**.
3. En **Fuente**, el volumen de origen está seleccionado de forma predeterminada. Haga clic en **otro volumen** si desea elegir un volumen distinto al de origen.
4. En **Destino**, elija la instantánea que desea restaurar.
5. Si su origen y destino se encuentran en diferentes clústeres, en el clúster remoto, haga clic en **Protección > Relaciones** para supervisar el progreso de la restauración.

CLI

1. Enumere las copias Snapshot en el volumen de destino:

```
volume snapshot show -vserver <SVM> -volume <volume>
```

   En el ejemplo siguiente se muestran las copias de Snapshot en el `vserverB:secondary1` destino:

```
cluster_dst::> volume snapshot show -vserver vserverB -volume
secondary1

Vserver     Volume      Snapshot                State    Size
Total% Used%
-------     ------      ---------- ----------- ------   -----
------ -----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. Restaure el contenido de un volumen a partir de una copia Snapshot en un volumen de destino de SnapMirror:

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
<snapshot>
```

Se debe ejecutar este comando desde la SVM de origen original o desde el clúster de origen original.

El siguiente comando restaura el contenido del volumen de origen original `primary1` a partir de la copia Snapshot `daily.2013-01-25_0010` en el volumen de destino original `secondary1` :

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than snapshot daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. Vuelva a montar el volumen restaurado y reinicie todas las aplicaciones que utilizan el volumen.

Otras maneras de hacerlo en ONTAP

Para ejecutar estas tareas con…	Ver este contenido…
System Manager Classic (disponible con ONTAP 9.7 y versiones anteriores)	"Información general sobre la restauración de volúmenes mediante SnapVault"

Información relacionada

- "restauración de snapmirror"
- "visualización de copias de snapshot de volumen"

Actualizar manualmente una relación de replicación de ONTAP SnapMirror

Es posible que deba actualizar una relación de replicación manualmente si falla una actualización debido a que se trasladó el volumen de origen.

Acerca de esta tarea

SnapMirror cancela todas las transferencias desde un volumen de origen movido hasta que se actualice la relación de replicación de forma manual.

A partir de ONTAP 9.5, se admiten las relaciones síncronas de SnapMirror. Si bien los volúmenes de origen y destino están sincronizados en todo momento en estas relaciones, la vista del clúster secundario se sincroniza con el primario solo por hora. Si desea ver los datos de un momento específico en el destino, debe realizar una actualización manual ejecutando `snapmirror update` el comando.

Paso

1. Actualice manualmente una relación de replicación:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

> Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. El comando genera un error si no existe una snapshot común en el origen y el destino. Se utiliza `snapmirror initialize` para reinicializar la relación. Obtenga más información sobre `snapmirror initialize` en el "Referencia de comandos del ONTAP".

En el ejemplo siguiente se actualiza la relación entre el volumen de origen `volA` en `svm1` y el de destino `volA_dst` en `svm_backup`:

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

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

Resincronizar una relación de replicación de ONTAP SnapMirror

Es necesario volver a sincronizar la relación de replicación después de que un volumen de destino se pueda escribir, una vez que se produce un error en la actualización debido a que no existe una Snapshot común en los volúmenes de origen y destino, o si desea cambiar la política de replicación para la relación.

A partir de ONTAP 9.8, es posible usar System Manager para realizar una operación de resincronización inversa a fin de eliminar una relación de protección existente y revertir las funciones de los volúmenes de origen y de destino. A continuación, se utilizará el volumen de destino para suministrar datos mientras se repara o se sustituye el origen, se actualiza el origen y se establece la configuración original de los sistemas.

> System Manager no admite la resincronización inversa con relaciones dentro del clúster. Puede usar la CLI de ONTAP para realizar operaciones de resincronización inversa con relaciones entre clústeres.

Acerca de esta tarea

- Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.
- Los volúmenes que forman parte de una configuración en cascada o de dispersión pueden tardar más en resincronizar. No es poco frecuente ver la relación de SnapMirror que informa sobre el estado "preparación" para un periodo de tiempo prolongado.
- A partir de ONTAP 9.13.1, ONTAP intenta utilizar la resincronización rápida de forma predeterminada para reducir el tiempo de resincronización. Para que la resincronización rápida se utilice de forma predeterminada, deben cumplirse las siguientes condiciones:
  - Los volúmenes FlexVol no tienen clones en el volumen.
  - Al usar la política MirrorAllSnapshots

Usando `-quick-resync` puede consumir espacio adicional en el volumen de destino de resincronización debido a la pérdida de eficiencia de almacenamiento en los bloques de datos transferidos. Este consumo de espacio adicional se recupera como parte de la aplicación de eficiencia de almacenamiento en línea o posterior a la replicación en el destino de resincronización.

El `-quick-resync` El parámetro es opcional. Puede activar o desactivar la resincronización rápida mediante el siguiente método: `-quick-resync true|false` parámetro con el `snapmirror resync` dominio.

Para obtener más información sobre `-quick-resync`, ver el "Referencia de comandos del ONTAP".

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para ejecutar esta tarea. Si utiliza la CLI de ONTAP, el procedimiento es el mismo independientemente de si va a hacer que un volumen de destino sea editable o si va a actualizar la relación de replicación.

System Manager resincronización inversa

Una vez "rompe una relación"que haya hecho que un destino pueda escribirse en el modo de escritura, resincronice la relación:

1. En el clúster de destino, haga clic en **Protección > Relaciones**.
2. Pase el ratón sobre la relación interrumpida que desea revertir, haga clic en ⋮ y seleccione **Resincronización inversa**.
3. En la ventana **Relación de resincronización inversa**, haz clic en **Resincronización inversa**.
4. En **Relaciones**, supervise el progreso de la resincronización inversa visualizando **Estado de transferencia** para la relación.

Siguientes pasos

Cuando el origen original vuelva a estar disponible, puede restablecer la relación original rompiendo la relación invertida y realizando otra operación de resincronización inversa. El proceso de resincronización inversa copiará cualquier cambio del sitio que esté sirviendo datos a la fuente original y hará que la fuente original sea de nuevo de lectura y escritura.

Resincronizar System Manager

1. Haga clic en **Protección > Relaciones**.
2. Pase el cursor sobre la relación que desea resincronizar y haga clic en ⋮ y luego seleccione **Romper**.
3. Cuando el estado de la relación muestre “Rotos”, haga clic ⋮ y luego seleccione **Resincronizar**.
4. En **Relaciones**, supervise el progreso de la resincronización comprobando el estado de la relación. El estado cambia a "reflejado" cuando se completa la resincronización.

CLI

1. Resincronización de los volúmenes de origen y destino:

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

ⓘ Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el ejemplo siguiente se vuelve a sincronizar la relación entre el volumen de origen `volA` en `svm1` y el volumen de destino `volA_dst` en `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

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

Información relacionada

- "Vuelva a sincronizar los datos en una SVM de destino de ONTAP SnapMirror"

Elimine una relación de replicación de volumen ONTAP SnapMirror

Puede usar `snapmirror delete` `snapmirror release` los comandos y para eliminar una relación de replicación de volumen. A continuación, puede eliminar manualmente los volúmenes de destino innecesarios.

Acerca de esta tarea

El `snapmirror release` comando elimina todas las copias Snapshot creadas por una SnapMirror del origen. Puede usar `-relationship-info-only` la opción para preservar las snapshots.

Pasos

1. Desactive la relación de replicación:

   `snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>`

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

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

2. (Opcional) rompa la relación de replicación si requiere que el volumen de destino sea un volumen de lectura/escritura. Puede omitir este paso si planea eliminar el volumen de destino o si no necesita que el volumen sea de lectura/escritura:

   ```
   snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

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

3. Elimine la relación de replicación:

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   Debe ejecutar este comando desde el clúster de destino o la SVM de destino.

   En el ejemplo siguiente se elimina la relación entre el volumen de origen `volA` en `svm1` y el volumen de destino `volA_dst` en `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

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

4. Libere la información de relaciones de replicación desde la SVM de origen:

```
snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

Se debe ejecutar este comando desde el clúster de origen o la SVM de origen.

En el siguiente ejemplo se libera información de la relación de replicación especificada desde la SVM de origen `svm1`:

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

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

Gestione la eficiencia del almacenamiento en volúmenes de ONTAP SnapMirror

SnapMirror mantiene la eficiencia del almacenamiento en los volúmenes de origen y destino, excepto cuando la compresión de datos de posprocesamiento está habilitada en el volumen de destino. En ese caso, se pierde toda la eficiencia del almacenamiento en el volumen de destino. Para corregir este problema, debe deshabilitar la compresión de posprocesamiento en el volumen de destino, actualizar la relación manualmente y volver a habilitar la eficiencia de almacenamiento.

Acerca de esta tarea

El `volume efficiency show` comando se puede usar para determinar si la eficiencia está habilitada en un volumen. Obtenga más información sobre `volume efficiency show` en el "Referencia de comandos del ONTAP".

Puede comprobar si SnapMirror mantiene la eficiencia del almacenamiento consultando los registros de auditoría de SnapMirror y buscando la descripción de la transferencia. Si aparece la descripción de la transferencia `transfer_desc=Logical Transfer with Storage Efficiency`, SnapMirror mantiene la eficiencia del almacenamiento. Si se muestra la descripción de transferencia `transfer_desc=Logical Transfer`, SnapMirror no mantiene la eficiencia del almacenamiento. Por ejemplo:

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

Antes de empezar

- Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

  "Relaciones entre iguales de clústeres y SVM"

- Debe deshabilitar la compresión de posprocesamiento en el volumen de destino.
- Transferencia lógica con almacenamiento: A partir de ONTAP 9,3, ya no es necesaria una actualización manual para volver a habilitar la eficiencia del almacenamiento. Si SnapMirror detecta que la compresión de postprocesamiento se ha deshabilitado, vuelve a habilitar automáticamente la eficiencia del almacenamiento en la siguiente actualización programada. Tanto el origen como el destino deben ejecutar ONTAP 9.3.
- A partir de ONTAP 9.3, los sistemas AFF gestionan las configuraciones de eficiencia del almacenamiento de forma diferente a las de los sistemas FAS después de crear su escritura en un volumen de destino:
  - Después de hacer que un volumen de destino sea escribible mediante el `snapmirror break` comando, la política de almacenamiento en caché en el volumen se establece automáticamente en `auto` (el valor predeterminado).

    Este comportamiento se aplica solo a volúmenes FlexVol, y no se aplica a volúmenes FlexGroup.

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

  - Al resincronizar, la política de almacenamiento en caché se establece automáticamente en `none` , y la deduplicación y la compresión en línea se deshabilitan automáticamente, independientemente de su configuración original. Debe modificar los ajustes manualmente según sea necesario.

Las actualizaciones manuales con eficiencia del almacenamiento, que pueden ser laboriosas. Se recomienda ejecutar la operación en horas de menor actividad.

Pasos

1. Actualice una relación de replicación y vuelva a habilitar la eficiencia del almacenamiento:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

Se debe ejecutar este comando desde la SVM de destino o el clúster de destino. El comando genera un error si no existe una snapshot común en el origen y el destino. Se utiliza `snapmirror initialize` para reinicializar la relación. Obtenga más información sobre `snapmirror initialize` en el "Referencia de comandos del ONTAP".

En el ejemplo siguiente, se actualiza la relación entre el volumen de origen `volA` en `svm1` y el volumen de destino `volA_dst` en `svm_backup`, y se vuelve a habilitar la eficiencia del almacenamiento:

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

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

Utilice la limitación global de ONTAP SnapMirror

La limitación de red global está disponible para todas las transferencias de SnapMirror y SnapVault a nivel de nodo.

Acerca de esta tarea

La limitación global de SnapMirror restringe el ancho de banda utilizado por transferencias entrantes o salientes de SnapMirror y SnapVault. La restricción se aplica en todo el clúster en todos los nodos del clúster.

Por ejemplo, si el acelerador saliente está establecido en 100 Mbps, cada nodo del clúster tendrá el ancho de banda saliente establecido en 100 Mbps. Si la regulación global está deshabilitada, se desactiva en todos los nodos.

Aunque las velocidades de transferencia de datos a menudo se expresan en bits por segundo (bps), los valores del acelerador deben introducirse en kilobytes por segundo (kbps).

> En ONTAP 9.9,1 y versiones anteriores, el acelerador no afecta a `volume move` las transferencias ni a las transferencias de reflejos de uso compartido de carga. A partir de ONTAP 9.10.0, puede especificar una opción para acelerar una operación de movimiento de volumen. Para obtener más información, consulte "Cómo acelerar el movimiento del volumen en ONTAP 9,10 y posteriores".

La limitación global funciona con la función acelerador por relación para transferencias de SnapMirror y SnapVault. El acelerador por relación se aplica hasta que el ancho de banda combinado de las transferencias por relación supere el valor de la aceleración global, después de lo cual se aplica la aceleración global. Un valor de acelerador `0` implica que la regulación global está desactivada.

> La limitación global de SnapMirror no afecta a las relaciones síncronas de SnapMirror cuando están sincronizadas. Sin embargo, el acelerador afecta a las relaciones síncronas de SnapMirror cuando realizan una fase de transferencia asíncrona, como una operación de inicialización o después de un evento no sincronizado. Por este motivo, no se recomienda habilitar la limitación global con relaciones síncronas de SnapMirror.

Pasos

1. Habilitar la limitación global:

   ```
   options -option-name replication.throttle.enable on|off
   ```

   El siguiente ejemplo muestra cómo activar la limitación global de SnapMirror en `cluster_dst`:

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. Especifique el ancho de banda total máximo utilizado por las transferencias entrantes en el clúster de destino:

   ```
   options -option-name replication.throttle.incoming.max_kbs <KBps>
   ```

   El ancho de banda mínimo recomendado es de 4 kilobytes por segundo (kbps) y el máximo es de hasta 2 terabytes por segundo (Tbps). El valor por defecto de esta opción es `unlimited`, lo que significa que no hay límite en el ancho de banda total utilizado.

El siguiente ejemplo muestra cómo establecer el ancho de banda total máximo utilizado por las transferencias entrantes a 100 megabits por segundo (Mbps):

```
cluster_dst::> options -option-name
replication.throttle.incoming.max_kbs 12500
```

100 megabits por segundo (Mbps) = 12500 kilobytes por segundo (kbps)

3. Especifique el ancho de banda total máximo que utilizan las transferencias salientes en el clúster de origen:

   `options -option-name replication.throttle.outgoing.max_kbs <KBps>`

   El ancho de banda mínimo recomendado del acelerador es de 4 kbps y el máximo es de 2 TB/s. El valor por defecto de esta opción es `unlimited`, lo que significa que no hay límite en el ancho de banda total utilizado. Los valores de los parámetros están en kilobytes por segundo (kbps).

   En el siguiente ejemplo se muestra cómo establecer el ancho de banda total máximo utilizado por las transferencias salientes en 100 Mbps:

   ```
   cluster_src::> options -option-name
   replication.throttle.outgoing.max_kbs 12500
   ```

Gestione la replicación de SVM de SnapMirror

Obtenga más información sobre la replicación de SVM de ONTAP SnapMirror

Puede usar SnapMirror para crear una relación de protección de datos entre SVM. En este tipo de relación de protección de datos, se replica toda o parte de la configuración de la SVM, desde las exportaciones NFS y los recursos compartidos de SMB hasta el RBAC, así como los datos en los volúmenes que posee la SVM.

Tipos de relaciones admitidos

Solo los SVM que proporcionan servicios de datos pueden replicarse. Se admiten los siguientes tipos de relaciones de protección de datos:

- *SnapMirror DR,* en el que el destino normalmente contiene solo las instantáneas actualmente en el origen.

  A partir de ONTAP 9.9.1, este comportamiento cambia cuando se utiliza la directiva mirror-vault. A partir de ONTAP 9,9.1, se pueden crear distintas políticas Snapshot en el origen y el destino, y las copias Snapshot en el destino no se sobrescriben por las del origen:

  - No se sobrescriben del origen al destino durante las operaciones programadas normales, las actualizaciones y la resincronización
  - No se eliminan durante las operaciones de interrupción.
  - No se eliminan durante las operaciones de resincronización. Cuando configura una relación de

desastre de SVM con la política de reflejo-almacén con ONTAP 9.9.1 y versiones posteriores, la política se comporta de la siguiente manera:

  - Las políticas de snapshots definidas por el usuario en el origen no se copian en el destino.
  - Las políticas de snapshots definidas por el sistema no se copian en el destino.
  - La asociación de volumen con políticas de snapshots definidas por el usuario y el sistema no se copian en el destino. + SVM.

- *Replicación unificada SnapMirror*, en la que el destino está configurado tanto para recuperación ante desastres como para retención a largo plazo.

Para obtener más información sobre la replicación unificada de SnapMirror, consulte "Conceptos básicos de la replicación unificada de SnapMirror".

El *policy type* de la directiva de replicación determina el tipo de relación que admite. La siguiente tabla muestra los tipos de políticas disponibles.

Tipo de política	Tipo de relación
reflejo asíncrono	Recuperación ante desastres de SnapMirror
mirror-vault	Replicación unificada

XDP sustituye a DP como la replicación SVM predeterminada en ONTAP 9.4

A partir de ONTAP 9.4, las relaciones de protección de datos de la SVM se establecen en el modo XDP de manera predeterminada. Las relaciones de protección de datos de SVM siguen siendo las predeterminadas para el modo DP en ONTAP 9.3 y versiones anteriores.

Las relaciones existentes no se ven afectadas por el valor por defecto de XDP. Si una relación ya es del tipo DP, seguirá siendo del tipo DP. La siguiente tabla muestra el comportamiento que puede esperar.

Si especifica…	El tipo es…	La política predeterminada (si no se especifica una política) es…
PROTECCIÓN DE DATOS	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)
Nada	XDP	MirrorAllSnapshots (recuperación ante desastres de SnapMirror)
XDP	XDP	MirrorAndVault (replicación unificada)

Puede encontrar información sobre cómo convertir relaciones de DP en relaciones XDP y otros detalles aquí: "Convertir una relación de tipo DP de ONTAP existente a XDP".

La independencia de la versión no se admite para la replicación de SVM. En una configuración de recuperación ante desastres de SVM, la máquina virtual de almacenamiento de destino debe estar en un clúster que ejecute la misma versión de ONTAP que el clúster de SVM de origen para admitir operaciones de conmutación al nodo de respaldo y conmutación de conmutación por error.

"Versiones de ONTAP compatibles para relaciones de SnapMirror"

Cómo se replican las configuraciones de SVM

El contenido de una relación de replicación de SVM se determina por la interacción de los siguientes campos:

- `-identity-preserve true`La opción `snapmirror create` del comando replica toda la configuración de SVM.

  `-identity-preserve false`La opción replica solo los volúmenes y las configuraciones de autenticación y autorización de la SVM, y los ajustes del protocolo y el servicio de nombres que figuran en xref:{relative_path}snapmirror-svm-replication-concept.html#configurations-replicated-in-svm-disaster-recovery-relationships["Configuraciones replicadas en las relaciones de recuperación ante desastres de máquina virtual de almacenamiento"].

- `-discard-configs network`La opción `snapmirror policy create` del comando excluye las LIF y la configuración de red relacionada desde la replicación de SVM, para utilizarlo en casos en los que las SVM de origen y de destino están en subredes diferentes.
- `-vserver-dr-protection unprotected`La opción del `volume modify` comando excluye el volumen especificado de la replicación de SVM.

De lo contrario, la replicación de SVM es casi idéntica a la replicación de volúmenes. Puede utilizar prácticamente el mismo flujo de trabajo para la replicación de SVM que el que utiliza para la replicación de volúmenes.

Detalles de soporte

La siguiente tabla muestra detalles de soporte para la replicación de SVM de SnapMirror.

Recurso o característica	Detalles de soporte
Tipos de implementación	• Origen único en destino único • A partir de ONTAP 9.4, punto de salida. Solo puede fan-out a dos destinos. De forma predeterminada, solo se permite una relación de conservación de identidad real por SVM de origen.

Tipos de relación	• Recuperación ante desastres con SnapMirror • Replicación unificada de SnapMirror
Alcance de replicación	Solo interconexión de clústeres. No puede replicar SVM en el mismo clúster.
Protección autónoma de ransomware	• Compatible a partir de ONTAP 9.12.1. Para obtener más información, consulte "Protección autónoma de ransomware".
Compatibilidad asíncrona de grupos de coherencia	A partir de ONTAP 9.14.1, se admiten un máximo de 32 relaciones de recuperación ante desastres de SVM cuando hay grupos de coherencia. Consulte "Proteja un grupo de consistencia" y "Límites del grupo de consistencia" para obtener más información.
FabricPool	A partir de ONTAP 9,6, la replicación de SVM de SnapMirror es compatible con FabricPool. Cuando están en una relación de recuperación ante desastres de la SVM, los volúmenes de origen y de destino no necesitan usar agregados de FabricPool, pero deben usar la misma política de organización en niveles. A partir de la versión 9.12.1 de ONTAP, la replicación de SVM de SnapMirror es compatible con volúmenes FabricPool y FlexGroup juntos. Antes de la 9.12.1, cualquiera de estas dos funciones funcionaba conjuntamente, pero no las tres a la vez.

MetroCluster	A partir de ONTAP 9.11.1, ambos lados de una relación de recuperación ante desastres de SVM dentro de una configuración de MetroCluster pueden actuar como origen para configuraciones de recuperación ante desastres adicionales de SVM. A partir de ONTAP 9.5, la replicación de SVM de SnapMirror es compatible con las configuraciones de MetroCluster. • En versiones anteriores a ONTAP 9,10.X, una configuración de MetroCluster no puede ser el destino de una relación de recuperación ante desastres de SVM. • En ONTAP 9.10,1 y versiones posteriores, una configuración de MetroCluster puede ser el destino de una relación de recuperación ante desastres de SVM únicamente con fines de migración y debe cumplir todos los requisitos necesarios descritos en "TR-4966: Migración de una SVM a una solución de MetroCluster". • Solo una SVM activa en una configuración de MetroCluster puede ser el origen de una relación de recuperación ante desastres de SVM. Un origen puede ser una SVM sincronizada en origen antes de realizar una conmutación de sitios o una SVM sincronizada en destino después de efectuar una conmutación de sitios. • Cuando una configuración de MetroCluster presenta un estado estable, la SVM sincronizada en destino de MetroCluster no puede ser el origen de una relación de recuperación ante desastres de SVM, ya que los volúmenes no están en línea. • Cuando la SVM sincronizada en origen es el origen de una relación de recuperación ante desastres de SVM, la información sobre la relación de recuperación ante desastres de SVM de origen se replica en el partner de MetroCluster. • Durante los procesos de conmutación de sitios y conmutación de estado, se podría producir un error en la replicación al destino de recuperación ante desastres de SVM. Sin embargo, una vez que finalice el proceso de conmutación de sitios o conmutación de estado, se realizarán las siguientes actualizaciones programadas para la recuperación ante desastres de la máquina virtual de almacenamiento.

Grupo de consistencia	Compatible a partir de ONTAP 9.14.1. Para obtener más información, consulte Proteja un grupo de consistencia.
ONTAP S3	No compatible con la recuperación ante desastres de SVM.
SnapMirror síncrono	No compatible con la recuperación ante desastres de SVM.
Independencia de versiones	No admitido.
Cifrado de volúmenes	• Los volúmenes cifrados en el origen se cifran en el destino. • Los servidores incorporados de Key Manager o KMIP deben configurarse en el destino. • En el destino se generan nuevas claves de cifrado. • Si el destino no contiene un nodo compatible con el cifrado de volúmenes ., la replicación se realiza correctamente, pero los volúmenes de destino no están cifrados.

Configuraciones replicadas en las relaciones de recuperación ante desastres de máquina virtual de almacenamiento

La siguiente tabla muestra la interacción de `snapmirror create -identity-preserve` la opción y la `snapmirror policy create -discard-configs network` opción:

Configuración replicada		`-identity-preserve true`		`-identity-preserve false`
		Política sin `-discard-configs network` set	**Política con `-discard-configs network` set**	
Red	LIF NAS	Sí	No	No
Configuración de Kerberos para LIF	Sí	No	No	LIF SAN
No	No	No	Directivas de firewall	Sí
Sí	No	Normativas de servicio	Sí	Sí
No	Rutas	Sí	No	No

Dominio de retransmisión	No	No	No	Subred
No	No	No	Espacio IP	No
No	No	SMB	Servidor SMB	Sí
Sí	No	Grupos locales y usuario local	Sí	Sí
Sí	Privilegio	Sí	Sí	Sí
Copia oculta	Sí	Sí	Sí	BranchCache
Sí	Sí	Sí	Opciones del servidor	Sí
Sí	Sí	Seguridad del servidor	Sí	Sí
No	Directorio inicial, compartir	Sí	Sí	Sí
Enlace simbólico	Sí	Sí	Sí	Política de Fpolicy, política de FSecurity y NTFS de FSecurity
Sí	Sí	Sí	Asignación de nombres y asignación de grupos	Sí
Sí	Sí	Información de auditoría	Sí	Sí
Sí	NFS	Políticas de exportación	Sí	Sí
No	Reglas de la política de exportación	Sí	Sí	No
Servidor NFS	Sí	Sí	No	RBAC

Certificados de seguridad	Sí	Sí	No	Inicio de sesión de usuario, clave pública, función y configuración de funciones
Sí	Sí	Sí	SSL	Sí
Sí	No	Servicios de nombres	Hosts DNS y DNS	Sí
Sí	No	Usuario UNIX y grupo UNIX	Sí	Sí
Sí	Kerberos Reino y bloques de claves Kerberos	Sí	Sí	No
Cliente LDAP y LDAP	Sí	Sí	No	Grupo de red
Sí	Sí	No	NIS	Sí
Sí	No	Acceso Web y Web	Sí	Sí
No	Volumen	Objeto	Sí	Sí
Sí	Snapshot y política de Snapshot	Sí	Sí	Sí
Política de eliminación automática	No	No	No	Política de eficiencia
Sí	Sí	Sí	Regla de política de cuotas y de política de cuotas	Sí
Sí	Sí	Cola de recuperación	Sí	Sí
Sí	Volumen raíz	Espacio de nombres	Sí	Sí
Sí	Datos de usuarios	No	No	No
Qtrees	No	No	No	Cuotas

No	No	No	Calidad de servicio en el nivel de los archivos	No
No	No	Atributos: estado del volumen raíz, garantía de espacio, tamaño, tamaño automático y número total de archivos	No	No
No	Calidad de servicio del almacenamiento	Grupo de políticas de calidad de servicio	Sí	Sí
Sí	Fibre Channel (FC)	No	No	No
iSCSI	No	No	No	LUN
Objeto	Sí	Sí	Sí	grupos de iniciadores
No	No	No	conjuntos de puertos	No
No	No	Números de serie	No	No
No	SNMP	usuarios v3	Sí	Sí

Límites de almacenamiento para recuperación ante desastres de SVM

En la siguiente tabla se muestra el número máximo recomendado de volúmenes y relaciones de recuperación ante desastres de SVM admitidas por objeto de almacenamiento. Debe ser consciente de que los límites dependen a menudo de la plataforma. Consulte el "Hardware Universe" para conocer los límites de su configuración específica.

Objeto de almacenamiento	Límite
SVM	300 volúmenes flexibles
Pareja de HA	1,000 volúmenes flexibles
Clúster	128 Relaciones de desastre de SVM

Información relacionada

- "snapmirror create"

- "Crear política de SnapMirror"

Replicar las configuraciones de SVM

Flujo de trabajo de replicación de SVM de ONTAP SnapMirror

La replicación SVM de SnapMirror implica la creación de la SVM de destino, la creación de una programación de trabajos de replicación y la creación e inicialización de una relación de SnapMirror.

Debe determinar qué flujo de trabajo de replicación se adapta mejor a sus necesidades:

- "Replique toda una configuración de SVM"
- "Excluya las LIF y la configuración de red relacionada desde la replicación de SVM"
- "Exlude red, servicio de nombres y otros ajustes de la configuración de la máquina virtual de almacenamiento"

Criterios para colocar volúmenes en SVM de destino de ONTAP SnapMirror

Al replicar volúmenes de la SVM de origen a la SVM de destino, es importante conocer los criterios para la selección de agregados.

Los agregados se seleccionan según los siguientes criterios:

- Los volúmenes siempre se colocan en agregados que no son raíz.
- Los agregados no raíz se seleccionan en función del espacio libre disponible y de la cantidad de volúmenes que ya se encuentran alojados en el agregado.

  Los agregados con más espacio libre y menos volúmenes tienen prioridad. Se selecciona el agregado con la prioridad más alta.

- Los volúmenes de origen en agregados de FabricPool se colocan en agregados de FabricPool en el destino con la misma política de organización en niveles.
- Si un volumen de la SVM de origen se encuentra en un agregado de Flash Pool, el volumen se coloca en un agregado de Flash Pool en la SVM de destino, si existe un agregado de este tipo y tiene suficiente espacio libre.
- Si la `-space-guarantee` opción del volumen que se replica se establece en `volume`, solo se tendrán en cuenta los agregados con espacio libre mayor al tamaño del volumen.
- El tamaño del volumen crece automáticamente en la SVM de destino durante la replicación, según el tamaño del volumen de origen.

  Si desea reservar de antemano el tamaño en la SVM de destino, debe cambiar el tamaño del volumen. El tamaño del volumen no se reduce automáticamente en la SVM de destino según la SVM de origen.

Si desea mover un volumen de un agregado a otro, puede usar `volume move` el comando en la SVM de destino.

Replicación de una configuración completa de SVM de ONTAP

Puede crear una relación de recuperación ante desastres (DR de SVM) para replicar una

configuración de SVM a otra. En caso de desastre en el sitio principal, puede activar rápidamente la SVM de destino.

Antes de empezar

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales. Para obtener más información, consulte "Cree una relación de paridad entre clústeres" y "Cree una relación de interconexión de clústeres entre iguales de SVM".

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Acerca de esta tarea

Este flujo de trabajo supone que ya está usando una directiva predeterminada o una directiva de replicación personalizada.

A partir de ONTAP 9,9.1, cuando se utiliza la política de reflejo-almacén, se pueden crear distintas políticas de Snapshot en la SVM de origen y destino, y las snapshots del destino no se sobrescriben en el origen. Para obtener más información, consulte "Replicación de SVM de SnapMirror".

Complete este procedimiento desde el destino. Si necesita crear una nueva política de protección, por ejemplo, cuando su VM de almacenamiento de origen tiene SMB configurado, debe crear la política y usar la opción **Identity preserve**. Para obtener más información, consulte "Cree políticas de protección de datos personalizadas".

Pasos

Puede realizar esta tarea desde System Manager o la CLI de ONTAP.

System Manager

1. En el clúster de destino, haga clic en **Protección > Relaciones**.
2. En **Relaciones**, haz clic en **Proteger** y elige **Storage VMs (DR)**.
3. Seleccione una política de protección. Si creó una política de protección personalizada, selecciónela, elija el clúster de origen y la máquina virtual de almacenamiento que desea replicar. También puede crear una máquina virtual de almacenamiento de destino introduciendo un nuevo nombre de máquina virtual de almacenamiento.
4. Si lo desea, cambie la configuración de destino para sustituir la conservación de identidad e incluir o excluir interfaces y protocolos de red.
5. Haga clic en **Guardar**.

CLI

1. Cree una SVM de destino:

   ```
   vserver create -vserver <SVM_name> -subtype dp-destination
   ```

   El nombre de SVM debe ser único en los clústeres de origen y destino.

   En el ejemplo siguiente se crea una SVM de destino llamada `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-
   destination
   ```

   Obtenga más información sobre `vserver create` en el "Referencia de comandos del ONTAP".

2. Desde el clúster de destino, cree una relación entre iguales de SVM mediante `vserver peer create` el comando.

   Para obtener más información, consulte "Cree una relación de interconexión de clústeres entre iguales de SVM".

   Obtenga más información sobre `vserver peer create` en el "Referencia de comandos del ONTAP".

3. Crear una programación de trabajo de replicación:

   ```
   job schedule cron create -name <job_name> -month <month> -dayofweek
   <day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
   ```

   Para `-month` `-dayofweek` , y `-hour`, puede especificar `all` que se ejecute el trabajo cada mes, día de la semana y hora, respectivamente.

   > La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror de SVM es de 15 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror de SVM es de 30 minutos.

El siguiente ejemplo crea una programación de trabajo llamada `my_weekly` que se ejecuta los sábados a las 3:00 a.m.:

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

Obtenga más información sobre `job schedule cron create` en el "Referencia de comandos del ONTAP".

4. A partir de la SVM de destino o el clúster de destino, cree una relación de replicación:

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y.

En el ejemplo siguiente se crea una relación de recuperación ante desastres de SnapMirror con la `MirrorAllSnapshots` política predeterminada:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

En el siguiente ejemplo, se crea una relación de replicación unificada mediante la `MirrorAndVault` política predeterminada:

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

Suponiendo que ha creado una política personalizada con el tipo de política `async-mirror` , en el siguiente ejemplo se crea una relación de DR de SnapMirror:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

Suponiendo que ha creado una política personalizada con el tipo de política `mirror-vault` , en el siguiente ejemplo se crea una relación de replicación unificada:

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

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

5. Detenga la SVM de destino:

```
vserver stop -vserver <SVM_name>
```

En el ejemplo siguiente se detiene una SVM de destino llamada svm_backup:

```
cluster_dst::> vserver stop -vserver svm_backup
```

Obtenga más información sobre `vserver stop` en el "Referencia de comandos del ONTAP".

6. En la SVM de destino o el clúster de destino, inicialice la relación de replicación de SVM:

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y.

En el ejemplo siguiente, se inicializa la relación entre la SVM de origen y `svm1` la SVM de destino, `svm_backup`:

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

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

Excluya las LIF y la configuración de red relacionada de la replicación de SVM de ONTAP SnapMirror

Si las SVM de origen y de destino están en subredes diferentes, puede usar `-discard -configs network` la opción `snapmirror policy create` del comando para excluir las LIF y la configuración de red relacionada de la replicación de la SVM.

Antes de empezar

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

Para obtener más información, consulte "Cree una relación de paridad entre clústeres" y "Cree una relación de interconexión de clústeres entre iguales de SVM".

Acerca de esta tarea

```
`-identity-preserve`La opción `snapmirror create` del comando debe
establecerse en `true` cuando crea la relación de replicación de SVM.
```

Pasos

1. Cree una SVM de destino:

   `vserver create -vserver SVM -subtype dp-destination`

   El nombre de SVM debe ser único en los clústeres de origen y destino.

   En el ejemplo siguiente se crea una SVM de destino llamada `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Desde el clúster de destino, cree una relación entre iguales de SVM mediante `vserver peer create` el comando.

   Para obtener más información, consulte "Cree una relación de interconexión de clústeres entre iguales de SVM".

   Obtenga más información sobre `vserver peer create` en el "Referencia de comandos del ONTAP".

3. Crear un programa de trabajo:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para `-month` `-dayofweek` , y `-hour`, puede especificar `all` que se ejecute el trabajo cada mes, día de la semana y hora, respectivamente.

   > La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror de SVM es de 15 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror de SVM es de 30 minutos.

   El siguiente ejemplo crea una programación de trabajo llamada `my_weekly` que se ejecuta los sábados a las 3:00 a.m.:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Cree una política de replicación personalizada:

   `snapmirror policy create -vserver SVM -policy policy -type async-`

`mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer -priority low|normal -is-network-compression-enabled true|false -discard -configs network`

En el ejemplo siguiente se crea una normativa de replicación personalizada para recuperación ante desastres de SnapMirror que excluye las LIF:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_exclude_LIFs -type async-mirror -discard-configs network
```

En el ejemplo siguiente se crea una directiva de replicación personalizada para la replicación unificada que excluye las LIF:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

> Considere la posibilidad de crear la misma política de SnapMirror personalizada en el clúster de origen para futuras situaciones de conmutación por error y conmutación de retorno tras recuperación.

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

5. A partir de la SVM de destino o el clúster de destino, ejecute el siguiente comando para crear una relación de replicación:

`snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP -schedule schedule -policy policy -identity-preserve true|false -discard -configs true|false`

> Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path -destination-path` opciones y. Vea los ejemplos a continuación.

En el ejemplo siguiente se crea una relación de recuperación ante desastres de SnapMirror que excluye las LIF:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
-identity-preserve true
```

En el ejemplo siguiente se crea una relación de replicación unificada de SnapMirror que excluye las LIF:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
-identity-preserve true -discard-configs true
```

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

6. Detenga la SVM de destino:

   `vserver stop`

   `SVM name`

   En el ejemplo siguiente se detiene la SVM de destino llamada svm_backup:

   ```
   cluster_dst::> vserver stop -vserver svm_backup
   ```

7. En la SVM de destino o el clúster de destino, inicialice una relación de replicación:

   `snapmirror initialize -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   En el siguiente ejemplo se inicializa la relación entre el origen `svm1` y el destino `svm_backup`:

   ```
   cluster_dst::> snapmirror initialize -source-path svm1: -destination
   -path svm_backup:
   ```

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

Después de terminar

Es necesario configurar la red y los protocolos en la SVM de destino para acceder a los datos en caso de que se produzca un desastre.

Información relacionada

- "snapmirror create"
- "inicializar snapmirror"
- "Crear política de SnapMirror"

Excluya la red, el servicio de nombres y otras configuraciones de la replicación de SVM con ONTAP

Tal vez desee excluir la red, el servicio de nombres y otras configuraciones de una relación de replicación de SVM para evitar conflictos o diferencias de configuración con la SVM de destino.

Puede usar `-identity-preserve false` la opción `snapmirror create` del comando para replicar solo los volúmenes y las configuraciones de seguridad de una SVM. También se conservan algunos ajustes de protocolo y servicio de nombres.

Acerca de esta tarea

Para obtener una lista de los valores de protocolo y servicio de nombres conservados, consulte "Configuraciones replicadas en relaciones de recuperación ante desastres de SVM".

Antes de empezar

Las SVM y los clústeres de origen y destino deben tener una relación entre iguales.

Para obtener más información, consulte "Cree una relación de paridad entre clústeres" y "Cree una relación de interconexión de clústeres entre iguales de SVM".

Pasos

1. Cree una SVM de destino:

   `vserver create -vserver SVM -subtype dp-destination`

   El nombre de SVM debe ser único en los clústeres de origen y destino.

   En el ejemplo siguiente se crea una SVM de destino llamada `svm_backup`:

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. Desde el clúster de destino, cree una relación entre iguales de SVM mediante `vserver peer create` el comando.

   Para obtener más información, consulte "Cree una relación de interconexión de clústeres entre iguales de SVM".

   Obtenga más información sobre `vserver peer create` en el "Referencia de comandos del ONTAP".

3. Crear una programación de trabajo de replicación:

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   Para `-month` `-dayofweek` , y `-hour`, puede especificar `all` que se ejecute el trabajo cada mes, día de la semana y hora, respectivamente.

   > La programación mínima admitida (RPO) para volúmenes FlexVol en una relación de SnapMirror de SVM es de 15 minutos. La programación mínima admitida (RPO) para volúmenes FlexGroup en una relación de SnapMirror de SVM es de 30 minutos.

   El siguiente ejemplo crea una programación de trabajo llamada `my_weekly` que se ejecuta los sábados a las 3:00 a.m.:

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. Cree una relación de replicación que excluya la red, el servicio de nombres y otras opciones de configuración:

   `snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP -schedule schedule -policy policy -identity-preserve false`

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea los ejemplos a continuación. Se debe ejecutar este comando desde la SVM de destino o el clúster de destino.

En el siguiente ejemplo se crea una relación de recuperación ante desastres de SnapMirror con la `MirrorAllSnapshots` política predeterminada. La relación excluye la red, el servicio de nombres y otras opciones de configuración de la replicación de SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
-identity-preserve false
```

En el siguiente ejemplo, se crea una relación de replicación unificada mediante la `MirrorAndVault` política predeterminada. La relación excluye la red, el servicio de nombres y otras opciones de configuración:

```
cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
-type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
false
```

Suponiendo que ha creado una política personalizada con el tipo de política `async-mirror` , en el siguiente ejemplo se crea una relación de DR de SnapMirror. La relación excluye la red, el servicio de nombres y otras opciones de configuración de la replicación de SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

Suponiendo que ha creado una política personalizada con el tipo de política `mirror-vault` , en el siguiente ejemplo se crea una relación de replicación unificada. La relación excluye la red, el servicio de nombres y otras opciones de configuración de la replicación de SVM:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

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

5. Detenga la SVM de destino:

   `vserver stop`

   `SVM name`

   En el ejemplo siguiente se detiene una SVM de destino denominada dvs1:

```
destination_cluster::> vserver stop -vserver dvs1
```

6. Si utiliza SMB, también debe configurar un servidor SMB.

   Consulte "Solo SMB: Crear un servidor SMB".

7. En la SVM de destino o el clúster de destino, inicialice la relación de replicación de SVM:

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

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

Después de terminar

Es necesario configurar la red y los protocolos en la SVM de destino para acceder a los datos en caso de que se produzca un desastre.

Especifique los niveles locales que se van a utilizar para las relaciones de recuperación ante desastres de SVM de ONTAP SnapMirror

Después de crear una SVM de recuperación ante desastres, puede usar la `aggr-list` opción con el comando `vserver modify` para limitar qué niveles locales se usan para alojar volúmenes de destino de DR de SVM.

Pasos

1. Cree una SVM de destino:

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

2. Modifique la lista de agregados de la SVM de recuperación ante desastres para limitar los niveles locales que se utilizan para alojar el volumen de la SVM de recuperación ante desastres:

   `cluster_dest::> vserver modify -vserver` *`SVM`* `-aggr-list <comma-separated-list>`

Cree un servidor SMB para una SVM de destino de ONTAP SnapMirror en una relación de recuperación ante desastres

Si la SVM de origen tiene una configuración de SMB y decide establecerse `identity-preserve` en `false`, debe crear un servidor SMB para la SVM de destino. Se necesita un servidor SMB para algunas configuraciones SMB, como los recursos compartidos durante la inicialización de la relación de SnapMirror.

Pasos

1. Inicie la SVM de destino con `vserver start` el comando.

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

Obtenga más información sobre `vserver start` en el "Referencia de comandos del ONTAP".

2. Compruebe que la SVM de destino está en `running` estado y que el subtipo lo está `dp-destination` mediante `vserver show` el comando.

```
destination_cluster::> vserver show
                                  Admin      Operational Root
Vserver  Type    Subtype          State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

Obtenga más información sobre `vserver show` en el "Referencia de comandos del ONTAP".

3. Cree una LIF mediante `network interface create` el comando.

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

Obtenga más información sobre `network interface create` en el "Referencia de comandos del ONTAP".

4. Cree una ruta mediante el `network route create` comando.

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"Gestión de redes"

Obtenga más información sobre `network route create` en el "Referencia de comandos del ONTAP".

5. Configure DNS mediante `vserver services dns create` el comando.

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

Obtenga más información sobre `vserver services dns create` en el "Referencia de comandos del ONTAP".

6. Añada la controladora de dominio preferida mediante `vserver cifs domain preferred-dc add` el

comando.

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

Obtenga más información sobre `vserver cifs domain preferred-dc add` en el "Referencia de comandos del ONTAP".

7. Cree el servidor SMB mediante `vserver cifs create` el comando.

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

Obtenga más información sobre `vserver cifs create` en el "Referencia de comandos del ONTAP".

8. Detenga la SVM de destino mediante `vserver stop` el comando.

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

Obtenga más información sobre `vserver stop` en el "Referencia de comandos del ONTAP".

Excluye los volúmenes de una relación de recuperación ante desastres de SVM de ONTAP SnapMirror

De forma predeterminada, se replican todos los volúmenes de datos RW de la SVM de origen. Si no desea proteger todos los volúmenes en la SVM de origen, puede usar `-vserver-dr-protection unprotected` la opción `volume modify` del comando para excluir volúmenes de la replicación de SVM.

Pasos

1. Excluya un volumen de la replicación SVM:

   `volume modify -vserver` *`SVM`* `-volume` *`volume`* `-vserver-dr-protection unprotected`

   Obtenga más información sobre `volume modify` en el "Referencia de comandos del ONTAP".

   En el ejemplo siguiente se excluye el volumen `volA_src` de la replicación de la máquina virtual de almacenamiento:

```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection unprotected
```

Si más adelante desea incluir un volumen en la replicación de SVM que originalmente excluyó, ejecute el siguiente comando:

`volume modify -vserver *SVM* -volume *volume* -vserver-dr-protection protected`

En el ejemplo siguiente se incluye el volumen `volA_src` en la replicación de SVM:

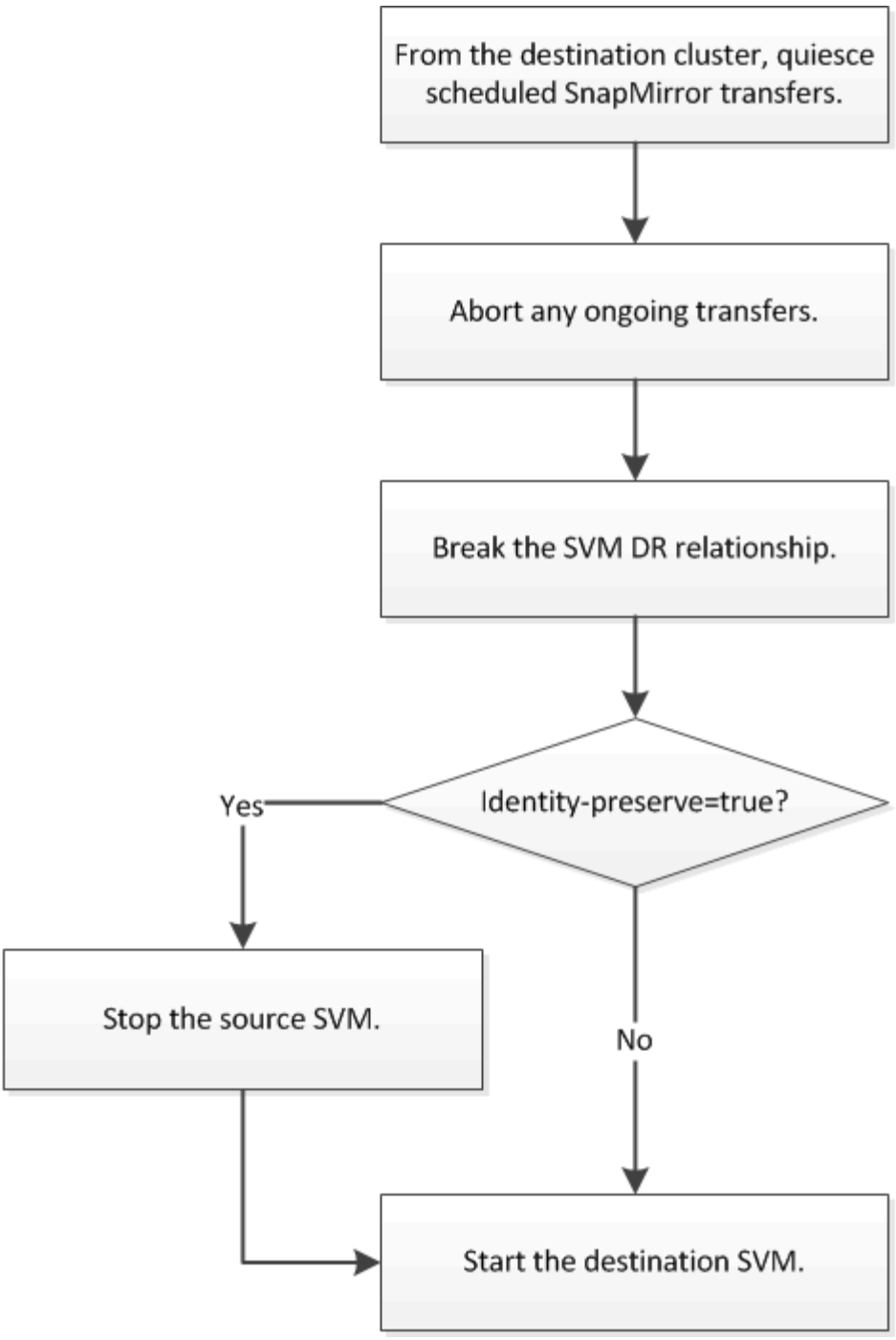
```
cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
-protection protected
```

2. Crear e inicializar la relación de replicación de SVM tal y como se describe en "Replicar una configuración de SVM completa".

Sirva datos desde un destino de recuperación ante desastres de SVM de SnapMirror

Flujo de trabajo de recuperación ante desastres de SVM de ONTAP SnapMirror

Para la recuperación ante desastres y proporcionar datos desde la SVM de destino, debe activar la SVM de destino. La activación de la SVM de destino implica la detención de transferencias programadas de SnapMirror, la anulación de las transferencias continuas de SnapMirror, la ruptura de la relación de replicación, la detención de la SVM de origen y la inicio de la SVM de destino.



Configure el volumen de destino de la máquina virtual de almacenamiento ONTAP SnapMirror como modificable

Debe hacer que los volúmenes de destino de SVM sean editables antes de proporcionar datos a los clientes.

El procedimiento es en gran medida idéntico al procedimiento de replicación de volúmenes, con una excepción. Si estableció `-identity-preserve true` cuando creó la relación de replicación de SVM, debe detener la SVM de origen antes de activar la SVM de destino.

Acerca de esta tarea

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de

comandos del ONTAP".

> En una situación de recuperación ante desastres, no puede realizar una actualización de SnapMirror del SVM de origen a la SVM de destino de recuperación ante desastres porque no podrá acceder a la SVM de origen y a sus datos, así como porque las actualizaciones desde la última resincronización pueden estar dañadas o estar dañadas.

A partir de ONTAP 9.8, es posible utilizar System Manager para activar una máquina virtual de almacenamiento de destino después de un desastre. Si activa la máquina virtual de almacenamiento de destino, es posible escribir en los volúmenes de destino de SVM y proporcionar datos a los clientes.

Pasos

Puede realizar esta tarea desde System Manager o la CLI de ONTAP.

System Manager

1. Si se puede acceder al clúster de origen, compruebe que la SVM está detenida: Vaya a **almacenamiento > Storage VMs** y compruebe la columna **Estado** de la SVM.
2. Si el estado de la SVM de origen es “En ejecución”, deténgalo: Seleccione ⋮ y elija **Detener**.
3. En el clúster de destino, localice la relación de protección deseada: Vaya a **Protección > Relaciones**.
4. Pase el ratón sobre el nombre de la VM de almacenamiento de origen deseado, haga clic en ⋮ y seleccione **Activar la VM de almacenamiento de destino**.
5. En la ventana **Activar VM de almacenamiento de destino**, seleccione **Activar la VM de almacenamiento de destino y romper la relación**.
6. Haga clic en **Activar**.

CLI

1. Desde la SVM de destino o el clúster de destino, inactive la SVM para detener las transferencias programadas al destino:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

ⓘ Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

En el siguiente ejemplo, se detienen las transferencias programadas entre la SVM de origen `svm1` y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

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

2. Desde la SVM de destino o el clúster de destino, detenga las transferencias continuas al destino:

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```

ⓘ Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

El ejemplo siguiente detiene las transferencias continuas entre la SVM de origen `svm1` y la SVM de destino `svm_backup`:

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

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

3. Desde la SVM de destino o el clúster de destino, rompa la relación de replicación:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

En el siguiente ejemplo, se interrumpe la relación entre la SVM de origen `svm1` y la de destino `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

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

4. Si establece `-identity-preserve true` cuando creó la relación de replicación de SVM, detenga la SVM de origen:

```
vserver stop -vserver <SVM>
```

En el siguiente ejemplo se detiene la SVM de origen `svm1`:

```
cluster_src::> vserver stop svm1
```

5. Inicie la SVM de destino:

```
vserver start -vserver <SVM>
```

En el ejemplo siguiente, se inicia la SVM de destino `svm_backup` :

```
cluster_dst::> vserver start svm_backup
```

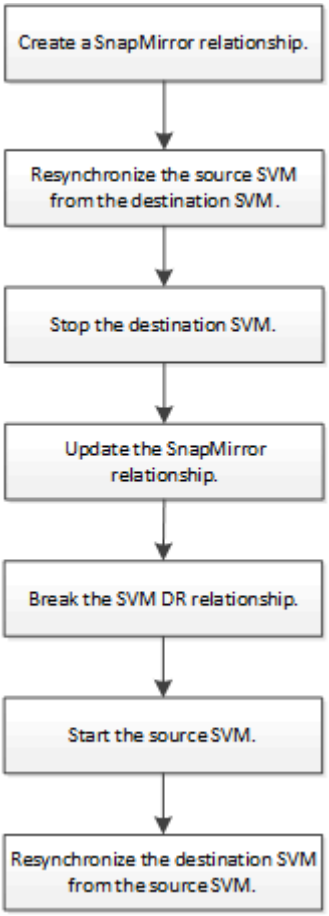
Después de terminar

Configure los volúmenes de destino de SVM para el acceso a los datos, como se describe en "Configurar el volumen de destino para acceder a los datos".

Vuelva a activar la SVM de origen de SnapMirror

Flujo de trabajo de reactivación de SVM de origen de ONTAP SnapMirror

Si la SVM de origen existe después de un desastre, puede reactivarlo y protegerlo; para ello, vuelva a crear la relación de recuperación ante desastres de SVM.



Vuelva a activar la SVM de origen de ONTAP SnapMirror original

Puede restablecer la relación original de protección de datos entre la SVM de origen y la de destino cuando ya no necesite servir datos desde el destino. El procedimiento es en gran medida idéntico al procedimiento de replicación de volúmenes, con una excepción. Debe detener la SVM de destino antes de volver a activar la SVM de origen.

Antes de empezar

- Si ha aumentado el tamaño del volumen de destino mientras se sirven los datos, antes de reactivar el volumen de origen, debería aumentar manualmente el tamaño máximo automático en el volumen de origen original para garantizar que pueda crecer lo suficiente.

"Cuando un volumen de destino aumenta automáticamente"

> El administrador del clúster debe pausar las escrituras del cliente antes de reactivar el SVM de origen original para evitar la pérdida de datos.

Acerca de esta tarea

A partir de ONTAP 9.11,1, puede reducir el tiempo de resincronización durante un ensayo de recuperación ante desastres utilizando `-quick-resync true`la opción CLI `snapmirror resync`del comando y realizando una resincronización inversa de una relación de recuperación ante desastres de SVM. Una resincronización rápida puede reducir el tiempo que lleva volver a la producción evitando las operaciones de reconstrucción y restauración del almacén de datos. Obtenga más información sobre `snapmirror resync` en el "Referencia de comandos del ONTAP".

> Una resincronización rápida no conserva la eficiencia del almacenamiento de los volúmenes de destino. Al habilitar una resincronización rápida, puede aumentar el espacio de volumen utilizado por los volúmenes de destino.

En este procedimiento se asume que la línea base del volumen de origen original está intacta. Si la base de referencia no está intacta, debe crear e inicializar la relación entre el volumen desde el que se sirven datos y el volumen de origen original antes de realizar el procedimiento.

A partir de ONTAP 9.8, puede usar el Administrador del sistema para reactivar una máquina virtual de almacenamiento de origen después de un desastre.

Pasos

Puede realizar esta tarea mediante el Administrador del sistema o la CLI de ONTAP .

Administrador del sistema ONTAP 9.17.1 y posteriores

1. En el clúster de destino, seleccione la relación de protección deseada: haga clic en **Protección > Replicación**.
2. Coloque el cursor sobre el nombre de la fuente y haga clic y haga clic en **Resincronización inversa**.
3. En la ventana **Relación de resincronización inversa**, haz clic en **Resincronización inversa**.

   La relación desaparece de la tabla **Replicación** y ahora la administra el clúster de origen original.
4. En el clúster de origen original, haga clic en **Protección > Replicación** y verifique que la resincronización inversa esté completa verificando que el estado muestre **Reflejado**.
5. En el clúster de destino original, navegue a **Clúster > Máquinas virtuales de almacenamiento**.
6. Ubique la máquina virtual de almacenamiento, coloque el cursor sobre el nombre de la máquina virtual de almacenamiento y haga clic en y haga clic en **Detener**.
7. En la ventana **Detener máquina virtual de almacenamiento**, haga clic en **Detener**.
8. En el clúster de origen, navegue a **Protección > Replicación** y localice la máquina virtual de almacenamiento que desea reactivar, coloque el cursor sobre el nombre de la máquina virtual de almacenamiento y haga clic y haga clic en **Activar máquina virtual de almacenamiento de destino**.
9. En la ventana **Activar VM de almacenamiento de destino**, seleccione **Activar la VM de almacenamiento de destino y romper la relación** y haga clic en **Activar**.
10. Cuando regrese a la página **Replicación**, vuelva a colocar el cursor sobre el nombre de la máquina virtual de almacenamiento y haga clic en y haga clic en **Resincronización inversa**.

Administrador del sistema ONTAP 9.16.1 y anteriores

1. En el clúster de destino, seleccione la relación de protección deseada: haga clic en **Protección > Relaciones**.
2. Coloque el cursor sobre el nombre de la fuente y haga clic y haga clic en **Resincronización inversa**.
3. En la ventana **Relación de resincronización inversa**, haz clic en **Resincronización inversa**.

   La relación desaparece de la tabla **Relaciones** porque ahora la administra el clúster de origen original.
4. En el clúster de origen original, haga clic en **Protección > Relaciones** y verifique que la resincronización inversa esté completa verificando que el estado se muestre como **Reflejado**.
5. En el clúster de destino original, navegue a **Almacenamiento > Máquinas virtuales de almacenamiento**.
6. Ubique la máquina virtual de almacenamiento, coloque el cursor sobre el nombre de la máquina virtual de almacenamiento y haga clic en y haga clic en **Detener**.
7. En la ventana **Detener máquina virtual de almacenamiento**, haga clic en **Detener**.
8. En el clúster de origen, ubique la VM de almacenamiento (que ahora es la SVM de origen de la relación invertida), coloque el cursor sobre el nombre de la SVM y haga clic y haga clic en **Activar máquina virtual de almacenamiento de destino**.
9. En la ventana **Activar VM de almacenamiento de destino**, seleccione **Activar la VM de almacenamiento de destino y romper la relación** y haga clic en **Activar**.

10. Cuando regrese a la página **Relaciones**, vuelva a colocar el cursor sobre el nombre de la máquina virtual de almacenamiento y haga clic en ⋮ y haga clic en **Resincronización inversa**.

CLI

1. A partir de la SVM de origen original o del clúster de origen original, cree una relación de recuperación ante desastres de SVM inversa con la misma configuración, política y conservación de identidad que la relación de recuperación ante desastres de SVM original:

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```

ⓘ Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path -destination-path` opciones y. Vea el ejemplo siguiente.

En el ejemplo siguiente se crea una relación entre la SVM desde la que se están sirviendo datos, `svm_backup`, y la SVM de origen original, `svm1`:

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

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

2. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para invertir la relación de protección de datos:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

ⓘ Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path -destination-path` opciones y. Vea el ejemplo siguiente.

Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

ⓘ El comando genera un error si no existe una snapshot común en el origen y el destino. Se utiliza `snapmirror initialize` para reinicializar la relación.

En el siguiente ejemplo se revierte la relación entre la SVM de origen original `svm1` y la SVM desde la que sirve datos, `svm_backup`:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

Ejemplo con la opción -Quick-resync:

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. Cuando esté listo para restablecer el acceso a los datos a la SVM de origen original, detenga la SVM de destino original para desconectar los clientes que actualmente estén conectados a la SVM de destino original.

```
vserver stop -vserver <SVM>
```

En el ejemplo siguiente se detiene la SVM de destino original, que actualmente proporciona datos:

```
cluster_dst::> vserver stop svm_backup
```

4. Compruebe que la SVM de destino original esté en estado Detenido mediante `vserver show` el comando.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

5. A partir de la SVM de origen original o del clúster de origen original, ejecute el siguiente comando para realizar la actualización final de la relación inversa para transferir todos los cambios de la SVM de destino original a la SVM de origen original:

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

En el ejemplo siguiente se actualiza la relación entre la SVM de destino original desde la cual se están sirviendo datos,`svm_backup`, y la SVM de origen original, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

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

6. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para detener las transferencias programadas para la relación inversa:

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

En el ejemplo siguiente se detienen las transferencias programadas entre la SVM desde la que está sirviendo datos, `svm_backup` y la SVM original, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. Cuando la actualización final se completa y la relación indica "Quiesced" para el estado de la relación, ejecute el siguiente comando desde la SVM de origen original o el clúster de origen original para romper la relación inversa:

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

En el siguiente ejemplo, se interrumpe la relación entre la SVM de destino original desde la que se estaban sirviendo datos, `svm_backup`, y la SVM de origen original, `svm1`:

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

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

8. Si la SVM de origen se había detenido anteriormente, desde el clúster de origen original, inicie la SVM de origen original:

```
vserver start -vserver <SVM>
```

En el ejemplo siguiente se inicia la SVM de origen original:

```
cluster_src::> vserver start svm1
```

9. A partir de la SVM de destino original o del clúster de destino original, restablezca la relación de protección de datos original:

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path -destination-path` opciones y. Vea el ejemplo siguiente.

En el ejemplo siguiente se restablece la relación entre la SVM de origen original `svm1` y la SVM de destino original, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para eliminar la relación de protección de datos inversa:

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path -destination-path` opciones y. Vea el ejemplo siguiente.

En el ejemplo siguiente se elimina la relación inversa entre la SVM de destino original `svm_backup` y la SVM de origen original, `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. Desde la SVM de destino original o el clúster de destino original, libere la relación de protección de datos inversa:

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path -destination-path` opciones y. Vea el ejemplo siguiente.

En el siguiente ejemplo se libera la relación inversa entre la SVM de destino original, svm_backup y la SVM de origen, `svm1`

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

El futuro

- Utilice `snapmirror show` el comando para verificar que la relación de SnapMirror se ha creado.

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

- Reanude las operaciones de escritura desde su cliente al SVM de origen original.

Información relacionada

- "snapmirror create"
- "snapmirror elimina"
- "inicializar snapmirror"
- "Snapmirror en reposo"
- "versión de snapmirror"
- "resincronización de SnapMirror"

Vuelva a activar la SVM de origen de ONTAP SnapMirror original para volúmenes FlexGroup

Puede restablecer la relación original de protección de datos entre la SVM de origen y la de destino cuando ya no necesite servir datos desde el destino. Para reactivar la SVM de origen original cuando usa volúmenes de FlexGroup, debe realizar algunos pasos adicionales, como la eliminación de la relación de recuperación ante desastres de SVM original y la liberación de la relación original antes de revertir la relación. También debe liberar la relación inversa y volver a crear la relación original antes de detener las transferencias programadas.

Pasos

1. De la SVM de destino original o del clúster de destino original, elimine la relación de recuperación ante desastres de SVM original:

   ```
   snapmirror delete -source-path SVM: -destination-path SVM:
   ```

   Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

   En el ejemplo siguiente se elimina la relación original entre la SVM de origen, la svm1 y la SVM de destino original, `svm_backup`:

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. Desde la SVM de origen original o del clúster de origen, libere la relación original manteniendo las snapshots intactas:

   ```
   snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
   -only true
   ```

Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path -destination-path` opciones y. Vea el ejemplo siguiente.

En el siguiente ejemplo se libera la relación original entre la SVM de origen, la svm1 y la de destino original, `svm_backup`.

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup: -relationship-info-only true
```

3. A partir de la SVM de origen original o del clúster de origen original, cree una relación de recuperación ante desastres de SVM inversa con la misma configuración, política y conservación de identidad que la relación de recuperación ante desastres de SVM original:

   `snapmirror create -source-path SVM: -destination-path SVM:`

   Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path -destination-path` opciones y. Vea el ejemplo siguiente.

   En el ejemplo siguiente se crea una relación entre la SVM desde la que se están sirviendo datos, `svm_backup`, y la SVM de origen original, `svm1`:

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

4. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para invertir la relación de protección de datos:

   `snapmirror resync -source-path` *`SVM`*`: -destination-path` *`SVM`*`:`

   Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path -destination-path` opciones y. Vea el ejemplo siguiente.

   Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

   El comando genera un error si no existe una snapshot común en el origen y el destino. Se utiliza `snapmirror initialize` para reinicializar la relación.

   En el siguiente ejemplo se revierte la relación entre la SVM de origen original `svm1` y la SVM desde la que sirve datos, `svm_backup`:

   ```
   cluster_src::> snapmirror resync -source-path svm_backup: -destination
   -path svm1:
   ```

5. Cuando esté listo para restablecer el acceso a los datos a la SVM de origen original, detenga la SVM de

destino original para desconectar los clientes que actualmente estén conectados a la SVM de destino original.

`vserver stop -vserver SVM`

En el ejemplo siguiente se detiene la SVM de destino original, que actualmente proporciona datos:

```
cluster_dst::> vserver stop svm_backup
```

6. Compruebe que la SVM de destino original esté en estado Detenido mediante `vserver show` el comando.

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

7. A partir de la SVM de origen original o del clúster de origen original, ejecute el siguiente comando para realizar la actualización final de la relación inversa para transferir todos los cambios de la SVM de destino original a la SVM de origen original:

`snapmirror update -source-path SVM: -destination-path SVM:`

> Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

En el ejemplo siguiente se actualiza la relación entre la SVM de destino original desde la cual se están sirviendo datos,`svm_backup`, y la SVM de origen original, `svm1`:

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

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

8. Desde la SVM de origen original o el clúster de origen original, ejecute el siguiente comando para detener las transferencias programadas para la relación inversa:

`snapmirror quiesce -source-path SVM: -destination-path SVM:`

> Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

En el ejemplo siguiente se detienen las transferencias programadas entre la SVM desde la que está sirviendo datos, `svm_backup` y la SVM original, `svm1`:

```
cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
-path svm1:
```

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

9. Cuando la actualización final se completa y la relación indica "Quiesced" para el estado de la relación, ejecute el siguiente comando desde la SVM de origen original o el clúster de origen original para romper la relación inversa:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

   En el siguiente ejemplo, se interrumpe la relación entre la SVM de destino original desde la que se estaban sirviendo datos, `svm_backup`, y la SVM de origen original, `svm1`:

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

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

10. Si la SVM de origen se había detenido anteriormente, desde el clúster de origen original, inicie la SVM de origen original:

    `vserver start -vserver SVM`

    En el ejemplo siguiente se inicia la SVM de origen original:

    ```
    cluster_src::> vserver start svm1
    ```

11. En la SVM de origen original o en el clúster de origen, elimine la relación de recuperación ante desastres de SVM inversa:

    `snapmirror delete -source-path SVM: -destination-path SVM:`

    Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

    En el ejemplo siguiente se elimina la relación inversa entre la SVM de destino original, svm_backup y la SVM de origen original `svm1`:

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. Desde la SVM de destino original o el clúster de destino original, libere la relación inversa manteniendo las copias Snapshot intactas:

    `snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

    Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

    En el siguiente ejemplo, se libera la relación inversa entre la SVM de destino original, svm_backup y la SVM de origen original, svm1:

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

13. Desde la SVM de destino original o el clúster de destino original, vuelva a crear la relación original. Utilice la misma configuración, política y conservación de identidad que la relación de recuperación ante desastres original de la SVM:

    `snapmirror create -source-path SVM: -destination-path SVM:`

    Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

    En el ejemplo siguiente se crea una relación entre la SVM de origen original `svm1` y la SVM de destino original, `svm_backup`:

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup:
```

14. A partir de la SVM de destino original o del clúster de destino original, restablezca la relación de protección de datos original:

    `snapmirror resync -source-path SVM: -destination-path SVM:`

    Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

    En el ejemplo siguiente se restablece la relación entre la SVM de origen original `svm1` y la SVM de destino original, `svm_backup`:

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Información relacionada

- "snapmirror create"
- "snapmirror elimina"
- "inicializar snapmirror"
- "Snapmirror en reposo"
- "versión de snapmirror"
- "resincronización de SnapMirror"

Vuelva a sincronizar los datos en una SVM de destino de ONTAP SnapMirror

ONTAP 9.11.1 introduce una opción para omitir una reconstrucción completa del almacén de datos al realizar un ensayo de recuperación ante desastres, lo que permite volver a la producción más rápido.

A partir de ONTAP 9.8, es posible usar System Manager para volver a sincronizar los datos y los detalles de configuración de la máquina virtual de almacenamiento de origen con la máquina virtual de almacenamiento de destino en una relación de protección romada y restablecer la relación.

La operación de resincronización solo se realiza desde el destino de la relación original. La resincronización elimina los datos del equipo virtual de almacenamiento de destino que son más nuevos que los de la máquina virtual de almacenamiento de origen.

Pasos

Puede usar System Manager o la interfaz de línea de comandos de ONTAP para ejecutar esta tarea.

System Manager

1. En el destino, seleccione la relación de protección deseada: Haga clic en **Protección > Relaciones**.
2. Opcionalmente, seleccione **realizar una resincronización rápida** para omitir una reconstrucción completa del almacén de datos durante un ensayo de recuperación ante desastres.
3. Haga ⋮ clic y haga clic en **Resincronizar**.
4. En **Relaciones**, supervise el progreso de la resincronización visualizando **Estado de transferencia** para la relación.

CLI

1. En el clúster de destino, vuelva a sincronizar la relación:

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

Información relacionada

- "resincronización de SnapMirror"

Convertir una relación de recuperación ante desastres de volúmenes de ONTAP SnapMirror en una relación de recuperación ante desastres de Storage Virtual Machine

Puede convertir relaciones de replicación entre volúmenes en una relación de replicación entre las máquinas virtuales de almacenamiento (SVM) a las que pertenecen los volúmenes, siempre que se replique cada volumen del origen (excepto el volumen raíz), y cada volumen del origen (incluido el volumen raíz) tiene el mismo nombre que el volumen en el destino.

Acerca de esta tarea

Use `volume rename` el comando cuando la relación de SnapMirror esté inactiva para cambiar el nombre de los volúmenes de destino si es necesario. Obtenga más información sobre `volume rename` en el "Referencia de comandos del ONTAP".

Pasos

1. Desde la SVM de destino o el clúster de destino, ejecute el siguiente comando para volver a sincronizar los volúmenes de origen y destino:

   ```
   snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
   -type DP|XDP -policy <policy>
   ```

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

   > Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

   En el siguiente ejemplo, se vuelve a sincronizar la relación entre el volumen `volA` `svm1` de origen en y el de destino `volA` en `svm_backup`:

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA
   ```

2. Cree una relación de replicación SVM entre las SVM de origen y de destino, tal y como se describe en "Replicando configuraciones de SVM".

   Debe usar `-identity-preserve true` la opción `snapmirror create` del comando cuando cree la relación de replicación.

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

3. Detenga la SVM de destino:

   ```
   vserver stop -vserver SVM
   ```

   Obtenga más información sobre `vserver stop` en el "Referencia de comandos del ONTAP".

En el ejemplo siguiente se detiene la SVM de destino `svm_backup`:

```
cluster_dst::> vserver stop svm_backup
```

4. Desde la SVM de destino o el clúster de destino, ejecute el siguiente comando para volver a sincronizar las SVM de origen y destino:

   `snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP -policy <policy>`

   > Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.
   >
   > Aunque la resincronización no requiere una transferencia básica, puede requerir mucho tiempo. Puede que desee ejecutar la resincronización en horas de menor actividad.

   En el siguiente ejemplo se vuelve a sincronizar la relación entre la SVM de origen `svm1` y la SVM de destino `svm_backup` :

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

Información relacionada

- "snapmirror create"
- "resincronización de SnapMirror"

Elimine una relación de replicación de SVM de ONTAP SnapMirror

Puede usar `snapmirror delete` `snapmirror release` los comandos y para eliminar una relación de replicación de SVM. A continuación, puede eliminar manualmente los volúmenes de destino innecesarios. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Acerca de esta tarea

El `snapmirror release` comando elimina todas las copias Snapshot creadas por una SnapMirror del origen. Puede usar `-relationship-info-only` la opción para preservar las snapshots.

Pasos

1. Ejecute el siguiente comando desde la SVM de destino o el clúster de destino para romper la relación de replicación:

   `snapmirror break -source-path SVM: -destination-path SVM:`

   > Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

En el siguiente ejemplo, se interrumpe la relación entre la SVM de origen `svm1` y la de destino `svm_backup`:

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

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

2. Ejecute el siguiente comando desde la SVM de destino o el clúster de destino para eliminar la relación de replicación:

   `snapmirror delete -source-path` *SVM*`: -destination-path` *SVM*`:`

   > Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

   En el ejemplo siguiente se elimina la relación entre la SVM de origen `svm1` y la SVM de destino `svm_backup` :

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

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

3. Ejecute el siguiente comando desde la SVM de origen o el clúster de origen para liberar la información de relaciones de replicación desde la SVM de origen:

   `snapmirror release -source-path` *SVM*`: -destination-path` *SVM*`:`

   > Debe introducir dos puntos (:) después del nombre de la SVM en las `-source-path` `-destination-path` opciones y. Vea el ejemplo siguiente.

   En el siguiente ejemplo se libera información de la relación de replicación especificada desde la SVM de origen `svm1`:

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup:
   ```

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

Gestionar la replicación de volúmenes raíz de SnapMirror

Obtenga más información sobre la replicación de volúmenes raíz de ONTAP SnapMirror

Cada SVM de un entorno NAS cuenta con un espacio de nombres único. El volumen SVM *root,* que contiene sistema operativo e información relacionada, es el punto de entrada de la jerarquía del espacio de nombres. Para garantizar que los clientes puedan acceder a los datos en caso de interrupción del servicio o conmutación al nodo de respaldo, debería crear una copia de mirroring con uso compartido de la carga del volumen raíz de la SVM.

El principal objetivo de los reflejos de uso compartido de carga para los volúmenes raíz de SVM ya no es para el uso compartido de carga; en su lugar, su finalidad es la recuperación ante desastres.

- Si el volumen raíz no está disponible temporalmente, el reflejo de uso compartido de carga proporciona acceso de solo lectura a los datos del volumen raíz.
- Si el volumen raíz no está disponible permanentemente, se puede promocionar uno de los volúmenes compartidos de carga para proporcionar acceso de escritura a los datos del volumen raíz.

Crear e inicializar relaciones de reflejos de uso compartido de carga de ONTAP

Debe crear un espejo de carga compartida (LSM) para cada volumen raíz de SVM que sirva datos NAS en el clúster. En clústeres con dos o más pares de alta disponibilidad (HA), considere espejos de carga compartida de volúmenes raíz de SVM para garantizar que el espacio de nombres permanezca accesible para los clientes en caso de que ambos nodos de un par de alta disponibilidad (HA) fallen. Los espejos de carga compartida no son adecuados para clústeres con un solo par de alta disponibilidad (HA).

Antes de empezar

A partir de ONTAP 9.16.1, cuando se crea una relación de espejo de uso compartido de carga, la SVM de destino no puede tener un límite de almacenamiento habilitado.

Acerca de esta tarea

Si crea un LSM en el mismo nodo y el nodo no está disponible, tendrá un único punto de error y no tendrá una segunda copia para garantizar que los datos sigan siendo accesibles para los clientes. Pero cuando crea el LSM en un nodo distinto al que contiene el volumen raíz o en un par de alta disponibilidad diferente, todavía se puede acceder a los datos en caso de una interrupción del servicio.

Por ejemplo, en un clúster de cuatro nodos con volumen raíz en tres nodos:

- Para el volumen raíz en el nodo 1 de alta disponibilidad, cree el LSM en el nodo 1 de alta disponibilidad 2 o el nodo 2 de alta disponibilidad.
- Para el volumen raíz en el nodo de alta disponibilidad 1 2, cree el LSM en el nodo de alta disponibilidad 2 1 o el nodo de alta disponibilidad 2.
- Para el volumen raíz en el nodo 1 de alta disponibilidad 2, cree el LSM en el nodo 1 de alta disponibilidad o el nodo 2 de alta disponibilidad 1.

Pasos

1. Crear un volumen de destino para el LSM:

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

El tamaño del volumen de destino debe ser igual o mayor que el del volumen raíz.

Se recomienda asignar un nombre al volumen raíz y de destino con sufijos, `_root` como y. `_m1`

Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

En el ejemplo siguiente se crea un volumen de reflejos de uso compartido de carga para el volumen raíz `svm1_root` en `cluster_src`:

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "Cree un programa de trabajo de replicaciones".
3. Crear una relación de mirroring de uso compartido de carga entre el volumen raíz de SVM y el volumen de destino para LSM:

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

En el siguiente ejemplo se crea una relación de reflejo de uso compartido de carga entre `svm1_root` el volumen raíz y el volumen de reflejo de uso compartido de carga `svm1_m1` :

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

El atributo type del reflejo de carga compartida cambia de `DP` a `LS`.

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

4. Inicialice el reflejo de uso compartido de carga:

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

En el ejemplo siguiente se inicializa el reflejo de uso compartido de carga para el volumen raíz `svm1_root` :

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

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

Actualizar una relación de reflejo de uso compartido de carga de ONTAP

Las relaciones de reflejos de uso compartido de carga (LSM) se actualizan automáticamente para los volúmenes raíz de SVM después de montar o desmontar un volumen en la SVM, y durante `volume create` las operaciones que incluyen la `junction-path` opción. Puede actualizar manualmente una relación LSM si desea actualizarla antes de la siguiente actualización programada.

Las relaciones de reflejos de uso compartido de carga se actualizan automáticamente en las siguientes circunstancias:

- Ha llegado el momento de realizar una actualización programada
- Se realiza una operación de montaje o desmontaje en un volumen del volumen raíz de la SVM
- A `volume create` Se emite una orden que incluye la `junction-path` opción

  Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP".

Paso

1. Actualice manualmente una relación de reflejo de carga compartida:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   snapmirror update-ls-set -source-path <SVM:volume>
   ```

   En el ejemplo siguiente se actualiza la relación de reflejo de uso compartido de carga para el volumen raíz `svm1_root`:

   ```
   cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
   ```

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

Promocione un reflejo de uso compartido de carga de ONTAP

Si un volumen raíz no está disponible de forma permanente, se puede promocionar el volumen de reflejos de uso compartido de carga (LSM) para proporcionar acceso de escritura a los datos del volumen raíz.

Antes de empezar

Para esta tarea, debe utilizar comandos de nivel de privilegio avanzado.

Pasos

1. Cambie al nivel de privilegio avanzado:

```
set -privilege advanced
```

2. Ascender un volumen LSM:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   snapmirror promote -destination-path <SVM:volume>
   ```

   En el ejemplo siguiente, se promociona el `svm1_m2` volumen como volumen raíz de la SVM nuevo:

   ```
   cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

   Warning: Promote will delete the offline read-write volume
            cluster_src://svm1/svm1_root and replace it with
            cluster_src://svm1/svm1_m2. Because the volume is offline,
            it is not possible to determine whether this promote will
            affect other relationships associated with this source.
   Do you want to continue? {y|n}: y
   ```

   Introduzca `y`. ONTAP convierte al volumen LSM en un volumen de lectura/escritura y elimina el volumen raíz original, si es accesible.

   > Es posible que el volumen raíz promocionado no tenga todos los datos que estaban en el volumen raíz original, si no se realizó la última actualización recientemente.

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

3. Volver al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

4. Cambie el nombre del volumen promocionado según la convención de nomenclatura que utilizó para el volumen raíz:

   Antes de ejecutar este comando, debe sustituir las variables entre paréntesis angulares por los valores requeridos.

   ```
   volume rename -vserver <SVM> -volume <volume> -newname <new_name>
   ```

   En el ejemplo siguiente se cambia el `svm1_m2` nombre del volumen promocionado con el nombre `svm1_root`:

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. Proteja el volumen raíz renombrado, como se describe en el paso 3 hasta el paso 4 en "Creación e inicialización de relaciones de mirroring de uso compartido de carga".

Backup en el cloud

Instalar una licencia en la nube de ONTAP SnapMirror

Las relaciones de cloud de SnapMirror se pueden orquestar utilizando aplicaciones de backup de terceros cualificadas previamente. A partir de ONTAP 9.9,1, también puede usar System Manager para orquestar la replicación en el cloud de SnapMirror. Tanto las licencias de capacidad de cloud de SnapMirror como de SnapMirror son necesarias al utilizar System Manager para orquestar backups de almacenamiento de objetos de ONTAP en las instalaciones. También tendrás que solicitar e instalar la licencia de la API de nube de SnapMirror.

Acerca de esta tarea

Las licencias de cloud de SnapMirror y SnapMirror S3 son licencias de clúster, no de nodos, por lo que se suministran *not* con el paquete de licencia de ONTAP One. Estas licencias están incluidas en el paquete de compatibilidad ONTAP One aparte. Si desea habilitar SnapMirror cloud, debe solicitar este paquete.

Además, la orquestación de System Manager de backups en el cloud de SnapMirror en el almacenamiento de objetos requiere una clave de la API del cloud de SnapMirror. Esta licencia de API es una licencia para todo el clúster de instancia única, lo que significa que no es necesario instalarla en todos los nodos del clúster.

Pasos

Necesita solicitar y descargar el paquete de compatibilidad de ONTAP One y la licencia de API en cloud de SnapMirror y, a continuación, instalarlos mediante System Manager.

1. Localice y registre el UUID de clúster del clúster para el que desea obtener licencia.

   El UUID de clúster se requiere cuando envía la solicitud para solicitar el bundle de compatibilidad ONTAP One para el clúster.

2. Póngase en contacto con su equipo de ventas de NetApp y solicite el paquete de compatibilidad de ONTAP One.
3. Solicite la licencia de la API de cloud de SnapMirror siguiendo las instrucciones que se proporcionan en el sitio de soporte de NetApp.

   "Solicite una clave de licencia de la API de cloud de SnapMirror"

4. Cuando haya recibido y descargado los archivos de licencia, utilice System Manager para cargar al clúster el NLF de compatibilidad con cloud de ONTAP y el NLF de la API de cloud de SnapMirror:
   a. Haga clic en **clúster > Configuración**.
   b. En la ventana **Configuración**, haz clic en **Licencias**.
   c. En la ventana **Licencias**, haga clic en + Add .

d. En el cuadro de diálogo **Agregar licencia**, haga clic en **examinar** para seleccionar el NLF que descargó y, a continuación, haga clic en **Agregar** para cargar el archivo en el clúster.

Información relacionada

"Realice backups de datos en el cloud con SnapMirror"

"Búsqueda de licencias de software de NetApp"

Realice backups de los datos en el cloud con ONTAP SnapMirror

A partir de ONTAP 9.9.1, puede realizar backups de sus datos en el cloud y restaurar sus datos desde el almacenamiento en cloud a un volumen diferente mediante System Manager. Es posible usar StorageGRID o ONTAP S3 como almacén de objetos en el cloud.

Desde ONTAP 9.18.1:

- SnapMirror cloud admite operaciones de copia de seguridad y restauración para volúmenes FlexGroup en configuraciones MetroCluster usando el "API de REST de ONTAP" existente. Esta funcionalidad te permite crear relaciones de SnapMirror cloud para volúmenes FlexGroup en configuraciones MetroCluster que se mantienen desde el sitio asociado después de una conmutación de sitios y switchback.

A partir de ONTAP 9,16.1:

- El backup en el cloud de SnapMirror admite relaciones ramificadas. Esto significa que los backups de SnapMirror se pueden crear de manera simultánea en dos almacenes de objetos diferentes. Con ONTAP 9.16.1, el cloud de SnapMirror admite dos relaciones de dispersión. Las salidas ramificadas pueden ser de dos almacenes de objetos y de uno o dos bloques en dos almacenes de objetos diferentes. Los intentos de crear más de dos relaciones de dispersión fallarán.
- SnapMirror Cloud admite backups de volúmenes migrados a la nube mediante un proceso de sincronización más eficiente con "API de REST de ONTAP"los existentes. La funcionalidad admite backups de cloud SnapMirror desde un volumen migrado en el cloud al mismo extremo de almacén de objetos de destino sin necesidad de realizar una operación de referencia. Se admiten los volúmenes FlexVol y FlexGroup.

Antes de usar la función cloud de SnapMirror, debe solicitar una clave de licencia para la API de cloud de SnapMirror en el sitio de soporte de NetApp"Solicite una clave de licencia de la API de cloud de SnapMirror": . Siguiendo las instrucciones, debe proporcionar una descripción simple de su oportunidad de negocio y solicitar la clave API mediante el envío de un correo electrónico a la dirección de correo electrónico proporcionada. Debe recibir una respuesta por correo electrónico en un plazo de 24 horas con instrucciones adicionales sobre cómo adquirir la clave API.

Añadir un almacén de objetos en la nube

Antes de configurar backups en cloud de SnapMirror, tiene que añadir un almacén de objetos en cloud StorageGRID o ONTAP S3.

Pasos

1. Haga clic en **Protección > Descripción general > Tiendas de objetos en la nube**.
2. Haga clic en + Add .

Realice un backup con la política predeterminada

Puede configurar rápidamente un backup en la nube de SnapMirror para un volumen existente mediante la política de protección de nube predeterminada, DailyBackup.

Pasos

1. Haga clic en **Protección > Descripción general** y seleccione **copia de seguridad de volúmenes en la nube**.
2. Si es la primera vez que realiza backups en el cloud, introduzca su clave de licencia de API de cloud de SnapMirror en el campo de licencia como se indica.
3. Haga clic en **autenticar y continuar**.
4. Seleccione un volumen de origen.
5. Seleccione un almacén de objetos en la nube.
6. Haga clic en **Guardar**.

Cree una política de backup en el cloud personalizada

Si no desea usar la política de nube predeterminada de DailyBackup para sus copias de seguridad en la nube de SnapMirror, puede crear su propia política.

Pasos

1. Haga clic en **Protección > Descripción general > Configuración de directivas locales** y seleccione **Directivas de protección**.
2. Haga clic en **Agregar** e introduzca los nuevos detalles de la directiva.
3. En la sección **Tipo de directiva**, seleccione **copia de seguridad en la nube** para indicar que está creando una política de nube.
4. Haga clic en **Guardar**.

Cree una copia de seguridad desde la página Volumes

Puede usar la página **Volúmenes** de System Manager cuando desee seleccionar y crear copias de seguridad en la nube para varios volúmenes a la vez o cuando desee usar una política de protección personalizada.

Pasos

1. Haga clic en **almacenamiento > volúmenes**.
2. Seleccione los volúmenes de los que desea realizar una copia de seguridad en la nube y haga clic en **proteger**.
3. En la ventana **proteger volumen**, haga clic en **más opciones**.
4. Seleccionar una política.

   Puede seleccionar la política predeterminada, DailyBackup o una política de cloud personalizada que haya creado.

5. Seleccione un almacén de objetos en la nube.
6. Haga clic en **Guardar**.

Restaure desde el cloud

Puede usar System Manager para restaurar datos con backups del almacenamiento de cloud a otro volumen en el clúster de origen.

> Si utiliza ONTAP 9.16.1 o posterior y va a restaurar un archivo único cloud de SnapMirror a un volumen de FlexGroup, solo debe restaurar los archivos en un directorio nuevo en el volumen de FlexGroup, y los datos granulares deben establecerse en `advanced` el volumen de FlexGroup de destino. Para obtener más información acerca de la configuración de la `-granular-data advanced` opción, consulte "Equilibre los volúmenes de ONTAP FlexGroup mediante la redistribución de los datos de los archivos".

Pasos

1. En el clúster de origen de una relación de SnapMirror a la nube, haga clic en **Almacenamiento > Volúmenes**.
2. Seleccione el volumen que desea restaurar.
3. Seleccione la ficha **copia de seguridad en la nube**.
4. Haga clic ⋮ junto al volumen de origen que desea restaurar para mostrar el menú y seleccione **Restaurar**.
5. En **Source**, seleccione una VM de almacenamiento y, a continuación, escriba el nombre del volumen en el que desea restaurar los datos.
6. En **Destino**, seleccione la instantánea que desea restaurar.
7. Haga clic en **Guardar**.

Elimine una relación de cloud de SnapMirror

Puede usar System Manager para eliminar una relación de cloud.

Pasos

1. Haga clic en **almacenamiento > volúmenes** y seleccione el volumen que desea eliminar.
2. Haga clic ⋮ junto al volumen de origen y seleccione **Eliminar**.
3. Seleccione **Eliminar el extremo del almacén de objetos en la nube (opcional)** si desea eliminar el extremo del almacén de objetos en la nube.
4. Haga clic en **Eliminar**.

Quitar un almacén de objetos en la nube

Puede usar System Manager para quitar un almacén de objetos en cloud si no forma parte de una relación de backup en el cloud. Cuando un almacén de objetos en cloud forma parte de una relación de backup en el cloud, no se puede eliminar.

Pasos

1. Haga clic en **Protección > Descripción general > Tiendas de objetos en la nube**.
2. Seleccione el almacén de objetos que desea eliminar, haga clic ⋮ y seleccione **Eliminar**.

Realice copias de seguridad de datos con NetApp Backup and Recovery

A partir de ONTAP 9.9.1, puede usar System Manager para realizar copias de seguridad de datos en la nube mediante el servicio NetApp Backup and Recovery.

Backup and Recovery admite volúmenes de lectura y escritura FlexVol y volúmenes de protección de datos (DP). A partir de ONTAP 9.12.1, Backup and Recovery admite volúmenes FlexGroup y volúmenes SnapLock .

Obtenga más información sobre "Copia de seguridad y recuperación de NetApp" .

Antes de empezar

Debe realizar los siguientes procedimientos para establecer una cuenta en la consola de NetApp . Para la cuenta de servicio, debe crear el rol como "Administrador de cuenta". (Otros roles de cuenta de servicio no tienen los privilegios necesarios para establecer una conexión desde el Administrador del sistema).

1. "Crear una cuenta en la consola de NetApp" .
2. "Crear un agente de consola en la consola de NetApp"con uno de los siguientes proveedores de nube:
   - Microsoft Azure
   - Amazon Web Services (AWS)
   - Google Cloud Platform (GCP)
   - StorageGRID (ONTAP 9.10.1)

   > A partir de ONTAP 9.10.1, puede seleccionar StorageGRID como proveedor de respaldo en la nube, pero solo si NetApp Console está implementada en las instalaciones. El agente de la consola debe estar instalado en las instalaciones y disponible a través de la aplicación de software como servicio (SaaS) de la consola de NetApp .
3. "Suscríbase a NetApp Backup and Recovery en la consola de NetApp"(requiere la licencia correspondiente).
4. "Genere una clave de acceso y una clave secreta mediante la consola de NetApp" .

Registrar el clúster con la consola de NetApp

Puede registrar el clúster con la consola de NetApp utilizando la consola o el administrador del sistema.

Pasos

1. En System Manager, vaya a **Descripción general de la protección**.
2. En * NetApp Backup and Recovery*, proporcione los siguientes detalles:
   - ID del cliente
   - Clave secreta de cliente
3. Seleccione **Registrar y continuar**.

Habilitar NetApp Backup and Recovery

Una vez registrado el clúster en la consola de NetApp , debe habilitar NetApp Backup and Recovery e iniciar la primera copia de seguridad en la nube.

Pasos

1. En el Administrador del sistema, seleccione **Protección > Descripción general** y, a continuación, desplácese a la sección **Cloud Backup Service**.
2. Introduzca **ID de cliente** y **Secreto de cliente**.

A partir de ONTAP 9.10.1, puede obtener información sobre el costo de usar la nube seleccionando **Más información sobre el costo de usar la nube**.

3. Selecciona **Conectar y Habilitar Cloud Backup Service**.
4. En la página **Habilitar NetApp Backup and Recovery**, proporcione los siguientes detalles, según el proveedor que haya seleccionado.

Para este proveedor de cloud…	Introduzca los siguientes datos…
Azure	• ID de suscripción de Azure • Región • Nombre del grupo de recursos (existente o nuevo)
AWS	• ID de cuenta de AWS • Clave de acceso • Clave secreta • Región
Google Cloud Project (GCP)	• Nombre del proyecto de Google Cloud • Clave de acceso a Google Cloud • Clave secreta de Google Cloud • Región
StorageGRID (ONTAP 9.10.1 y posteriores, y solo para la implementación local de la consola de NetApp)	• Servidor • Clave de acceso de SG • Clave secreta de SG

5. Seleccione una **Política de protección**:
   - **Política existente**: Elija una política existente.
   - **Nueva directiva**: Especifique un nombre y configure un programa de transferencia.

     A partir de ONTAP 9.10.1, es posible especificar si desea habilitar el archivado con Azure o AWS.

     Si habilita el archivado para un volumen con Azure o AWS, no podrá deshabilitar el archivado.

     Si habilita el archivado para Azure o AWS, especifique lo siguiente:

     - El número de días después de los cuales se archiva el volumen.
     - La cantidad de backups que se retendrán en el archivo. Especifique «0» (cero) para archivar al último backup.
     - Para AWS, seleccione la clase de almacenamiento de archivado.

6. Seleccione los volúmenes de los que desea realizar el backup.
7. Seleccione **Guardar**.

Editar la política de protección utilizada para NetApp Backup and Recovery

Puede cambiar la política de protección que se utiliza con NetApp Backup and Recovery.

Pasos

1. En el Administrador del sistema, seleccione **Protección > Descripción general** y, a continuación, desplácese a la sección **Cloud Backup Service**.
2. Seleccione y, a continuación, * Editar *.
3. Seleccione una **Política de protección**:
   - **Política existente**: Elija una política existente.
   - **Nueva directiva**: Especifique un nombre y configure un programa de transferencia.

     A partir de ONTAP 9.10.1, es posible especificar si desea habilitar el archivado con Azure o AWS.

     Si habilita el archivado para un volumen con Azure o AWS, no podrá deshabilitar el archivado.

     Si habilita el archivado para Azure o AWS, especifique lo siguiente:

     - El número de días después de los cuales se archiva el volumen.
     - La cantidad de backups que se retendrán en el archivo. Especifique «0» (cero) para archivar al último backup.
     - Para AWS, seleccione la clase de almacenamiento de archivado.
4. Seleccione **Guardar**.

Proteja nuevos volúmenes o LUN en el cloud

Cuando se crea un volumen o LUN nuevo, puede establecer una relación de protección de SnapMirror que permita realizar backups en el cloud del volumen o LUN.

Antes de empezar

- Debe tener una licencia de SnapMirror.
- Deben configurarse las LIF de interconexión de clústeres.
- NTP debe configurarse.
- El clúster debe ejecutar ONTAP 9.9.1 o una versión posterior.

Acerca de esta tarea

No puede proteger volúmenes o LUN nuevos en el cloud para las siguientes configuraciones de clúster:

- El clúster no puede estar en un entorno de MetroCluster.
- No se admite SVM-DR.
- No es posible realizar copias de seguridad de los volúmenes FlexGroup mediante NetApp Backup and Recovery.

Pasos

1. Al aprovisionar un volumen o LUN, en la página **Protección** del Administrador del sistema, seleccione la casilla de verificación con la etiqueta **Activar SnapMirror (local o remoto)**.
2. Seleccione el tipo de política de copia de seguridad y recuperación.
3. Si la función de Copia de seguridad y recuperación no está habilitada, seleccione *Habilitar copia de seguridad mediante Copia de seguridad y recuperación de NetApp *.

Proteja los volúmenes o LUN existentes en el cloud

Puede establecer una relación de protección de SnapMirror para volúmenes y LUN existentes.

Pasos

1. Seleccione un volumen o LUN existente y seleccione **Proteger**.
2. En la página **Proteger volúmenes**, especifique **Realizar copia de seguridad mediante NetApp Backup and Recovery** para la política de protección.
3. Seleccione **Proteger**.
4. En la página **Protección**, seleccione la casilla de verificación **Activar SnapMirror (local o remoto)**.
5. Seleccione **Conectar y habilitar NetApp Backup and Recovery**.

Restaurar datos de archivos de copia de seguridad

Puede realizar operaciones de administración de copias de seguridad, como restaurar datos, actualizar relaciones y eliminar relaciones, solo cuando utilice la consola de NetApp . Consulte "Restaurar datos a partir de archivos de copia de seguridad" Para más información.

Archivado y cumplimiento de normativas con tecnología SnapLock

Obtenga más información sobre ONTAP SnapLock

SnapLock es una solución de cumplimiento de normativas de alto rendimiento para organizaciones que utilizan almacenamiento WORM para conservar archivos de forma no modificada a efectos de regulación y gobernanza.

SnapLock ayuda a evitar la eliminación, el cambio o el cambio de nombre de los datos para cumplir normativas como SEC 17a-4(f), HIPAA, FINRA, CFTC y RGPD. Gracias a SnapLock, puede crear volúmenes con fines especiales en los que los archivos se pueden almacenar y comprometidos a mantener su estado no borrable y no modificable durante un período de retención determinado o de forma indefinida. SnapLock permite llevar a cabo esta retención en el nivel de archivo mediante protocolos de archivos abiertos estándar como CIFS y NFS. Los protocolos de archivos abiertos compatibles con SnapLock son NFS (versiones 2, 3 y 4) y CIFS (SMB 1.0, 2.0 y 3.0).

Mediante SnapLock, podrá conservar archivos e copias Snapshot en ALMACENAMIENTO WORM y establecer periodos de retención para los datos protegidos WORM. El ALMACENAMIENTO WORM de SnapLock utiliza la tecnología Snapshot de NetApp y puede aprovechar la replicación de SnapMirror y los backups de SnapVault como tecnología base para brindar protección de recuperación de datos de backup. Obtenga más información sobre el almacenamiento WORM: "Almacenamiento WORM conforme a la normativa con SnapLock de NetApp: TR-4526".

Puede usar una aplicación para comprometer archivos a WORM mediante NFS o CIFS, o utilizar la función de compromiso automático de SnapLock para comprometer archivos automáticamente a WORM. Puede utilizar un *WORM appable file* para conservar datos que se escriben de forma incremental, como la información de registro. Para obtener más información, consulte "Use el modo de adición de volúmenes para crear archivos WORM flexibles".

SnapLock admite métodos de protección de datos que deberían satisfacer la mayoría de los requisitos de cumplimiento de normativas:

- Es posible usar SnapLock para SnapVault para proteger WORM en el almacenamiento secundario. Consulte "Repetir snapshots en WORM".
- Puede usar SnapMirror para replicar archivos WORM a otra ubicación geográfica a fin de realizar la recuperación ante desastres. Consulte "Refleje los archivos WORM".

SnapLock es una función de ONTAP basada en licencia. Una sola licencia le permite utilizar SnapLock en un modo de cumplimiento estricto, para satisfacer mandatos externos como la Regla 17a-4(f) de la SEC, y un modo empresarial más flexible, para cumplir con las regulaciones internas obligatorias para la protección de activos digitales. Las licencias SnapLock son parte de la "ONTAP One" paquete de software.

SnapLock es compatible con todos los sistemas AFF y FAS, así como con ONTAP Select. SnapLock no es una solución exclusivamente de software, es una solución integrada de hardware y software. Esta distinción es importante para regulaciones WORM estrictas como SEC 17a-4(f), que requiere una solución de hardware y software integrada. Para obtener más información, consulte "Guía de LA SEC para los intermediarios comerciales sobre el uso de medios de almacenamiento electrónico".

Puede hacer con SnapLock

Después de configurar SnapLock, es posible completar las siguientes tareas:

- "Los archivos cumplen CON WORM"
- "Repetir snapshots en WORM para el almacenamiento secundario"
- "Refleje los archivos WORM para la recuperación ante desastres"
- "Conserve los archivos WORM durante su litigio gracias a su conservación legal"
- "Elimine los archivos WORM utilizando la función de eliminación privilegiada"
- "Defina el período de retención de archivos"
- "Mover un volumen de SnapLock"
- "Bloquea una snapshot para protegerte frente a ataques de ransomware"
- "Revisar el uso de SnapLock con el registro de auditoría"
- "Utilice las API de SnapLock"

Modos SnapLock Compliance y Enterprise

Los modos SnapLock Compliance y Enterprise difieren principalmente en el nivel en el que cada modo protege los archivos WORM:

Modo SnapLock	Nivel de protección	Archivo WORM eliminado durante la retención

Modo de cumplimiento de normativas	En el nivel de disco	No se puede eliminar
Modo empresarial	A nivel de archivo	El administrador de cumplimiento puede eliminarlo mediante un procedimiento de "eliminación privilegiada" auditado.

Una vez transcurrido el período de retención, es responsable de eliminar los archivos que ya no se necesiten. Una vez que un archivo se ha comprometido con WORM, ya sea en modo Compliance o Enterprise, no se podrá modificar, ni siquiera después de que haya caducado el período de retención.

No se puede mover un archivo WORM durante el período de retención o después del mismo. Puede copiar un archivo WORM, pero la copia no conservará sus características WORM.

En la siguiente tabla se muestran las diferencias en las capacidades que admiten los modos SnapLock Compliance y Enterprise:

Capacidad	Cumplimiento de normativas SnapLock	Empresa SnapLock
Activar y eliminar archivos mediante la eliminación con privilegios	No	Sí
Reinicie los discos	No	Sí
Destrucción de agregados y volúmenes de SnapLock durante el período de retención	No	Sí, con la excepción del volumen de registro de auditoría de SnapLock
Cambie el nombre de los agregados o volúmenes	No	Sí
Utilice discos que no sean de NetApp	No	No
Use el volumen SnapLock para el registro de auditoría	Sí	Sí, a partir de ONTAP 9,5

Funciones compatibles y no compatibles con SnapLock

En la siguiente tabla se muestran las funciones compatibles con el modo de cumplimiento de normativas SnapLock, el modo SnapLock Enterprise o ambos:

Función	Compatible con SnapLock Compliance	Compatible con SnapLock Enterprise
Grupos de consistencia	No	No

Volúmenes cifrados	Sí, aprenda más sobre Cifrado y SnapLock .	Sí, aprenda más sobre Cifrado y SnapLock .
FabricPool en agregados de SnapLock	No	Sí, a partir de ONTAP 9,8. Más información sobre FabricPool en agregados de SnapLock Enterprise.
Agregados de Flash Pool	Sí.	Sí.
FlexClone	Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock.	Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock.
Volúmenes de FlexGroup	Sí, a partir de ONTAP 9,11.1. Más información sobre [flexgroup].	Sí, a partir de ONTAP 9,11.1. Más información sobre [flexgroup].
LUN	No. Obtenga más información sobre Soporte de LUNSnapLock.	No. Obtenga más información sobre Soporte de LUNSnapLock.
Configuraciones de MetroCluster	Sí, a partir de ONTAP 9,3. Más información sobre Soporte de MetroCluster.	Sí, a partir de ONTAP 9,3. Más información sobre Soporte de MetroCluster.
Verificación multi-admin (MAV)	Sí, a partir de ONTAP 9,13.1. Más información sobre Soporte de MAV.	Sí, a partir de ONTAP 9,13.1. Más información sobre Soporte de MAV.
SAN	No	No
SnapRestore de archivo único	No	Sí
SnapMirror síncrono activo	No	No
SnapRestore	No	Sí
SMTape	No	No
SnapMirror síncrono	No	No
SSD	Sí.	Sí.
Funcionalidades de eficiencia del almacenamiento	Sí, a partir de ONTAP 9,9.1. Más información sobre soporte de eficiencia del almacenamiento.	Sí, a partir de ONTAP 9,9.1. Más información sobre soporte de eficiencia del almacenamiento.

FabricPool en agregados de SnapLock Enterprise

Las instancias de FabricPool son compatibles con los agregados empresariales de SnapLock, a partir de ONTAP 9.8. Sin embargo, su equipo de cuenta tiene que abrir una solicitud de variación de productos que documente que SnapLock ya no protege los datos de FabricPool organizados en niveles en un cloud público o privado porque un administrador de cloud puede eliminar dichos datos.

Cualquier dato que FabricPool proporcione en niveles en un cloud público o privado ya no está protegido por SnapLock, ya que un administrador de cloud puede eliminar estos datos.

Volúmenes de FlexGroup

SnapLock admite volúmenes FlexGroup que comiencen con ONTAP 9.11.1; sin embargo, no se admiten las siguientes funciones:

- Conservación legal
- Retención basada en eventos
- SnapLock para SnapVault (compatible a partir de ONTAP 9.12.1)

También debe ser consciente de los siguientes comportamientos:

- El reloj de cumplimiento de volumen (VCC) de un volumen FlexGroup está determinado por el VCC del componente raíz. Todos los componentes que no son de raíz tendrán su VCC estrechamente sincronizado con la VCC raíz.
- Las propiedades de configuración de SnapLock se establecen únicamente en la FlexGroup en su conjunto. Los componentes individuales no pueden tener diferentes propiedades de configuración, como el tiempo de retención predeterminado y el período de compromiso automático.

Soporte de LUN

Los LUN solo se admiten en volúmenes de SnapLock en casos en los que las snapshots creadas en un volumen no de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Sin embargo, las copias Snapshot a prueba de manipulación son compatibles tanto en los volúmenes de origen como en los volúmenes de destino de SnapMirror que contienen LUN.

Soporte de MetroCluster

La compatibilidad con SnapLock en configuraciones MetroCluster es diferente del modo de cumplimiento de normativas SnapLock al modo empresarial de SnapLock.

Cumplimiento de normativas SnapLock

- A partir de ONTAP 9.3, SnapLock Compliance se admite en los agregados de MetroCluster no reflejados.
- A partir de ONTAP 9.3, SnapLock Compliance se admite en agregados reflejados, pero solo si el agregado se utiliza para alojar los volúmenes de registros de auditoría de SnapLock.
- Las configuraciones de SnapLock específicas para SVM se pueden replicar en sitios principales y secundarios mediante MetroCluster.

Empresa SnapLock

- Se admiten agregados SnapLock Enterprise .
- A partir de ONTAP 9.3, se admiten los agregados de SnapLock Enterprise con eliminación privilegiada.

- Las configuraciones de SnapLock específicas para SVM se pueden replicar en ambos sitios mediante MetroCluster.

Configuraciones de MetroCluster y relojes de cumplimiento

Las configuraciones de MetroCluster utilizan dos mecanismos de reloj de conformidad, el reloj de cumplimiento de volumen (VCC) y el reloj de cumplimiento del sistema (SCC). El VCC y el SCC están disponibles para todas las configuraciones SnapLock. Cuando se crea un nuevo volumen en un nodo, su VCC se inicializa con el valor actual del SCC en ese nodo. Una vez creado el volumen, el VCC siempre se realiza un seguimiento del volumen y del tiempo de retención de archivos.

Cuando un volumen se replica en otro sitio, su VCC también se replica. Cuando se produce una conmutación de volumen, del sitio A al sitio B, por ejemplo, el VCC continúa siendo actualizado en el sitio B mientras que el SCC en el sitio A se detiene cuando el sitio A se desconecta.

Cuando el sitio A se vuelve a poner en línea y se realiza la vuelta de volumen, el reloj SCC del sitio se reinicia mientras el VCC del volumen continúa siendo actualizado. Como el VCC se actualiza continuamente, independientemente de las operaciones de conmutación de sitios y conmutación de estado, los tiempos de retención de archivos no dependen de los relojes SCC y no se amplían.

Compatibilidad con verificación multiadministrador (MAV)

A partir de la versión ONTAP 9.13.1, un administrador de clúster puede habilitar de forma explícita la verificación multiadministrador en un clúster para requerir la aprobación de quórum antes de ejecutar algunas operaciones de SnapLock. Cuando MAV está activado, las propiedades del volumen SnapLock como default-retention-time, minimum-retention-time, maximum-retention-time, volume-append-mode, autocommit-period y privileged-delete requerirán aprobación del quórum. Más información sobre "MAV".

Eficiencia del almacenamiento

A partir de ONTAP 9.9.1, SnapLock admite funciones de eficiencia del almacenamiento, como la compactación de datos, la deduplicación entre volúmenes y la compresión adaptativa para volúmenes y agregados de SnapLock. Para obtener más información acerca de la eficiencia del almacenamiento, consulte "Información general de la eficiencia del almacenamiento de ONTAP".

Cifrado

ONTAP ofrece tecnologías de cifrado basadas en software y hardware para garantizar que los datos en reposo no se puedan leer en caso de reasignación, devolución, pérdida o robo del medio de almacenamiento.

Exención de responsabilidad: NetApp no puede garantizar que los archivos WORM protegidos SnapLock en unidades o volúmenes de autocifrado se puedan recuperar si se pierde la clave de autenticación o si el número de intentos de autenticación con errores supera el límite especificado y hace que la unidad se bloquee de forma permanente. Usted es responsable de garantizar el cumplimiento de los fallos de autenticación.

Los volúmenes cifrados son compatibles con los agregados SnapLock .

Transición de 7-Mode

Puede migrar volúmenes SnapLock de 7-Mode a ONTAP usando la función de transición basada en copias (CBT) de la herramienta de transición de 7-Mode. El modo SnapLock del volumen de destino, Compliance o Enterprise, debe coincidir con el modo SnapLock del volumen de origen. No se puede usar la transición sin copia (CFT) para migrar volúmenes de SnapLock.

Configure SnapLock

Obtenga información sobre cómo configurar ONTAP SnapLock

Antes de usar SnapLock, debe configurar SnapLock realizando diversas tareas, como "Instale la licencia de SnapLock"para cada nodo que aloje un agregado con un volumen de SnapLock, inicializar "Reloj de cumplimiento", crear un agregado de SnapLock para los clústeres que ejecuten versiones de ONTAP anteriores a ONTAP 9.10,1, "Cree y monte un volumen de SnapLock"etc.

Inicializar el reloj de cumplimiento de ONTAP

SnapLock utiliza *volume Compliance Clock* para garantizar la manipulación que puede alterar el período de retención de los archivos WORM. Primero, debe inicializar *system ComplianceClock* en cada nodo que aloje un agregado de SnapLock.

A partir de ONTAP 9.14.1, puede inicializar o reinicializar el reloj de cumplimiento de normativas del sistema cuando no hay volúmenes de SnapLock o ningún volumen con el bloqueo de snapshots habilitado. La capacidad de reinicializar permite a los administradores del sistema restablecer el reloj de cumplimiento del sistema en casos en los que podría haberse inicializado incorrectamente o corregir la desviación del reloj del sistema. En ONTAP 9.13.1 y versiones anteriores, una vez que se inicializa el reloj de cumplimiento de normativas en un nodo, no puede volver a inicializarlo.

Antes de empezar

Para reinicializar el reloj de conformidad:

- Todos los nodos del clúster deben tener el estado correcto.
- Todos los volúmenes deben estar en línea.
- No puede haber volúmenes presentes en la cola de recuperación.
- No hay volúmenes SnapLock presentes.
- No se puede presentar ningún volumen con bloqueo de snapshots habilitado.

Requisitos generales para inicializar el reloj de conformidad:

- Para realizar esta tarea, debe ser un administrador de clústeres.
- "La licencia de SnapLock debe instalarse en el nodo".

Acerca de esta tarea

La hora en el reloj de cumplimiento del sistema se hereda por el *volume Compliance Clock*, este último de los cuales controla el período de retención de los archivos WORM en el volumen. El reloj de cumplimiento de normativas del volumen se inicializa automáticamente cuando se crea un volumen de SnapLock nuevo.

> El ajuste inicial del reloj de cumplimiento del sistema se basa en el reloj del sistema de hardware actual. Por este motivo, debe verificar que la hora y la zona horaria del sistema sean correctas antes de inicializar el reloj de cumplimiento de normativas del sistema en cada nodo. Una vez que se inicializa el reloj de cumplimiento de normativas del sistema en un nodo, no se puede volver a inicializar cuando hay volúmenes de SnapLock o volúmenes con el bloqueo habilitado.

Pasos

Es posible usar la interfaz de línea de comandos de ONTAP para inicializar el reloj de cumplimiento de normativas o, a partir de ONTAP 9.12.1, puede utilizar System Manager para inicializar el reloj de cumplimiento de normativas.

System Manager

1. Vaya a **Cluster > Overview**.
2. En la sección **Nodes**, haga clic en **inicializar reloj de cumplimiento de SnapLock**.
3. Para mostrar la columna **Reloj de cumplimiento** y verificar que el Reloj de cumplimiento está inicializado, en la sección **Clúster > Descripción general > Nodos**, haga clic en **Mostrar/ocultar** y seleccione **Reloj de cumplimiento de SnapLock**.

CLI

1. Inicialice el reloj de cumplimiento del sistema:

   `snaplock compliance-clock initialize -node` *`node_name`*

   El siguiente comando inicializa el reloj de cumplimiento del sistema en `node1`:

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

   Obtenga más información sobre `snaplock compliance-clock initialize` en el "Referencia de comandos del ONTAP".

2. Cuando se le solicite, confirme que el reloj del sistema es correcto y que desea inicializar el reloj de conformidad:

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. Repita este procedimiento para cada nodo que aloje un agregado de SnapLock.

Habilite la resincronización del reloj de cumplimiento de normativas para un sistema configurado por NTP

Puede habilitar la función de sincronización del reloj de SnapLock Compliance cuando se configura un servidor NTP.

Antes de empezar

- Esta función solo está disponible en el nivel de privilegios avanzado.

- Para realizar esta tarea, debe ser un administrador de clústeres.
- "La licencia de SnapLock debe instalarse en el nodo".
- Esta función sólo está disponible para plataformas Cloud Volumes ONTAP, ONTAP Select y VSIM.

Acerca de esta tarea

Cuando el daemon de reloj seguro de SnapLock detecta una desviación más allá del umbral, ONTAP utiliza la hora del sistema para restablecer los relojes de cumplimiento del sistema y del volumen. Se establece un período de 24 horas como umbral de desviación. Esto significa que el reloj de cumplimiento del sistema se sincroniza con el reloj del sistema solo si la inclinación tiene más de un día de antigüedad.

El daemon de reloj seguro de SnapLock detecta una inclinación y cambia el reloj de cumplimiento a la hora del sistema. Cualquier intento de modificar la hora del sistema para forzar que el reloj de cumplimiento se sincronice con la hora del sistema falla, ya que el reloj de cumplimiento se sincroniza con la hora del sistema solo si la hora del sistema está sincronizada con la hora NTP.

Pasos

1. Habilite la función de sincronización del reloj de SnapLock Compliance cuando se configure un servidor NTP:

   `snaplock compliance-clock ntp`

   El siguiente comando habilita la función de sincronización del reloj de cumplimiento del sistema:

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

   Obtenga más información sobre `snaplock compliance-clock ntp modify` en el "Referencia de comandos del ONTAP".

2. Cuando se le solicite, confirme que los servidores NTP configurados son de confianza y que el canal de comunicación es seguro para habilitar la función:
3. Compruebe que la función está activada:

   `snaplock compliance-clock ntp show`

   El siguiente comando verifica que la función de sincronización del reloj de cumplimiento del sistema esté habilitada:

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

   Obtenga más información sobre `snaplock compliance-clock ntp show` en el "Referencia de comandos del ONTAP".

Crear un agregado SnapLock de ONTAP

`-snaplock-type`La opción volume se usa para especificar un tipo de volumen Compliance o Enterprise SnapLock. Para las versiones anteriores a ONTAP 9.10.1, se debe crear un agregado de SnapLock independiente. A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- La SnapLock "se debe instalar la licencia"en el nodo. Esta licencia se incluye en "ONTAP One".
- "Se debe inicializar el reloj de cumplimiento de normativas del nodo".
- Si ha particionado los discos como «'root'», «dn1» y «atado2», deberá asegurarse de que los discos de repuesto están disponibles.

Consideraciones de renovación

Al actualizar a ONTAP 9.10.1, los agregados existentes de SnapLock y otros componentes de SnapLock se actualizan para admitir la existencia de volúmenes SnapLock y distintos de SnapLock; sin embargo, los atributos de volumen de SnapLock existentes no se actualizan automáticamente. Por ejemplo, los campos de compactación de datos, deduplicación entre volúmenes y deduplicación entre volúmenes en segundo plano siguen sin cambios. Los nuevos volúmenes SnapLock creados en agregados existentes tienen los mismos valores predeterminados que los volúmenes que no son de SnapLock, y los valores predeterminados de los nuevos volúmenes y agregados dependen de la plataforma.

Consideraciones sobre la reversión

Si necesita volver a una versión de ONTAP anterior a la 9.10.1, debe mover todos los volúmenes de SnapLock Compliance, SnapLock Enterprise y SnapLock a sus propios agregados de SnapLock.

Acerca de esta tarea

- No se pueden crear agregados de cumplimiento con la opción SyncMirror.
- Solo se pueden crear agregados de cumplimiento reflejado en una configuración de MetroCluster si el agregado se utiliza para alojar volúmenes de registro de auditoría de SnapLock.

> En una configuración MetroCluster, es compatible con SnapLock Enterprise con los agregados reflejados y no reflejados. SnapLock Compliance solo se admite en agregados no reflejados.

Pasos

1. Cree un agregado de SnapLock:

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

El siguiente comando crea `Compliance` un agregado de SnapLock llamado `aggr1` con tres discos `node1` en:

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

Obtenga más información sobre `storage aggregate create` en el "Referencia de comandos del ONTAP".

Crear y montar volúmenes SnapLock de ONTAP

Debe crear un volumen de SnapLock para los archivos o copias de Snapshot que desea comprometer en el estado WORM. A partir de ONTAP 9.10.1, todos los volúmenes que cree, independientemente del tipo de agregado, se crearán de forma predeterminada como volumen que no sea de SnapLock. Debe usar `-snaplock-type` la opción para crear explícitamente un volumen de SnapLock especificando Compliance o Enterprise como tipo de SnapLock. De forma predeterminada, el tipo de SnapLock se establece en `non-snaplock`.

Antes de empezar

- El agregado de SnapLock debe estar en línea.
- Debería "Compruebe que hay instalada una licencia de SnapLock". Si no hay una licencia de SnapLock instalada en el nodo, debe "instale" esa licencia. 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 necesario, los clientes existentes pueden optar por "Actualice a ONTAP One".
- "Se debe inicializar el reloj de cumplimiento de normativas del nodo".

Acerca de esta tarea

Con los permisos de SnapLock adecuados, puede destruir un volumen empresarial o cambiar su nombre en cualquier momento. No se puede destruir un volumen de cumplimiento hasta que haya transcurrido el período de retención. Nunca se puede cambiar el nombre de un volumen de cumplimiento.

Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock. El volumen clonado tendrá el mismo tipo de SnapLock que el volumen principal.

> Los LUN no son compatibles con los volúmenes de SnapLock. Los LUN solo se admiten en volúmenes de SnapLock en casos en los que las snapshots creadas en un volumen no de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Sin embargo, las copias Snapshot a prueba de manipulación son compatibles tanto en los volúmenes de origen como en los volúmenes de destino de SnapMirror que contienen LUN.

Lleve a cabo esta tarea mediante System Manager de ONTAP o la interfaz de línea de comandos de ONTAP.

System Manager

A partir de ONTAP 9.12.1, se puede usar System Manager para crear un volumen de SnapLock.

Pasos

1. Vaya a **almacenamiento > volúmenes** y haga clic en **Agregar**.
2. En la ventana **Agregar volumen**, haga clic en **más opciones**.
3. Introduzca la nueva información del volumen, incluidos el nombre y el tamaño del volumen.
4. Seleccione **Activar SnapLock** y elija el tipo de SnapLock, ya sea Compliance o Enterprise.
5. En la sección **Archivos de registro automático**, seleccione **modificado** e introduzca la cantidad de tiempo que un archivo debe permanecer sin cambios antes de que se confirme automáticamente. El valor mínimo es de 5 minutos y el valor máximo es de 10 años.
6. En la sección **retención de datos**, seleccione el período de retención mínimo y máximo.
7. Seleccione el período de retención predeterminado.
8. Haga clic en **Guardar**.
9. Seleccione el nuevo volumen en la página **Volumes** para verificar la configuración de SnapLock.

CLI

1. Cree un volumen de SnapLock:

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

Obtenga más información sobre `volume create` en el "Referencia de comandos del ONTAP". Las siguientes opciones no están disponibles para SnapLock Volumes `-nvfail:,,,,` `-atime-update` `-is-autobalance-eligible` `-space-mgmt-try-first` Y `vmalign`.

El siguiente comando crea `Compliance` un volumen SnapLock llamado `vol1` en `aggr1` `vs1` :

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

Montar un volumen de SnapLock

Puede montar un volumen SnapLock en una ruta de unión en el espacio de nombres de la SVM para el acceso de clientes NAS.

Antes de empezar

El volumen SnapLock debe estar en línea.

Acerca de esta tarea

- Los volúmenes de SnapLock solo se pueden montar en la raíz de la SVM.
- No se puede montar un volumen normal en un volumen de SnapLock.

Pasos

1. Montar un volumen de SnapLock:

   `volume mount -vserver *SVM_name* -volume *volume_name* -junction-path *path*`

   Obtenga más información sobre `volume mount` en el "Referencia de comandos del ONTAP".

   El siguiente comando monta un volumen SnapLock llamado `vol1` en la ruta de unión `/sales` en el `vs1` espacio de nombres:

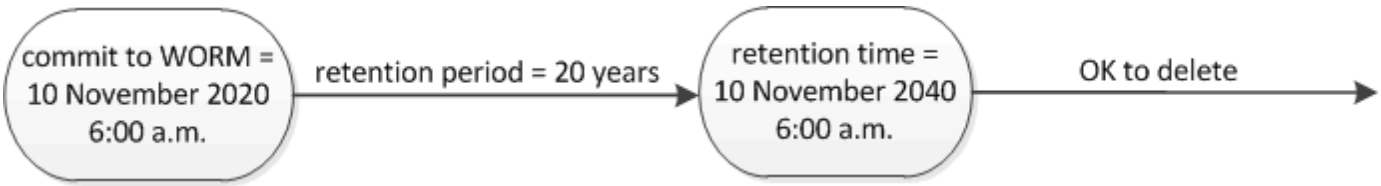
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

Establecer el tiempo de retención de ONTAP SnapLock

Se puede establecer el tiempo de retención de un archivo explícitamente o se puede usar el período de retención predeterminado para el volumen a fin de obtener el tiempo de retención. A menos que se establezca el tiempo de retención explícitamente, SnapLock utiliza el período de retención predeterminado para calcular el tiempo de retención. También es posible configurar la retención de archivos después de un evento.

Acerca del período de retención y del tiempo de retención

El *retention period* para un archivo WORM especifica la cantidad de tiempo que debe conservarse el archivo después de comprometerse al estado WORM. El *retention time* para un archivo WORM es el tiempo a partir del cual ya no es necesario retener el archivo. Un período de retención de 20 años para un archivo comprometido con EL estado WORM el 10 de noviembre a las 2020 6:00, por ejemplo, daría como resultado un período de retención de 10 de noviembre a las 2040 6:00 a.m.



> A partir de ONTAP 9.10.1, se puede establecer un tiempo de retención hasta el 26 de octubre de 3058 y un período de retención de hasta 100 años. Al ampliar las fechas de retención, las directivas más antiguas se convierten automáticamente. En ONTAP 9.9.1 y versiones anteriores, a menos que se establezca el período de retención predeterminado en infinito, el tiempo de retención máximo admitido es el 19 2071 de enero (GMT).

Consideraciones importantes sobre la replicación

Cuando se establece una relación de SnapMirror con un volumen de origen de SnapLock con una fecha de retención posterior al 19 de enero de 2071 (GMT), el clúster de destino debe ejecutar ONTAP 9.10.1 o una versión posterior, o se producirá un error en la transferencia de SnapMirror.

Consideraciones importantes sobre la reversión

ONTAP le impide revertir un clúster de ONTAP 9.10.1 a una versión anterior de ONTAP cuando hay archivos con un período de retención posterior al "19 de enero de 2071 8:44:07 a. m.".

Descripción de los períodos de retención

Los volúmenes de empresa o de cumplimiento de normativas de SnapLock tienen cuatro períodos de retención:

- Período de retención mínimo (`min`), con un valor por defecto de 0
- Período de retención máximo (`max`), con un valor por defecto de 30 años
- Período de retención predeterminado, con un valor predeterminado igual a `min` para el modo de cumplimiento y el modo de empresa a partir de ONTAP 9.10,1. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el período de retención predeterminado depende del modo:
  - Para el modo Cumplimiento, el valor por defecto es igual a `max`.
  - Para el modo Enterprise, el valor por defecto es igual a `min`.
- Período de retención no especificado.

> En versiones anteriores a ONTAP 9.10.1, si no establece el tiempo de retención explícitamente antes de confirmar un archivo en modo de cumplimiento en el estado WORM y no modifica los valores predeterminados, el archivo se conservará durante 30 años. Este cambio no se puede deshacer. De manera similar, en ONTAP 9.10.1 y versiones posteriores, si no establece el tiempo de retención explícitamente antes de confirmar un archivo en modo Enterprise en el estado WORM y no modifica los valores predeterminados, el archivo se conservará durante 0 años o, efectivamente, no se conservará en absoluto.

A partir de ONTAP 9.8, puede establecer el período de retención de los archivos de un volumen en `unspecified`, para permitir que el archivo se retenga hasta que se establezca un tiempo de retención absoluto. Puede establecer un archivo con tiempo de retención absoluto en retención no especificada y volver a la retención absoluta siempre y cuando el nuevo tiempo de retención absoluto sea posterior al tiempo absoluto establecido anteriormente.

A partir de ONTAP 9.12,1, `unspecified` se garantiza que los archivos WORM con el período de retención definido en tengan un período de retención establecido en el período de retención mínimo configurado para el volumen de SnapLock. Al cambiar el período de retención del archivo de `unspecified` a un tiempo de retención absoluto, el nuevo tiempo de retención especificado debe ser mayor que el tiempo de retención mínimo establecido en el archivo.

Establecer el período de retención predeterminado

Puede usar el `volume snaplock modify` comando para configurar el período de retención predeterminado para los archivos en un volumen de SnapLock.

Antes de empezar

El volumen SnapLock debe estar en línea.

Acerca de esta tarea

En la siguiente tabla se muestran los posibles valores para la opción de período de retención predeterminado:

> El período de retención predeterminado debe ser mayor o igual que (>=) el período de retención mínimo y menor o igual que (<=) el período de retención máximo.

Valor	Unidad	Notas
0 - 65535	segundos	

Valor	Unidad	Notas
0 - 24	horas	
0 - 365	días	
0 - 12	meses	
0 - 100	años	A partir de ONTAP 9.10.1, Para versiones anteriores de ONTAP, el valor es 0 - 70.
capacidad	-	Usar el período de retención máximo.
espacio	-	Use el período de retención mínimo.
infinita	-	Conserve los archivos para siempre.
sin especificar	-	Conserve los archivos hasta que se defina un período de retención absoluto.

Los valores y rangos para los períodos de retención máximo y mínimo son idénticos, excepto para `max` y `min`, que no son aplicables. Para obtener más información sobre esta tarea, consulte "Establezca la visión general de la hora de retención".

Puede usar el `volume snaplock show` comando para ver la configuración del período de retención del volumen. Obtenga más información sobre `volume snaplock show` en el "Referencia de comandos del ONTAP".

Después de que un archivo se haya comprometido con el estado WORM, puede ampliar el período de retención, pero no acortar.

Pasos

1. Establezca el período de retención predeterminado para los archivos en un volumen de SnapLock:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-default -retention-period` *`default_retention_period`* `-minimum-retention-period` *`min_retention_period`* `-maximum-retention-period` *`max_retention_period`*

   Obtenga más información sobre `volume snaplock modify` en el "Referencia de comandos del ONTAP".

   En los siguientes ejemplos se asume que los períodos de retención mínimo y máximo no se han modificado previamente.

El siguiente comando establece el período de retención predeterminado para un volumen de Compliance o Enterprise en 20 días:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period 20days
```

El siguiente comando establece el período de retención predeterminado para un volumen de cumplimiento en 70 años:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
-retention-period 70years
```

El comando siguiente establece el período de retención predeterminado para un volumen de Enterprise en 10 años:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period max -maximum-retention-period 10years
```

Los siguientes comandos establecen el período de retención predeterminado para un volumen de empresa en 10 días:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

El siguiente comando establece el período de retención predeterminado para un volumen de cumplimiento en infinito:

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

Establezca explícitamente el tiempo de retención de un archivo

Puede establecer explícitamente el tiempo de retención de un archivo modificando su última hora de acceso. Puede usar cualquier comando o programa adecuado a través de NFS o CIFS para modificar la última hora de acceso.

Acerca de esta tarea

Después de haber comprometido un archivo con WORM, puede ampliar el tiempo de retención, pero no reducir este. El tiempo de retención se almacena en `atime` el campo del archivo.

No puede definir explícitamente el tiempo de retención de un archivo en `infinite`. Ese valor solo está disponible cuando se utiliza el período de retención predeterminado para calcular el tiempo de retención.

Pasos

1. Utilice un comando o programa adecuado para modificar la última hora de acceso para el archivo cuyo tiempo de retención desee establecer.

   En un shell UNIX, utilice el siguiente comando para establecer un tiempo de retención del 21 de noviembre de 2020 6:00 a.m. en un archivo llamado `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

   Puede utilizar cualquier comando o programa adecuado para modificar la última hora de acceso en Windows.

Establezca el período de retención de archivos después de un evento

A partir de ONTAP 9.3, puede definir cuánto tiempo se retiene un archivo después de que se produzca un evento mediante la función SnapLock *Event Based Retention (EBR)*.

Antes de empezar

- Debe ser un administrador de SnapLock para realizar esta tarea.

  "Cree una cuenta de administrador de SnapLock"

- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Acerca de esta tarea

La directiva *event retention* define el período de retención del archivo después de que se produzca el evento. La directiva se puede aplicar a un único archivo o a todos los archivos de un directorio.

- Si un archivo no es UN archivo WORM, se comprometerá con el estado WORM para el período de retención definido en la política.
- Si un archivo es UN archivo WORM o un archivo ampliable WORM, su período de retención se extenderá por el período de retención que se define en la política.

Puede usar un volumen de modo de cumplimiento o de modo empresarial.

Las políticas de EBR no se pueden aplicar a los archivos de una retención legal.

Para un uso avanzado, consulte "Almacenamiento WORM conforme a la normativa con SnapLock de NetApp".

usar EBR para ampliar el período de retención de archivos WORM ya existentes

EBR resulta muy práctico cuando se desea ampliar el período de retención de archivos WORM ya existentes. Por ejemplo, podría ser la política de su empresa retener los registros del empleado W-4 en forma no modificada durante tres años después de que el empleado cambie una elección de retención. Otra política de la empresa podría requerir que los registros W-4 se retengan durante cinco años después de que el empleado haya terminado.

En este caso, podría crear una política EBR con un período de retención de cinco años. Una vez que el empleado ha terminado (el "'evento'"), aplicaría la política de EBR al registro W-4 del empleado, lo que provocaría que se ampliara su período de retención. Esto suele ser más sencillo que ampliar el período de retención manualmente, especialmente cuando se trata de un gran número de archivos.

Pasos

1. Crear una política EBR:

   `snaplock event-retention policy create -vserver` *`SVM_name`* `-name` *`policy_name`* `-retention-period` *`retention_period`*

   El siguiente comando crea la política EBR `employee_exit` ON `vs1` con un período de retención de diez años:

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. Aplicar una política EBR:

   `snaplock event-retention apply -vserver` *`SVM_name`* `-name` *`policy_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   El siguiente comando aplica la política EBR `employee_exit` `vs1` a todos los archivos del directorio `d1`:

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

Información relacionada

- "Crear política de retención de eventos de Snaplock"
- "Se aplica retención de eventos de Snaplock"

Cree un registro de auditoría protegido con ONTAP SnapLock

Si utiliza ONTAP 9.9.1 o una versión anterior, primero debe crear un agregado de SnapLock y, a continuación, debe crear un registro de auditoría protegido por SnapLock antes de ejecutar una eliminación con privilegios o mover volúmenes de SnapLock. El registro de auditoría registra la creación y eliminación de cuentas de administrador de SnapLock, las modificaciones realizadas en el volumen de registro, si la eliminación con privilegios está habilitada, las operaciones de eliminación con privilegios y las operaciones de movimiento de volúmenes SnapLock.

A partir de ONTAP 9.10.1, ya no se crea un agregado de SnapLock. Debe utilizar la opción -SnapLock-type a "Crear explícitamente un volumen SnapLock"especificando Compliance o Enterprise como tipo SnapLock.

Antes de empezar

Si se utiliza ONTAP 9.9.1 o una versión anterior, debe ser un administrador de clústeres para crear un agregado de SnapLock.

Acerca de esta tarea

No se puede eliminar un registro de auditoría hasta que haya transcurrido el período de retención del archivo de registro. No es posible modificar un registro de auditoría incluso después de transcurrido el período de retención. Esto es así tanto para el modo de cumplimiento de normativas SnapLock como para el modo de empresa.

> En ONTAP 9.4 y versiones anteriores, no se puede usar un volumen de empresa SnapLock para el registro de auditoría. Se debe usar un volumen de cumplimiento de normativas de SnapLock. En ONTAP 9.5 y versiones posteriores, se puede usar un volumen de empresa SnapLock o un volumen de cumplimiento de SnapLock para el registro de auditoría. En todos los casos, el volumen del registro de auditoría debe montarse en la ruta de unión `/snaplock_audit_log` . Ningún otro volumen puede utilizar esta ruta de unión.

Puede encontrar los registros de auditoría de SnapLock en `/snaplock_log` el directorio bajo la raíz del volumen de registro de auditoría, en subdirectorios denominados `privdel_log` (operaciones de eliminación con privilegios) y `system_log` (todo lo demás). Los nombres de archivos de registro de auditoría contienen la Marca de hora de la primera operación de registro, lo que facilita la búsqueda de registros en el momento aproximado en que se ejecutaron las operaciones.

- Puede usar `snaplock log file show` el comando para ver los archivos de registro del volumen de registro de auditoría.
- Puede utilizar `snaplock log file archive` el comando para archivar el archivo de registro actual y crear uno nuevo, lo que resulta útil en los casos en los que necesite registrar la información del registro de auditoría en un archivo independiente.

Obtenga más información sobre `snaplock log file show` y `snaplock log file archive` en el "Referencia de comandos del ONTAP".

> No se puede usar un volumen de protección de datos como volumen de registro de auditoría de SnapLock.

Pasos

1. Cree un agregado de SnapLock.

   Cree un agregado de SnapLock

2. En la SVM que desee configurar para el registro de auditoría, cree un volumen de SnapLock.

   Cree un volumen de SnapLock

3. Configure la SVM para el registro de auditoría:

   ```
   snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
   -size size -retention-period default_retention_period
   ```

> El período de retención mínimo predeterminado para archivos de registro de auditoría es de seis meses. Si el período de retención de un archivo afectado es más largo que el período de retención del registro de auditoría, el período de retención del registro hereda el período de retención del archivo. Por lo tanto, si el período de retención de un archivo eliminado mediante eliminación privilegiada es de 10 meses y el período de retención del registro de auditoría de 8 meses, el período de retención del registro se extiende a 10 meses. Para obtener más información sobre el tiempo de retención y el período de retención por defecto, consulte "Establezca el tiempo de retención".

El siguiente comando configura `SVM1` para el registro de auditorías mediante el volumen de SnapLock `logVol` . El registro de auditoría tiene un tamaño máximo de 20 GB y se conserva durante ocho meses.

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

Obtenga más información sobre `snaplock log create` en el "Referencia de comandos del ONTAP".

4. En la SVM que haya configurado para el registro de auditorías, monte el volumen SnapLock en la ruta de unión `/snaplock_audit_log` .

   Montar un volumen de SnapLock

Verificar la configuración de ONTAP SnapLock

Puede usar `volume file fingerprint start` `volume file fingerprint dump` los comandos y para ver información clave sobre archivos y volúmenes, incluido el tipo de archivo (normal, WORM o WORM aplicable), la fecha de caducidad del volumen, etc.

Pasos

1. Generar una huella digital de archivo:

   ```
   volume file fingerprint start -vserver <SVM_name> -file <file_path>
   ```

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   El comando genera una Session ID que puede usar como entrada del `volume file fingerprint dump` comando.

   > Puede utilizar `volume file fingerprint show` el comando con Session ID para supervisar el progreso de la operación de huella digital. Asegúrese de que la operación haya finalizado antes de intentar mostrar la huella.

2. Mostrar la huella digital del archivo:

`volume file fingerprint dump -session-id <session_ID>`

```
svm1::> volume file fingerprint dump -session-id 33619976
        Vserver:svm1
        Session-ID:33619976
        Volume:slc_vol
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
```

```
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

Gestione los archivos WORM

Administre archivos WORM con ONTAP SnapLock

Puede gestionar archivos WORM de las siguientes formas:

- "Los archivos cumplen CON WORM"
- "Confirma snapshots en WORM en un destino de almacén"
- "Refleje los archivos WORM para la recuperación ante desastres"
- "Conserve los archivos WORM durante su proceso de litigio"
- "Eliminar los archivos WORM"

Confirmar archivos en WORM usando ONTAP SnapLock

Puede confirmar archivos a WORM (escritura única y lectura múltiple) o bien manualmente, o bien conserva los archivos automáticamente. También puede crear archivos flexibles WORM.

Confirmar los archivos a WORM manualmente

Los archivos se comprometen a WORM manualmente haciendo que el archivo sea de solo lectura. Puede utilizar cualquier comando o programa adecuado a través de NFS o CIFS para cambiar el atributo de lectura y escritura de un archivo a sólo lectura. Puede optar por confirmar los archivos manualmente si desea garantizar que una aplicación haya terminado de escribir en un archivo de modo que el archivo no se confirme prematuramente o si hay problemas de escalado para el analizador de compromiso automático debido a un gran número de volúmenes.

Antes de empezar

- El archivo que desea confirmar debe residir en un volumen de SnapLock.
- El archivo debe ser editable.

Acerca de esta tarea

La hora de ComplianceClock del volumen se escribe en `ctime` el campo del archivo cuando se ejecuta el comando o el programa. La hora de la instancia de ComplianceClock determina cuándo se ha alcanzado el tiempo de retención del archivo.

Pasos

1. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura de un archivo a sólo lectura.

   En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` de sólo lectura:

   ```
   chmod -w document.txt
   ```

   En un shell de Windows, utilice el siguiente comando para crear un archivo denominado `document.txt` de sólo lectura:

   ```
   attrib +r document.txt
   ```

Confirmar archivos a WORM automáticamente

La función de compromiso automático de SnapLock le permite confirmar los archivos automáticamente a WORM. La función de compromiso automático confirma el estado DE un archivo CON EL estado WORM en un volumen SnapLock si el archivo no cambió durante el período de compromiso automático. La función de compromiso automático está deshabilitada de forma predeterminada.

Antes de empezar

- Los archivos que desea confirmar automáticamente deben residir en un volumen de SnapLock.
- El volumen SnapLock debe estar en línea.
- El volumen SnapLock debe ser un volumen de lectura/escritura.

> La función SnapLock autocommit analiza todos los archivos del volumen y confirma un archivo si cumple con el requisito de compromiso automático. Es posible que haya un intervalo de tiempo entre cuando el archivo esté listo para la confirmación automática y cuando el escáner de confirmación automática de SnapLock lo confirme realmente. Sin embargo, el sistema de archivos sigue protegiendo el archivo de las modificaciones y eliminaciones en cuanto sea apto para la confirmación automática.

Acerca de esta tarea

El *autocommit Period* especifica la cantidad de tiempo que los archivos deben permanecer sin cambios antes de que se autocompretan. Al cambiar un archivo antes de que haya transcurrido el período de compromiso automático, se reinicia el período de compromiso automático del archivo.

En la siguiente tabla se muestran los posibles valores para el período de compromiso automático:

Valor	Unidad	Notas
ninguno	-	El valor predeterminado.
5 - 5256000	minutos	-
1 - 87600	horas	-

Valor	Unidad	Notas
1 - 3650	días	-
1 - 120	meses	-
1 - 10	años	-

El valor mínimo es de 5 minutos y el valor máximo es de 10 años.

Pasos

1. Los archivos de confirmación automática en un volumen SnapLock a WORM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-autocommit -period` *`autocommit_period`*

   Obtenga más información sobre `volume snaplock modify` en el "Referencia de comandos del ONTAP".

   El siguiente comando confirma automáticamente los archivos en el volumen de `vol1` SVM VS1, siempre y cuando los archivos permanezcan sin cambios durante 5 horas:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
   -period 5hours
   ```

Crear un archivo ampliable WORM

Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Puede utilizar cualquier comando o programa adecuado para crear un archivo que pueda adaptarse A WORM o la función SnapLock *volume append mode* para crear archivos WORM adaptados de forma predeterminada.

Utilice un comando o programa para crear un archivo que puede adaptarse A WORM

Puede utilizar cualquier comando o programa adecuado a través de NFS o CIFS para crear un archivo ampliable WORM. Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Los datos se agregan al archivo en fragmentos de 256 KB. A medida que se escribe cada fragmento, el fragmento anterior se convierte en CON protección WORM. No se puede eliminar el archivo hasta que haya transcurrido el período de retención.

Antes de empezar

El archivo ampliable WORM debe residir en un volumen SnapLock.

Acerca de esta tarea

Los datos no tienen que escribirse secuencialmente en el fragmento de 256 KB activo. Cuando se escriben datos en el byte n×256KB+1 del archivo, el segmento de 256 KB anterior se protege WORM.

Cualquier escritura sin ordenar más allá del fragmento activo actual de 256 KB provocará que el fragmento activo de 256KB KB se restablezca al desplazamiento más reciente y provocará que las escrituras en los

offsets más antiguos fallen con un error de 'Sistema de archivos de solo lectura (ROFS)'. Los desplazamientos de escritura dependen de la aplicación cliente. Un cliente que no cumpla con la semántica de escritura de archivos adjuntos WORM puede provocar una terminación incorrecta del contenido de escritura. Por lo tanto, se recomienda asegurarse de que el cliente siga las restricciones de desplazamiento para las escrituras sin ordenar o garantizar las escrituras síncronas montando el sistema de archivos en modo síncrono.

Pasos

1. Utilice un comando o programa adecuado para crear un archivo de longitud cero con el tiempo de retención deseado.

   En un shell UNIX, utilice el siguiente comando para establecer un tiempo de retención del 21 de noviembre de 2020 6:00 a.m. en un archivo de longitud cero denominado `document.txt`:

   ```
   touch -a -t 202011210600 document.txt
   ```

2. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura del archivo a sólo lectura.

   En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` de sólo lectura:

   ```
   chmod 444 document.txt
   ```

3. Utilice un comando o programa adecuado para cambiar el atributo de lectura y escritura del archivo a grabable.

   > Este paso no se considera un riesgo de cumplimiento de normativas porque no hay datos en el archivo.

   En un shell UNIX, utilice el siguiente comando para crear un archivo denominado `document.txt` editable:

   ```
   chmod 777 document.txt
   ```

4. Utilice un comando o programa adecuado para iniciar la escritura de datos en el archivo.

   En un shell UNIX, utilice el siguiente comando para escribir datos en `document.txt`:

   ```
   echo test data >> document.txt
   ```

   > Vuelva a cambiar los permisos de archivo a sólo lectura cuando ya no necesite agregar datos al archivo.

Use el modo de adición de volúmenes para crear archivos WORM flexibles

A partir de ONTAP 9.3, se puede utilizar la función SnapLock *volume append mode* (VAM) para crear archivos WORM flexibles de forma predeterminada. Un archivo ampliable WORM conserva los datos escritos de forma incremental, como las entradas del registro. Los datos se agregan al archivo en fragmentos de 256 KB. A medida que se escribe cada fragmento, el fragmento anterior se convierte en CON protección WORM. No se puede eliminar el archivo hasta que haya transcurrido el período de retención.

Antes de empezar

- El archivo ampliable WORM debe residir en un volumen SnapLock.
- El volumen SnapLock debe desmontarse y estar vacío de copias Snapshot y archivos creados por el usuario.

Acerca de esta tarea

Los datos no tienen que escribirse secuencialmente en el fragmento de 256 KB activo. Cuando se escriben datos en el byte n×256KB+1 del archivo, el segmento de 256 KB anterior se protege WORM.

Si especifica un período de compromiso automático para el volumen, se comprometen a WORM los archivos flexibles que no se modifican durante un período superior al período de compromiso automático a WORM.

No se admite el VAM en los volúmenes de registros de auditoría de SnapLock.

Pasos

1. Habilitar VAM:

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-is-volume-append -mode-enabled true|false`

   Obtenga más información sobre `volume snaplock modify` en el "Referencia de comandos del ONTAP".

   El siguiente comando habilita VAM en el volumen de `vol1` SVM`vs1`:

   ```
   cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
   -append-mode-enabled true
   ```

2. Utilice un comando o programa adecuado para crear archivos con permisos de escritura.

   De forma predeterminada, los archivos se pueden APPWORM.

Confirmar instantáneas en WORM en un destino de bóveda de ONTAP

Es posible usar SnapLock para SnapVault para proteger WORM en el almacenamiento secundario. Todas las tareas básicas de SnapLock se realizan en el destino del almacén. El volumen de destino se monta automáticamente de solo lectura, por lo que no es necesario comprometer explícitamente las snapshots en WORM.

Antes de empezar

- Si desea usar System Manager para configurar la relación, tanto el clúster de origen como el de destino deben ejecutar ONTAP 9.15.1 o una versión posterior.

- En el clúster de destino:
  - "Instale la licencia de SnapLock".
  - "Inicialice el reloj de cumplimiento".
  - Si utiliza la CLI con una versión de ONTAP anterior a 9.10.1, "Cree un agregado de SnapLock".
- La política de protección debe ser del tipo «vault».
- Los agregados de origen y destino deben tener 64 bits.
- El volumen de origen no puede ser un volumen de SnapLock.
- Si utiliza la CLI de ONTAP, los volúmenes de origen y destino deben crearse en "clústeres con conexión entre iguales" y "SVM".

Acerca de esta tarea

El volumen de origen puede utilizar almacenamiento NetApp o no NetApp .

> No se puede cambiar el nombre de una copia de Snapshot que se confirme en el estado WORM.

Es posible clonar volúmenes de SnapLock, pero no es posible clonar archivos en un volumen de SnapLock.

> Los LUN no son compatibles con los volúmenes de SnapLock. Los LUN solo se admiten en volúmenes de SnapLock en casos en los que las snapshots creadas en un volumen no de SnapLock se transfieren a un volumen de SnapLock para la protección como parte de la relación de almacén de SnapLock. Los LUN no son compatibles con los volúmenes de SnapLock de lectura/escritura. Sin embargo, las copias Snapshot a prueba de manipulación son compatibles tanto con los volúmenes de origen como con los volúmenes de destino de SnapMirror que contienen LUN.

A partir de ONTAP 9.10.1, los volúmenes de SnapLock y otros de SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado de SnapLock separado si se utiliza ONTAP 9.10.1. Puede usar la opción '-snaplock-type' del volumen para especificar un tipo de volumen Compliance o Enterprise SnapLock. En las versiones de ONTAP anteriores a ONTAP 9.10.1, el modo SnapLock, Compliance o Enterprise, se hereda del agregado. No se admiten los volúmenes de destino con versión flexible. La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

Un volumen SnapLock que es un destino de almacén tiene asignado un período de retención predeterminado. El valor correspondiente a este período se establece inicialmente en un mínimo de 0 años para volúmenes de SnapLock Enterprise y un máximo de 30 años para volúmenes de SnapLock Compliance. Cada snapshot de NetApp se confirma con este período de retención predeterminado al principio. El período de retención se puede ampliar más adelante, si fuera necesario. Para obtener más información, consulte "Establecer información general sobre el tiempo de retención".

A partir de ONTAP 9.14.1, puede especificar períodos de retención para etiquetas de SnapMirror específicas en la política de SnapMirror de la relación de SnapMirror, de modo que las snapshots replicadas del volumen de origen al de destino se conserven durante el período de retención especificado en la regla. Si no se especifica ningún período de retención, se utiliza el período de retención predeterminado del volumen de destino.

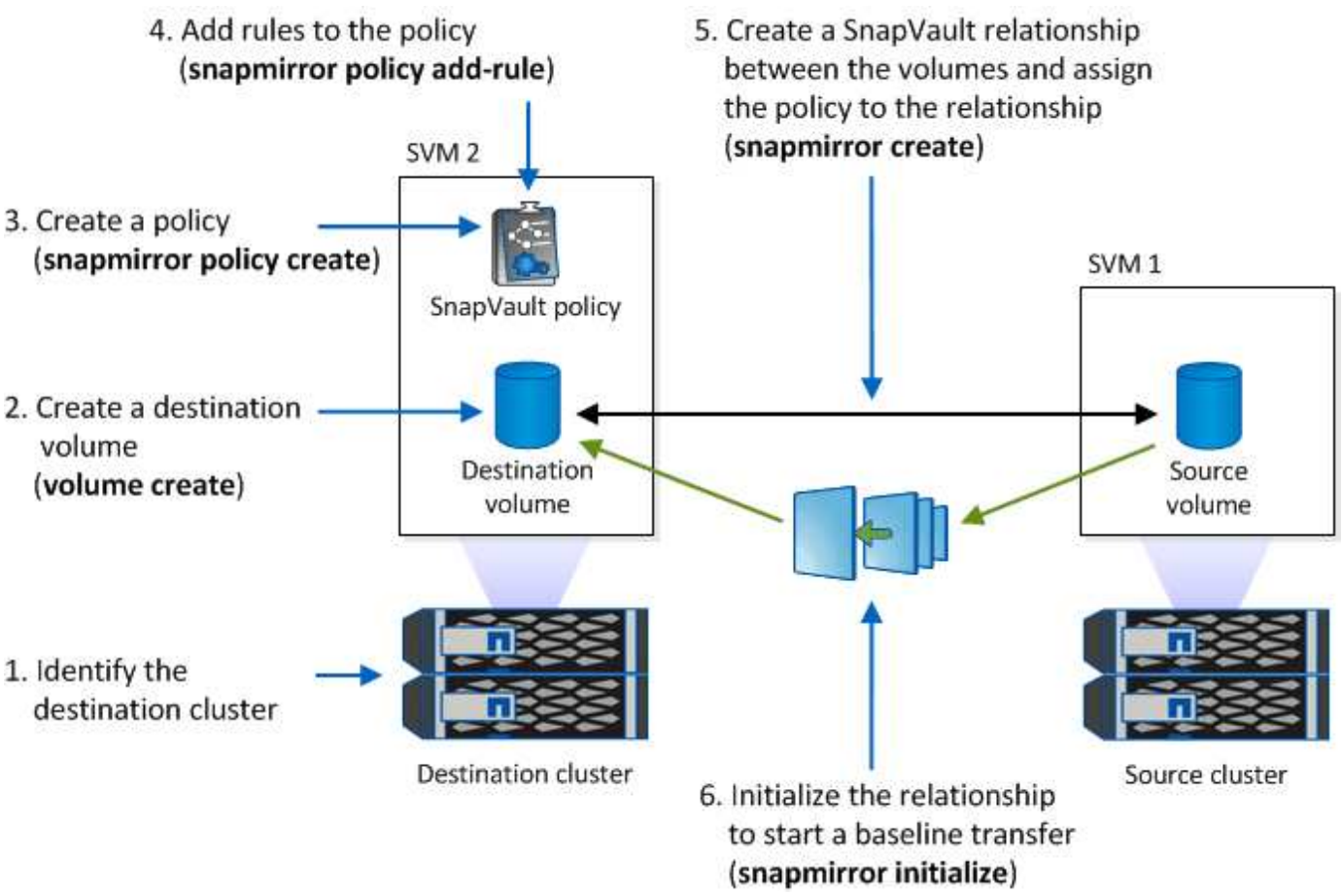
A partir de ONTAP 9.13.1, puede restaurar de forma instantánea una snapshot bloqueada en el volumen de SnapLock de destino de una relación de almacén de SnapLock. Para ello, cree una FlexClone con la opción establecida en `non-snaplock` y especifique la snapshot como la «snapshot principal» al ejecutar la

operación de creación de clones de volúmenes. `snaplock-type` Más información sobre "Creación de un volumen FlexClone con un tipo de SnapLock".

Para las configuraciones de MetroCluster, debe tener en cuenta lo siguiente:

- Solo puede crear relaciones de SnapVault entre varias SVM sincronizada en origen, no entre una SVM sincronizada en origen y una SVM sincronizada en destino.
- Puede crear una relación de SnapVault entre un volumen en una SVM sincronizada en origen y una SVM que sirva datos.
- Puede crear una relación de SnapVault entre un volumen en una SVM que sirva datos y un volumen de DP en una SVM sincronizada en origen.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de almacén de SnapLock:



Pasos

Puede usar la interfaz de línea de comandos de ONTAP para crear una relación de almacén de SnapLock o, a partir de ONTAP 9.15.1, puede usar System Manager para crear una relación de almacén de SnapLock.

System Manager

1. Si el volumen aún no existe, en el clúster de origen, vaya a **Almacenamiento > Volúmenes** y seleccione **Agregar**.
2. En la ventana **Añadir volumen**, selecciona **Más opciones**.
3. Introduzca el nombre del volumen, el tamaño, la política de exportación y el nombre del recurso compartido.
4. Guarde los cambios.
5. En el clúster de destino, vaya a **Protection > Relationships**.
6. Encima de la columna **Fuente**, selecciona **Proteger** y elige **Volúmenes** en el menú.
7. En la ventana **Proteger volúmenes**, selecciona **Vault** como política de protección.
8. En la sección **Source**, seleccione el clúster, la VM de almacenamiento y el volumen que desea proteger.
9. En la sección **Destino**, en **Detalles de configuración**, selecciona **Bloquear instantáneas de destino** y luego selecciona **SnapLock for SnapVault** como método de bloqueo. **El método de bloqueo** no se muestra si el tipo de política seleccionado no es del tipo `vault`, si la licencia de SnapLock no está instalada o si el reloj de cumplimiento no se ha inicializado.
10. Si aún no está habilitado, selecciona **Inicializar reloj de cumplimiento de SnapLock**.
11. Guarde los cambios.

CLI

1. En el clúster de destino, cree un volumen de destino de SnapLock del tipo `DP` que tenga un tamaño igual o mayor que el volumen de origen:

   ```
   volume create -vserver <SVM_name> -volume <volume_name> -aggregate
   <aggregate_name> -snaplock-type <compliance|enterprise> -type DP
   -size <size>
   ```

   El siguiente comando crea un volumen SnapLock Compliance de 2GB GB llamado `dstvolB` `SVM2` en el agregado `node01_aggr`:

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -snaplock-type compliance -type DP -size 2GB
   ```

2. En el clúster de destino, "establezca el período de retención predeterminado".
3. "Cree una nueva relación de replicación" Entre el origen que no es de SnapLock y el nuevo destino de SnapLock que ha creado.

   En este ejemplo, se crea una nueva relación de SnapMirror con el volumen SnapLock de destino `dstvolB` mediante una política de `XDPDefault` almacenar las copias Snapshot etiquetadas diariamente y semanalmente en una programación por hora:

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

"Cree una política de replicación personalizada" o un "programación personalizada" si los valores predeterminados disponibles no son adecuados.

4. En la SVM de destino, inicialice la relación de SnapVault creada:

```
snapmirror initialize -destination-path <destination_path>
```

El siguiente comando inicializa la relación entre el volumen de origen `srcvolA` en `SVM1` y el volumen de destino en `dstvolB` `SVM2`:

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. Una vez inicializada la relación e inactiva, utilice `snapshot show` el comando en el destino para comprobar el tiempo de caducidad del SnapLock aplicado a las copias Snapshot replicadas.

En este ejemplo, se enumeran las Snapshot de volumen `dstvolB` que tienen la etiqueta SnapMirror y la fecha de caducidad de SnapLock:

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

Información relacionada

- "Relaciones entre iguales de clústeres y SVM"
- "Backup de volúmenes mediante SnapVault"
- "inicializar snapmirror"

Refleje archivos WORM con ONTAP SnapMirror para recuperación ante desastres

Puede usar SnapMirror para replicar archivos WORM a otra ubicación geográfica a efectos de recuperación ante desastres y otros fines. Tanto el volumen de origen como el de destino deben configurarse para SnapLock, y ambos volúmenes deben tener el mismo modo SnapLock, Compliance o Enterprise. Se replican todas las propiedades clave de la SnapLock del volumen y los archivos.

Requisitos previos

Los volúmenes de origen y destino deben crearse en clústeres con una relación entre iguales con SVM. Para obtener más información, consulte "Relaciones entre iguales de clústeres y SVM".

Acerca de esta tarea

- A partir de ONTAP 9.5, puede replicar archivos WORM con la relación de tipo XDP (protección de datos ampliada) de SnapMirror en lugar de la relación de tipo DP (protección de datos). El modo XDP es independiente de las versiones de ONTAP y es capaz de diferenciar los archivos almacenados en el mismo bloque, facilitando de este modo la resincronización de los volúmenes replicados de modo de cumplimiento. Para obtener información sobre cómo convertir una relación de tipo DP existente en una relación de tipo XDP, consulte "Protección de datos".
- Una operación de resincronización de tipo DP relación SnapMirror genera un error en un volumen de modo de cumplimiento si SnapLock determina que provocará la pérdida de datos. Si se produce un error en una operación de resincronización, puede usar `volume clone create` el comando para crear un clon del volumen de destino. A continuación, puede volver a sincronizar el volumen de origen con el clon.
- Una relación SnapMirror de un volumen SnapLock solo admite la `MirrorAllSnapshots` política de tipo async-mirror. El período de retención de un volumen SnapLock está determinado por el período de retención máximo entre todos los archivos WORM que contiene. Dado que el destino es una copia DR del origen, el período de retención del volumen SnapLock de destino será el mismo que el del origen.
- Una relación de SnapMirror del tipo XDP entre volúmenes compatibles con SnapLock admite una resincronización después de una interrupción aunque los datos del destino hayan divergido del origen posterior a la interrupción.

  En un resincronización, cuando se detecta una divergencia de datos entre el destino de origen más allá de la instantánea común, se corta una nueva instantánea en el destino para capturar esta divergencia. La nueva snapshot y la snapshot común están bloqueadas con un tiempo de retención de la siguiente manera:

  - La hora de caducidad del volumen del destino
  - Si el tiempo de caducidad del volumen es pasado o no se ha establecido, la copia de Snapshot se bloquea durante un período de 30 días
  - Si el destino tiene una conservación legal, el período de caducidad del volumen real se oculta y se muestra como "indefinido"; sin embargo, la instantánea se bloquea durante el período de caducidad real del volumen.

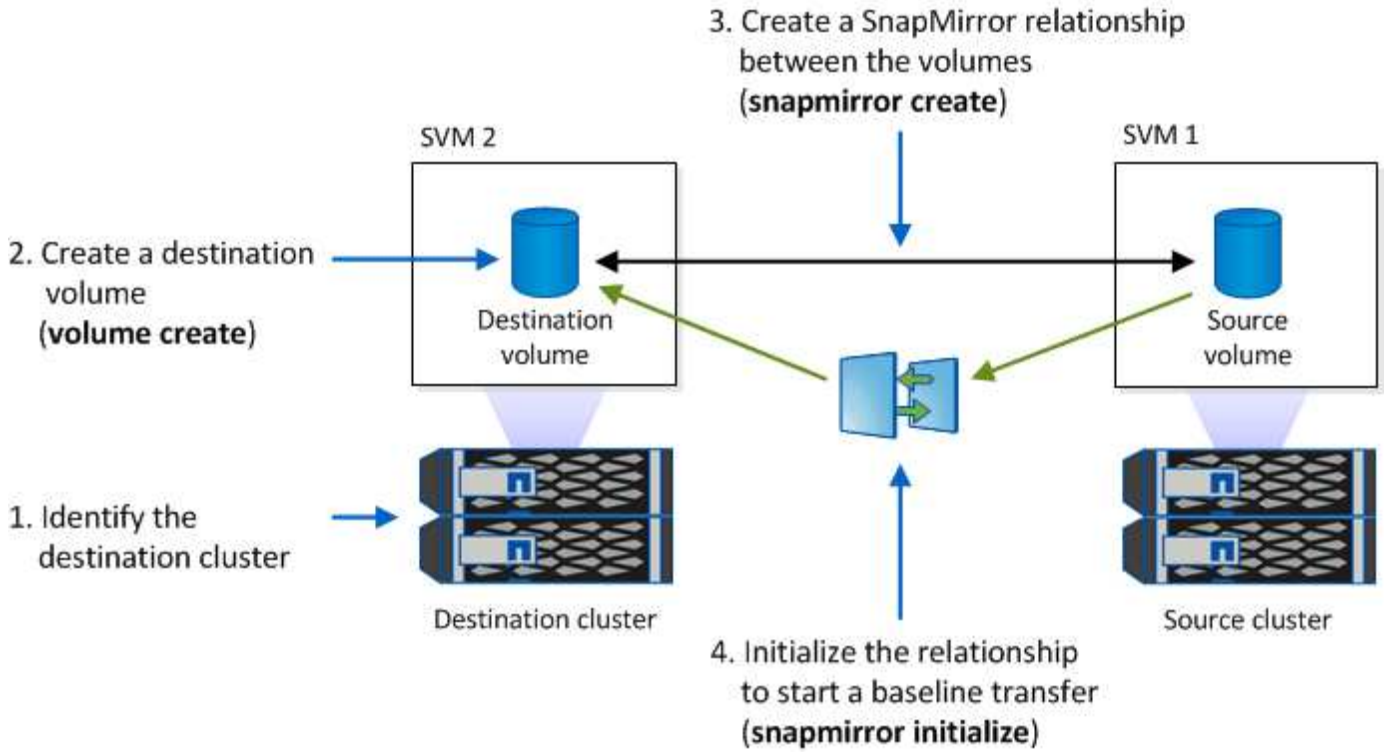
Si el volumen de destino tiene un período de caducidad posterior al origen, se conserva el período de caducidad del destino y no se sobrescribe con el período de caducidad del volumen de origen posterior a la resincronización.

Si el destino tiene retenciones legales en él que difieren de la fuente, no se permite una resincronización. El origen y el destino deben tener idénticas retenciones legales o todas las retenciones legales del destino deben liberarse antes de intentar realizar una resincronización.

Una instantánea bloqueada en el volumen de destino creada para capturar los datos divergentes se puede copiar al origen mediante la CLI ejecutando el comando. `snapmirror update -s snapshot` La instantánea una vez copiada seguirá bloqueada en la fuente.

- No se admiten las relaciones de protección de datos de SVM.
- No se admiten las relaciones de protección de datos con uso compartido de carga.

En la siguiente ilustración, se muestra el procedimiento para inicializar una relación de SnapMirror:


3. Create a SnapMirror relationship between the volumes (**snapmirror create**)
SVM 2
SVM 1
2. Create a destination volume (**volume create**)
Destination volume
Source volume
1. Identify the destination cluster
Destination cluster
Source cluster
4. Initialize the relationship to start a baseline transfer (**snapmirror initialize**)

System Manager

A partir de ONTAP 9.12.1, puede usar System Manager para configurar la replicación de SnapMirror de archivos WORM.

Pasos

1. Vaya a **almacenamiento > volúmenes**.
2. Haga clic en **Mostrar/Ocultar** y seleccione **Tipo de SnapLock** para visualizar la columna en la ventana **volúmenes**.
3. Busque un volumen de SnapLock.
4. Haga clic ⋮ y seleccione **Proteger**.
5. Elija el clúster de destino y la máquina virtual de almacenamiento de destino.
6. Haga clic en **más opciones**.
7. Seleccione **Mostrar políticas heredadas** y seleccione **DPDefault (Legacy)**.
8. En la sección **Detalles de la configuración de destino**, seleccione **Anular programa de transferencia** y seleccione **por hora**.
9. Haga clic en **Guardar**.
10. A la izquierda del nombre del volumen de origen, haga clic en la flecha para expandir los detalles del volumen y, en el lado derecho de la página, consulte los detalles de la protección remota de SnapMirror.
11. En el clúster remoto, vaya a **Relaciones de protección**.
12. Busque la relación y haga clic en el nombre del volumen de destino para ver los detalles de la relación.
13. Compruebe que el tipo de SnapLock del volumen de destino y otra información de SnapLock.

CLI

1. Identifique el clúster de destino.
2. En el clúster de destino, "Instale la licencia de SnapLock" "Inicialice el reloj de cumplimiento", y, si utiliza una versión de ONTAP anterior a 9.10.1, "Cree un agregado de SnapLock".
3. En el clúster de destino, cree un volumen de destino de SnapLock del tipo `DP` que tenga el mismo tamaño o mayor que el volumen de origen:

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate
   aggregate_name -snaplock-type compliance|enterprise -type DP -size size
   ```

   > ⓘ A partir de ONTAP 9.10.1, los volúmenes SnapLock y no SnapLock pueden existir en el mismo agregado; por lo tanto, ya no es necesario crear un agregado SnapLock separado si está usando ONTAP 9.10.1. Utilice la opción de volumen -snaplock-type para especificar un tipo de volumen SnapLock de cumplimiento o empresarial. En versiones de ONTAP anteriores a ONTAP 9.10.1, el modo SnapLock (Cumplimiento o Empresa) se hereda del agregado. La configuración de idioma del volumen de destino debe coincidir con la configuración de idioma del volumen de origen.

   El siguiente comando crea un `Compliance` volumen SnapLock de 2 GB llamado `dstvolB SVM2` en el agregado `node01_aggr`:

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

4. En la SVM de destino, cree una política de SnapMirror:

   `snapmirror policy create -vserver` *`SVM_name`* `-policy` *`policy_name`*

   El siguiente comando crea la política para toda la SVM `SVM1-mirror` :

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. En la SVM de destino, cree una programación de SnapMirror:

   `job schedule cron create -name` *`schedule_name`* `-dayofweek` *`day_of_week`* `-hour` *`hour`* `-minute` *`minute`*

   El siguiente comando crea una programación de SnapMirror llamada `weekendcron`:

```
SVM2::> job schedule cron create -name weekendcron -dayofweek
"Saturday, Sunday" -hour 3 -minute 0
```

6. En la SVM de destino, cree una relación de SnapMirror:

   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-type XDP|DP -policy` *`policy_name`* `-schedule` *`schedule_name`*

   El siguiente comando crea una relación de SnapMirror entre el volumen de origen `srcvolA` en `SVM1` y el volumen de destino `dstvolB` en `SVM2`, y asigna la política `SVM1-mirror` y la programación `weekendcron`:

```
SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
weekendcron
```

   > El tipo XDP está disponible en ONTAP 9.5 y posterior. Debe usar el tipo de DP en ONTAP 9.4 y versiones anteriores.

7. En la SVM de destino, inicialice la relación de SnapMirror:

   `snapmirror initialize -destination-path` *`destination_path`*

   El proceso de inicialización realiza una *transferencia basal* al volumen de destino. SnapMirror realiza una copia Snapshot del volumen de origen y, luego, transfiere la copia y todos los bloques de datos a los que hace referencia al volumen de destino. También transfiere todas las otras copias de Snapshot del volumen de origen al volumen de destino.

El siguiente comando inicializa la relación entre el volumen de origen `srcvolA` en `SVM1` y el volumen de destino en `dstvolB` `SVM2`:

```
SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
```

Información relacionada

- "Relaciones entre iguales de clústeres y SVM"
- "Preparación para la recuperación ante desastres de volúmenes"
- "Protección de datos"
- "snapmirror create"
- "inicializar snapmirror"
- "Crear política de SnapMirror"

Conserve los archivos WORM durante el litigio utilizando ONTAP SnapLock Legal Hold

A partir de ONTAP 9.3, puede conservar archivos WORM en modo de cumplimiento durante un litigio con la función *Legal Hold*.

Antes de empezar

- Debe ser un administrador de SnapLock para realizar esta tarea.

  "Cree una cuenta de administrador de SnapLock"

- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Acerca de esta tarea

Un archivo de retención legal se comporta como un archivo WORM con un período de retención indefinido. Es su responsabilidad especificar cuándo termina el período de retención legal.

El número de archivos que se pueden colocar en una conservación legal depende del espacio disponible en el volumen.

Pasos

1. Inicie una conservación legal:

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   El siguiente comando inicia una retención legal para todos los archivos de `vol1`:

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. Terminar una conservación legal:

```
snaplock legal-hold end -litigation-name <litigation_name> -volume
<volume_name> -path <path_name>
```

El siguiente comando finaliza una retención legal para todos los archivos de `vol1`:

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

Información relacionada

- "inicio de retención legal con cierre a presión"
- "extremo de sujeción legal con cierre a presión"

Eliminar archivos WORM con ONTAP SnapLock

Puede eliminar archivos WORM en modo de empresa durante el período de retención mediante la función de eliminación con privilegios. Antes de poder usar esta función, debe crear una cuenta de administrador de SnapLock y, a continuación, utilizar la cuenta, habilitar la función.

Cree una cuenta de administrador de SnapLock

Para realizar una eliminación con privilegios, debe tener privilegios de administrador de SnapLock. Estos privilegios se definen en el rol vsadmin-snaplock. Si todavía no ha asignado ese rol, puede solicitar al administrador de clúster que cree una cuenta de administrador de SVM con el rol de administrador de SnapLock.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Pasos

1. Cree una cuenta de administrador de SVM con el rol de administrador de SnapLock:

   security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment

   El siguiente comando habilita la cuenta de administrador de SVM `SnapLockAdmin` con el `vsadmin-snaplock` rol predefinido para acceder `SVM1` con una contraseña:

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

   Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

Active la función de eliminación con privilegios

Debe habilitar explícitamente la función de eliminación con privilegios en el volumen de Enterprise que contiene los archivos WORM que desea eliminar.

Acerca de esta tarea

El valor de `-privileged-delete` la opción determina si la supresión con privilegios está activada. Los valores posibles son `enabled` `disabled` , y `permanently-disabled`.

> `permanently-disabled` es el estado del terminal. No puede habilitar la eliminación con privilegios en el volumen después de establecer el estado en `permanently-disabled`.

Pasos

1. Habilitar la eliminación con privilegios para un volumen de SnapLock Enterprise:

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   El siguiente comando activa la función DELETE con privilegios para el volumen de Enterprise `dataVol` en `SVM1`:

   ```
   SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
   -delete enabled
   ```

Elimine los archivos WORM de modo empresarial

Puede utilizar la función de eliminación con privilegios para eliminar archivos WORM en modo de empresa durante el período de retención.

Antes de empezar

- Debe ser un administrador de SnapLock para realizar esta tarea.
- Debe haber creado un registro de auditoría de SnapLock y habilitado la función de eliminación privilegiada en el volumen empresarial.

Acerca de esta tarea

No puede utilizar una operación de eliminación privilegiada para eliminar un archivo WORM caducado. Puede usar el `volume file retention show` comando para ver el tiempo de retención del ARCHIVO WORM que desea eliminar. Obtenga más información sobre `volume file retention show` en el "Referencia de comandos del ONTAP".

Paso

1. Eliminar un archivo WORM en un volumen empresarial:

   volume file privileged-delete -vserver *SVM_name* -file *file_path*

   El siguiente comando elimina el archivo de `/vol/dataVol/f1` la SVM`SVM1`:

```
SVM1::> volume file privileged-delete -file /vol/dataVol/f1
```

Mover un volumen SnapLock de ONTAP

A partir de ONTAP 9.8, puede mover un volumen SnapLock a un agregado de destino del mismo tipo, ya sea de empresa a empresa o de cumplimiento de normativas. Debe tener asignado el rol de seguridad SnapLock para mover un volumen de SnapLock.

Cree una cuenta de administrador de seguridad de SnapLock

Debe tener privilegios de administrador de seguridad de SnapLock para realizar un movimiento de volúmenes de SnapLock. Este privilegio se le concede con el rol *SnapLock*, introducido en ONTAP 9.8. Si todavía no ha recibido ese rol, puede solicitar al administrador del clúster que cree un usuario de seguridad SnapLock con este rol de seguridad SnapLock.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Debe haber iniciado sesión en una conexión segura (SSH, Console o ZAPI).

Acerca de esta tarea

El rol SnapLock se asocia con la SVM de administrador, a diferencia del rol vsadmin-snaplock, que está asociada con la SVM de datos.

Paso

1. Cree una cuenta de administrador de SVM con el rol de administrador de SnapLock:

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   El siguiente comando habilita la cuenta de administrador de SVM `SnapLockAdmin` con `snaplock` el rol predefinido para acceder a la SVM de administrador `cluster1` con una contraseña:

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

   Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

Mover un volumen de SnapLock

Puede utilizar `volume move` el comando para mover un volumen de SnapLock a un agregado de destino.

Antes de empezar

- Debe haber creado un registro de auditoría protegido en SnapLock antes de ejecutar el movimiento de volúmenes de SnapLock.

  "Cree un registro de auditoría".

- Si utiliza una versión de ONTAP anterior a ONTAP 9.10.1, el agregado de destino debe ser el mismo tipo de SnapLock que el volumen de SnapLock que desea mover: Compliance to Compliance o Enterprise to Enterprise. A partir de ONTAP 9.10.1, esta restricción se elimina y un agregado puede incluir volúmenes SnapLock de Compliance y Enterprise, así como volúmenes que no son de SnapLock.
- Debe haberse registrado como usuario con el rol de seguridad SnapLock.

Pasos

1. Con una conexión segura, inicie sesión en la LIF de gestión de clústeres de ONTAP:

   ```
   ssh snaplock_user@cluster_mgmt_ip
   ```

2. Mover un volumen de SnapLock:

   ```
   volume move start -vserver SVM_name -volume SnapLock_volume_name -destination
   -aggregate destination_aggregate_name
   ```

3. Compruebe el estado de la operación de movimiento de volúmenes:

   ```
   volume move show -volume SnapLock_volume_name -vserver SVM_name -fields
   volume,phase,vserver
   ```

Bloquear una instantánea de ONTAP para protegerse contra ataques de ransomware

A partir de ONTAP 9.12.1, puede bloquear una copia Snapshot en un volumen no perteneciente a SnapLock para proporcionar protección contra ataques de ransomware. El bloqueo de instantáneas garantiza que no se puedan eliminar por accidente o de forma malintencionada.

Puede utilizar la función de reloj de SnapLock Compliance para bloquear las instantáneas durante un período especificado, de modo que no se puedan eliminar hasta que se alcance la hora de caducidad. Bloquear snapshots las copias snapshot las protege frente a cualquier manipulación y las protege de las amenazas de ransomware. Puede usar snapshots bloqueados para recuperar datos si un volumen se ve afectado por un ataque de ransomware.

A partir de ONTAP 9.14.1, el bloqueo de copias Snapshot es compatible con instantáneas de retención a largo plazo en destinos de almacenes SnapLock y en volúmenes de destino no SnapLock SnapMirror. El bloqueo de instantáneas se activa mediante la definición del período de retención mediante las reglas de política de SnapMirror asociadas a un etiqueta de política existente. La regla anula el período de retención predeterminado establecido en el volumen. Si no existe un período de retención asociado con la etiqueta de SnapMirror, se utiliza el período de retención predeterminado del volumen.

Requisitos y consideraciones de Snapshot a prueba de manipulación

- Si utiliza la CLI de ONTAP, todos los nodos del clúster deben ejecutar ONTAP 9.12.1 o una versión posterior. Si utiliza System Manager, todos los nodos deben ejecutar ONTAP 9.13.1 o una versión posterior.
- "La licencia de SnapLock debe instalarse en el clúster". Esta licencia está incluida en "ONTAP One".
- "Es necesario inicializar el reloj de cumplimiento de normativas del clúster".
- Cuando se habilita el bloqueo de snapshots en un volumen, se pueden actualizar los clústeres a una versión de ONTAP posterior a ONTAP 9.12.1. Sin embargo, no se puede revertir a una versión anterior de

ONTAP hasta que todas las Snapshot bloqueadas hayan alcanzado su fecha de caducidad, se eliminen y se deshabilite el bloqueo de snapshots.

- Cuando una copia de Snapshot está bloqueada, la hora de caducidad del volumen se establece en la hora de caducidad de la copia de Snapshot. Si más de una instantánea está bloqueada, el tiempo de caducidad del volumen refleja el mayor tiempo de caducidad de todas las instantáneas.
- El período de retención para instantáneas bloqueadas tiene prioridad sobre el recuento de instantáneas guardadas, lo que significa que no se respeta el límite de mantenimiento de recuento si el período de retención de instantáneas para instantáneas bloqueadas no ha caducado.
- En una relación de SnapMirror, se puede establecer un período de retención en una regla de política de reflejo-almacén y el período de retención se aplica a las copias de Snapshot replicadas en el destino si el volumen de destino tiene bloqueo de Snapshot habilitado. El período de retención tiene prioridad sobre el recuento KEEP; por ejemplo, las instantáneas que no hayan superado su caducidad se conservarán incluso si se supera el recuento KEEP.
- Es posible cambiar el nombre de una copia Snapshot en un volumen que no sea de SnapLock. Las operaciones de cambio de nombre de Snapshot en el volumen primario de una relación de SnapMirror se reflejan en el volumen secundario solo si la política es MirrorAllSnapshots. Para otros tipos de directivas, la instantánea a la que se ha cambiado el nombre no se propaga durante las actualizaciones.
- Si utiliza la CLI de ONTAP, puede restaurar una instantánea bloqueada con el `volume snapshot restore` comando solo si la instantánea bloqueada es la más reciente. Si hay alguna instancia de Snapshot sin caducar más tarde que la que se está restaurando, la operación de restauración de Snapshot falla.

Funciones compatibles con instantáneas a prueba de manipulaciones

- "Cloud Volumes ONTAP"
- Volúmenes de FlexGroup

  Se admite el bloqueo de snapshots en los volúmenes de FlexGroup. El bloqueo de instantáneas sólo se produce en la instantánea del componente raíz. Solo se permite eliminar el volumen FlexGroup si ha transcurrido el tiempo de caducidad del componente raíz.

- Conversión de FlexVol a FlexGroup

  Es posible convertir un FlexVol volume con copias Snapshot bloqueadas en un volumen de FlexGroup. Las instantáneas permanecen bloqueadas después de la conversión.

- SnapMirror asíncrono

  El reloj de cumplimiento debe inicializarse tanto en el origen como en el destino.

- Movilidad de datos de SVM (se usa para migrar o reubicar una SVM desde un clúster de origen a un clúster de destino)

  Compatible a partir de ONTAP 9.14.1.

- Reglas de política de SnapMirror con `-schedule` el parámetro
- DR DE SVM

  El reloj de cumplimiento debe inicializarse tanto en el origen como en el destino.

- Clon de volumen y clon de archivo

  Es posible crear clones de volúmenes y archivos a partir de una copia de Snapshot bloqueada.

- Volúmenes de FlexCache

  Compatible a partir de ONTAP 9.16.1.

Funciones no admitidas

Actualmente, las siguientes funciones no se admiten con instantáneas a prueba de manipulaciones:

- Grupos de consistencia
- "FabricPool"

  Las instantáneas a prueba de manipulaciones proporcionan protecciones inmutables que no se pueden eliminar. Dado que FabricPool necesita la capacidad para eliminar datos, no se podrán habilitar los bloqueos de instantáneas y FabricPool en el mismo volumen.

- SMTape
- SnapMirror síncrono activo
- SnapMirror síncrono

Active el bloqueo de instantáneas al crear un volumen

A partir de ONTAP 9.12.1, puede habilitar el bloqueo de snapshots al crear un volumen nuevo o cuando se modifica un volumen existente con la opción con `volume create` los comandos y `volume modify` de la CLI. `-snapshot-locking-enabled` A partir de ONTAP 9.13.1, se puede usar System Manager para habilitar el bloqueo de snapshots.

System Manager

1. Navegue hasta **Almacenamiento > Volúmenes** y seleccione **Agregar**.
2. En la ventana **Añadir volumen**, selecciona **Más opciones**.
3. Introduzca el nombre del volumen, el tamaño, la política de exportación y el nombre del recurso compartido.
4. Selecciona **Habilitar Bloqueo de instantáneas**. Esta selección no se muestra si la licencia de SnapLock no está instalada.
5. Si aún no está habilitado, selecciona **Inicializar reloj de cumplimiento de SnapLock**.
6. Guarde los cambios.
7. En la ventana **Volúmenes**, selecciona el volumen que actualizaste y selecciona **Resumen**.
8. Compruebe que **SnapLock Bloqueo de instantáneas** se muestra como **habilitado**.

CLI

1. Para crear un volumen nuevo y habilitar el bloqueo de instantáneas, escriba el siguiente comando:

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

   El siguiente comando habilita el bloqueo Snapshot en un nuevo volumen llamado vol1:

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: snapshot locking is being enabled on volume "vol1" in
   Vserver "vs1". It cannot be disabled until all locked snapshots are
   past their expiry time. A volume with unexpired locked snapshots
   cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

Active el bloqueo de instantáneas en un volumen existente

A partir de ONTAP 9.12.1, puede habilitar el bloqueo de snapshots en un volumen existente mediante la interfaz de línea de comandos de ONTAP. A partir de ONTAP 9.13.1, puede usar System Manager para habilitar el bloqueo de instantáneas en un volumen existente.

System Manager

1. Vaya a **almacenamiento > volúmenes**.
2. Selecciona ⋮ y selecciona **Editar > Volumen**.
3. En la ventana **Editar volumen**, localice la sección Ajustes de instantáneas (locales) y seleccione **Habilitar bloqueo de instantáneas**.

   Esta selección no se muestra si la licencia de SnapLock no está instalada.
4. Si aún no está habilitado, selecciona **Inicializar reloj de cumplimiento de SnapLock**.
5. Guarde los cambios.
6. En la ventana **Volúmenes**, selecciona el volumen que actualizaste y selecciona **Resumen**.
7. Verifique que la opción **Bloqueo de instantáneas SnapLock * se muestre como *Habilitado**.

CLI

1. Para modificar un volumen existente y habilitar el bloqueo Snapshot, introduzca el siguiente comando:

   ```
   volume modify -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

Crear una política de instantáneas bloqueadas y aplicar retención

A partir de ONTAP 9.12.1, puede crear políticas de Snapshot para aplicar un período de retención de Snapshot y aplicar la política a un volumen para bloquear las copias de Snapshot durante el período especificado. También es posible bloquear una copia de Snapshot mediante la configuración manual de un período de retención. A partir de ONTAP 9.13.1, puede usar System Manager para crear políticas de bloqueo de snapshots y aplicarlas a un volumen.

Cree una política de bloqueo de instantáneas

System Manager

1. Vaya a **Storage > Storage VMs** y seleccione una VM de almacenamiento.
2. Selecciona **Ajustes**.
3. Localice **Políticas de instantánea** y seleccione →.
4. En la ventana **Add Snapshot Policy**, introduzca el nombre de la política.
5. Seleccione + Add .
6. Proporcione los detalles de la programación de Snapshot, incluido el nombre de la programación, el número máximo de Snapshot que se deben conservar y el período de retención de SnapLock.
7. En la columna **SnapLock Retention Period**, introduzca el número de horas, días, meses o años para retener las instantáneas. Por ejemplo, una política de Snapshot con un período de retención de 5 días bloquea una snapshot durante 5 días desde el momento en que se creó y no se puede eliminar durante ese periodo. Se admiten los siguientes rangos de períodos de retención:
   - Años: 0 - 100
   - Meses: 0 - 1200
   - Días: 0 - 36500
   - Horario: 0 - 24
8. Guarde los cambios.

CLI

1. Para crear una política de Snapshot, introduzca el siguiente comando:

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   El siguiente comando crea una política de bloqueo de instantáneas:

   ```
   cluster1> volume snapshot policy create -policy lock_policy -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   Una instantánea no se sustituye si se encuentra bajo retención activa; es decir, el recuento de retención no se respetará si hay instantáneas bloqueadas que aún no han caducado.

Aplicar una política de bloqueo a un volumen

System Manager

1. Vaya a **almacenamiento > volúmenes**.
2. Selecciona ⋮ y selecciona **Editar > Volumen**.
3. En la ventana **Editar volumen**, selecciona **Programar instantáneas**.
4. Seleccione la política de instantáneas de bloqueo de la lista.
5. Si el bloqueo de instantáneas aún no está activado, seleccione **Activar bloqueo de instantáneas**.
6. Guarde los cambios.

CLI

1. Para aplicar una política de bloqueo de Snapshot a un volumen existente, introduzca el siguiente comando:

```
volume modify -volume <volume_name> -vserver <vserver_name> -snapshot
-policy <policy_name>
```

Aplicar período de retención durante la creación manual de instantáneas

Es posible aplicar el período de retención de Snapshot cuando se crea manualmente una copia de Snapshot. Debe estar habilitado el bloqueo de snapshots en el volumen; de lo contrario, se ignorará la configuración del período de retención.

System Manager

1. Navegue hasta **Almacenamiento > Volúmenes** y seleccione un volumen.
2. En la página de detalles del volumen, seleccione la pestaña **Snapshots**.
3. Seleccione + Add .
4. Introduzca el nombre de la snapshot y la hora de caducidad del SnapLock. Puede seleccionar el calendario para elegir la fecha y la hora de caducidad de la retención.
5. Guarde los cambios.
6. En la página **Volúmenes > Instantáneas**, seleccione **Mostrar/Ocultar** y elija **Tiempo de caducidad de SnapLock** para mostrar la columna **Tiempo de caducidad de SnapLock** y verifique que el tiempo de retención esté establecido.

CLI

1. Para crear una instantánea manualmente y aplicar un período de retención de bloqueo, introduzca el siguiente comando:

   ```
   volume snapshot create -volume <volume_name> -snapshot <snapshot name>
   -snaplock-expiry-time <expiration_date_time>
   ```

   El siguiente comando crea una nueva copia de Snapshot y configura el período de retención:

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Aplicar el período de retención a una instantánea existente

System Manager

1. Navegue hasta **Almacenamiento > Volúmenes** y seleccione un volumen.
2. En la página de detalles del volumen, seleccione la pestaña **Snapshots**.
3. Seleccione la instantánea, seleccione ⋮ y elija **Modificar hora de caducidad de SnapLock**. Puede seleccionar el calendario para elegir la fecha y la hora de caducidad de la retención.
4. Guarde los cambios.
5. En la página **Volúmenes > Instantáneas**, seleccione **Mostrar/Ocultar** y elija **Tiempo de caducidad de SnapLock** para mostrar la columna **Tiempo de caducidad de SnapLock** y verifique que el tiempo de retención esté establecido.

CLI

1. Para aplicar manualmente un período de retención a una snapshot existente, introduzca el siguiente comando:

   ```
   volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot
   <snapshot name> -snaplock-expiry-time <expiration_date_time>
   ```

   En el siguiente ejemplo se aplica un período de retención a una copia de Snapshot existente:

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

Modifique una política existente para aplicar la retención a largo plazo

En una relación de SnapMirror, se puede establecer un período de retención en una regla de política de reflejo-almacén y el período de retención se aplica a las copias de Snapshot replicadas en el destino si el volumen de destino tiene bloqueo de Snapshot habilitado. El período de retención tiene prioridad sobre el recuento KEEP; por ejemplo, las instantáneas que no hayan superado su caducidad se conservarán incluso si se supera el recuento KEEP.

A partir de ONTAP 9.14.1, puede modificar una política de SnapMirror existente añadiendo una regla para establecer la retención a largo plazo de copias Snapshot. La regla se utiliza para anular el período de retención de volúmenes predeterminado en destinos de almacén de SnapLock y en volúmenes de destino que no son de SnapMirror de SnapLock.

1. Agregue una regla a una política de SnapMirror existente:

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of snapshots> -retention-period
   [<integer> days|months|years]
   ```

   En el siguiente ejemplo se crea una regla que aplica un período de retención de 6 meses a la política existente denominada «lockvault»:

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

Obtenga más información sobre `snapmirror policy add-rule` en el "Referencia de comandos del ONTAP".

Grupos de consistencia

Obtenga más información sobre los grupos de consistencia de ONTAP

Un grupo de coherencia es una recogida de volúmenes que se gestionan como una sola unidad. En ONTAP, los grupos de coherencia proporcionan una gestión fácil y una garantía de protección para una carga de trabajo de la aplicación que abarca varios volúmenes.

Puede utilizar grupos de consistencia para simplificar la gestión del almacenamiento. Imagine que dispone de una base de datos importante que abarca veinte LUN. Puede administrar las LUN de forma individual o tratar las LUN como un conjunto de datos solitario, organizándolas en un único grupo de consistencia.

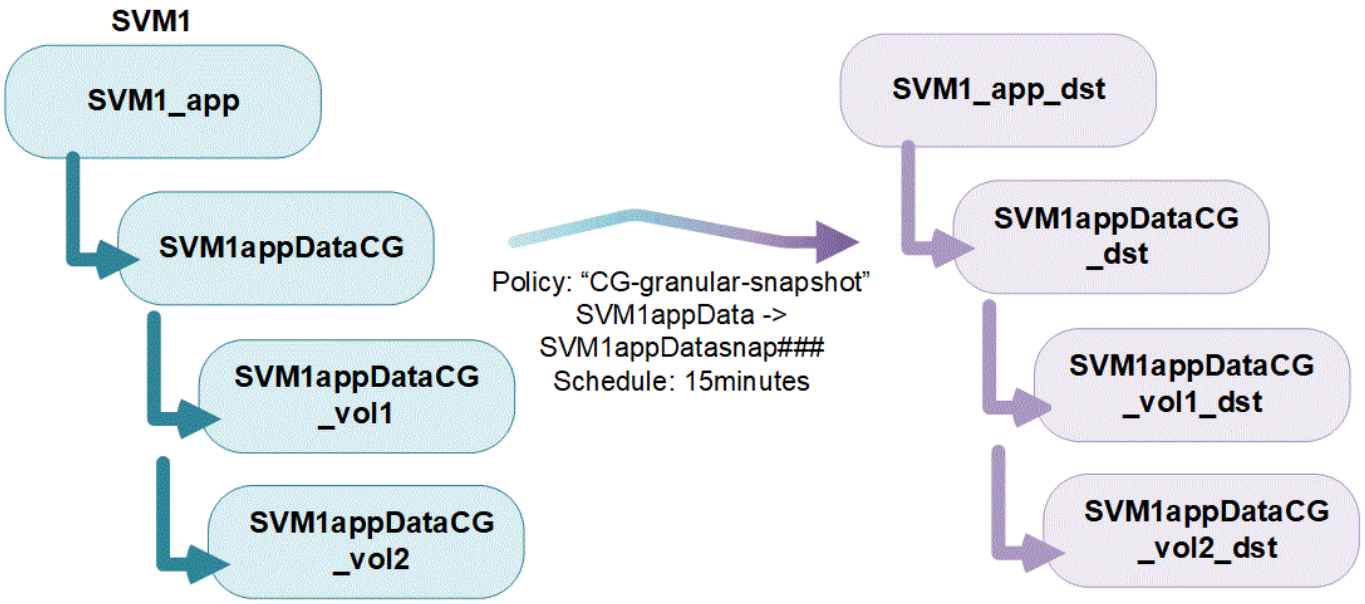
Los grupos de coherencia facilitan la gestión de cargas de trabajo de aplicaciones, proporcionando políticas de protección local y remota fáciles de configurar, así como copias Snapshot simultáneas consistentes con las aplicaciones y con los fallos de una colección de volúmenes en un momento específico. Las snapshots de un grupo de coherencia permiten restaurar una carga de trabajo de la aplicación completa.

Obtenga más información sobre los grupos de consistencia

Los grupos de consistencia admiten cualquier volumen de FlexVol independientemente del protocolo (NAS, SAN o NVMe) y pueden gestionarse a través de la API REST de ONTAP o en System Manager, en el elemento de menú **almacenamiento > grupos de consistencia**. A partir de ONTAP 9.14.1, los grupos de consistencia se pueden administrar con la CLI de ONTAP.

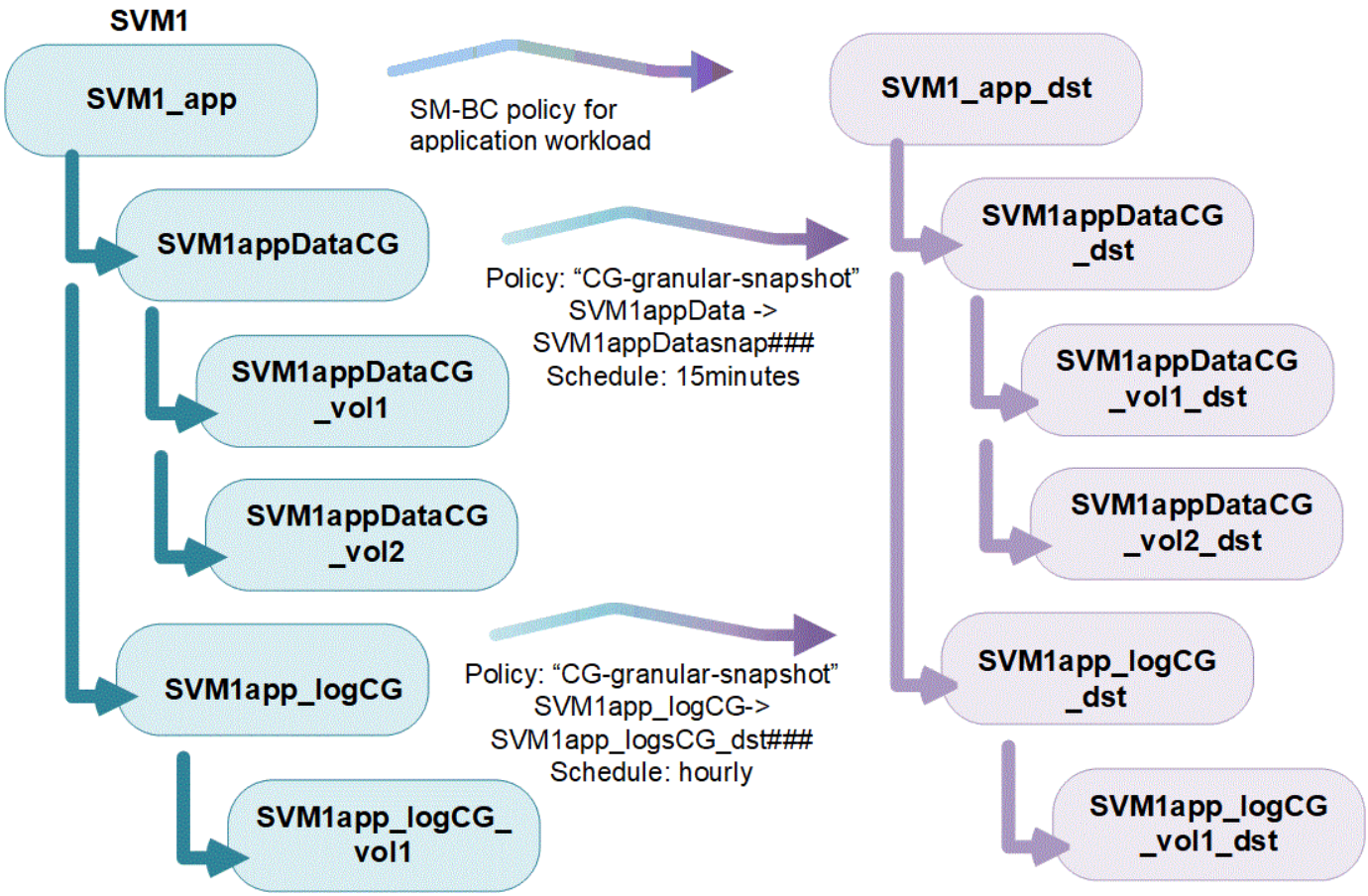
Los grupos de consistencia pueden existir como entidades individuales (como una colección de volúmenes) o en una relación jerárquica, que consiste en otros grupos de consistencia. Los volúmenes individuales pueden tener su propia política de copias Snapshot granulares de volumen. Además, puede haber una política de Snapshot para todo el grupo de coherencia. El grupo de coherencia solo puede tener una relación de sincronización activa de SnapMirror y una política de SnapMirror compartida, que puede utilizarse para recuperar todo el grupo de coherencia.

En el siguiente diagrama se muestra cómo se puede utilizar un grupo de consistencia individual. Los datos de una aplicación alojada en `SVM1` abarcan dos volúmenes: `vol1` Y `vol2`. Una política de Snapshot en el grupo de coherencia captura Snapshot de los datos cada 15 minutos.



Las cargas de trabajo de aplicaciones más grandes pueden requerir varios grupos de coherencia. En estas situaciones, puede crear grupos de consistencia jerárquicos, donde un solo grupo de consistencia se convierte en componentes secundarios de un grupo de coherencia primario. El grupo de consistencia primario puede incluir hasta cinco grupos de consistencia secundarios. Al igual que en grupos de coherencia individuales, una política de protección de sincronización activa de SnapMirror remoto se puede aplicar a toda la configuración de grupos de coherencia (principal y secundario) para recuperar la carga de trabajo de la aplicación.

En el siguiente ejemplo, una aplicación está alojada en `SVM1`. El administrador ha creado un grupo de consistencia primario `SVM1_app` , que incluye dos grupos de consistencia secundarios: `SVM1appDataCG` Para los datos y `SVM1app_logCG` para los registros. Cada grupo de coherencia secundario tiene su propia política de Snapshot. Las snapshots de los volúmenes de `SVM1appDataCG` se realizan cada 15 minutos. Las instantáneas de `SVM1app_logCG` se realizan cada hora. El grupo de consistencia primario `SVM1_app` tiene una política de sincronización activa de SnapMirror que replica los datos para garantizar la continuidad del servicio en caso de desastre.



A partir de ONTAP 9.12,1, los grupos de consistencia admiten clonado y modifican los miembros de la consistencia agregar o quitar volúmenestanto en System Manager como en la API REST DE ONTAP. A partir de ONTAP 9.12.1, la API de REST DE ONTAP también admite:

- Creación de grupos de coherencia con volúmenes NFS o SMB o espacios de nombres NVMe nuevos.
- Añadir volúmenes NFS o SMB o espacios de nombres NVMe nuevos o existentes a grupos de coherencia existentes.

Para obtener más información sobre la API de REST DE ONTAP, consulte "Documentación de referencia de la API DE REST de ONTAP" .

Supervisar grupos de consistencia

A partir de ONTAP 9.13.1, los grupos de consistencia ofrecen supervisión de capacidad y rendimiento en tiempo real e históricos, lo que proporciona información sobre el rendimiento de aplicaciones y grupos de coherencia individuales.

Los datos de supervisión se actualizan cada cinco minutos y se mantienen hasta un año. Puede realizar un seguimiento de las métricas para:

- Rendimiento: IOPS, latencia y rendimiento
- Capacidad: Tamaño, lógico utilizado, disponible

Puede ver los datos de supervisión en la pestaña **Información general** del menú del grupo de consistencia de System Manager o solicitándolos en la API DE REST. A partir de ONTAP 9.14,1, puede ver las métricas del grupo de consistencia con la CLI con `consistency-group metrics show` el comando. Obtenga más

información sobre `consistency-group metrics show` en el "Referencia de comandos del ONTAP".

> En ONTAP 9.13.1, solo puede recuperar métricas históricas mediante la API de REST. A partir de ONTAP 9.14.1, las métricas históricas también están disponibles en System Manager.

Proteger los grupos de consistencia

Los grupos de coherencia ofrecen una protección coherente con las aplicaciones, lo que garantiza la coherencia de los datos en varios volúmenes o LIF. Al crear una Snapshot de un grupo de coherencia, se establece una barrera en el grupo de coherencia. El cercado inicia una cola para I/O hasta que se completa la operación Snapshot, lo que garantiza la coherencia de un momento específico de los datos en todas las entidades del grupo de coherencia. El límite puede provocar un pico transitorio en latencia durante las operaciones de creación de copias Snapshot, como una política de Snapshot programada o la creación de una copia de Snapshot con System Manager. Obtenga más información sobre el contexto de la API de REST y la CLI en "Documentación de la API de REST de ONTAP"y."Referencia de comandos del ONTAP"

Los grupos de consistencia ofrecen protección mediante:

- Políticas de Snapshot
- SnapMirror síncrono activo
- [mcc] (A partir de ONTAP 9.11.1)
- SnapMirror asíncrono (A partir de ONTAP 9.13.1)
- "Recuperación ante desastres de SVM" (A partir de ONTAP 9.14.1)

La creación de un grupo de consistencia no habilita la protección automáticamente. Las políticas de protección local y remota se pueden establecer al crear o después de crear un grupo de coherencia.

Para configurar la protección en un grupo de consistencia, consulte "Proteja un grupo de consistencia".

Para utilizar la protección remota, debe cumplir con los requisitos para SnapMirror síncrono activo.

> No es posible establecer relaciones de sincronización activa de SnapMirror en volúmenes montados para acceso NAS.

Compatibilidad de verificación multiadministradora para grupos de coherencia

A partir de ONTAP 9.16,1, puede usar la verificación multiadministrador (MAV) con grupos de consistencia para garantizar que ciertas operaciones, como la creación, la modificación o la eliminación de grupos de consistencia, solo se puedan ejecutar después de las aprobaciones de los administradores designados. De este modo, se evita que los administradores comprometidos, malintencionados o sin experiencia realicen cambios no deseables en las configuraciones existentes.

"Leer más"

Grupos de consistencia en configuraciones de MetroCluster

A partir de ONTAP 9.11.1, puede aprovisionar grupos de consistencia con nuevos volúmenes en un clúster dentro de una configuración de MetroCluster. Estos volúmenes se aprovisionan en agregados reflejados.

Después de que se hayan aprovisionado, puede mover los volúmenes asociados con grupos de coherencia entre los agregados reflejados y no reflejados. Por lo tanto, los volúmenes asociados con grupos de coherencia pueden ubicarse en agregados reflejados, agregados no reflejados o en ambos. Es posible

modificar los agregados reflejados que contienen volúmenes asociados con grupos de coherencia para que no se reflejen. De igual manera, se pueden modificar los agregados no reflejados que contienen volúmenes asociados con grupos de coherencia para habilitar el mirroring.

Los volúmenes y las snapshots asociados con grupos de coherencia ubicados en agregados reflejados se replican en el sitio remoto (sitio B). El contenido de los volúmenes del sitio B ofrece una garantía de escritura para el grupo de coherencia, lo que le permite recuperar desde el sitio B en caso de desastre. Puede acceder a las copias de Snapshot de grupo de coherencia mediante un grupo de coherencia con la API de REST y System Manager en los clústeres que ejecutan ONTAP 9.11.1 o una versión posterior. A partir de ONTAP 9.14.1, también puede acceder a las snapshots con la CLI de ONTAP.

Si algunos o todos los volúmenes asociados con un grupo de consistencia se encuentran en agregados no reflejados a los que no se puede acceder actualmente, las operaciones GET o DELETE en el grupo de coherencia se comportan como si los volúmenes locales o los agregados de alojamiento están sin conexión.

Configuraciones del grupo de consistencia para la replicación

Si el sitio B ejecuta ONTAP 9.10,1 o una versión anterior, solo los volúmenes asociados con los grupos de coherencia ubicados en agregados reflejados se replican en el sitio B. Las configuraciones del grupo de consistencia solo se replican en el sitio B, si ambos sitios ejecutan ONTAP 9.11,1 o una versión posterior. Una vez que el sitio B se actualiza a ONTAP 9.11.1, los datos de los grupos de consistencia del sitio A que tienen todos los volúmenes asociados ubicados en agregados reflejados se replican en el sitio B.

> Se recomienda mantener al menos un 20 % de espacio libre para agregados reflejados para lograr un rendimiento y una disponibilidad de almacenamiento óptimos. Aunque la recomendación es del 10% para agregados no reflejados, el sistema de archivos puede usar el 10% adicional de espacio para absorber cambios incrementales. Los cambios incrementales incrementan la utilización del espacio para los agregados reflejados debido a la arquitectura basada en instantáneas de redirección en escritura de ONTAP. El incumplimiento de estas prácticas recomendadas puede tener un impacto negativo en el rendimiento.

Consideraciones de renovación

Cuando se actualiza a ONTAP 9.10,1 o posterior, los grupos de consistencia creados con SnapMirror Active Sync (anteriormente conocido como SnapMirror Business Continuity) en ONTAP 9.8 y 9.9.1 se actualizan automáticamente y se pueden gestionar en **Almacenamiento > Grupos de consistencia** en System Manager o la API REST DE ONTAP para obtener más información acerca de la actualización desde ONTAP 9.8 o 9,9.1, consulte "Consideraciones de actualización y reversión de sincronización activa de SnapMirror".

Las snapshots de grupo de consistencia creadas en la API de REST pueden gestionarse a través de la interfaz del grupo de consistencia de System Manager y mediante extremos de la API de REST del grupo de consistencia. A partir de ONTAP 9.14.1, las copias Snapshot de grupo de consistencia también se pueden gestionar con la CLI de ONTAP.

> Las Snapshot creadas con los comandos de ONTAPI `cg-start` y `cg-commit` no se reconocen como snapshots de grupo de consistencia y, por lo tanto, no se pueden gestionar mediante la interfaz de grupo de consistencia de System Manager ni los extremos del grupo de consistencia en la API REST DE ONTAP. A partir de ONTAP 9.14.1, estas copias de Snapshot se pueden reflejar en el volumen de destino si se utiliza una política asíncrona de SnapMirror. Para obtener más información, consulte Configurar SnapMirror asíncrono.

Funciones compatibles por versión

	ONTAP 9.16.1	ONTAP 9.15.1	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1
Grupos de consistencia jerárquicos	✓	✓	✓	✓	✓	✓	✓
Protección local con snapshots	✓	✓	✓	✓	✓	✓	✓
SnapMirror síncrono activo	✓	✓	✓	✓	✓	✓	✓
Soporte de MetroCluster	✓	✓	✓	✓	✓	✓	
Confirmaciones bifásicas (solo API de REST)	✓	✓	✓	✓	✓	✓	
Etiquetas de aplicaciones y componentes	✓	✓	✓	✓	✓		
Clonar grupos de consistencia	✓	✓	✓	✓	✓		
Añadir y quitar volúmenes	✓	✓	✓	✓	✓		
Cree CG con los nuevos volúmenes NAS	✓	✓	✓	✓	Solo API DE REST		
Crear CG con nuevos espacios de nombres NVMe	✓	✓	✓	✓	Solo API DE REST		
Mueva volúmenes entre grupos de coherencia secundarios	✓	✓	✓	✓			
Modificar la geometría del grupo de consistencia	✓	✓	✓	✓			
Supervisión	✓	✓	✓	✓			
Verificación de varios administradores	✓						
SnapMirror asíncrono (solo grupos de coherencia individuales)	✓	✓	✓	✓			
Recuperación ante desastres de SVM (solo grupos de consistencia individuales)	✓	✓	✓				
Soporte de CLI	✓	✓	✓				

Más información sobre los grupos de consistencia

Información relacionada

- "Documentación de automatización de ONTAP"
- SnapMirror síncrono activo
- Aspectos básicos para la recuperación ante desastres asíncrona de SnapMirror
- "Documentación de MetroCluster"
- "Verificación de varios administradores"
- "Referencia de comandos del ONTAP"

Obtenga información sobre los límites del grupo de consistencia de ONTAP

Al planificar y administrar los grupos de consistencia, tenga en cuenta los límites de objetos en el ámbito del clúster y del grupo de consistencia primario o secundario.

Límites impuestos

La siguiente tabla captura los límites de los grupos de coherencia. Los límites separados se aplican a los grupos de coherencia mediante SnapMirror con sincronización activa. Para obtener más información, consulte "Límites de sincronización activa de SnapMirror".

Límite	Ámbito	Mínimo	Máximo
Número de grupos de consistencia	Clúster	0	Igual que el recuento máximo de volúmenes en cluster*
Número de grupos de consistencia primarios	Clúster	0	Igual que el número máximo de volúmenes en el clúster

Número de grupos de consistencia individuales y primarios	Clúster	0	Igual que el número máximo de volúmenes en el clúster
Número de volúmenes en un grupo de consistencia	Grupo de consistencia único	1 tb de volumen	80 volúmenes
Cantidad de volúmenes en un grupo de consistencia con SnapMirror asíncrono	Grupo de consistencia único	1 tb de volumen	• En ONTAP 9.15.1 y versiones posteriores: Volúmenes de 80 TB • En ONTAP 9.13.1 y 9.14.1: Volúmenes de 16 GB
El número de volúmenes en el secundario de un grupo de consistencia primario	Grupo de consistencia primario	1 tb de volumen	80 volúmenes
El número de volúmenes en un grupo de coherencia secundario	Grupo de consistencia secundario	1 tb de volumen	80 volúmenes
Número de grupos de consistencia secundarios de un grupo de consistencia primario	Grupo de consistencia primario	1 grupo de consistencia	5 grupos de consistencia
Número de relaciones de recuperación ante desastres de SVM donde existe un grupo de consistencia (disponible a partir de ONTAP 9.14.1).	Clúster	0	32

* Un máximo de 50 grupos de consistencia habilitados con SnapMirror asíncrono se pueden alojar en un clúster.

Límites no aplicados

La programación Snapshot mínima admitida para grupos de coherencia es de 30 minutos. Este se basa en "Prueba de FlexGroup Volumes", que comparten la misma infraestructura Snapshot que los grupos de coherencia.

Configurar un único grupo de consistencia de ONTAP

Los grupos de consistencia se pueden crear con volúmenes existentes o con LUN o volúmenes nuevos (según la versión de ONTAP). Un volumen o LUN solo pueden asociarse a un grupo de coherencia a la vez.

Acerca de esta tarea

- No se admite la modificación de los volúmenes miembro de un grupo de coherencia después de su creación en ONTAP 9.10.1 a 9.11.1.

A partir de ONTAP 9.12.1, es posible modificar los volúmenes miembro de un grupo de coherencia. Para obtener más información sobre este proceso, consulte Modificar un grupo de consistencia.

- A partir de ONTAP 9.17.1, puede seleccionar el protocolo NVMe para asignar un host a un subsistema NVMe para cargas de trabajo de VMware en una configuración de sincronización activa de SnapMirror .

Cree un grupo de consistencia con nuevas LUN o volúmenes

En ONTAP 9.10.1 a 9.12.1, puede crear un grupo de consistencia utilizando nuevas LUN. A partir de ONTAP 9.13.1, System Manager también admite la creación de un grupo de consistencia con espacios de nombres NVMe nuevos o volúmenes NAS nuevos. (También es compatible con la API REST DE ONTAP a partir de ONTAP 9.12.1).

Administrador del sistema (ONTAP 9.16.1 y anteriores)

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y, a continuación, seleccione el protocolo para el objeto de almacenamiento.

   En ONTAP 9.10.1 a 9.12.1, la única opción para un nuevo objeto de almacenamiento es **utilizando nuevas LUN**. A partir de ONTAP 9.13.1, System Manager admite la creación de grupos de consistencia con espacios de nombres NVMe nuevos y volúmenes NAS nuevos.

3. Asigne un nombre al grupo de consistencia. Designe el número de volúmenes o LUN y la capacidad por volumen o LUN.
   a. **Tipo de aplicación**: Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de aplicación. Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre cómo etiquetar consistencia en Etiquetas de aplicaciones y componentes. Si planea crear un grupo de consistencia con una política de protección remota, debe usar **Other**.
   b. Para **Nuevas LUN**: Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
   c. Para **Nuevos volúmenes NAS**: Elija la opción de exportación apropiada (NFS o SMB/CIFS) según la configuración NAS de su SVM.
   d. Para **Nuevos espacios de nombres NVMe**: Seleccione el sistema operativo del host y el subsistema NVMe.
4. Para configurar políticas de protección, agregar un grupo de consistencia secundario o permisos de acceso, seleccione **Más opciones**.
5. Seleccione **Guardar**.
6. Para confirmar que se ha creado el grupo de consistencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo. Si establece una política de protección, sabrá que se ha aplicado cuando ve un escudo verde bajo la directiva apropiada, remoto o local.

Administrador del sistema (ONTAP 9.17.1 y posteriores)

Pasos

1. Seleccione **Protección > Grupos de consistencia**.
2. Seleccione **+Agregar** y, a continuación, seleccione el protocolo para el objeto de almacenamiento.
3. Asigne un nombre al grupo de consistencia. Indique la cantidad de volúmenes o LUN y la capacidad por volumen o LUN. **Tipo de aplicación**: Seleccione un tipo de aplicación. Si no se selecciona ningún valor, el grupo de consistencia se asignará al tipo **Otro** de forma predeterminada. Obtenga más información sobre el etiquetado de consistencia en Etiquetas de aplicaciones y componentes Si planea crear un grupo de consistencia con una política de protección remota, debe usar **Otro**.
   a. Para **Nuevas LUN**: Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
   b. Para **Nuevos volúmenes NAS**: Elija la opción de exportación apropiada (NFS o SMB/CIFS) según la configuración NAS de su SVM.
   c. Para **Nuevos espacios de nombres NVMe**: Seleccione el sistema operativo del host y el subsistema NVMe.
4. Para configurar políticas de protección, agregar un grupo de consistencia secundario o permisos de

acceso, seleccione **Más opciones**.

5. Seleccione **Guardar**.
6. Para confirmar que se ha creado el grupo de consistencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo. Si establece una política de protección, sabrá que se ha aplicado cuando ve un escudo verde bajo la directiva apropiada, remoto o local.

CLI

A partir de ONTAP 9.14.1, puede crear un grupo de consistencia nuevo con volúmenes nuevos mediante la CLI de ONTAP. Los parámetros específicos dependen de si los volúmenes son SAN, NVMe o NFS.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Crear un grupo de consistencia con volúmenes NFS

1. Cree el grupo de consistencia:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>
-volume-count <number> -size <size> -export-policy <policy_name>
```

Crear un grupo de consistencia con volúmenes SAN

1. Cree el grupo de consistencia:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>
-lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
```

Cree un grupo de consistencia con espacios de nombres NVMe

1. Cree el grupo de consistencia:

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -namespace <namespace_name> -volume-count <number>
-namespace-count <number> -size <size> -subsystem <subsystem_name>
```

   Obtenga más información sobre `consistency-group create` en el "Referencia de comandos del ONTAP".

Después de terminar

1. Confirme que el grupo de consistencia se ha creado con `consistency-group show` el comando.

   Obtenga más información sobre `consistency-group show` en el "Referencia de comandos del ONTAP".

Cree un grupo de coherencia con volúmenes existentes

Es posible utilizar volúmenes existentes para crear un grupo de coherencia.

Administrador del sistema (ONTAP 9.16.1 y anteriores)

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y **utilizando volúmenes existentes**.
3. Asigne un nombre al grupo de consistencia y seleccione la máquina virtual de almacenamiento.
   a. **Tipo de aplicación**: Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de aplicación. Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre cómo etiquetar consistencia en Etiquetas de aplicaciones y componentes. Si el grupo de consistencia tiene una relación de sincronización activa de SnapMirror, debe usar **Otro**.

   > En versiones de ONTAP anteriores a ONTAP 9.15.1, la sincronización activa de SnapMirror se conoce como continuidad del negocio de SnapMirror.

4. Seleccione los volúmenes existentes que desea incluir. Solo se podrá seleccionar los volúmenes que todavía no sean parte de un grupo de coherencia.

   > Si crea un grupo de coherencia con volúmenes existentes, el grupo de coherencia es compatible con volúmenes FlexVol. Se pueden agregar volúmenes con relaciones síncronas o asíncronas de SnapMirror o asíncronas de SnapMirror a grupos de coherencia, pero no tienen en cuenta los grupos de coherencia. Los grupos de coherencia no admiten bloques de S3 ni máquinas virtuales de almacenamiento con relaciones de SVMDR.

5. Seleccione **Guardar**.
6. Para confirmar que el grupo de consistencia se ha creado, vuelva al menú principal del grupo de consistencia, donde aparece una vez que se completa el trabajo de ONTAP. Si ha elegido una política de protección, confirme que se configuró correctamente al seleccionar un grupo de coherencia en el menú. Si establece una política de protección, sabe que se ha aplicado cuando ve un escudo verde bajo la directiva correspondiente, remota o local.

CLI

A partir de ONTAP 9.14.1, puede crear un grupo de consistencia con volúmenes existentes mediante la CLI de ONTAP.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Pasos

1. Ejecute `consistency-group create` el comando. `-volumes`El parámetro acepta una lista de nombres de volúmenes separados por comas.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency-group-name> -volume <volumes>
   ```

   Obtenga más información sobre `consistency-group create` en el "Referencia de comandos del ONTAP".

2. Puede ver el grupo de consistencia con `consistency-group show` el comando.

   Obtenga más información sobre `consistency-group show` en el "Referencia de comandos del ONTAP".

Siguientes pasos

- Proteja un grupo de consistencia
- Modificar un grupo de consistencia
- Clonar un grupo de consistencia

Configurar un grupo de consistencia ONTAP jerárquico

Los grupos de coherencia jerárquicos permiten gestionar cargas de trabajo grandes que abarcan varios volúmenes, creando un grupo de coherencia primario que funciona como un paraguas para los grupos de coherencia secundarios.

Los grupos de consistencia jerárquicos tienen un primario que puede incluir hasta cinco grupos de consistencia individuales. Los grupos de coherencia jerárquicos pueden admitir diferentes políticas Snapshot locales en grupos de coherencia o volúmenes individuales. Si utiliza una política de protección remota, que se aplicará a todo el grupo de consistencia jerárquico (primario y secundario).

Comenzando con ONTAP 9.13,1, usted puede modifique la geometría de sus grupos de consistencia y mueva volúmenes entre grupos de coherencia secundarios.

Para obtener información sobre los límites de objeto en los grupos de consistencia, consulte Límites de objetos para los grupos de consistencia.

Cree un grupo de consistencia jerárquico con nuevas LUN o volúmenes

Al crear un grupo de consistencia jerárquico, puede rellenarlo con nuevas LUN. A partir de ONTAP 9.13.1, también se pueden usar nuevos espacios de nombres NVMe y volúmenes NAS.

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y, a continuación, seleccione el protocolo para el objeto de almacenamiento.

   En ONTAP 9.10.1 a 9.12.1, la única opción para un nuevo objeto de almacenamiento es **utilizando nuevas LUN**. A partir de ONTAP 9.13.1, System Manager admite la creación de grupos de consistencia con espacios de nombres NVMe nuevos y volúmenes NAS nuevos.

3. Asigne un nombre al grupo de consistencia. Designe el número de volúmenes o LUN y la capacidad por volumen o LUN.
   a. **Tipo de aplicación**: Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de aplicación. Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre cómo etiquetar consistencia en Etiquetas de aplicaciones y componentes. Si planea usar una política de protección remota, debe elegir **Otro**.
4. Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
   a. Para **Nuevas LUN**: Seleccione el sistema operativo del host y el formato de LUN. Introduzca la información del iniciador del host.
   b. Para **Nuevos volúmenes NAS**: Elija la opción de exportación apropiada (NFS o SMB/CIFS) según la configuración NAS de su SVM.
   c. Para **Nuevos espacios de nombres NVMe**: Seleccione el sistema operativo del host y el subsistema NVMe.
5. Para agregar un grupo de consistencia hijo, seleccione **Más opciones** y luego **+Agregar grupo de consistencia hijo**.
6. Seleccione el nivel de rendimiento, el número de LUN o volúmenes y la capacidad por LUN o volumen. Designe las configuraciones de exportación adecuadas o la información del sistema operativo en función del protocolo que esté utilizando.
7. Opcionalmente, seleccione una política de Snapshot local y establezca los permisos de acceso.
8. Repita desde un máximo de cinco grupos de consistencia secundarios.
9. Seleccione **Guardar**.
10. Para confirmar que se ha creado el grupo de coherencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo de ONTAP. Si establece una directiva de protección, mire bajo la directiva apropiada, remota o local, que debe mostrar un escudo verde con una Marca de verificación en ella.

CLI

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Al crear un grupo de coherencia jerárquico en la CLI con volúmenes nuevos, debe crear cada grupo de coherencia secundario por separado.

Paso

1. Cree el nuevo grupo de consistencia mediante `consistency-group create` el comando.

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency_group_name> -parent-consistency-group
   <parent_consistency_group_name> -volume-prefix <volume_prefix> -volume
   -count <number_of_volumes> -size <size>
   ```

2. Cuando se le solicite la CLI, confirme que desea crear el nuevo grupo de consistencia primario. Introduzca `y`.
3. De manera opcional, repita el paso 1 para crear más grupos de consistencia secundarios.

   Obtenga más información sobre `consistency-group create` en el "Referencia de comandos del ONTAP".

Cree un grupo de coherencia jerárquico con volúmenes existentes

Se pueden organizar los volúmenes existentes en un grupo de coherencia jerárquico.

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione **+Agregar** y **utilizando volúmenes existentes**.
3. Seleccione la máquina virtual de almacenamiento.
4. Seleccione los volúmenes existentes que desea incluir. Solo se podrá seleccionar los volúmenes que todavía no sean parte de un grupo de coherencia.
5. Para agregar un grupo de consistencia hijo, seleccione **+Agregar grupo de consistencia hijo**. Cree los grupos de consistencia necesarios, que se nombrarán automáticamente.
   a. **Tipo de componente**: Si está utilizando ONTAP 9.12.1 o posterior, seleccione un tipo de componente de "datos", "registros" u "otro". Si no se selecciona ningún valor, se asignará al grupo de consistencia el tipo de **Other** de forma predeterminada. Obtenga más información sobre cómo etiquetar consistencia en Etiquetas de aplicaciones y componentes. Si planea usar una política de protección remota, debe usar **Otro**.
6. Asigne volúmenes existentes a cada grupo de coherencia.
7. De manera opcional, seleccione una política de Snapshot local.
8. Repita desde un máximo de cinco grupos de consistencia secundarios.
9. Seleccione **Guardar**.
10. Para confirmar que se ha creado el grupo de coherencia, vuelva al menú del grupo de consistencia principal, donde aparecerá una vez que se complete el trabajo de ONTAP. Si ha elegido una política de protección, confirme que se ha configurado correctamente seleccionando su grupo de consistencia en el menú; en el tipo de política correspondiente, verá un escudo verde con una Marca de verificación en el interior de la misma.

CLI

A partir de ONTAP 9.14.1, puede crear un grupo de consistencia jerárquico mediante la CLI.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Pasos

1. Aprovisione un nuevo grupo de coherencia primario y asigne volúmenes a un nuevo grupo de consistencia secundario:

   ```
   consistency-group create -vserver <svm_name> -consistency-group
   <child_consistency_group_name> -parent-consistency-group
   <parent_consistency_group_name> -volumes <volume_names>
   ```

2. `y`Introduzca para confirmar que desea crear un nuevo grupo de consistencia primario y secundario.

   Obtenga más información sobre `consistency-group create` en el "Referencia de comandos del ONTAP".

Siguientes pasos

- Modificar la geometría de un grupo de consistencia
- Modificar un grupo de consistencia
- Proteja un grupo de consistencia

Proteger los grupos de consistencia de ONTAP

Los grupos de coherencia ofrecen una protección local y remota de fácil gestión para aplicaciones SAN, NAS y NVMe que abarcan varios volúmenes.

La creación de un grupo de consistencia no habilita la protección automáticamente. Las políticas de protección se pueden establecer en el momento de la creación o después de crear el grupo de consistencia. Puede proteger grupos de consistencia mediante:

- Snapshots locales
- Sincronización activa de SnapMirror (conocida como Continuidad del negocio SnapMirror en versiones de ONTAP anteriores a 9.15.1)
- MetroCluster (principios de 9.11.1)
- SnapMirror asíncrono (inicio de 9.13.1)
- Recuperación ante desastres asíncrona de SVM (comenzando 9.14.1)

Si utiliza grupos de consistencia anidados, puede establecer políticas de protección distintas para los grupos de coherencia primario y secundario.

Comenzando con ONTAP 9.11,1, los grupos de consistencia ofrecen creación de snapshots de grupo de consistencia en dos fases. La operación de instantánea en dos fases ejecuta una comprobación previa, asegurando que la instantánea se capture correctamente.

Se puede producir la recuperación de un grupo de consistencia completo, de un solo grupo de consistencia en una configuración jerárquica o de volúmenes individuales en el grupo de consistencia. Para lograr la recuperación, seleccione el grupo de coherencia desde el que desea recuperar, seleccione el tipo de snapshot y luego identifique la snapshot en la que se basará la restauración. Para obtener más información sobre este proceso, consulte "Restaure un volumen a partir de una copia de Snapshot anterior".

Configure una política de snapshots local

Configurar una política de protección Snapshot local permite crear una política que abarque todos los volúmenes en un grupo de coherencia.

Acerca de esta tarea

La programación Snapshot mínima admitida para grupos de coherencia es de 30 minutos. Este se basa en "Prueba de FlexGroup Volumes", que comparten la misma infraestructura Snapshot que los grupos de coherencia.

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia que ha creado en el menú del grupo de consistencia.
3. En la parte superior derecha de la página de descripción general del grupo de consistencia, seleccione **Editar**.
4. Marque la casilla junto a **Programar instantáneas (locales)**.
5. Seleccione una política de Snapshot. Para configurar una nueva política personalizada, consulte "Cree una política de protección de datos personalizada".
6. Seleccione **Guardar**.
7. Volver al menú de descripción general del grupo de consistencia. En la columna de la izquierda bajo **Snapshots (Local)**, el estado dirá Protegido junto a .

CLI

A partir de ONTAP 9.14.1, puede modificar la política de protección de un grupo de consistencia con la CLI.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Paso

1. Ejecute el siguiente comando para establecer o modificar la política de protección:

   Si modifica la política de protección de una consistencia secundaria, debe identificar el grupo de consistencia primario mediante `-parent-consistency-group` *`parent_consistency_group_name`* el parámetro.

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

Crear una snapshot bajo demanda

Si necesita crear una Snapshot de su grupo de coherencia fuera de una política normalmente programada, puede crear una bajo demanda.

System Manager

Pasos

1. Vaya a **Almacenamiento** > **Grupos de consistencia**.
2. Seleccione el grupo de coherencia para el que desea crear una copia Snapshot bajo demanda.
3. Cambie a la pestaña **Copias de instantánea** y seleccione **+Agregar**.
4. Proporcione un **Nombre** y una **Etiqueta de SnapMirror**. En el menú desplegable de **Consistencia**, selecciona **Consistente a la aplicación** o **Consistente a la caída**.
5. Seleccione **Guardar**.

CLI

A partir de ONTAP 9.14.1, se puede crear una Snapshot bajo demanda de un grupo de coherencia mediante la CLI.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Paso

1. Cree la instantánea:

   De forma predeterminada, el tipo de snapshot es coherente con los fallos. Puede modificar el tipo de Snapshot con el parámetro opcional `-type`.

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

Cree snapshots de grupo de consistencia en dos fases

A partir de ONTAP 9.11.1, los grupos de coherencia admiten confirmaciones de dos fases para la creación de snapshots de grupo de coherencia (CG), que ejecutan una comprobación previa antes de confirmar la snapshot. Esta función solo está disponible con la API de REST de ONTAP.

La creación de Snapshot de CG de dos fases solo está disponible para la creación de Snapshot, no para aprovisionar grupos de coherencia ni restaurar grupos de coherencia.

Una snapshot de CG en dos fases divide el proceso de creación de snapshots en dos fases:

1. En la primera fase, la API ejecuta comprobaciones previas y activa la creación de snapshots. La primera fase incluye un parámetro de tiempo de espera, que designa la cantidad de tiempo para que la instantánea se confirme correctamente.
2. Si la solicitud de la fase uno se completa correctamente, puede invocar la segunda fase dentro del intervalo designado desde la primera fase, confirmando la instantánea en el punto final adecuado.

Antes de empezar

- Para utilizar la creación de copias Snapshot de CG de dos fases, todos los nodos del clúster deben ejecutar ONTAP 9.11.1 o una versión posterior.

- Solo se admite una llamada activa de una operación Snapshot de grupo de coherencia en una instancia de grupo de coherencia a la vez, ya sea una fase o dos fases. Al intentar invocar una operación de instantánea mientras otra está en curso, se produce un error.
- Cuando se invoca la creación de una copia de Snapshot, puede configurarse un valor de tiempo de espera opcional de entre 5 y 120 segundos. Si no se proporciona ningún valor de tiempo de espera, se agota el tiempo de espera de la operación en el valor predeterminado de 7 segundos. En la API, configure el valor de tiempo de espera con `action_timeout` el parámetro. En la CLI, utilice `-timeout` la marca.

Pasos

Es posible completar una snapshot en dos fases con la API de REST o, a partir de ONTAP 9.14.1, la CLI de ONTAP. Esta operación no es compatible con System Manager.

Si invoca la creación de la snapshot con la API, debe confirmar la snapshot con la API. Si invoca la creación de la snapshot con la CLI, debe confirmar la snapshot con la CLI. No se admiten métodos de mezcla.

CLI

A partir de ONTAP 9.14.1, puede crear una instantánea de dos fases con la CLI.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Pasos

1. Inicie la instantánea:

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. Compruebe que la instantánea se ha realizado:

   ```
   consistency-group snapshot show
   ```

3. Confirme la instantánea:

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API

1. Invoque la creación de la instantánea. Envíe una solicitud POST al extremo del grupo de consistencia con el `action=start` parámetro.

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. Si la solicitud POST se realiza correctamente, la salida incluye un uuid de instantánea. Con ese uuid, envíe una solicitud de PARCHE para confirmar la instantánea.

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

Configurar la protección remota para un grupo de coherencia

Los grupos de coherencia ofrecen protección remota mediante sincronización activa SnapMirror y, a partir de ONTAP 9.13,1, SnapMirror asíncrono.

Configurar la protección con SnapMirror Active Sync

Es posible usar SnapMirror active sync para garantizar que las Snapshot de los grupos de consistencia creados en el grupo de consistencia se copien en el destino. Para obtener más información sobre la sincronización activa de SnapMirror o sobre cómo configurar la sincronización activa de SnapMirror mediante la CLI, consulte Configure la protección para la continuidad del negocio.

Antes de empezar

- No es posible establecer relaciones de sincronización activa de SnapMirror en volúmenes montados para acceso NAS.
- Las etiquetas de políticas del clúster de origen y destino deben coincidir.
- La sincronización activa de SnapMirror no replicará snapshots de forma predeterminada a menos que se añada una regla con una etiqueta de SnapMirror a la política predefinida `AutomatedFailOver` y las snapshots se creen con esa etiqueta.

  Para obtener más información sobre este proceso, consulte "Proteger con SnapMirror sincronización activa".

- Implementaciones en cascada No son compatibles con la sincronización activa de SnapMirror.
- A partir de ONTAP 9.13,1, se puede sin interrupciones añada volúmenes a un grupo de coherencia con una relación de sincronización activa de SnapMirror. Cualquier otro cambio en un grupo de consistencia requiere interrumpir la relación de sincronización activa de SnapMirror, modificar el grupo de consistencia y, a continuación, volver a establecer y volver a sincronizar la relación.

> Para configurar la sincronización activa de SnapMirror con la CLI, consulte Proteger con SnapMirror sincronización activa.

Pasos para System Manager

1. Asegúrese de haber cumplido con el "Requisitos previos para utilizar SnapMirror Active Sync".
2. Seleccione **almacenamiento > grupos de consistencia**.
3. Seleccione el grupo de consistencia que ha creado en el menú del grupo de consistencia.

4. En la parte superior derecha de la página de descripción general, seleccione **más** y, a continuación, **proteger**.
5. System Manager rellena automáticamente la información del origen. Seleccione la máquina virtual de almacenamiento y clúster apropiado para el destino. Seleccione una política de protección. Asegúrese de que **Initialize Relationship** está activada.
6. Seleccione **Guardar**.
7. El grupo de consistencia debe inicializar y sincronizar. Confirme que la sincronización se ha completado correctamente volviendo al menú **Grupo de consistencia**. El estado de **SnapMirror (Remote)** se muestra `Protected` junto a .

Configurar SnapMirror asíncrono

A partir de ONTAP 9.13.1, puede configurar la protección asíncrona de SnapMirror para un grupo de coherencia único. A partir de ONTAP 9.14.1, se puede usar SnapMirror asíncrono para replicar copias Snapshot granulares de volúmenes en el clúster de destino mediante la relación del grupo de coherencia.

Acerca de esta tarea

Para replicar snapshots granulares de volumen, debe ejecutar ONTAP 9.14.1 o una versión posterior. Para las políticas de MirrorAndVault y Vault, la etiqueta de SnapMirror de la política de Snapshot granular de volumen debe coincidir con la regla de política SnapMirror del grupo de coherencia. Las copias de Snapshot granulares del volumen rigen el valor conservar de la política SnapMirror del grupo de coherencia, que se calcula independientemente de las copias de Snapshot del grupo de coherencia. Por ejemplo, si tiene una política para mantener dos Snapshot en el destino, puede tener dos copias de Snapshot granulares de volumen y dos copias de Snapshot de grupo de coherencia.

Al volver a sincronizar la relación de SnapMirror con snapshots granulares de volumen, se pueden conservar snapshots granulares de volumen con `-preserve` la marca. Se conservan las copias Snapshot granulares del volumen más recientes que las de grupo de consistencia. Si no existe una snapshot de grupo de consistencia, no se pueden transferir copias Snapshot granulares de volumen en la operación de resincronización.

Antes de empezar

- La protección asíncrona de SnapMirror solo está disponible para un grupo de consistencia único. No se admite para grupos de coherencia jerárquicos. Para convertir un grupo de consistencia jerárquico en un grupo de consistencia único, consulte modificar la arquitectura del grupo de consistencia.
- Las etiquetas de políticas del clúster de origen y destino deben coincidir.
- añada volúmenes a un grupo de coherenciaUna relación asíncrona de SnapMirror activa se puede producir sin interrupciones. Cualquier otro cambio en un grupo de consistencia requiere que rompa la relación de SnapMirror, modifique el grupo de consistencia y, a continuación, vuelva a establecer y vuelva a sincronizar la relación.
- Los grupos de consistencia habilitados para la protección con SnapMirror asíncrono tienen diferentes límites. Para obtener más información, consulte Límites del grupo de consistencia.
- Si se configuró una relación de protección asíncrona de SnapMirror para varios volúmenes individuales, puede convertir esos volúmenes en un grupo de coherencia y conservar las snapshots existentes. Para convertir volúmenes correctamente:
  - Debe haber una snapshot común de los volúmenes.
  - Debe romper la relación de SnapMirror existente y añada los volúmenes a un único grupo de consistenciavolver a sincronizar la relación mediante el siguiente flujo de trabajo.

Pasos

1. En el clúster de destino, seleccione **Almacenamiento > Grupos de consistencia**.
2. Seleccione el grupo de consistencia que ha creado en el menú del grupo de consistencia.
3. En la parte superior derecha de la página de descripción general, seleccione **más** y, a continuación, **proteger**.
4. System Manager rellena automáticamente la información del origen. Seleccione la máquina virtual de almacenamiento y clúster apropiado para el destino. Seleccione una política de protección. Asegúrese de que **Initialize Relationship** está activada.

   Al seleccionar una política asíncrona, tiene la opción de **Anular horario de transferencia**.

   > La programación mínima admitida (objetivo de punto de recuperación o RPO) para grupos de consistencia con SnapMirror asíncrono es de 30 minutos.

5. Seleccione **Guardar**.
6. El grupo de consistencia debe inicializar y sincronizar. Confirme que la sincronización se ha completado correctamente volviendo al menú **Grupo de consistencia**. El estado de **SnapMirror (Remote)** se muestra `Protected` junto a .

Configurar la recuperación ante desastres de la SVM

A partir de ONTAP 9.14.1, Recuperación ante desastres de SVM admite grupos de coherencia y le permite reflejar información del grupo de coherencia del origen en el clúster de destino.

Si va a habilitar la recuperación ante desastres de SVM en una SVM que ya contiene un grupo de consistencia, siguiendo los flujos de trabajo de configuración de SVM para System Manager o el CLI de ONTAP.

Si va a añadir un grupo de coherencia a una SVM que esté en una relación de recuperación ante desastres de SVM activa y en buen estado, debe actualizar la relación de recuperación ante desastres de SVM desde el clúster de destino. Para obtener más información, consulte Actualice manualmente una relación de replicación. Debe actualizar la relación cada vez que expanda el grupo de consistencia.

Limitaciones

- La recuperación ante desastres de SVM no admite grupos de consistencia jerárquicos.
- La recuperación ante desastres de SVM no admite grupos de consistencia protegidos con SnapMirror asíncrono. Debe interrumpir la relación de SnapMirror antes de configurar la recuperación ante desastres de SVM.
- Ambos clústeres deben ejecutar ONTAP 9.14.1 o una versión posterior.
- Las relaciones de dispersión no se admiten para las configuraciones de recuperación ante desastres de SVM que contienen grupos de coherencia.
- Para conocer otros límites, consulte límites del grupo de consistencia.

Visualizar relaciones

System Manager visualiza los mapas de LUN en el menú **Protección > Relaciones**. Cuando selecciona una relación de origen, System Manager muestra una visualización de las relaciones de origen. Al seleccionar un volumen, puede profundizar en estas relaciones para ver una lista de las LUN contenidas y las relaciones con el iGroup. Esta información se puede descargar como un libro de Excel desde la vista de volumen individual; la operación de descarga se ejecuta en segundo plano.

Información relacionada

- "Clonar un grupo de consistencia"
- "Configurar las instantáneas"
- "Cree políticas de protección de datos personalizadas"
- "Recuperar desde snapshots"
- "Restaure un volumen a partir de una copia de Snapshot anterior"
- "Información general sobre sincronización activa de SnapMirror"
- "Documentación de automatización de ONTAP"
- Aspectos básicos para la recuperación ante desastres asíncrona de SnapMirror

Modificar volúmenes de miembros en un grupo de consistencia de ONTAP

A partir de ONTAP 9.12.1, puede modificar un grupo de coherencia quitando volúmenes o añadiendo volúmenes (expandiendo el grupo de coherencia). A partir de ONTAP 9.13.1, se pueden mover volúmenes entre grupos de coherencia secundarios si comparten un volumen primario común.

Añadir volúmenes a un grupo de coherencia

A partir de ONTAP 9.12.1, es posible añadir volúmenes a un grupo de coherencia sin interrupciones.

Acerca de esta tarea

- No es posible añadir volúmenes asociados con otro grupo de coherencia.
- Los grupos de consistencia admiten los protocolos NAS, SAN y NVMe.
- Puede añadir hasta 16 volúmenes a la vez a un grupo de coherencia si los ajustes se encuentran dentro de la límites del grupo de consistencia.
- A partir de ONTAP 9.13,1, es posible añadir volúmenes sin interrupciones a un grupo de coherencia con una sincronización activa de SnapMirror o una política de protección asíncrona de SnapMirror.
- Cuando se añaden volúmenes a un grupo de coherencia protegido por SnapMirror Active Sync, el estado de la relación de la sincronización activa de SnapMirror cambia a «Expanding» hasta que el mirroring y la protección se configuran para el nuevo volumen. Si se produce un desastre en el clúster primario antes de que se complete este proceso, el grupo de consistencia revierte a su composición original como parte de la operación de conmutación al nodo de respaldo.
- En ONTAP versión 9.12.1 y versiones anteriores, *no puede* añadir volúmenes a un grupo de coherencia de una relación de sincronización activa de SnapMirror. Primero, es necesario eliminar la relación de sincronización activa de SnapMirror, modificar el grupo de coherencia y, a continuación, restaurar la protección con la sincronización activa de SnapMirror.
- A partir de ONTAP 9.12.1, la API DE REST DE ONTAP admite la adición *new* o volúmenes existentes a un grupo de coherencia. Para obtener más información sobre la API de REST DE ONTAP, consulte "Documentación de referencia de la API DE REST de ONTAP".

  A partir de ONTAP 9.13.1, esta funcionalidad es compatible con System Manager.

- Al expandir un grupo de coherencia, las Snapshot del grupo de coherencia capturado antes de la modificación se considerarán parciales. Cualquier operación de restauración basada en esa Snapshot reflejará el grupo de coherencia en el momento específico de la Snapshot.

- Si utiliza ONTAP 9.10.1 a 9.11.1, no puede modificar un grupo de consistencia. Para cambiar la configuración de un grupo de coherencia en ONTAP 9.10.1 o 9.11.1, debe eliminar el grupo de coherencia y, a continuación, crear un nuevo grupo de coherencia con los volúmenes que desea incluir.
- A partir de ONTAP 9.14.1, se pueden replicar copias Snapshot granulares de volúmenes en el clúster de destino cuando se utiliza SnapMirror asíncrono. Cuando se amplía un grupo de coherencia mediante SnapMirror asíncrono, las Snapshot granulares de volumen solo se replican después de expandir el grupo de coherencia cuando la política de SnapMirror es MirrorAll o MirrorAndVault. Solo se replican las copias Snapshot granulares de volumen más recientes que la copia Snapshot del grupo de consistencia base.
- Si agrega volúmenes a un grupo de consistencia en una relación de recuperación ante desastres de SVM (compatible a partir de ONTAP 9.14.1), debe actualizar la relación de recuperación ante desastres de SVM desde el clúster de destino después de expandir el grupo de consistencia. Para obtener más información, consulte Actualice manualmente una relación de replicación .
- Si está utilizando NVMe con ONTAP 9.17.1, no puede modificar un grupo de consistencia.

Ejemplo 2. Pasos

System Manager

A partir de ONTAP 9.12.1, puede realizar esta operación con System Manager.

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia que desea modificar.
3. Si va a modificar un solo grupo de consistencia, en la parte superior del menú **Volumes**, seleccione **más** y, a continuación, **ampliar** para añadir un volumen.

   Si va a modificar un grupo de consistencia secundario, identifique el grupo de consistencia primario que desea modificar. Seleccione el botón **>** para ver los grupos de consistencia secundarios y, a continuación, ⋮ seleccione junto al nombre del grupo de consistencia secundario que desea modificar. En ese menú, seleccione **ampliar**.
4. Seleccione hasta 16 volúmenes para añadir al grupo de coherencia.
5. Seleccione **Guardar**. Cuando la operación se complete, vea los volúmenes recién agregados en el menú **Volúmenes** del grupo de consistencia.

CLI

A partir de ONTAP 9.14.1, puede añadir volúmenes a un grupo de coherencia mediante la CLI de ONTAP.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Añadir volúmenes existentes

1. Ejecute el siguiente comando. `-volumes`El parámetro acepta una lista de volúmenes separados por comas.

   ⓘ Solo incluya `-parent-consistency-group` el parámetro si el grupo de consistencia se encuentra en una relación jerárquica.

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

Añadir volúmenes nuevos

El procedimiento para añadir volúmenes nuevos depende del protocolo que utilice.

ⓘ Incluir únicamente el `-parent-consistency-group` parámetro si el grupo de consistencia está en una relación jerárquica.

- Para añadir volúmenes nuevos sin exportarlos, realice lo siguiente:

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  child_consistency_group -parent-consistency-group existingParentCg -volume
  volume_name -size size
  ```

- Para añadir nuevos volúmenes de NFS:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- Para añadir nuevos volúmenes de SAN:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- Para añadir nuevos espacios de nombres de NVMe:

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

Quite volúmenes de un grupo de coherencia

Los volúmenes que se quitan de un grupo de consistencia no se eliminan. Permanecen activos en el clúster.

Acerca de esta tarea

- No se pueden quitar volúmenes de un grupo de consistencia de una relación de recuperación ante desastres de sincronización activa de SnapMirror o de SVM. Primero, debe eliminar la relación de sincronización activa de SnapMirror para modificar el grupo de coherencia y, a continuación, volver a establecer la relación.
- Si un grupo de coherencia no tiene volúmenes en él después de la operación de eliminación, se eliminará el grupo de coherencia.
- Cuando se elimina un volumen de un grupo de coherencia, las Snapshot existentes del grupo de coherencia permanecen, pero se consideran no válidas. Las Snapshot existentes no se pueden usar para restaurar el contenido del grupo de coherencia. Las copias Snapshot granulares del volumen siguen siendo válidas.
- Si elimina un volumen del clúster, se elimina automáticamente del grupo de coherencia.
- Para cambiar la configuración de un grupo de coherencia en ONTAP 9.10.1 o 9.11.1, debe eliminar el grupo de coherencia y, a continuación, crear un grupo de coherencia nuevo con los volúmenes miembro deseados.
- Al eliminar un volumen del clúster, se eliminará automáticamente del grupo de consistencia.

System Manager

A partir de ONTAP 9.12.1, puede realizar esta operación con System Manager.

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia único o secundario que desea modificar.
3. En el menú **volúmenes**, seleccione las casillas de verificación junto a los volúmenes individuales que desea quitar del grupo de consistencia.
4. Seleccione **Eliminar volúmenes del grupo de coherencia**.
5. Confirme que comprende que al eliminar los volúmenes, todas las instantáneas del grupo de consistencia dejarán de ser válidas y seleccione **Quitar**.

CLI

A partir de ONTAP 9.14.1, puede quitar volúmenes de un grupo de consistencia mediante la CLI.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Paso

1. Quite los volúmenes. `-volumes`El parámetro acepta una lista de volúmenes separados por comas.

   Solo incluya `-parent-consistency-group` el parámetro si el grupo de consistencia se encuentra en una relación jerárquica.

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

Mover volúmenes entre grupos de coherencia

A partir de ONTAP 9.13.1, se pueden mover volúmenes entre grupos de coherencia secundarios que comparten un volumen primario.

Acerca de esta tarea

- Solo puede mover volúmenes entre grupos de coherencia anidados bajo el mismo grupo de consistencia primario.
- Las Snapshot de grupo de consistencia existentes quedan no válidas y ya no se puede acceder a ellas como snapshots de grupo de coherencia. Las copias de Snapshot de volúmenes individuales siguen siendo válidas.
- Las snapshots del grupo de coherencia primario siguen siendo válidas.
- Si mueve todos los volúmenes de un grupo de consistencia secundario, se eliminará ese grupo de coherencia.
- Las modificaciones a un grupo de consistencia deben respetar límites del grupo de consistencia.

System Manager

A partir de ONTAP 9.12.1, puede realizar esta operación con System Manager.

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia primario que contiene los volúmenes que desea mover. Encuentre el grupo de consistencia secundario y luego expanda el menú **VOLUMES**. Seleccione los volúmenes que desea mover.
3. Selecciona **Mover**.
4. Seleccione si desea mover los volúmenes a un grupo de coherencia nuevo o a un grupo existente.
   a. Para desplazarse a un grupo de consistencia existente, seleccione **Grupo de consistencia secundario existente** y, a continuación, elija el nombre del grupo de consistencia en el menú desplegable.
   b. Para desplazarse a un nuevo grupo de consistencia, seleccione **Nuevo grupo de consistencia secundario**. Introduzca un nombre para el nuevo grupo de consistencia secundario y seleccione un tipo de componente.
5. Selecciona **Mover**.

CLI

A partir de ONTAP 9.14.1, puede mover volúmenes entre grupos de consistencia mediante la interfaz de línea de comandos de ONTAP.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Mueva volúmenes a un nuevo grupo de coherencia secundario

1. El siguiente comando crea un nuevo grupo de coherencia secundario que contiene los volúmenes designados.

   Cuando se crea el nuevo grupo de coherencia, se pueden designar nuevas políticas de snapshot, calidad de servicio y organización en niveles.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

Mueva volúmenes a un grupo de coherencia secundario existente

1. Reasigne los volúmenes. `-volumes`El parámetro acepta una lista de nombres de volúmenes separados por comas.

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

Información relacionada

- Límites del grupo de consistencia
- Clonar un grupo de consistencia

Modificar la geometría del grupo de consistencia de ONTAP

A partir de ONTAP 9.13.1, puede modificar la geometría de un grupo de consistencia. Modificar la geometría de un grupo de coherencia permite modificar la configuración de grupos de coherencia secundarios o primarios sin interrupciones en las operaciones de I/O en curso.

La modificación de la geometría del grupo de consistencia tiene un impacto en las snapshots existentes del grupo de consistencia. Para obtener más información, consulte la modificación específica de la geometría que desea realizar.

> No puede modificar la geometría de un grupo de consistencia configurado con una política de protección remota. Primero debe romper la relación de protección, modificar la geometría y, a continuación, restaurar la protección remota.

Agregue un nuevo grupo de consistencia secundario

A partir de ONTAP 9.13.1, puede agregar un nuevo grupo de consistencia secundario a un grupo de consistencia primario existente.

Acerca de esta tarea

- Un grupo de coherencia primario puede contener un máximo de cinco grupos de coherencia secundarios. Consulte límites del grupo de consistencia para ver otros límites.
- No puede agregar un grupo de consistencia secundario a un grupo de consistencia único. Primero, debe [promocionar]el grupo de consistencia y, luego, puede agregar un grupo de consistencia secundario.
- Las Snapshot existentes del grupo de coherencia capturadas antes de la operación de ampliación se considerarán parciales. Cualquier operación de restauración basada en esa Snapshot reflejará el grupo de coherencia en el momento específico de la Snapshot.

Ejemplo 3. Pasos

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

Agregue un nuevo grupo de consistencia secundario

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia primario al que desea añadir un grupo de consistencia secundario.
3. Junto al nombre del grupo de consistencia primario, seleccione **Más** y luego **Agregar nuevo grupo de consistencia secundario**.
4. Introduzca un nombre para su grupo de consistencia.
5. Seleccione si desea añadir volúmenes nuevos o existentes.
   a. Si va a agregar volúmenes existentes, seleccione **Volúmenes existentes** y, a continuación, elija los volúmenes en el menú desplegable.
   b. Si va a agregar nuevos volúmenes, seleccione **Nuevos volúmenes** y luego designe el número de volúmenes y su tamaño.
6. Seleccione **Agregar**.

CLI

A partir de ONTAP 9.14.1, puede agregar un grupo de consistencia secundario mediante la CLI de ONTAP.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Añada un grupo de coherencia secundario con volúmenes nuevos

1. Cree el nuevo grupo de consistencia. Proporcionar valores para el nombre del grupo de coherencia, el prefijo del volumen, la cantidad de volúmenes, el tamaño de volumen, el servicio de almacenamiento, y el nombre de la política de exportación:

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   -volume-prefix prefix -volume-count number -size size -storage-service
   service -export-policy policy_name
   ```

Añada un grupo de coherencia secundario con volúmenes existentes

1. Cree el nuevo grupo de consistencia. `volumes`El parámetro acepta una lista de nombres de volúmenes separados por comas.

   ```
   consistency-group create -vserver SVM_name -consistency-group
   new_consistency_group -parent-consistency-group parent_consistency_group
   -volumes volume
   ```

Desvincular un grupo de consistencia secundario

A partir de ONTAP 9.13.1, puede quitar un grupo de consistencia secundario de su primario, convirtiéndolo en un grupo de consistencia individual.

Acerca de esta tarea

- Al desvincular un grupo de coherencia secundario, las snapshots del grupo de coherencia primario dejan de ser válidas y no se puede acceder a ellas. Las copias Snapshot granulares de volúmenes siguen siendo válidas.
- Las Snapshot existentes del grupo de coherencia individual siguen siendo válidas.
- Se producirá un error en esta operación si existe un grupo de coherencia único existente con el mismo nombre que el grupo de coherencia secundario que se pretende desvincular. Si se encuentra con esta situación, debe cambiar el nombre del grupo de consistencia al desconectarlo.

Ejemplo 4. Pasos

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

Desvincular un grupo de consistencia secundario

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia primario que contiene el secundario que desea desvincular.
3. Junto al grupo de consistencia hijo que desea separar, seleccione **Más** y luego **Desasociar del padre**.
4. Opcionalmente, cambie el nombre del grupo de coherencia y seleccione un tipo de aplicación.
5. Seleccione **Desasociar**.

CLI

A partir de ONTAP 9.14.1, puede desvincular un grupo de consistencia secundario mediante la CLI de ONTAP.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Desvincular un grupo de consistencia secundario

1. Desvincule el grupo de consistencia. De manera opcional, cambie el nombre del grupo de coherencia desconectado con `-new-name` el parámetro.

   ```
   consistency-group detach -vserver SVM_name -consistency-group
   child_consistency_group -parent-consistency-group parent_consistency_group
   [-new-name new_name]
   ```

Mueva un grupo de consistencia único existente bajo un grupo de consistencia primario

A partir de ONTAP 9.13.1, puede convertir un grupo de consistencia único existente en un grupo de consistencia secundario. Puede mover el grupo de consistencia por un grupo de consistencia primario

existente o crear un grupo de consistencia primario nuevo durante la operación de movimiento.

Acerca de esta tarea

- El grupo de coherencia primario debe tener cuatro o menos hijos. Un grupo de coherencia primario puede contener un máximo de cinco grupos de coherencia secundarios. Consulte límites del grupo de consistencia para ver otros límites.
- Las snapshots existentes del grupo de consistencia *parent* capturadas antes de esta operación se consideran parciales. Cualquier operación de restauración basada en una de esas copias de Snapshot refleja el grupo de coherencia en el momento específico de la copia de Snapshot.
- Las copias de Snapshot de grupo de consistencia existentes del grupo de consistencia único siguen siendo válidas.

Ejemplo 5. Pasos

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

Mueva un grupo de consistencia único existente bajo un grupo de consistencia primario

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia que desea convertir.
3. Seleccione **Más** y luego **Mover bajo diferente grupo de consistencia**.
4. De manera opcional, introduzca un nuevo nombre para el grupo de consistencia y seleccione un tipo de componente. De forma predeterminada, el tipo de componente será Otro.
5. Elija si desea migrar a un grupo de consistencia primario existente o crear un nuevo grupo de consistencia primario:
   a. Para migrar a un grupo de consistencia primario existente, seleccione **Grupo de consistencia existente** y, a continuación, elija el grupo de consistencia en el menú desplegable.
   b. Para crear un grupo de consistencia primario nuevo, seleccione **Nuevo grupo de consistencia** y, a continuación, proporcione un nombre para el nuevo grupo de consistencia.
6. Selecciona **Mover**.

CLI

A partir de ONTAP 9.14.1, puede mover un solo grupo de consistencia debajo de un grupo de consistencia primario mediante la CLI de ONTAP.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Mover un grupo de consistencia debajo de un nuevo grupo de consistencia primario

1. Cree el nuevo grupo de consistencia primario. El `-consistency-groups` parámetro migrará cualquier grupo de consistencia existente al nuevo elemento primario.

   ```
   consistency-group attach -vserver svm_name -consistency-group
   parent_consistency_group -consistency-groups child_consistency_group
   ```

Mueva un grupo de consistencia bajo un grupo de consistencia existente

1. Mueva el grupo de consistencia:

   ```
   consistency-group add -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   ```

Promover un grupo de consistencia secundario

A partir de ONTAP 9.13.1, puede promover un grupo de consistencia a un grupo de consistencia primario. Cuando se promociona el grupo de coherencia único a un elemento primario, también se crea un nuevo grupo de coherencia secundario que hereda todos los volúmenes del grupo de coherencia único original.

Acerca de esta tarea

- Si desea convertir un grupo de consistencia secundario en un grupo de consistencia primario, debe primero [detach] el grupo de consistencia secundario y, a continuación, seguir este procedimiento.
- Las Snapshot existentes del grupo de coherencia siguen siendo válidas después de promocionar el grupo de coherencia.

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

Promover un grupo de consistencia secundario

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia que desea promocionar.
3. Seleccione **Más** y luego **Promocionar al grupo de consistencia primario**.
4. Introduzca un **Nombre** y seleccione un **Tipo de componente** para el grupo de consistencia hijo.
5. Selecciona **Promocionar**.

CLI

A partir de ONTAP 9.14.1, puede mover un solo grupo de consistencia debajo de un grupo de consistencia primario mediante la CLI de ONTAP.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Promover un grupo de consistencia secundario

1. Promocione el grupo de consistencia. Este comando creará un grupo de coherencia primario y un secundario.

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

Degrade un elemento principal a un solo grupo de consistencia

A partir de ONTAP 9.13.1, puede degradar un grupo de consistencia primario a un solo grupo de consistencia. Al degradar el elemento primario, se abre la jerarquía del grupo de consistencia y se eliminan todos los grupos de coherencia secundarios asociados. Todos los volúmenes del grupo de coherencia permanecerán bajo el nuevo grupo de coherencia único.

Acerca de esta tarea

- Las Snapshot existentes del grupo de consistencia *parent* siguen siendo válidas después de degradarlas a una única coherencia. Las snapshots existentes de cualquiera de los grupos de consistencia *child* asociados de ese principal dejan de ser válidas al degradar. Siguen accediendo a las snapshots de volumen individuales dentro del grupo de coherencia secundario como copias Snapshot granulares de volumen.

Ejemplo 6. Pasos

System Manager

A partir de ONTAP 9.13.1, puede realizar esta operación con System Manager.

Degradar un grupo de consistencia

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia primario que desea degradar.
3. Seleccione **Más** y luego **Descender a un solo grupo de consistencia**.
4. Una advertencia le aconsejará que se eliminen todos los grupos de coherencia secundarios asociados y que sus volúmenes se muevan al nuevo grupo de consistencia único. Selecciona **Descenso** para confirmar que entiendes el impacto.

CLI

A partir de ONTAP 9.14.1, puede degradar un grupo de consistencia mediante la CLI de ONTAP.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Degradar un grupo de consistencia

1. Degrade el grupo de consistencia. Utilice el parámetro opcional `-new-name` para cambiar el nombre del grupo de consistencia.

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

Modificar las etiquetas de aplicaciones y componentes del grupo de consistencia de ONTAP

A partir de ONTAP 9.12.1, los grupos de consistencia admiten el etiquetado de componentes y aplicaciones. Las etiquetas de aplicaciones y componentes son una herramienta de gestión que le permite filtrar e identificar diferentes cargas de trabajo en sus grupos de consistencia.

Acerca de esta tarea

Los grupos de consistencia ofrecen dos tipos de etiquetas:

- **Etiquetas de aplicación**: Estas se aplican a grupos de consistencia individuales y padre. Las etiquetas de las aplicaciones proporcionan etiquetas para cargas de trabajo como MongoDB, Oracle o SQL Server. La etiqueta de aplicación predeterminada para los grupos de consistencia es otra.
- **Etiquetas de componentes**: Los niños de los grupos de consistencia jerárquicos tienen etiquetas de componentes en lugar de etiquetas de aplicación. Las opciones para etiquetas de componentes son "datos", "registros" u "otros". El valor predeterminado es Other.

Puede aplicar las etiquetas al crear grupos de consistencia o después de crear los grupos de consistencia.

Si el grupo de consistencia tiene una relación de sincronización activa de SnapMirror, debe usar **other** como etiqueta de aplicación o componente.

Pasos

A partir de ONTAP 9.12.1, puede modificar las etiquetas de componentes y aplicaciones mediante System Manager. A partir de ONTAP 9.14.1, puede modificar la aplicación y las etiquetas de los componentes mediante la CLI de ONTAP.

System Manager

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia cuya etiqueta desea modificar. Seleccione el ⋮ junto al nombre del grupo de consistencia y luego **Editar**.
3. En el menú desplegable, seleccione la aplicación o etiqueta de componente adecuada.
4. Seleccione **Guardar**.

CLI

A partir de ONTAP 9.14.1, puede modificar la aplicación o la etiqueta de componente de un grupo de consistencia existente mediante la CLI de ONTAP.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Modifique la etiqueta de aplicación

1. Las etiquetas de aplicación aceptan un número limitado de cadenas predefinidas. Para ver la lista de cadenas aceptadas, ejecute el siguiente comando:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. Elija la cadena adecuada del resultado, el modifique el grupo de consistencia:
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

Modifique la etiqueta de componente

1. Modifique el tipo de componente. El tipo de componente puede ser datos, registros u otros. Si está utilizando la sincronización activa de SnapMirror, debe ser “Otro”.
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

Clonar un grupo de consistencia de ONTAP

A partir de ONTAP 9.12.1, puede clonar un grupo de consistencia para crear una copia de un grupo de consistencia y su contenido. La clonación de un grupo de coherencia crea una copia de la configuración del grupo de coherencia, sus metadatos, como el tipo de aplicación, y todos los volúmenes y su contenido, como archivos, directorios, LUN o

espacios de nombres NVMe.

Acerca de esta tarea

Al clonar un grupo de consistencia, puede clonarlo con su configuración actual, pero con el contenido del volumen a medida que lo está o basado en una copia de Snapshot de grupo de consistencia existente.

La clonación de un grupo de consistencia solo se admite para todo el grupo de consistencia. No puede clonar un grupo de consistencia secundario individual en una relación jerárquica: Solo se puede clonar la configuración completa del grupo de consistencia.

Cuando clona un grupo de consistencia, no se clonan los siguientes componentes:

- Grupos de iniciadores
- Mapas de LUN
- Subsistemas NVMe
- Asignaciones del subsistema de espacio de nombres de NVMe

Antes de empezar

- Cuando se clona un grupo de coherencia, ONTAP no creará recursos compartidos de SMB para los volúmenes clonados si no se especifica un nombre de recurso compartido. * Los grupos de consistencia clonados no están montados si no se especifica una ruta de unión.
- Si intenta clonar un grupo de coherencia basado en una snapshot que no refleja los volúmenes constituyentes actuales del grupo de coherencia, se producirá un error en la operación.
- Después de clonar un grupo de consistencia, debe realizar la operación de asignación adecuada.

  Consulte Asigne iGroups a varias LUNo Asignar un espacio de nombres NVMe a un subsistema para obtener más información.

- No se admite la clonado de un grupo de coherencia en una relación de sincronización activa de SnapMirror o con ningún volumen de DP asociado.

System Manager

Pasos

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de consistencia que desea clonar en el menú **Grupo de consistencia**.
3. En la parte superior derecha de la página de descripción general del grupo de consistencia, seleccione **Clonar**.
4. Introduzca un nombre para el nuevo grupo de consistencia clonado o acepte el nombre predeterminado.
   a. Seleccione si desea activar "**Thin Provisioning**".
   b. Elija **Split Clone** si desea disociar el grupo de consistencia de su origen y asignar espacio en disco adicional para el grupo de consistencia clonado.
5. Para clonar el grupo de consistencia en su estado actual, elija **Agregar una nueva instantánea**.

   Para clonar el grupo de consistencia basado en una instantánea, seleccione **Usar una instantánea existente**. Si selecciona esta opción, se abrirá un nuevo submenú. Seleccione la snapshot que desea usar como base para la operación de clonado.
6. Seleccione **Clonar**.
7. Vuelva al menú **Grupo de consistencia** para confirmar que el grupo de consistencia ha sido clonado.

CLI

A partir de ONTAP 9.14.1, puede clonar un grupo de consistencia mediante la CLI con credenciales de administrador del clúster.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Clonar un grupo de consistencia

1. El `consistency-group clone create` comando clona el grupo de coherencia en su estado actual de un momento específico. Para basar la operación de clonado en una snapshot, incluya `-source-snapshot` el parámetro.

   `consistency-group clone create -vserver` *`svm_name`* `-consistency-group` *`clone_name`* `-source-consistency-group` *`consistency_group_name`* `[-source-snapshot` *`snapshot_name`*`]`

   Obtenga más información sobre `consistency-group clone create` en el "Referencia de comandos del ONTAP".

Siguientes pasos

- Asigne iGroups a varias LUN
- Asignar un espacio de nombres NVMe a un subsistema

Eliminar un grupo de consistencia de ONTAP

Si decide que ya no necesita un grupo de consistencia, puede eliminarlo.

Acerca de esta tarea

- Al eliminar un grupo de coherencia se elimina la instancia del grupo de coherencia y *no* afecta a los volúmenes constituyentes o las LUN. Al eliminar un grupo de consistencia no, se eliminan las Snapshot presentes en cada volumen, pero ya no se podrá acceder a ellas como snapshots de grupo de coherencia. Sin embargo, las copias Snapshot pueden seguir gestionándose como snapshots granulares de volumen normales.
- ONTAP elimina automáticamente un grupo de coherencia si todos los volúmenes del grupo de coherencia se eliminan.
- Al eliminar un grupo de consistencia primario, se eliminan todos los grupos de consistencia secundarios asociados.
- Si utiliza una versión de ONTAP entre 9.10.1 y 9.12.0, los volúmenes solo se pueden eliminar de un grupo de coherencia si el volumen se elimina, en cuyo caso, el volumen se elimina automáticamente del grupo de coherencia. A partir de ONTAP 9.12.1, es posible quitar volúmenes de un grupo de consistencia sin eliminar el grupo de consistencia. Para obtener más información sobre este proceso, consulte Modificar un grupo de consistencia.

Ejemplo 7. Pasos

System Manager

1. Seleccione **almacenamiento > grupos de consistencia**.
2. Seleccione el grupo de coherencia que desea eliminar.
3. Junto al nombre del grupo de consistencia, seleccione ⋮ y luego **Eliminar**.

CLI

A partir de ONTAP 9.14.1, puede eliminar un grupo de consistencia mediante la CLI.

Antes de empezar

- Debe estar en el nivel de privilegio de administrador para realizar esta tarea.
- A partir de ONTAP 9.15.1, cualquier usuario con privilegios de administrador puede realizar esta tarea. En ONTAP 9.14.1, debe ser administrador del clúster o de SVM para realizarla.

Eliminar un grupo de consistencia

1. Elimine el grupo de consistencia:

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

SnapMirror síncrono activo

Introducción

Obtenga más información sobre la sincronización activa de ONTAP SnapMirror

La sincronización activa de SnapMirror , también conocida como SnapMirror Business Continuity (SM-BC), permite que los servicios comerciales sigan funcionando en caso de una falla total del sitio. Esta tecnología permite que las aplicaciones conmuten sin problemas a una copia secundaria sin intervención manual ni secuencias de comandos personalizadas.

NetApp SnapMirror active sync (SM-as) está diseñado para ser una protección a nivel de aplicación más granular, de menor costo y más fácil de usar con conmutación por error automática. La sincronización activa de SnapMirror permite que los servicios empresariales de misión crítica sigan funcionando, incluso durante una falla total del sitio. Con la sincronización activa de SnapMirror , ahora puede replicar de forma sincrónica múltiples volúmenes de una aplicación (agregándolos a un grupo de consistencia) entre sitios en ubicaciones geográficamente dispersas. Puede conmutar automáticamente por error a la copia secundaria en caso de interrupción de la copia principal, lo que permite la continuidad del negocio para las aplicaciones de nivel uno.

Las regulaciones para las instituciones financieras en algunos países requieren que las empresas brinden servicio periódicamente desde sus centros de datos secundarios. La sincronización activa de SnapMirror , con sus clústeres de alta disponibilidad, permite estas conmutaciones de centros de datos para la continuidad del negocio.

Disponible a partir de ONTAP 9.9.1, la sincronización activa de SnapMirror es compatible con clústeres AFF y All-Flash SAN Array (ASA). Los clústeres primarios y secundarios deben ser del mismo tipo: ASA, ASA r2 o AFF. La sincronización activa de SnapMirror protege las aplicaciones con LUN iSCSI o FCP o espacios de nombres NVMe.

La sincronización activa de SnapMirror admite configuraciones simétricas y asimétricas. El soporte para activo/activo simétrico se introdujo en ONTAP 9.15.1. La configuración activa/activa simétrica permite que ambas copias de un LUN protegido realicen operaciones de E/S de lectura y escritura con replicación sincrónica bidireccional, lo que permite que cada copia de LUN atienda solicitudes de E/S locales.

> A partir de julio de 2024, el contenido de informes técnicos publicados anteriormente como archivos PDF se ha integrado con la documentación de los productos de ONTAP. La documentación de sincronización activa de SnapMirror de ONTAP ahora incluye contenido de *TR-4878: SnapMirror active sync*.

Beneficios

SnapMirror Active Sync ofrece las siguientes ventajas:

- Disponibilidad continua para aplicaciones vitales para el negocio.
- Capacidad para alojar aplicaciones críticas alternativamente desde sitios primarios y secundarios.
- Gestión de aplicaciones simplificada utilizando grupos de coherencia para consistencia de escritura dependiente.
- Posibilidad de probar la conmutación al respaldo de cada aplicación.
- Creación instantánea de clones reflejados sin que afecte a la disponibilidad de las aplicaciones.
- La capacidad para poner en marcha cargas de trabajo protegidas y sin protección en el mismo clúster de ONTAP.
- El LUN, el espacio de nombres NVMe, el subsistema NVMe o la identidad de la unidad de almacenamiento siguen siendo los mismos, por lo que la aplicación los ve como un dispositivo virtual compartido.

- La capacidad de reutilizar clústeres secundarios con flexibilidad para crear clones instantáneos para el uso de las aplicaciones con fines de generación de informes, UAT o prueba de desarrollo, sin que el rendimiento ni la disponibilidad de las aplicaciones se vean afectados.

La sincronización activa de SnapMirror le permite proteger sus LUN de datos o espacios de nombres NVMe, lo que permite que las aplicaciones conmuten por error de forma transparente para garantizar la continuidad del negocio en caso de desastre. Para obtener más información, consulte "Casos de uso" .

Conceptos clave

La sincronización activa de SnapMirror utiliza grupos de consistencia para garantizar que sus datos se repliquen. La sincronización activa de SnapMirror utiliza ONTAP Mediator o, a partir de ONTAP 9.17.1, Cloud Mediator para conmutación por error automatizada, lo que garantiza que los datos se entreguen en caso de un desastre. Al planificar la implementación de la sincronización activa de SnapMirror , es importante comprender los conceptos esenciales de la sincronización activa de SnapMirror y su arquitectura.

Asimetría y simetría

En configuraciones simétricas activas/activas, ambos sitios pueden acceder al almacenamiento local para E/S activas. Esta configuración está optimizada para aplicaciones en clúster, como VMware vMSC, Windows Failover Cluster con SQL y Oracle RAC.

En configuraciones activas/activas asimétricas, los datos del sitio secundario se envían a un LUN, un espacio de nombres o una unidad de almacenamiento.

Para obtener más información, consulte Arquitectura de Active Sync de SnapMirror.

Grupo de consistencia

Para los sistemas AFF y ASA , "grupo de consistencia" Es una colección de volúmenes FlexVol que garantiza la consistencia de la carga de trabajo de la aplicación, la cual debe protegerse para la continuidad del negocio. En sistemas ASA r2, un grupo de consistencia es una colección de unidades de almacenamiento.

El propósito de un grupo de consistencia es tomar instantáneas simultáneas de una colección de volúmenes o unidades de almacenamiento, garantizando así copias de la colección consistentes ante fallos en un momento dado. Un grupo de consistencia garantiza que todos los volúmenes de un conjunto de datos se inactiven y luego se instale en el mismo momento. Esto proporciona un punto de restauración consistente con los datos en todos los volúmenes o unidades de almacenamiento que lo soportan. De este modo, un grupo de consistencia mantiene la consistencia del orden de escritura dependiente. Si decide proteger las aplicaciones para la continuidad del negocio, el grupo de volúmenes o unidades de almacenamiento correspondiente a esta aplicación debe agregarse a un grupo de consistencia para establecer una relación de protección de datos entre los grupos de consistencia de origen y destino. Los grupos de consistencia de origen y destino deben contener el mismo número y tipo de volúmenes.

Componente

Un volumen individual, LUN o espacio de nombres NVMe (a partir de ONTAP 9.17.1) que forma parte del grupo de consistencia protegido en la relación de sincronización activa de SnapMirror .

Mediador ONTAP

El "Mediador ONTAP" Recibe información sobre el estado de los clústeres y nodos de ONTAP emparejados, coordinando la conexión entre ambos y determinando si cada nodo/clúster está en buen estado y en funcionamiento. ONTAP Mediator proporciona información sobre el estado de:

- Clústeres de ONTAP entre iguales
- Nodos del clúster de ONTAP en paridad

- Grupos de consistencia (que definen las unidades de conmutación por error en una relación de sincronización activa de SnapMirror); para cada grupo de consistencia, se proporciona la siguiente información:
  - Estado de replicación: No inicializado, en sincronización o fuera de sincronización
  - Qué clúster aloja la copia principal
  - Contexto de operación (utilizado para failover planificado)

Con esta información de estado de ONTAP Mediator, los clusters pueden diferenciar entre distintos tipos de fallos y determinar si se debe realizar una conmutación por error automatizada. ONTAP Mediator es uno de los tres componentes del quórum de sincronización activa de SnapMirror junto con los dos clústeres ONTAP (primario y secundario). Para llegar a un consenso, al menos dos partes en el quórum deben acordar una determinada operación.

> A partir de ONTAP 9.15.1, System Manager muestra el estado de su relación de sincronización activa de SnapMirror en cualquier clúster. También puede supervisar el estado de los mediadores de ONTAP desde cualquier clúster en System Manager. En versiones anteriores de ONTAP, System Manager muestra el estado de las relaciones de sincronización activa de SnapMirror del clúster de origen.

Mediador de la nube de ONTAP

ONTAP Cloud Mediator está disponible a partir de ONTAP 9.17.1. ONTAP Cloud Mediator proporciona los mismos servicios que ONTAP Mediator, excepto que está alojado en la nube mediante la consola de NetApp .

Conmutación al respaldo planificada

Operación manual para cambiar los roles de las copias en una relación de sincronización activa de SnapMirror. Los sitios primarios se convierten en los secundarios y los secundarios se convierten en los primarios.

Conmutación automática al respaldo no planificada (AUFO)

Una operación automática para ejecutar una conmutación por error a la copia de mirroring. La operación requiere ayuda del Mediador ONTAP para detectar que la copia primaria no está disponible.

Sesgo primario-primero y primario

La sincronización activa de SnapMirror emplea un principio primario, que da preferencia a la copia primaria para servir E/S en caso de una partición de red.

El sesgo primario es una implementación de quórum especial que mejora la disponibilidad de un conjunto de datos protegido con SnapMirror con sincronización activa. Si la copia primaria está disponible, se aplica el sesgo primario cuando no se puede acceder al mediador ONTAP desde ambos clusters.

El sesgo primario-primero y primario se admiten en la sincronización activa de SnapMirror a partir de ONTAP 9.15.1. Las copias primarias se designan en System Manager y la salida con la API DE REST y la CLI.

Fuera de sincronización (OOS)

Cuando las operaciones de I/O de aplicaciones no se replican en el sistema de almacenamiento secundario, se informará como **fuera de sincronización**. Un estado fuera de sincronización significa que los volúmenes secundarios no se sincronizan con el primario (origen) y que no se está produciendo la replicación de SnapMirror.

Si el estado del espejo es `Snapmirrored` , esto indica que se ha establecido una relación SnapMirror y que la transferencia de datos está completa, lo que significa que el volumen de destino está actualizado con el volumen de origen.

La sincronización activa de SnapMirror admite la resincronización automática, lo cual permite que las copias regresen a un estado InSync.

A partir de ONTAP 9.15,1, SnapMirror active sync admite "reconfiguración automática en configuraciones ramificadas".

Configuración uniforme y no uniforme

- **El acceso uniforme al host** significa que los hosts de ambos sitios están conectados a todas las rutas a los clústeres de almacenamiento en ambos sitios. Las rutas entre sitios se extienden a distancias.
- **El acceso al host no uniforme** significa que los hosts en cada sitio están conectados solo al clúster en el mismo sitio. Las rutas entre sitios y las rutas extendidas no están conectadas.

Se admite el acceso uniforme de hosts en cualquier implementación de sincronización activa de SnapMirror; el acceso no uniforme de host solo se admite para implementaciones activo-activo simétricas.

RPO cero

RPO es la sigla en inglés para el objetivo de punto de recuperación, que es la cantidad de pérdida de datos que se considera aceptable durante un período de tiempo dado. El RPO de cero significa que no es aceptable ninguna pérdida de datos.

RTO CERO

El objetivo de tiempo de recuperación es el objetivo de tiempo de recuperación, que es la cantidad de tiempo que se considera aceptable para que una aplicación regrese a las operaciones normales sin interrupciones después de una interrupción, un fallo u otro evento de pérdida de datos. El objetivo de tiempo de recuperación cero significa que no se acepta ningún tiempo de inactividad.

Compatibilidad con la configuración de sincronización activa de SnapMirror según la versión de ONTAP

La compatibilidad con la sincronización activa de SnapMirror varía según la versión de ONTAP:

Versión de ONTAP	Clústeres compatibles	Protocolos compatibles	Configuraciones admitidas

9.17.1 y posteriores	• AFF • ASA • C-Series • ASA r2	• iSCSI • FC • NVMe para cargas de trabajo de VMware	• Asimétrico activo/activo Asymmetric active/active no es compatible con ASA r2 y NVMe. Para obtener más información sobre la compatibilidad con NVMe, consulta "Configuración, compatibilidad y limitaciones de NVMe". • Activo-activo simétrico
9.16.1 y posterior	• AFF • ASA • C-Series • ASA r2	• iSCSI • FC	• Asimétrico activo/activo • Activo/activo simétrico Las configuraciones activo/activo simétrico admiten clústeres de 4 nodos a 4 nodos en ONTAP 9.16.1 y versiones posteriores. Para ASA r2, solo se admiten clústeres de 2 nodos.

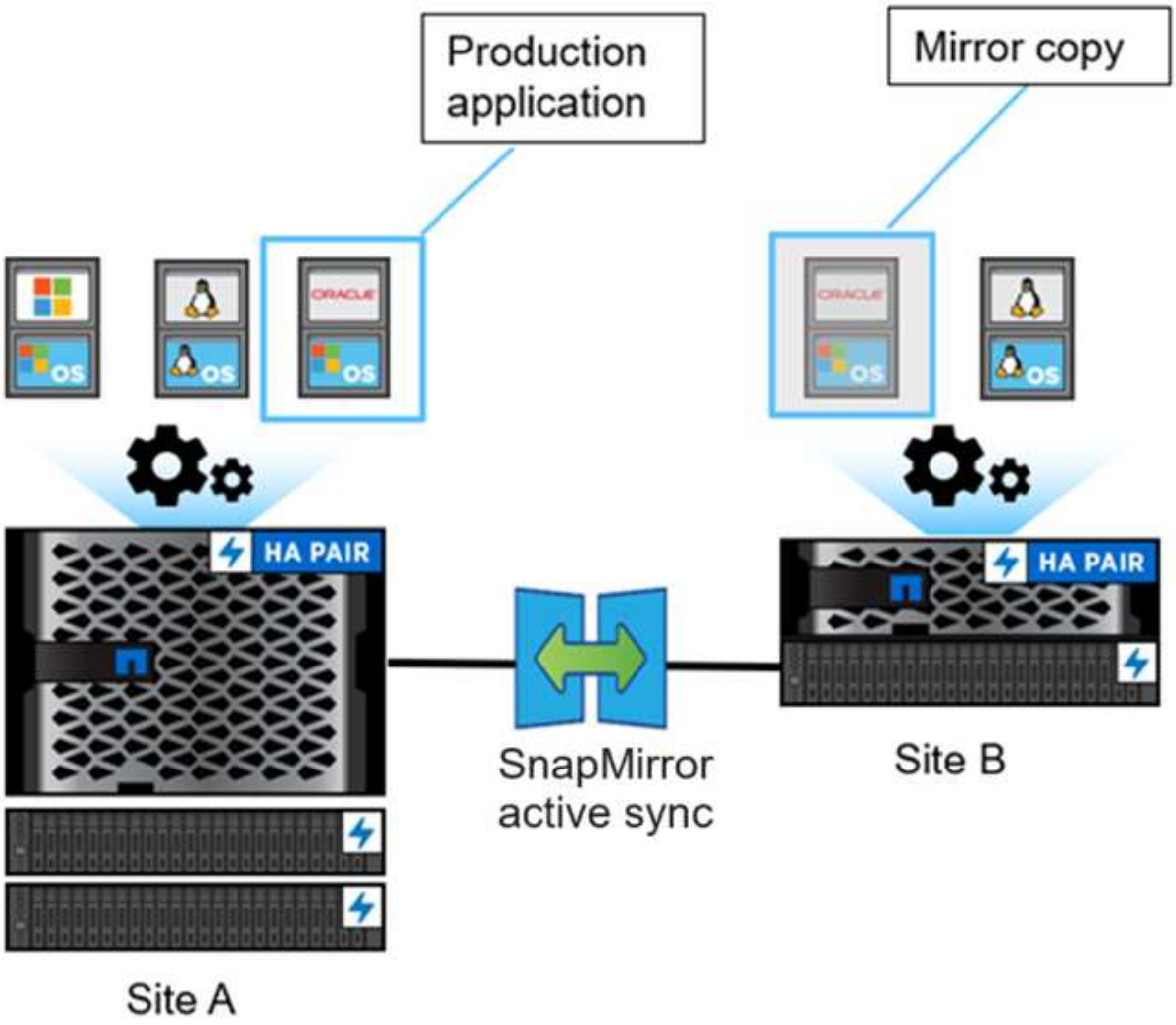
9.15.1 y posteriores	• AFF • ASA • C-Series	• iSCSI • FC	• Asimétrico activo/activo • Activo/activo simétrico Las configuraciones activo/activo simétricas admiten clústeres de 2 nodos en ONTAP 9.15.1. Los clústeres de 2 nodos a 2 nodos y los clústeres de 4 nodos a 4 nodos se admiten en ONTAP 9.16.1 y versiones posteriores.
9.9.1 y posterior	• AFF • ASA • C-Series	• iSCSI • FC	Asimétrico activo/activo

Los clústeres primarios y secundarios deben ser del mismo tipo: "ASA" , "ASA r2" , o AFF.

Arquitectura de sincronización activa de ONTAP SnapMirror

La arquitectura de sincronización activa de SnapMirror permite cargas de trabajo activas en ambos clústeres, donde las cargas de trabajo principales se pueden atender simultáneamente desde ambos clústeres. Las regulaciones para las instituciones financieras en algunos países también requieren que las empresas brinden servicio periódico desde sus centros de datos secundarios, implementaciones llamadas "Tick-Tock", que la sincronización activa de SnapMirror permite.

La relación de protección de datos para la continuidad del negocio se crea entre el sistema de almacenamiento de origen y el de destino, añadiendo al grupo de consistencia los LUN o espacios de nombres NVMe específicos de la aplicación de diferentes volúmenes dentro de una máquina virtual de almacenamiento (SVM). En condiciones normales de funcionamiento, la aplicación empresarial escribe en el grupo de consistencia principal, que replica sincrónicamente esta E/S en el grupo de consistencia espejo.



Aunque existen dos copias independientes de los datos en la relación de protección de datos, dado que la sincronización activa de SnapMirror mantiene la misma identidad de LUN o espacio de nombres NVMe, el host de la aplicación lo considera un dispositivo virtual compartido con múltiples rutas, mientras que solo se escribe en una copia de LUN o espacio de nombres NVMe a la vez. Cuando un fallo deja fuera de línea el sistema de almacenamiento principal, ONTAP lo detecta y utiliza el Mediador para la reconfirmación. Si ni ONTAP ni el Mediador pueden hacer ping al sitio principal, ONTAP realiza la conmutación por error automática. Este proceso da como resultado la conmutación por error de solo una aplicación específica sin la necesidad de intervención manual o scripts que antes eran necesarios para el propósito de la conmutación por error.

Otros puntos a considerar:

- Los volúmenes no reflejados que existen fuera de la protección para la continuidad del negocio son compatibles.
- Solo se admite otra relación asíncrona de SnapMirror para los volúmenes que se están protegiendo para la continuidad del negocio.
- La protección para la continuidad del negocio no admite las topologías en cascada.

El papel de los mediadores

La sincronización activa de SnapMirror utiliza un mediador que actúa como testigo pasivo de las copias de sincronización activa de SnapMirror . En caso de una partición de red o de indisponibilidad de una copia, la sincronización activa de SnapMirror utiliza el mediador para determinar qué copia continúa prestando servicios de E/S, mientras que interrumpe la E/S en la otra. Además de ONTAP Mediator local, a partir de ONTAP 9.17.1, puede instalar ONTAP Cloud Mediator para ofrecer la misma funcionalidad en una implementación en la nube. Puede usar ONTAP Mediator u ONTAP Cloud Mediator, pero no puede usar ambos a la vez.

El Mediador desempeña un papel crucial en las configuraciones de sincronización activa de SnapMirror como testigo pasivo de quórum, garantizando el mantenimiento del quórum y facilitando el acceso a los datos durante fallos. Actúa como un proxy de ping para que los controladores determinen la actividad de los controladores pares. Si bien el Mediador no activa las operaciones de conmutación, cumple una función vital al permitir que el nodo superviviente verifique el estado de su socio durante problemas de comunicación de red. Como testigo de quórum, el Mediador de ONTAP proporciona una ruta alternativa (que actúa como proxy) al clúster par.

Además, permite que los clústeres obtengan esta información como parte del proceso de quórum. Utiliza el LIF de administración de nodos y el LIF de administración de clústeres para fines de comunicación. Establece conexiones redundantes a través de múltiples rutas para diferenciar entre fallos de sitio y fallos de enlace entre conmutadores (ISL). Cuando un clúster pierde la conexión con el software Mediator y todos sus nodos debido a un evento, se considera inaccesible. Esto activa una alerta y habilita la conmutación por error automatizada al grupo de consistencia de espejo en el sitio secundario, lo que garantiza una E/S ininterrumpida para el cliente. La ruta de datos de replicación se basa en un mecanismo de latido, y si un fallo o evento de red persiste más allá de cierto período, puede resultar en fallos de latido, causando que la relación se desincronice. Sin embargo, la presencia de rutas redundantes, como la conmutación por error del LIF a otro puerto, puede mantener el latido y prevenir dichas interrupciones.

Mediador ONTAP

ONTAP Mediator se instala en un tercer dominio de fallos, distinto de los dos clústeres de ONTAP que supervisa. Esta configuración consta de tres componentes clave:

- Clúster de ONTAP principal que aloja el grupo de consistencia principal de SnapMirror Active Sync
- Clúster de ONTAP secundario que aloja el grupo de coherencia de reflejos
- Mediador ONTAP

ONTAP Mediator se utiliza para los siguientes fines:

- Establecer un quórum
- Disponibilidad continua mediante conmutación por error automática (AUFO)
- Conmutaciones al respaldo planificadas (PFO)

ONTAP Mediator 1.7 puede administrar diez pares de clústeres para la continuidad del negocio.

Cuando el Mediador de ONTAP no está disponible, no se pueden realizar conmutaciones por error planificadas o automatizadas. Los datos de la aplicación continúan replicándose de forma sincrónica sin interrupciones, sin pérdida de datos.

Mediador de la nube de ONTAP

A partir de ONTAP 9.17.1, ONTAP Cloud Mediator está disponible como un servicio basado en la nube en la consola de NetApp para usar con la sincronización activa de SnapMirror . Al igual que ONTAP Mediator, ONTAP Cloud Mediator ofrece las siguientes funciones en una relación de sincronización activa de SnapMirror

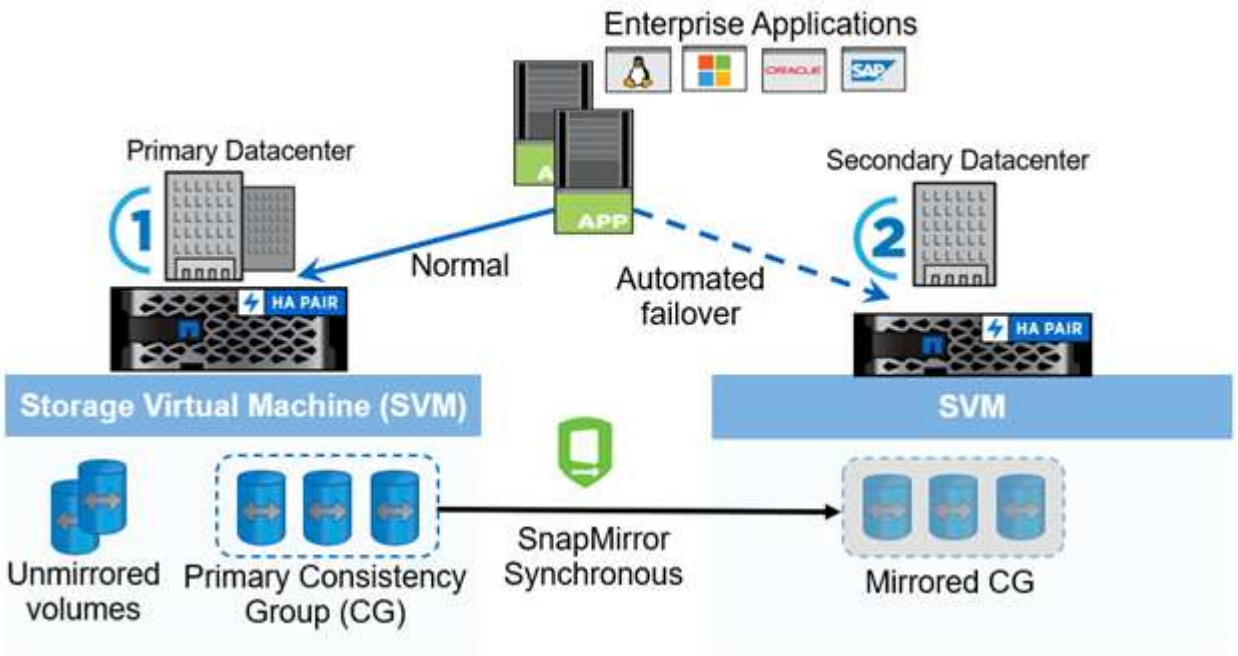
:

- Proporciona un almacenamiento persistente y protegido para metadatos de sincronización activa de HA o SnapMirror .
- Funciona como proxy ping para la vida útil de la controladora.
- Proporciona funcionalidad de consulta de estado de nodo síncrono para ayudar a determinar el quórum.

ONTAP Cloud Mediator ayuda a simplificar la implementación de sincronización activa de SnapMirror al usar el servicio de nube de la consola NetApp como un tercer sitio que no necesita administrar. ONTAP Cloud Mediator ofrece la misma funcionalidad que ONTAP Mediator local; sin embargo, reduce la complejidad operativa de mantener un sitio externo . Por otro lado, ONTAP Mediator está disponible como paquete y debe instalarse en un host Linux que se ejecute en un sitio externo con infraestructura de red y alimentación independiente para sus operaciones.

Flujo de trabajo de la operación de sincronización activa de SnapMirror

La siguiente figura muestra el diseño de SnapMirror sincronización activa a nivel superior.



El diagrama muestra una aplicación empresarial alojada en una máquina virtual de almacenamiento (SVM) en el centro de datos principal. La SVM contiene cinco volúmenes, tres de los cuales forman parte de un grupo de coherencia. Los tres volúmenes del grupo de coherencia se reflejan en un centro de datos secundario. En circunstancias normales, todas las operaciones de escritura se realizan en el centro de datos primario; en efecto, este centro de datos sirve como origen de operaciones de I/O, mientras que el centro de datos secundario sirve como destino.

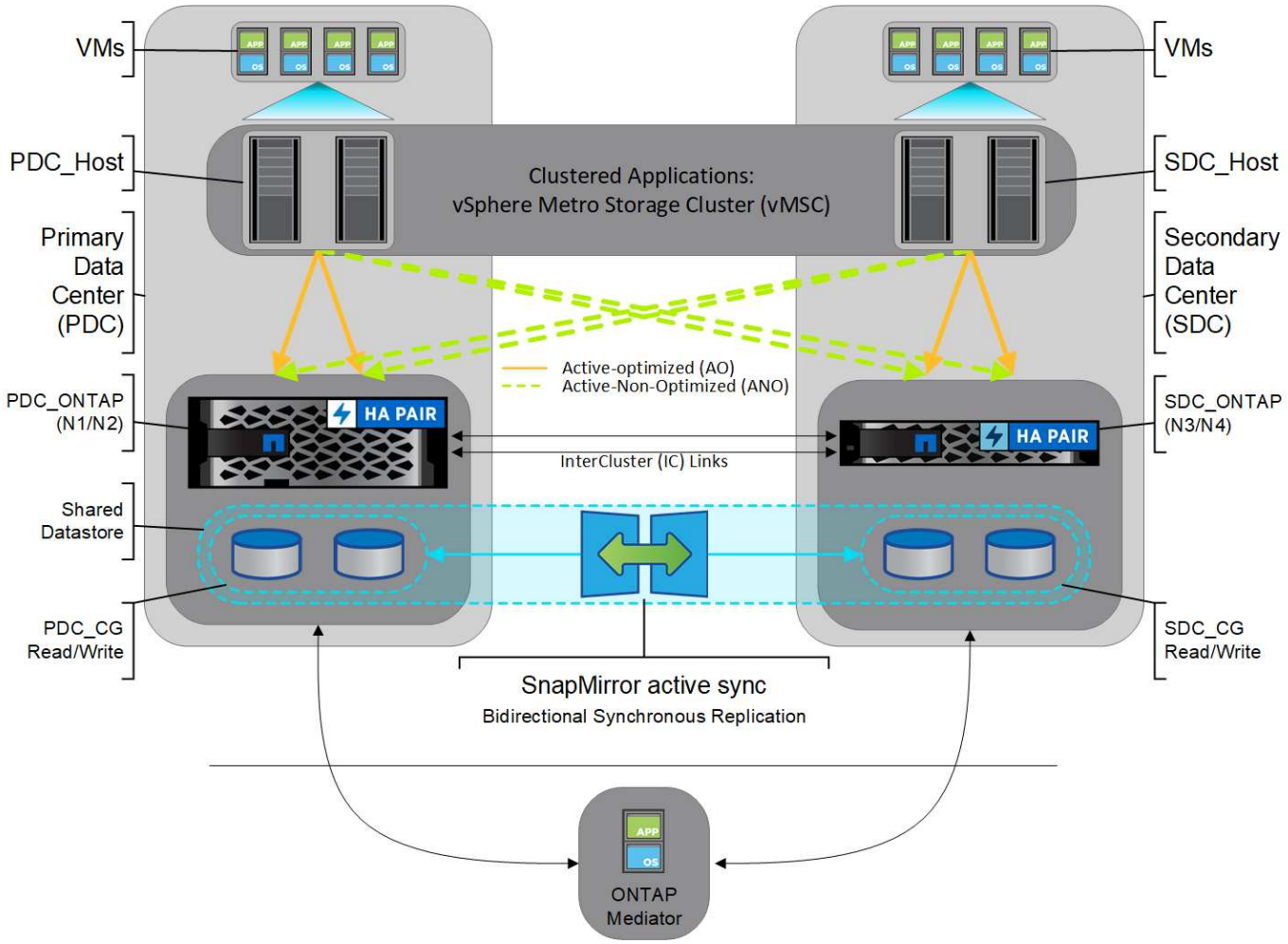
En caso de un desastre en el centro de datos principal, ONTAP ordena al centro de datos secundario que actúe como principal, atendiendo todas las operaciones de E/S. Solo se sirven los volúmenes que están reflejados en el grupo de consistencia. Cualquier operación relacionada con los otros dos volúmenes en el SVM se verá afectada por el evento de desastre.

Activo-activo simétrico

SnapMirror Active Sync ofrece soluciones asimétricas y simétricas.

En configuraciones asimétricas, la copia de almacenamiento principal expone una ruta optimizada activa y atiende activamente la E/S del cliente. El sitio secundario utiliza una ruta remota para la E/S. Las rutas de almacenamiento del sitio secundario se consideran activas no optimizadas. El acceso al LUN de escritura se redirige mediante proxy desde el sitio secundario. El protocolo NVMe no es compatible con las configuraciones asimétricas.

En *configuraciones activas/activas simétricas*, las rutas optimizadas para activas están expuestas en ambos sitios, son específicas de cada host y son configurables, lo que significa que los hosts de ambos lados pueden acceder al almacenamiento local para I/O activa. A partir de ONTAP 9.16.1, las activas/activas simétricas se admiten en clústeres de 2 nodos y en clústeres de 4 nodos. SnapMirror active sync admite configuraciones de clúster de 2 nodos a clúster de 2 nodos y configuraciones de clúster de 4 nodos a clúster de 4 nodos. No admite configuraciones de clúster de 4 nodos a clúster de 2 nodos ni configuraciones de clúster de 2 nodos a clúster de 4 nodos. A partir de ONTAP 9.17.1, las configuraciones activas/activas simétricas admiten el protocolo NVMe en clústeres de 2 nodos.



Activo/activo simétrico está dirigido a aplicaciones en clúster, incluidas VMware Metro Storage Cluster, Oracle RAC y Windows Failover Clustering con SQL.

Casos de uso para la sincronización activa de ONTAP SnapMirror

Las demandas de un entorno empresarial conectado globalmente exigen una

recuperación rápida de datos de aplicaciones críticas para el negocio con cero pérdida de datos en caso de una interrupción como un ciberataque, un corte de energía o un desastre natural. Estas demandas se acentúan en áreas como las finanzas y aquellas que se adhieren a mandatos regulatorios como el Reglamento General de Protección de Datos (GDPR).

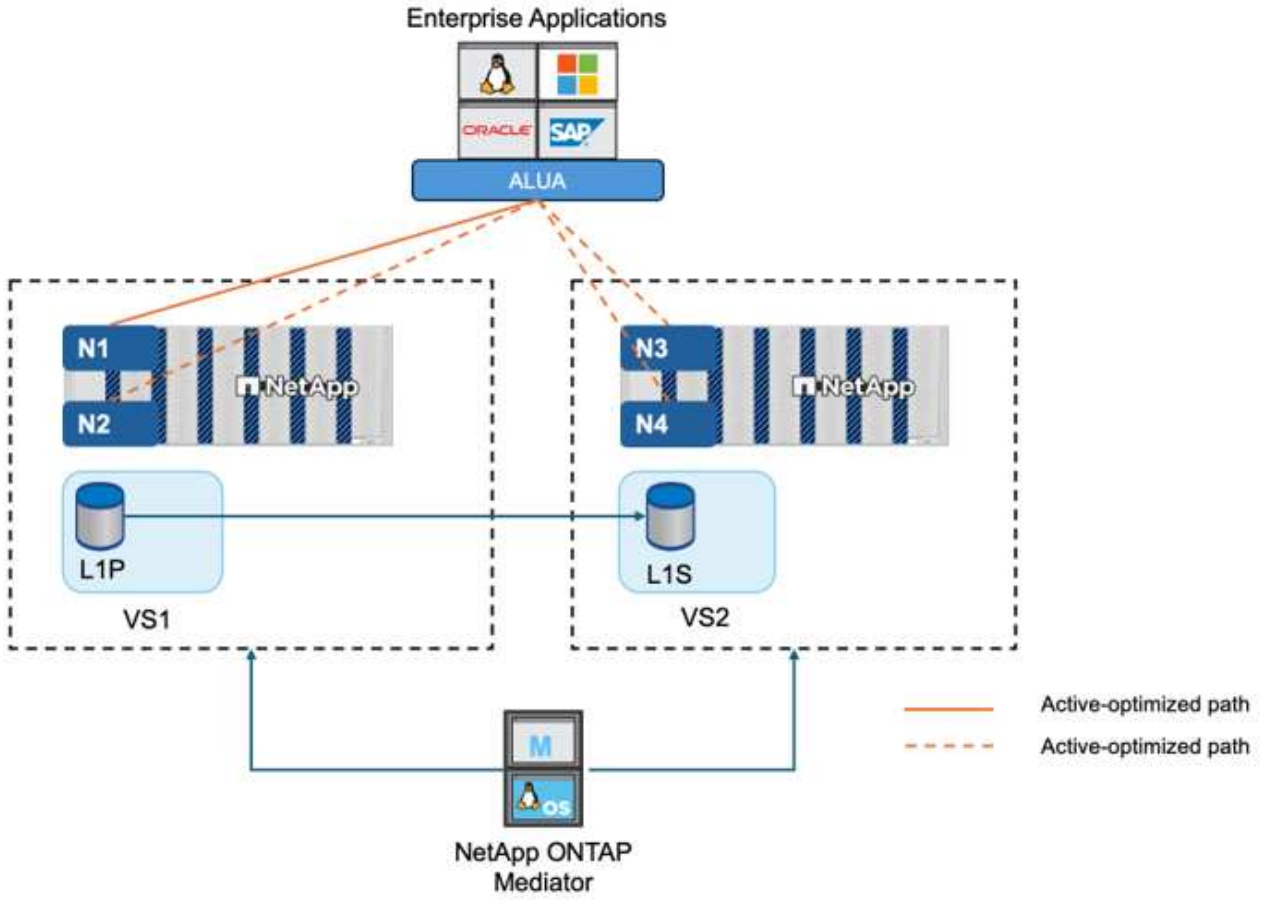
SnapMirror Active Sync proporciona los siguientes casos de uso:

Puesta en marcha de aplicaciones para un objetivo de tiempo de recuperación cero (RTO)

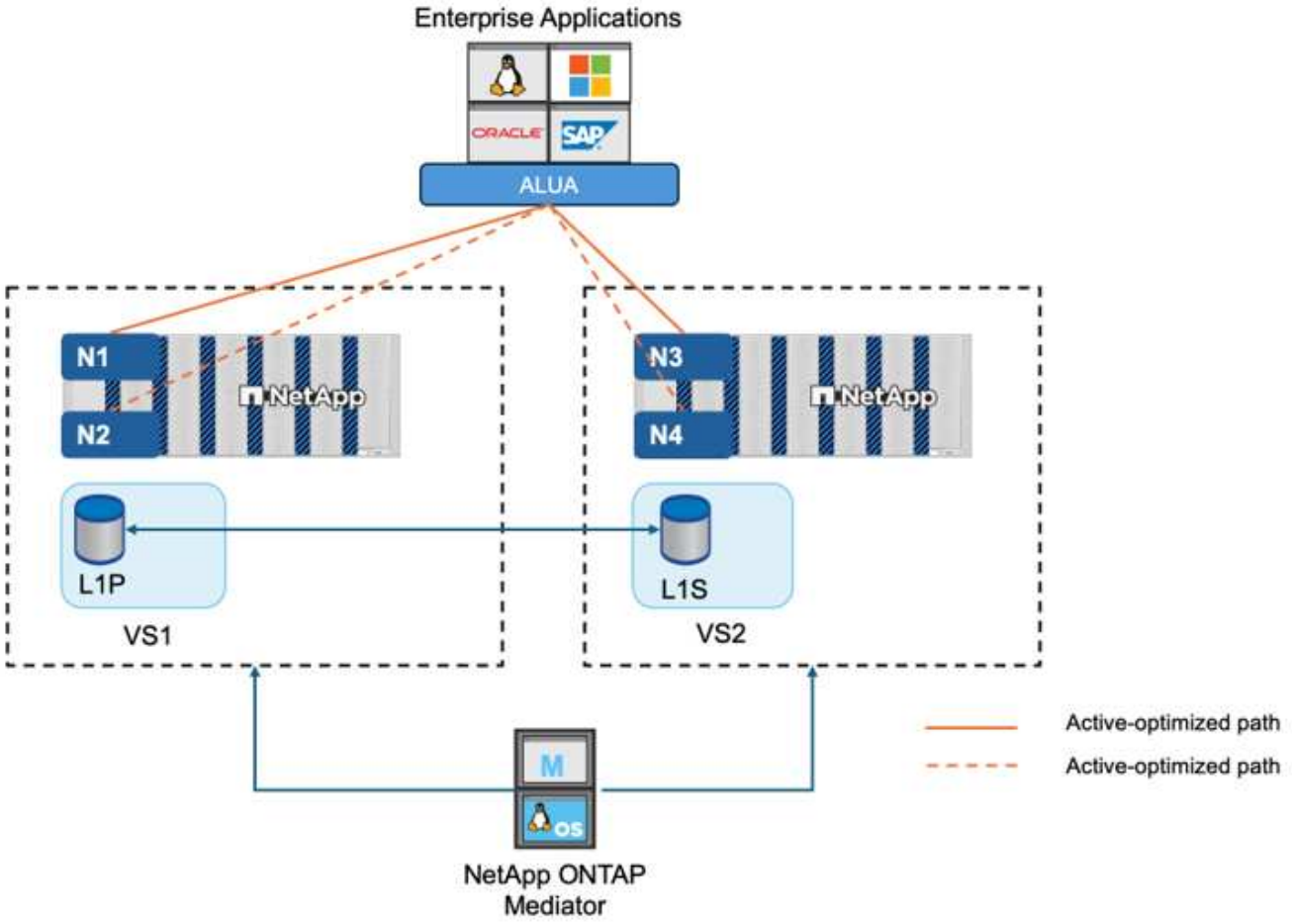
En una implementación de sincronización activa de SnapMirror , se cuenta con un clúster principal y uno secundario. Un LUN en el clúster principal `L1P`) tiene un espejo `L1S`) en el secundario; ambos LUN comparten el mismo ID de serie y se reportan como LUN de lectura y escritura al host. Sin embargo, en configuraciones asimétricas, las operaciones de lectura y escritura solo se realizan en el LUN principal. `L1P` Cualquier escritura en el espejo `L1S` son atendidos por poder.

Puesta en marcha de aplicaciones para un objetivo de tiempo de recuperación cero o una conmutación al respaldo transparente de aplicaciones (TAF)

TAF se basa en la conmutación por error de ruta basada en software MPIO del host para lograr un acceso sin interrupciones al almacenamiento. Ambas copias LUN (por ejemplo, la principal [L1P] y la copia espejo [L1S]) tienen la misma identidad (número de serie) y se informan como de lectura y escritura al host. Sin embargo, en configuraciones asimétricas, las lecturas y escrituras solo las atiende el volumen principal. Las E/S emitidas a la copia espejo se redirigen a la copia principal. La ruta preferida del host a L1 es VS1:N1, según el estado de acceso de unidad lógica asimétrica (ALUA) Activo Optimizado (A/O). ONTAP Mediator es necesario como parte de la implementación, principalmente para realizar la conmutación por error (planificada o no planificada) en caso de una interrupción del almacenamiento en el principal.



TAF opera en dos modos: Conmutación por error automatizada y Dúplex con conmutación por error automatizada. Con la conmutación por error automatizada, las lecturas y escrituras son atendidas únicamente por el volumen principal; por lo tanto, las E/S emitidas a la copia reflejada (que no puede atender escrituras por sí sola) se redirigen a la copia principal. Con la conmutación por error automatizada dúplex, tanto la copia principal como la secundaria pueden atender las E/S, por lo que no se requiere un proxy.



Si utiliza NVMe para el acceso al host con ONTAP 9.17.1, solo se admite la política AutomatedFailoverDuplex.

La sincronización activa de SnapMirror usa ALUA, un mecanismo que permite un software multivía de host de aplicaciones con rutas anunciadas con prioridades y disponibilidad de acceso para la comunicación del host de aplicaciones con la cabina de almacenamiento. ALUA marca las rutas activas optimizadas a las controladoras propietarias del LUN y otras como rutas activas no optimizadas, utilizadas solo si falla la ruta primaria.

La sincronización activa de SnapMirror con el protocolo NVMe utiliza acceso asimétrico al espacio de nombres (ANA), que permite a los hosts de aplicaciones descubrir rutas optimizadas y no optimizadas a los espacios de nombres NVMe que están siendo protegidos. El destino NVMe de ONTAP publica los estados de ruta adecuados para que los hosts de aplicaciones utilicen la ruta óptima para un espacio de nombres NVMe protegido.

Aplicaciones en clúster

Las aplicaciones agrupadas, incluidas VMware Metro Storage Cluster, Oracle RAC y Windows Failover Clustering con SQL, requieren acceso simultáneo para que las máquinas virtuales puedan conmutarse por error a otro sitio sin ninguna sobrecarga de rendimiento. SnapMirror active sync symmetric active/active sirve IO localmente con replicación bidireccional para satisfacer los requisitos de las aplicaciones en clúster. A partir

de ONTAP 9.16.1, se admite la configuración activa/activa simétrica en clústeres de cuatro nodos, ampliando el límite de clústeres de dos nodos en ONTAP 9.15.1.

Situación de desastre

Replique de forma síncrona varios volúmenes para una aplicación entre sitios ubicados en ubicaciones dispersas geográficamente. Puede conmutar automáticamente por respaldo a la copia secundaria en caso de interrupción del almacenamiento primario, con lo que se permite la continuidad del negocio para aplicaciones de nivel uno. Cuando el sitio que aloja el clúster principal experimenta un desastre, el software multivía del host marca todas las rutas a través del clúster como inactivas y utiliza las rutas del clúster secundario. El resultado es una conmutación al respaldo sin interrupciones habilitada por ONTAP Mediator en la copia mirror.

Soporte de aplicaciones ampliado

La sincronización activa de SnapMirror brinda flexibilidad con granularidad a nivel de aplicación fácil de usar y conmutación por error automática. SnapMirror active sync utiliza la replicación sincrónica probada de SnapMirror sobre una red IP para replicar datos a altas velocidades a través de LAN o WAN, para lograr una alta disponibilidad de datos y una rápida replicación de datos para sus aplicaciones críticas para el negocio, como Oracle, Microsoft SQL Server, etc., tanto en entornos virtuales como físicos.

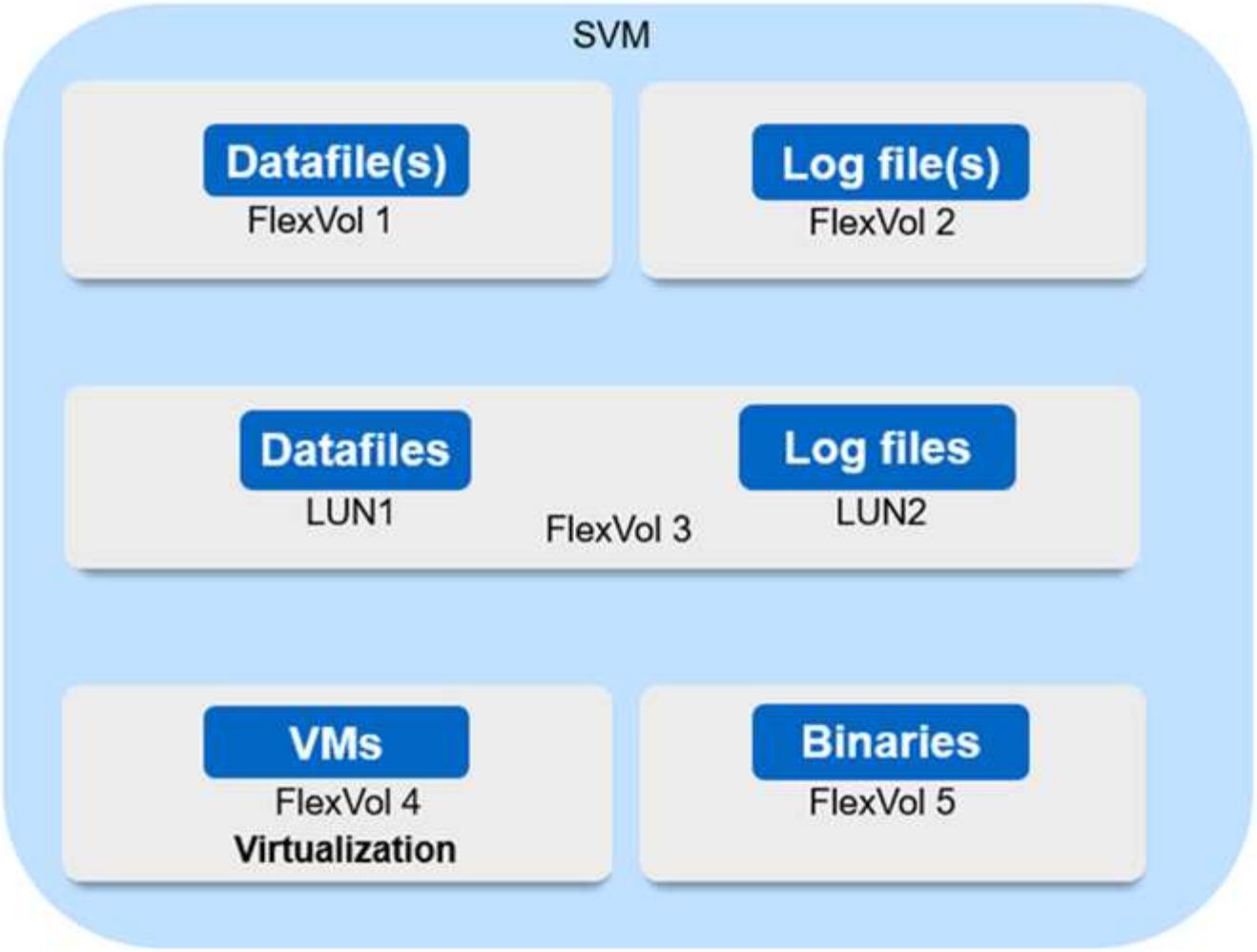
La sincronización activa de SnapMirror permite que los servicios empresariales de misión crítica sigan funcionando incluso ante una falla total del sitio, con TAF en la copia secundaria. No se requiere intervención manual ni secuencias de comandos adicionales para activar esta conmutación por error.

Estrategia de implementación y mejores prácticas para la sincronización activa de ONTAP SnapMirror

Es importante que su estrategia de protección de datos identifique claramente las cargas de trabajo que necesitan protegerse para la continuidad del negocio. El paso más crítico en su estrategia de protección de datos es tener claridad en el diseño de los datos de sus aplicaciones empresariales para que pueda decidir cómo distribuir los volúmenes y proteger la continuidad del negocio. Dado que la conmutación por error se produce a nivel del grupo de consistencia por aplicación, asegúrese de agregar los volúmenes de datos necesarios al grupo de consistencia.

Configuración de SVM

El diagrama captura una configuración de máquina virtual de almacenamiento (SVM) recomendada para la sincronización activa de SnapMirror.



- Para volúmenes de datos:
  - Las cargas de trabajo de lectura aleatoria están aisladas de escrituras secuenciales; por lo tanto, según el tamaño de la base de datos, los archivos de datos y de registro suelen colocarse en volúmenes independientes.
    - Para las bases de datos críticas de gran tamaño, el archivo de datos único se encuentra en FlexVol 1 y el archivo de registro correspondiente se encuentra en FlexVol 2.
    - Para una mejor consolidación, las bases de datos no críticas de tamaño pequeño a mediano se agrupan de modo que todos los archivos de datos se encuentran en FlexVol 1 y los archivos de registro correspondientes se encuentran en FlexVol 2. Sin embargo, perderá la granularidad a nivel de aplicación a través de esta agrupación.
  - Otra variante es tener todos los archivos dentro del mismo FlexVol 3, con archivos de datos en LUN1 y sus archivos de registro en LUN 2.
- Si su entorno está virtualizado, tendría todas las máquinas virtuales de varias aplicaciones empresariales compartidas en un almacén de datos. Normalmente, los equipos virtuales y los binarios de aplicaciones se replican de forma asíncrona mediante SnapMirror.

Planificación

Requisitos previos para la sincronización activa de ONTAP SnapMirror

Cuando planifique la implementación de sincronización activa de SnapMirror, asegúrese de haber cumplido los distintos requisitos de hardware, software y configuración del sistema.

Hardware subyacente

En la siguiente tabla se describen las configuraciones de clústeres de NetApp admitidas.

Tipo de clúster	Modelos compatibles	Funciones admitidas	Máximo de nodos de clúster admitidos
AFF	A-Series y C-Series	Conmutación por error automática dúplex (activo-activo simétrico), conmutación por error automatizada (activo-activo asimétrico)	• 2 (ONTAP 9.9.1 o posterior) • 4 (ONTAP 9.16.1 con configuraciones simétricas activa/activa)
ASA	A-Series y C-Series	Conmutación por error automática dúplex (activo-activo simétrico), conmutación por error automatizada (activo-activo asimétrico)	• 2 (ONTAP 9.9.1 o posterior • 4 (ONTAP 9.16.1 con configuraciones simétricas activa/activa)
ASA r2	Todo	Dúplex de conmutación por error automatizada (simétrico activo/activo)	• 2 (ONTAP 9.17.1 o anterior) • 4 (ONTAP 9.18.1 o posterior)

En la siguiente tabla se describe la capacidad de replicación entre tipos de cluster.

Tipo de clúster 1	Tipo de clúster 2	¿Es compatible con replicación?
Serie A de AFF	AFF C-Series	Sí
ASA r2 Serie A	ASA r2 Serie C	Sí
AFF	ASA	No
ASA	ASA r2	No
ASA r2	ASA r2	Sí

De NetApp

- ONTAP 9.9.1 o posterior
- Mediador ONTAP 1.2 o posterior
- Un servidor Linux o una máquina virtual para ONTAP Mediator que ejecute uno de los siguientes:

Versión de ONTAP Mediator	Versiones de Linux compatibles
1,11	• Red Hat Enterprise Linux ◦ Compatible: 9.5 [1] ◦ Recomendado: 10.1, 10.0, 9.7, 9.6, 9.4 y 8.10 • Rocky Linux 10,1, 9.7 y 8,10 • Oracle Linux 10.0 y 9.6
1,10	• Red Hat Enterprise Linux ◦ Compatible: 9.5 [1] ◦ Recomendado: 10.0, 9.6, 9.4 y 8,10 • Rocky Linux 10,0, 9.6 y 8,10
1.9.1	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendados: 9.5, 9.4, 9.2, 9.0, 8.10 y 8.8 • Rocky Linux 9.5 y 8.10
1,9	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendados: 9.5, 9.4, 9.2, 9.0, 8.10 y 8.8 • Rocky Linux 9.5 y 8.10
1,8	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendados: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 y 8.8 • Rocky Linux 9.4 y 8.10
1,7	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendado: 9.3, 9.2, 9.1, 9.0, 8.9 y 8.8 • Rocky Linux 9.3 y 8.9

1,6	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendado: 9.2, 9.1, 9.0 y 8,8 • Rocky Linux 9.2 y 8.8
1,5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6 • CentOS: 7.9, 7.8, 7.7 y 7.6
1,4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6 • CentOS: 7.9, 7.8, 7.7 y 7.6
1,3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6 • CentOS: 7.9, 7.8, 7.7 y 7.6
1,2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6 • CentOS: 7.9, 7.8, 7.7 y 7.6

1. Compatible significa que Red Hat ya no admite estas versiones de RHEL, pero ONTAP Mediator aún se puede instalar en ellas.

Licencia

Las siguientes licencias de SnapMirror están disponibles como parte del paquete de licencias ONTAP One y deben aplicarse en ambos clústeres:

- SnapMirror síncrono
- SnapMirror

> Si sus sistemas de almacenamiento ONTAP se adquirieron antes de junio de 2019, consulte "Claves de licencia maestra de ONTAP" para obtener la licencia sincrónica de SnapMirror requerida.

- Para vSphere Metro Storage Cluster (vMSC), se requiere una licencia de VMware vSphere.

Entorno de red

- El tiempo de ida y vuelta (RTT) de latencia entre clústeres debe ser inferior a 10 milisegundos.
- A partir de ONTAP 9.14,1, "Reservas persistentes de SCSI-3"es compatible con la sincronización activa de SnapMirror.

Protocolos compatibles

La sincronización activa de SnapMirror admite protocolos SAN.

- Los protocolos FC e iSCSI son compatibles a partir de ONTAP 9.9.1.
- El protocolo NVMe es compatible con cargas de trabajo de VMware a partir de ONTAP 9.17.1.

La sincronización activa de SnapMirror no admite lo siguiente con el protocolo NVMe:

- Configuraciones activas/activas simétricas de 4 nodos
- Configuraciones asimétricas activas/activas
- Cambios en el tamaño del grupo de consistencia

  No puedes ampliar ni reducir un grupo de coherencia de forma no disruptiva cuando usas el protocolo NVMe con SnapMirror active sync. Las operaciones de ampliación y reducción de grupos de coherencia son disruptivas cuando usas el protocolo NVMe con SnapMirror active sync.

- Coexistencia de LUN y espacios de nombres en el mismo grupo de consistencia.

Espacio IP

La sincronización activa de SnapMirror requiere el espacio IP predeterminado para las relaciones entre pares del clúster. No se admiten espacios IP personalizados.

Estilo de seguridad NTFS

El estilo de seguridad NTFS **no** es compatible con los volúmenes de sincronización activa de SnapMirror.

Mediador ONTAP

- El mediador de ONTAP debe aprovisionarse externamente y conectarse a ONTAP para lograr una conmutación por error transparente de la aplicación.
- Para que sea completamente funcional y permita la conmutación por error automática no planificada, el mediador ONTAP externo debe estar aprovisionado y configurado con clústeres ONTAP.
- ONTAP Mediator debe instalarse en un tercer dominio de falla, separado de los dos clústeres de ONTAP.
- Al instalar ONTAP Mediator, debe reemplazar el certificado autofirmado con un certificado válido firmado por una CA confiable y convencional.
- Para obtener más información sobre ONTAP Mediator, consulte "Prepárese para instalar ONTAP Mediator" .

Otros requisitos previos

- En versiones anteriores a ONTAP 9.15.1, las relaciones de sincronización activa de SnapMirror no son compatibles con volúmenes de destino de lectura y escritura (volúmenes convertidos a lectura y escritura desde DP en un activo-activo asimétrico). Antes de poder usar un volumen de lectura y escritura, debe convertirlo en un volumen DP creando una relación SnapMirror a nivel de volumen (asincrónica o sincrónica) y luego eliminando la relación. Para obtener más información, consulte "Convierta unas relaciones de SnapMirror existentes en sincronización activa de SnapMirror" .
- Las máquinas virtuales de almacenamiento que utilizan la sincronización activa de SnapMirror no se pueden unir a Active Directory como una computadora cliente.

Más información

- "Hardware Universe"
- "Descripción general de ONTAP Mediator"

Interoperabilidad de sincronización activa de ONTAP SnapMirror

SnapMirror Active Sync es compatible con numerosos sistemas operativos, hosts de aplicaciones y otras funciones en ONTAP.

Si desea obtener información específica sobre compatibilidad e interoperabilidad que no se cubre aquí, consulte la Herramienta de Matriz de Interoperabilidad ("IMT").

Hosts de aplicaciones

La sincronización activa de SnapMirror admite hipervisores, incluidos Hyper-V, ESXi, sistemas operativos como Red Hat Enterprise Linux (RHEL), Windows Server y soluciones de agrupamiento como vSphere Metro Storage Cluster (vMSC) y, a partir de ONTAP 9.14.1, Windows Server Failover Cluster.

Sistemas operativos

La sincronización activa de SnapMirror es compatible con numerosos sistemas operativos, como los siguientes:

- AIX mediante PVR (a partir de ONTAP 9.11.1)
- HP-UX (a partir de ONTAP 9.10.1)
- Solaris 11,4 (a partir de ONTAP 9.10.1)

AIX

A partir de ONTAP 9.11.1, AIX es compatible con la sincronización activa de SnapMirror a través de una solicitud de variación de política de funciones de ingeniería estándar (FPVR) con el acuerdo de que se entienden las siguientes estipulaciones:

- La sincronización activa de SnapMirror puede proporcionar protección de datos con objetivo de punto de recuperación cero, pero el proceso de conmutación por error con AIX requiere pasos adicionales para reconocer el cambio de ruta. Los LUN que no forman parte de un grupo de volúmenes raíz experimentarán una pausa de I/O hasta que `cfgmgr` se ejecute un comando. Esto puede automatizarse y la mayoría de las aplicaciones reanudarán las operaciones sin interrupciones adicionales.
- Por lo general, las LUN que forman parte de un grupo de volúmenes raíz no se deben proteger con la sincronización activa de SnapMirror. No es posible ejecutar `cfgmgr` el comando después de una conmutación al respaldo, lo que significa que se necesita un reinicio para reconocer los cambios en las rutas SAN. Todavía puede obtener una protección de datos con RPO cero del grupo de volúmenes raíz, pero la conmutación al respaldo provocará interrupciones.

Consulte con su equipo de cuenta de NetApp para obtener más información acerca de la sincronización activa de SnapMirror con AIX.

HP-UX

A partir de ONTAP 9.10.1, se admite la sincronización activa de SnapMirror para HP-UX.

Conmutación automática por error no planificada con HP-UX

Un evento de conmutación por error automática no planificada (AUFO) en el clúster maestro aislado puede ser causado por una falla de evento dual cuando se pierde la conexión entre el clúster principal y el secundario, y también se pierde la conexión entre el clúster principal y el mediador. Este se considera un evento raro, a diferencia de otros eventos AUFO.

- En este escenario, podría tardar más de 120 segundos en reanudarse la E/S en el host HP-UX. En función de las aplicaciones que se estén ejecutando, esto puede no provocar ninguna interrupción de I/o o o mensajes de error.
- Para remediar, debe reiniciar las aplicaciones en el host de HP-UX que tengan una tolerancia de interrupción inferior a 120 segundos.

Solaris

A partir de ONTAP 9.10.1, la sincronización activa de SnapMirror es compatible con Solaris 11,4.

Para garantizar que las aplicaciones cliente de Solaris no causen interrupciones cuando se produce un cambio de sitio no planificado en un entorno de sincronización activa de SnapMirror , modifique la configuración predeterminada del sistema operativo Solaris. Para configurar Solaris con la configuración recomendada, consulte la"Base de conocimientos de NetApp : Configuración recomendada de compatibilidad del host Solaris en la sincronización activa de SnapMirror" .

Interoperabilidad de ONTAP

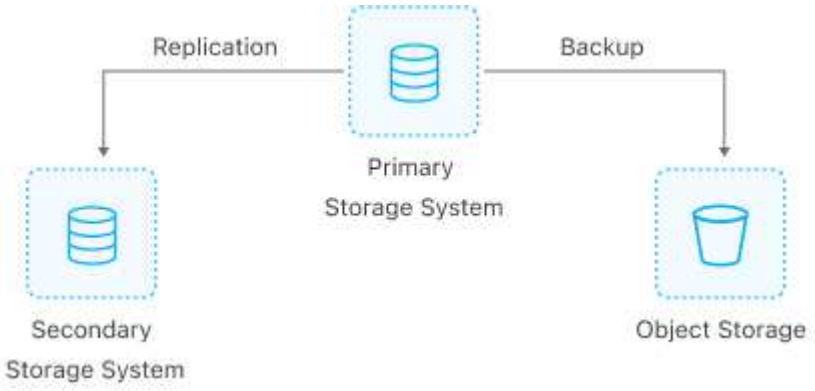
SnapMirror Active Sync se integra con componentes de ONTAP para ampliar sus funcionalidades de protección de datos.

FabricPool

La sincronización activa de SnapMirror admite volúmenes origen y destino en agregados de FabricPool con políticas de organización en niveles de Ninguna, Snapshot o Automática. La sincronización activa de SnapMirror no admite agregados de FabricPool usando una política de organización en niveles.

Configuraciones de dispersión

Enconfiguraciones de dispersión Su volumen de origen se puede reflejar en un punto final de destino de sincronización activa de SnapMirror y en una relación asincrónica de SnapMirror .



SnapMirror active sync es compatible configuraciones de dispersión con la `MirrorAllSnapshots` política y, a partir de ONTAP 9.11.1, la `MirrorAndVault` política. Las configuraciones de dispersión no se admiten en la sincronización activa de SnapMirror con `XDPDefault` la política.

A partir de ONTAP 9.15.1, la sincronización activa de SnapMirror admite la reconfiguración automática en la sección de distribución ramificada tras un evento de conmutación por error. Si la conmutación por error del sitio primario al secundario se ha realizado correctamente, el sitio terciario se vuelve a configurar automáticamente para tratar el sitio secundario como el origen. El tramo de distribución ramificada asíncrona puede ser una relación de grupo de coherencia o una relación de volumen independiente. La reconfiguración funcionará para cualquiera de los casos. La reconfiguración se activa mediante una conmutación al respaldo

planificada o sin planificar. La reconfiguración también se produce al realizar una conmutación de retorno tras recuperación en el sitio primario.

Para obtener información sobre la gestión de la configuración de distribución ramificada en versiones anteriores de ONTAP, consulte reanude la protección en la configuración de fan-out.

Restauración de NDMP

A partir de ONTAP 9.13.1, se puede usar NDMP para copiar y restaurar datoscon la sincronización activa de SnapMirror. El uso de NDMP le permite mover datos a la fuente de sincronización activa de SnapMirror para realizar una restauración sin pausar la protección. Esto resulta especialmente útil en configuraciones ramificadas.

SnapCenter

SnapMirror active sync es compatible con SnapCenter que comience por "SnapCenter 5,0". SnapCenter permite la creación de copias Snapshot que se pueden usar para proteger y recuperar aplicaciones y máquinas virtuales, lo que permite soluciones de almacenamiento siempre disponibles con granularidad en el nivel de las aplicaciones.

SnapRestore

La sincronización activa de SnapMirror admite SnapRestore parcial y de archivo único.

SnapRestore de archivo único

A partir de ONTAP 9.11,1, SnapRestore de archivo único se admite la sincronización activa de SnapMirror. Es posible restaurar un solo archivo desde una copia de Snapshot replicada desde el origen de sincronización activa de SnapMirror en el destino. Como los volúmenes pueden contener una o más LUN, esta función le ayuda a implementar una operación de restauración menos disruptiva, restaurando granularmente una única LUN sin interrumpir las otras LUN. Single File SnapRestore tiene dos opciones: In situ y fuera de sitio.

SnapRestore de archivo parcial

A partir de ONTAP 9.12,1, "Restauración parcial de LUN" se admite la sincronización activa de SnapMirror. Es posible restaurar los datos de copias de Snapshot creadas por la aplicación que se han replicado entre los volúmenes de origen (volumen) de sincronización activa de SnapMirror y los volúmenes de destino (Snapshot). Una restauración parcial del LUN o de archivos puede ser necesaria si necesita restaurar una base de datos en un host que almacena varias bases de datos en el mismo LUN. Para usar esta funcionalidad, se debe conocer el desplazamiento de bytes de inicio de los datos y el número de bytes.

Snapshots a prueba de manipulación

Las instantáneas a prueba de manipulaciones no son compatibles con SnapMirror active sync.

Grandes LUN y grandes volúmenes

La compatibilidad con LUN de gran tamaño y volúmenes de gran tamaño (más de 100 TB) depende de la versión de ONTAP que utilice y de su plataforma.

ONTAP 9.12.1P2 y versiones posteriores

- Para ONTAP 9.12,1 P2 y versiones posteriores, la sincronización activa de SnapMirror admite LUN grandes y volúmenes grandes de más de 100 TB en ASA y AFF (A-Series y C-Series). Los clústeres primario y secundario deben tener del mismo tipo: ASA o AFF. Se admite la replicación de AFF A-Series a AFF C-Series y viceversa.

> Para las versiones 9.12.1P2 de ONTAP y versiones posteriores, debe asegurarse de que los clústeres primario y secundario sean cabinas all-flash SAN (ASA) o cabina all-flash (AFF), y que ambas tengan instalado ONTAP 9.12.1 P2 o una versión posterior. Si el clúster secundario ejecuta una versión anterior a ONTAP 9.12.1P2, o si el tipo de cabina no es el mismo que el clúster primario, la relación síncrona puede desincronizarse si el volumen primario crece más de 100 TB.

ONTAP 9.9.1 - 9.12.1P1

- Para las versiones de ONTAP entre ONTAP 9.9.1 y 9.12.1 P1 (inclusive), las cabinas SAN all-flash solo admiten LUN de gran tamaño y volúmenes grandes superiores a 100TB TB. Se admite la replicación de AFF A-Series a AFF C-Series y viceversa.

> Para versiones de ONTAP entre ONTAP 9.9.1 y 9.12.1 P2, debe asegurarse de que los clústeres primario y secundario sean cabinas all-flash SAN, y que ambos tengan ONTAP 9.9.1 o una versión posterior instalada. Si el clúster secundario ejecuta una versión anterior a ONTAP 9.9.1, o si no es una cabina all-flash SAN, la relación síncrona puede desincronizarse si el volumen primario crece más de 100 TB.

Más información

- "Cómo configurar un host AIX para la sincronización activa de SnapMirror"

Límites de objetos para la sincronización activa de ONTAP SnapMirror

Cuando se prepare para usar la sincronización activa de SnapMirror, tenga en cuenta los siguientes límites de objetos.

Grupos de consistencia en un clúster

Los límites de grupos de consistencia de un clúster con sincronización activa de SnapMirror se calculan en función de las relaciones y dependen de la versión de ONTAP utilizada. Los límites son independientes de la plataforma.

Versión de ONTAP	Número máximo de relaciones
ONTAP 9.11.1 y versiones posteriores	50*
ONTAP 9.10.1	20
ONTAP 9.9.1	5

* A partir de ONTAP 9.16.1, la sincronización activa de SnapMirror admite clústeres de cuatro nodos en configuraciones activo-activo simétricas. En un clúster de cuatro nodos, se admiten 100 grupos de consistencia.

Volúmenes por grupo de coherencia

El número máximo de volúmenes por grupo de coherencia con la sincronización activa de SnapMirror es independiente de la plataforma.

Versión de ONTAP	Cantidad máxima de volúmenes admitidos en una relación de grupo de consistencia
ONTAP 9.15.1 y versiones posteriores	80
ONTAP 9.10.1-9.14.1	16
ONTAP 9.9.1	12

Volúmenes

Los límites de volúmenes en la sincronización activa de SnapMirror se calculan en función del número de extremos, no del número de relaciones. Un grupo de consistencia con 12 volúmenes contribuye con 12 extremos en el clúster primario y secundario. Tanto la sincronización activa de SnapMirror como las relaciones síncronas de SnapMirror contribuyen al número total de extremos.

Estos límites se aplican a los sistemas FAS, AFF y ASA . Si tiene un sistema ASA r2 (ASA A1K, ASA A90, ASA A70, ASA A50, ASA A30 o ASA A20), consulte "Documentación de ASA r2" .

En la siguiente tabla se incluyen los puntos finales máximos por plataforma.

Plataforma	Extremos por alta disponibilidad para sincronización activa de SnapMirror			Extremos de sincronización activa de SnapMirror y sincronización general por alta disponibilidad		
	ONTAP 9.11.1 y versiones posteriores	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.11.1 y versiones posteriores	ONTAP 9.10.1	ONTAP 9.9.1
AFF	400*	200	60	400	200	80
ASA	400*	200	60	400	200	80

* A partir de ONTAP 9.16.1, la sincronización activa de SnapMirror admite clústeres de cuatro nodos en configuraciones activo-activo simétricas. El límite total para un clúster de cuatro nodos es de 800 extremos.

Límites DE objetos DE SAN

En la siguiente tabla se incluyen los límites de objetos SAN. Los límites se aplican independientemente de la plataforma.

Objeto en una relación de sincronización activa de SnapMirror	Cuente
LUN por volumen	• 256 (ONTAP 9.9.1 - ONTAP 9.15.0) • 512 (ONTAP 9.15.1 y posterior)
Número de LUN, espacios de nombres o unidades de almacenamiento únicos por solución de sincronización activa SnapMirror 2 x 2	4.096

Objeto en una relación de sincronización activa de SnapMirror	Cuente
Número de LUN, espacios de nombres o unidades de almacenamiento únicos por solución de sincronización activa SnapMirror 4 x 4 (disponible a partir de ONTAP 9.16.1)	6.144
LIF por SVM (con al menos un volumen en una relación de sincronización activa de SnapMirror)	256
LIF entre clústeres por nodo	4
LIF entre clústeres por clúster	8

Límites de objetos NVMe

A partir de ONTAP 9.17.1, la sincronización activa de SnapMirror es compatible con el protocolo NVMe. Los límites de objetos NVMe se incluyen en la siguiente tabla.

Máximo de objetos en una relación de sincronización activa de SnapMirror	Cuente
Número de mapas de espacios de nombres por nodo	4K
Tamaño del clúster	2 nodos
Número de grupos de consistencia por par de HA	50
Número de volúmenes en un solo grupo de consistencia de sincronización activa de NVMe SnapMirror	80
Número de volúmenes en un par HA	400
Subsistemas NVMe por grupo de consistencia	16
Mapas de espacios de nombres por grupo de consistencia	256

Información relacionada

- "Hardware Universe"
- "Límites del grupo de consistencia"

Configurar

Configurar clústeres ONTAP para la sincronización activa de SnapMirror

La sincronización activa de SnapMirror utiliza clústeres emparejados para proteger sus datos en caso de conmutación por error. Antes de configurar ONTAP Mediator u ONTAP Cloud Mediator para la sincronización activa de SnapMirror , debe asegurarse de que el clúster esté configurado correctamente.

Antes de empezar

Antes de configurar ONTAP Mediator o ONTAP Cloud Mediator, debe confirmar lo siguiente:

1. Existe una relación de peering de clúster entre los clústeres.

   El espacio IP predeterminado es necesario en la sincronización activa de SnapMirror para las relaciones entre iguales de clústeres. No se admite un espacio IP personalizado.

   "Creación de una relación de paridad entre clústeres"

2. Las SVM se crean en cada clúster.

   "Creación de una SVM"

3. Existe una relación de pares entre las SVM de cada clúster.

   "Creación de una relación de paridad de SVM"

4. Los volúmenes existen para sus LUN.

   "Creación de un volumen"

5. Se crea al menos un SAN LIF (ya sea FC o iSCSI según corresponda) en cada nodo de ambos clústeres.

   "Consideraciones para los LIF en un entorno SAN de clúster"

   "Creación de una LIF"

6. Se crean los LUN necesarios y se asignan a un igroup, que se utiliza para asignar LUN al iniciador en el host de la aplicación.

   "Cree LUN y asigne iGroups"

7. Se vuelve a escanear el host de la aplicación para descubrir nuevos LUN.

Configurar el mediador de ONTAP para la sincronización activa de SnapMirror

SnapMirror Active Sync utiliza clústeres con conexión entre iguales para proteger los datos en caso de conmutación por error. ONTAP Mediator es un recurso clave que facilita la continuidad del negocio al supervisar el estado de cada clúster. Para configurar la sincronización activa de SnapMirror, primero debe instalar ONTAP Mediator y verificar que los clústeres principal y secundario estén configurados correctamente.

Una vez que haya instalado ONTAP Mediator y configurado sus clústeres, Inicializar ONTAP Mediator para la sincronización activa de SnapMirror mediante certificados autofirmados . Usted debe entonces Cree, inicialice y asigne el grupo de consistencia para la sincronización activa de SnapMirror.

Mediador ONTAP

ONTAP Mediator proporciona un almacenamiento persistente y protegido para metadatos de alta disponibilidad (HA) utilizados por los clústeres ONTAP en una relación de sincronización activa de SnapMirror. Además, ONTAP Mediator proporciona una funcionalidad de consulta de estado de nodos síncronos para ayudar a determinar el quórum y funciona como proxy de ping para la detección de vida de la controladora.

Cada relación de paridad de clústeres solo se puede asociar con una única instancia de ONTAP Mediator. Las instancias de HA Mediator no son compatibles. Cuando un clúster tiene varias relaciones entre iguales con otros clústeres, están disponibles las siguientes opciones de ONTAP Mediator:

- Si SnapMirror active sync está configurado en cada relación, cada relación de paridad de clústeres puede tener su propia instancia exclusiva de ONTAP Mediator.
- El cluster puede utilizar la misma instancia de Mediador de ONTAP para todas las relaciones entre iguales.

Por ejemplo, si el clúster B tiene una relación de paridad con el clúster A, el clúster C y el clúster D, las tres relaciones de paridad de clústeres pueden tener una instancia de mediador de ONTAP asociada única cuando SnapMirror active sync se configura en cada relación. Como alternativa, el clúster B puede utilizar la misma instancia de mediador de ONTAP para las tres relaciones entre iguales. En este escenario, la misma instancia de ONTAP Mediator aparece tres veces para el cluster.

A partir de ONTAP 9.17.1, puede configurar "Mediador de la nube de ONTAP" para monitorear la salud de su clúster en una configuración de sincronización activa de SnapMirror , sin embargo, no puede usar ambos mediadores al mismo tiempo.

Si está utilizando SnapMirror Active Sync y ONTAP Mediator o ONTAP Cloud Mediator con ONTAP 9.17.1, debe revisar los **Problemas y limitaciones conocidos** en"Notas de la versión de ONTAP" para obtener información importante sobre estas configuraciones.

Requisitos previos para el Mediador de ONTAP

- ONTAP Mediator incluye sus propios prerrequisitos. Debe cumplirlos antes de instalar ONTAP Mediator.

  Para obtener más información, consulte "Prepárese para instalar el servicio ONTAP Mediator" .

- De forma predeterminada, el mediador de ONTAP proporciona servicio a través del puerto TCP 31784. Debe asegurarse de que el puerto 31784 esté abierto y disponible entre los clústeres de ONTAP y el mediador de ONTAP .

Instalar ONTAP Mediator y confirmar la configuración del clúster

Realice cada uno de los siguientes pasos para instalar ONTAP Mediator y verificar la configuración del clúster. Para cada paso, debe confirmar que se ha realizado la configuración específica. Cada paso incluye un enlace al procedimiento específico que debe seguir.

Pasos

1. Instale ONTAP Mediator antes de verificar que sus clústeres de origen y destino estén configurados correctamente.

   Prepárese para instalar o actualizar ONTAP Mediator

2. Confirme que existe una relación de paridad entre los clústeres.

   El espacio IP predeterminado es necesario en la sincronización activa de SnapMirror para las relaciones entre iguales de clústeres. No se admite un espacio IP personalizado.

   "Configurar clústeres ONTAP para la sincronización activa de SnapMirror"

Inicializar ONTAP Mediator para la sincronización activa de SnapMirror mediante certificados autofirmados

Una vez instalado ONTAP Mediator y confirmada la configuración del clúster, debe inicializarlo para la monitorización del clúster. Puede inicializarlo mediante el Administrador del Sistema o la CLI de ONTAP.

System Manager

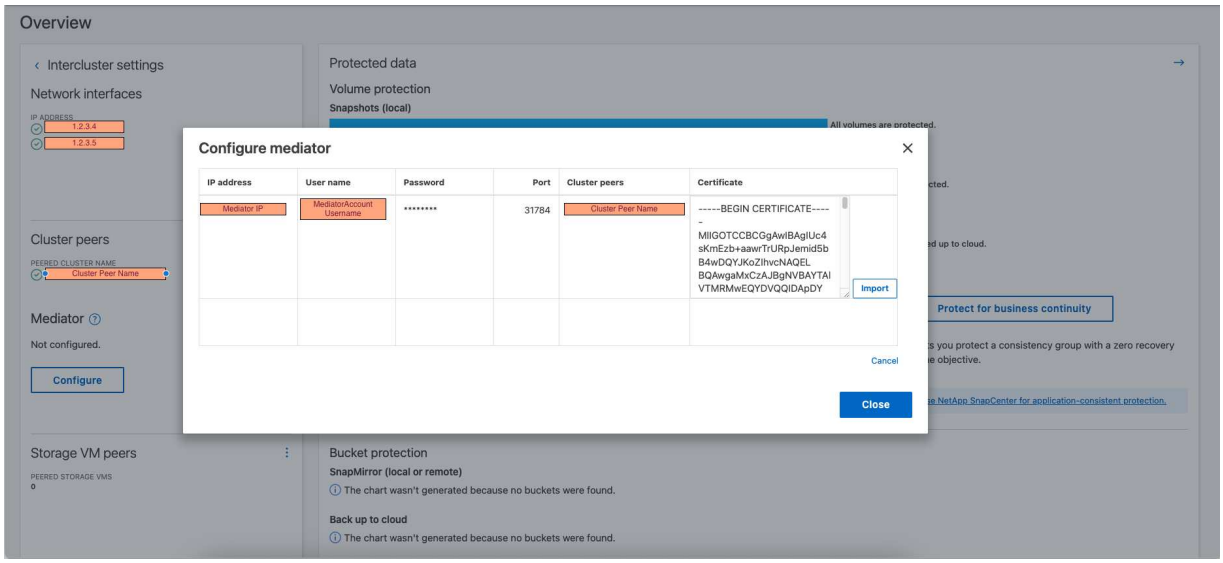
Con System Manager, puede configurar ONTAP Mediator para la conmutación por error automatizada. También puede reemplazar SSL y CA autofirmados por el certificado SSL y CA validados de terceros si aún no lo ha hecho.

Desde ONTAP 9.14.1 hasta 9.8, la sincronización activa de SnapMirror se conoce como SnapMirror Business Continuity (SM-BC).

ONTAP Mediator 1,9 y posteriores

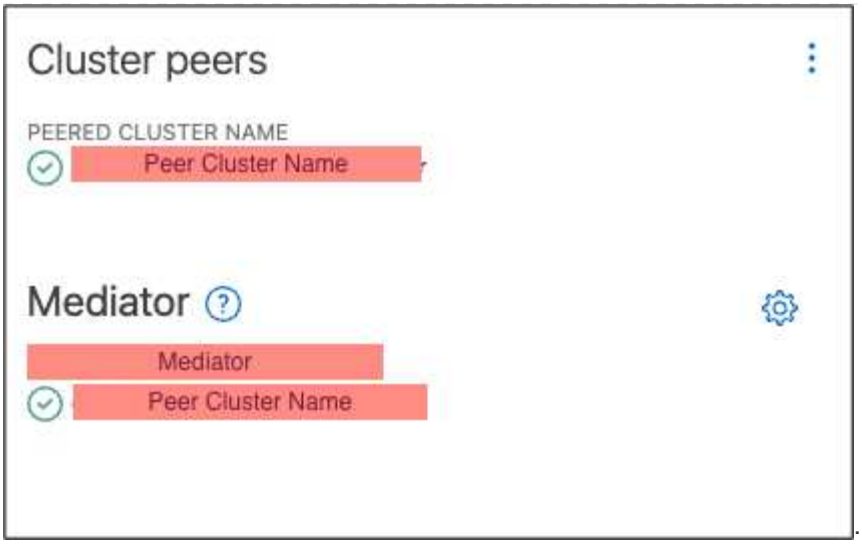
1. Vaya a **Protección > Descripción general > Mediador > Configurar**.
2. Seleccione **Agregar** e ingrese la siguiente información del Mediador de ONTAP:
   - Dirección IPv4
   - Nombre de usuario
   - Contraseña
   - Certificado
3. Puede proporcionar la entrada del certificado de dos formas:
   - **Opción (A)**: Selecciona **Importar** para navegar hasta el `intermediate.crt` archivo e importarlo.
   - **Opción (b)**: Copia el contenido del `intermediate.crt` archivo y pégalo en el campo **Certificado**.

     Cuando todos los detalles se introducen correctamente, el certificado proporcionado se instala en todos los clústeres de iguales.



Una vez completada la adición del certificado, ONTAP Mediator se agrega al clúster ONTAP.

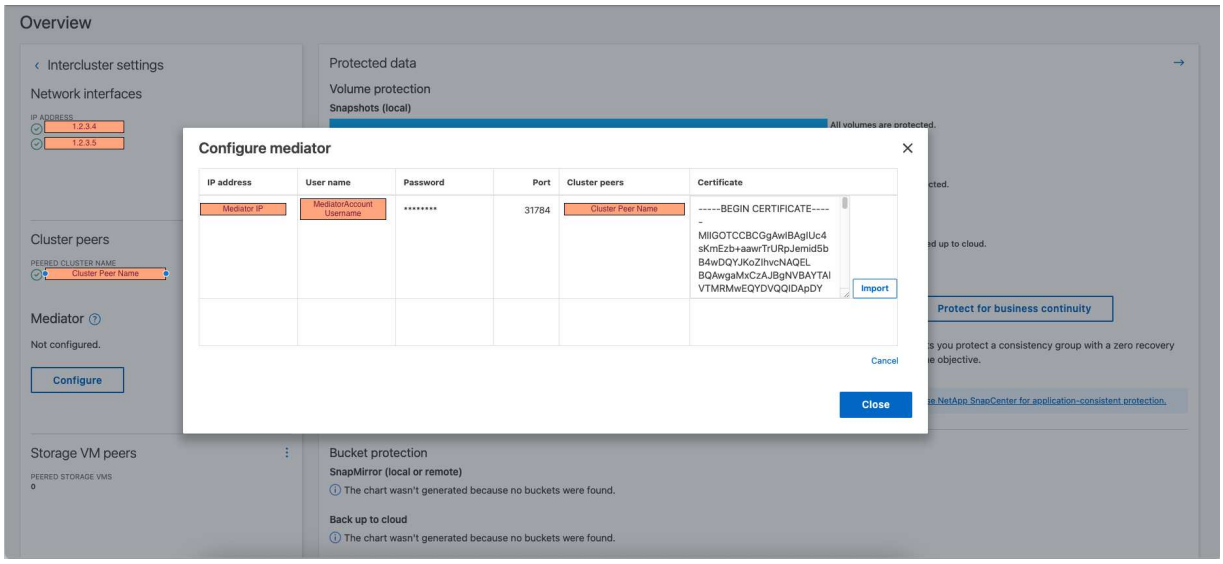
La siguiente imagen muestra una configuración correcta de ONTAP Mediator:



ONTAP Mediator 1,8 y anteriores

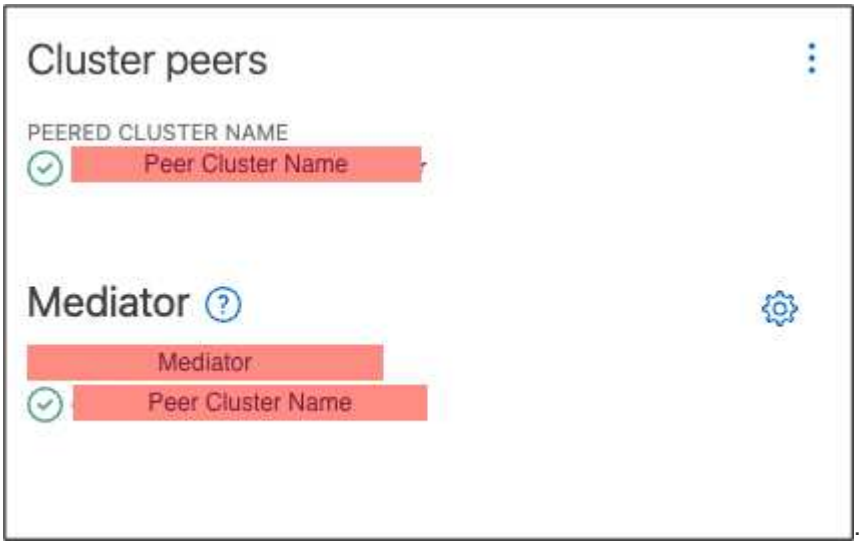
1. Vaya a **Protección > Descripción general > Mediador > Configurar**.
2. Seleccione **Agregar** e ingrese la siguiente información del Mediador de ONTAP:
   - Dirección IPv4
   - Nombre de usuario
   - Contraseña
   - Certificado
3. Puede proporcionar la entrada del certificado de dos formas:
   - **Opción (A)**: Selecciona **Importar** para navegar hasta el `ca.crt` archivo e importarlo.
   - **Opción (b)**: Copia el contenido del `ca.crt` archivo y pégalo en el campo **Certificado**.

     Cuando todos los detalles se introducen correctamente, el certificado proporcionado se instala en todos los clústeres de iguales.



Una vez completada la adición del certificado, ONTAP Mediator se agrega al clúster ONTAP.

La siguiente imagen muestra una configuración correcta de ONTAP Mediator:



CLI

Puede inicializar ONTAP Mediator desde el clúster principal o secundario mediante la CLI de ONTAP. Al ejecutar el comando `mediator add` comando en un clúster, ONTAP Mediator se agrega automáticamente en el otro clúster.

Al usar ONTAP Mediator para supervisar una relación de sincronización activa de SnapMirror, no se puede inicializar en ONTAP sin un certificado autofirmado o de una autoridad de certificación (CA) válido. Añada un certificado válido al almacén de certificados para clústeres entre iguales. Al usar ONTAP Mediator para supervisar sistemas IP de MetroCluster, no se utiliza HTTPS después de la configuración inicial; por lo tanto, no se requieren certificados.

ONTAP Mediator 1,9 y posteriores

1. Busque el certificado de CA de ONTAP Mediator en la ubicación de instalación del software ONTAP Mediator Linux VM/host `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`.
2. Agregue una autoridad de certificado válida al almacén de certificados en el clúster con relación de paridad.

   Ejemplo:

   ```
   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. Añada el certificado de CA de ONTAP Mediator a un clúster de ONTAP. Cuando se le solicite, inserte el certificado CA obtenido de ONTAP Mediator. Repita los pasos en todos los clústeres de iguales:

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   Ejemplo:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. Vea el certificado de CA autofirmado instalado con el nombre generado del certificado:

   `security certificate show -common-name <common_name>`

   Ejemplo:

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. Inicialice ONTAP Mediator en uno de los clústeres. ONTAP Mediator se agrega automáticamente al otro clúster.

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Si lo desea, compruebe el estado del identificador de trabajo `job show -id` para verificar si el comando SnapMirror Mediator add es correcto.

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. Compruebe el estado de la configuración de ONTAP Mediator:

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` Indica si las relaciones del grupo de consistencia de SnapMirror están sincronizadas con ONTAP Mediator; un estado de `true` Indica sincronización exitosa.

ONTAP Mediator 1,8 y anteriores

1. Busque el certificado de CA de ONTAP Mediator en la ubicación de instalación del software ONTAP Mediator Linux VM/host `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` .
2. Agregue una autoridad de certificado válida al almacén de certificados en el clúster con relación de paridad.

   Ejemplo:

   ```
   [root@ontap-mediator_config]# cat ca.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. Añada el certificado de CA de ONTAP Mediator a un clúster de ONTAP. Cuando se le solicite, inserte el certificado de CA obtenido del Mediador ONTAP. Repita los pasos en todos los clústeres de iguales:

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   Ejemplo:

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat ca.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. Vea el certificado de CA autofirmado instalado con el nombre generado del certificado:

   `security certificate show -common-name <common_name>`

   Ejemplo:

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. Inicialice ONTAP Mediator en uno de los clústeres. ONTAP Mediator se agrega automáticamente al otro clúster.

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. Si lo desea, compruebe el estado del identificador de trabajo `job show -id` para verificar si el comando SnapMirror Mediator add es correcto.

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. Compruebe el estado de la configuración de ONTAP Mediator:

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status` Indica si las relaciones del grupo de consistencia de SnapMirror están sincronizadas con ONTAP Mediator; un estado de `true` Indica sincronización exitosa.

Reinicie ONTAP Mediator con certificados de terceros

Es posible que deba reinicializar ONTAP Mediator. Puede haber situaciones que requieran la reinicialización de ONTAP Mediator, como un cambio en la dirección IP de ONTAP Mediator, la expiración del certificado, etc.

El siguiente procedimiento ilustra la reinicialización de ONTAP Mediator para un caso específico cuando un certificado autofirmado necesita ser reemplazado por un certificado de terceros.

Acerca de esta tarea

Debe reemplazar los certificados autofirmados del clúster de sincronización activa de SnapMirror con certificados de terceros, eliminar la configuración de ONTAP Mediator de ONTAP y luego agregar ONTAP Mediator.

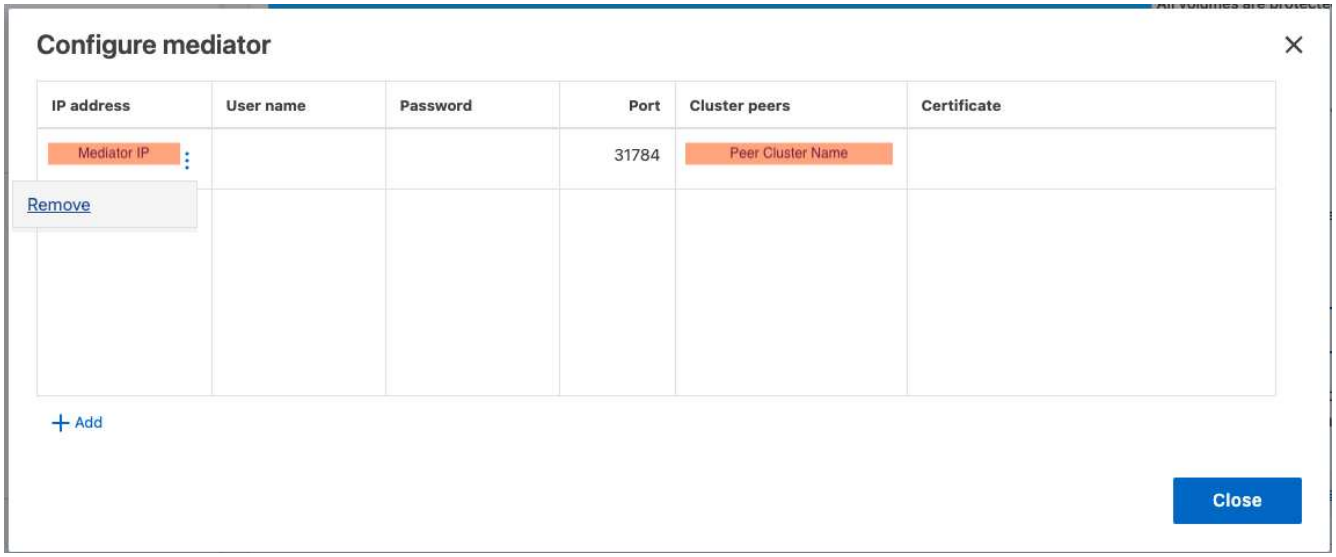
System Manager

Con el Administrador del sistema, debe eliminar la versión de ONTAP Mediator configurada con el antiguo certificado autofirmado del clúster de ONTAP y volver a configurar el clúster de ONTAP con el nuevo certificado de terceros.

Pasos

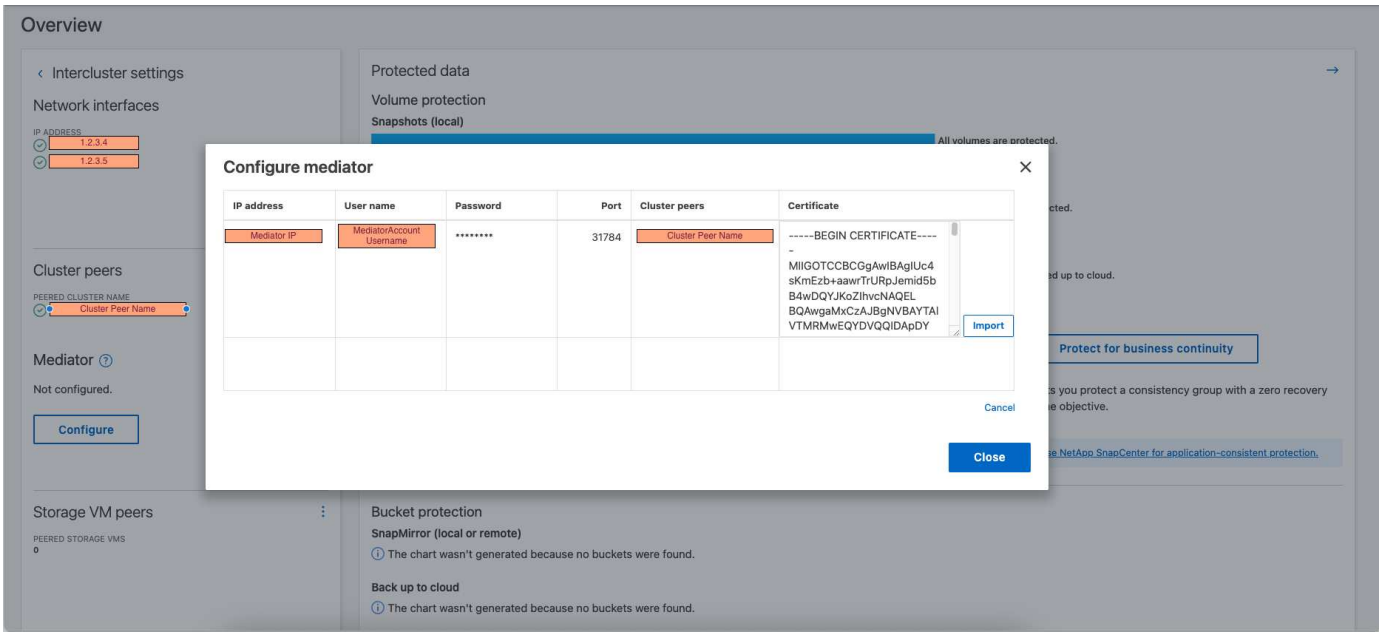
1. Seleccione el ícono de opciones del menú y seleccione **Eliminar** para eliminar ONTAP Mediator.

> Este paso no elimina la CA del servidor autofirmado del clúster de ONTAP. NetApp recomienda navegar a la pestaña **Certificado** y eliminarla manualmente antes de realizar el siguiente paso para agregar un certificado de terceros:



2. Agregue ONTAP Mediator nuevamente con el certificado correcto.

ONTAP Mediator ahora está configurado con el nuevo certificado autofirmado de terceros.



CLI

Puede reinicializar ONTAP Mediator desde el clúster primario o secundario utilizando la CLI de ONTAP para reemplazar el certificado autofirmado con el certificado de terceros.

ONTAP Mediator 1,9 y posteriores

1. Quite el autofirmado `intermediate.crt` instalado anteriormente cuando utilizó certificados autofirmados para todos los clústeres. En el siguiente ejemplo, hay dos clústeres:

   Ejemplo:

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. Elimine el Mediador de ONTAP configurado anteriormente del clúster de sincronización activa de SnapMirror mediante `-force true`:

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. Consulte los pasos descritos en "Sustituya los certificados autofirmados por certificados de terceros de confianza" para obtener instrucciones sobre cómo obtener certificados de una CA subordinada, denominada `intermediate.crt` . Sustituya los certificados autofirmados por certificados de terceros de confianza

El `intermediate.crt` tiene ciertas propiedades que deriva de la solicitud que se deben enviar a la autoridad PKI, definida en el archivo `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Agregue el nuevo certificado de CA de mediador ONTAP de terceros `intermediate.crt` desde la ubicación de instalación del software host/VM de ONTAP Mediator Linux:

   Ejemplo:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. Añada `intermediate.crt` el archivo al clúster entre iguales. Repita este paso para todos los clústeres de iguales:

   Ejemplo:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Quite el Mediador de ONTAP previamente configurado del clúster de sincronización activa de snapmirror:

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Agregue ONTAP Mediator nuevamente:

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` Indica si las relaciones del grupo de coherencia SnapMirror se sincronizan con el mediador; el estado de `true` indica una sincronización correcta.

ONTAP Mediator 1,8 y anteriores

1. Quite el autofirmado `ca.crt` instalado anteriormente cuando utilizó certificados autofirmados para todos los clústeres. En el siguiente ejemplo, hay dos clústeres:

   Ejemplo:

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. Elimine el Mediador de ONTAP configurado anteriormente del clúster de sincronización activa de SnapMirror mediante `-force true`:

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. Consulte los pasos descritos en "Sustituya los certificados autofirmados por certificados de terceros de confianza" para obtener instrucciones sobre cómo obtener certificados de una CA subordinada, denominada `ca.crt` . Sustituya los certificados autofirmados por certificados de terceros de confianza

   > El `ca.crt` tiene ciertas propiedades que deriva de la solicitud que se deben enviar a la autoridad PKI, definida en el archivo `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. Agregue el nuevo certificado de CA de mediador ONTAP de terceros `ca.crt` desde la ubicación de instalación del software host/VM de ONTAP Mediator Linux:

Ejemplo:

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. Añada `intermediate.crt` el archivo al clúster entre iguales. Repita este paso para todos los clústeres de iguales:

   Ejemplo:

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. Quite el Mediador de ONTAP previamente configurado del clúster de sincronización activa de snapmirror:

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. Agregue ONTAP Mediator nuevamente:

   Ejemplo:

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` Indica si las relaciones del grupo de coherencia SnapMirror se sincronizan con el mediador; el estado de `true` indica una sincronización correcta.

Información relacionada

- "exposición de trabajos"
- "eliminar certificado de seguridad"
- "instalación del certificado de seguridad"
- "Mostrar certificado de seguridad"
- "añadir mediador de snapmirror"
- "eliminar mediador de snapmirror"
- "Programa de mediación de Snapmirror"

Prepárese para configurar ONTAP Cloud Mediator

Antes de ti "configurar ONTAP Cloud Mediator" , debe asegurarse de que se cumplan los requisitos previos.

Requisitos del firewall

La configuración del firewall en el controlador de dominio debe permitir el tráfico HTTPS `api.bluexp.netapp.com` de ambos grupos.

Requisitos del servidor proxy

Si usa servidores proxy para la sincronización activa de SnapMirror , asegúrese de que los servidores proxy estén creados y de que tenga la siguiente información del servidor proxy:

- IP de proxy HTTPS
- Puerto
- Nombre de usuario
- Contraseña

Estado latente

La latencia de ping recomendada entre el servidor en la nube de la consola de NetApp y los pares del clúster de sincronización activa de SnapMirror es inferior a 200 ms.

Certificados de CA raíz

Comprobar el clúster en busca de certificados

ONTAP viene con certificados CA raíz conocidos preinstalados, por lo que en la mayoría de los casos no es necesario instalar el certificado CA raíz del servidor de la consola de NetApp . Antes de comenzar la configuración de ONTAP Cloud Mediator, puede comprobar el clúster para verificar la existencia de los certificados:

Ejemplo:

```
C1_cluster% openssl s_client -showcerts -connect
api.bluexp.netapp.com:443|egrep "s:|i:"
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Global Root G2
verify return:1
depth=1 C = US, O = Microsoft Corporation, CN = Microsoft Azure RSA TLS
Issuing CA 04
verify return:1
depth=0 C = US, ST = WA, L = Redmond, O = Microsoft Corporation, CN =
*.azureedge.net
verify return:1
 0 s:/C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=*.azureedge.net
   i:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
 1 s:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
```

```
04
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
<====

C1_cluster::> security certificate show -common-name DigiCert*
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
C1_cluster 0CE7E0EXXXXX46FE8FE560FC1BFXXXXX DigiCertAssuredIDRootCA
server-ca
    Certificate Authority: DigiCert Assured ID Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 0B931C3XXXXX67EA6723BFC3AF9XXXXX DigiCertAssuredIDRootG2
server-ca
    Certificate Authority: DigiCert Assured ID Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 0BA15AFXXXXXA0B54944AFCD24AXXXXX DigiCertAssuredIDRootG3
server-ca
    Certificate Authority: DigiCert Assured ID Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 083BE05XXXXX46B1A1756AC9599XXXXX DigiCertGlobalRootCA server-ca
    Certificate Authority: DigiCert Global Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 033AF1EXXXXXA9A0BB2864B11D0XXXXX DigiCertGlobalRootG2 server-ca
    Certificate Authority: DigiCert Global Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 055556BXXXXXA43535C3A40FD5AXXXXX DigiCertGlobalRootG3 server-ca
    Certificate Authority: DigiCert Global Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 02AC5C2XXXXX409B8F0B79F2AE4XXXXX DigiCertHighAssuranceEVRootCA
server-ca
    Certificate Authority: DigiCert High Assurance EV Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 059B1B5XXXXX2132E23907BDA77XXXXX DigiCertTrustedRootG4 server-
ca
    Certificate Authority: DigiCert Trusted Root G4
          Expiration Date: Fri Jan 15 17:30:00 2038
```

Comprobar el servidor proxy para ver los certificados instalados

Si está utilizando un proxy para conectarse al servicio ONTAP Cloud Mediator en la consola de NetApp , asegúrese de que los certificados CA raíz del servidor proxy estén instalados en ONTAP:

Ejemplo:

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.bluexp.netapp.com:443 |egrep "s:|i:"
```

Descargar el certificado CA:

Si es necesario, puede descargar los certificados de CA raíz del sitio web de la autoridad de certificación e instalarlos en los clústeres.

Ejemplo:

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

Configurar ONTAP Cloud Mediator para la sincronización activa de SnapMirror

A partir de ONTAP 9.17.1, puede usar ONTAP Cloud Mediator para facilitar la continuidad del negocio mediante la monitorización del estado de cada clúster. ONTAP Cloud Mediator es un servicio basado en la nube. Cuando utiliza ONTAP Cloud Mediator con la sincronización activa de SnapMirror , primero debe confirmar que los servicios de la consola de NetApp y la información del cliente estén configurados y garantizar un emparejamiento de clústeres adecuado.

Al igual que ONTAP Mediator, ONTAP Cloud Mediator proporciona un almacenamiento persistente y protegido para los metadatos de alta disponibilidad (HA) que utilizan los clústeres de ONTAP en una relación de sincronización activa de SnapMirror . ONTAP Cloud Mediator proporciona una función de consulta síncrona del estado del nodo para facilitar la determinación del quórum y funciona como proxy de ping para la detección de la actividad del controlador.

Si está utilizando SnapMirror Active Sync y ONTAP Mediator o ONTAP Cloud Mediator con ONTAP 9.17.1, debe revisar los **Problemas y limitaciones conocidos** en"Notas de la versión de ONTAP" para obtener información importante sobre estas configuraciones.

Antes de empezar

Antes de configurar ONTAP Cloud Mediator, debe confirmar la siguiente información:

- El cluster está configurado.

  "Configurar clústeres ONTAP para la sincronización activa de SnapMirror"

- Ha copiado su ID de organización de la consola de NetApp desde la consola de NetApp y ha creado una cuenta de servicio de miembro de la consola para usar cuando configure ONTAP Cloud Mediator. Al crear la cuenta de servicio, la organización debe estar configurada con la suscripción donde configuró ONTAP Cloud Mediator. La categoría debe ser **Aplicación** y el tipo de rol debe ser **Rol de configuración de ONTAP Mediator**. Debe guardar el ID y el secreto del cliente al crear el rol.

  "Agregar miembros de la consola de NetApp y cuentas de servicio"

Pasos

Puede agregar ONTAP Cloud Mediator mediante el Administrador del sistema o la CLI de ONTAP .

System Manager

1. Vaya a **Protección > Descripción general > Mediador** y seleccione **Agregar**.
2. En la ventana **Agregar un mediador**, seleccione **Nube** como tipo de mediador e ingrese la siguiente información:
   - ID de organización de la consola de NetApp
   - ID de cliente de la consola de NetApp
   - Secreto de cliente de la consola de NetApp
3. Seleccione el par del clúster.
4. Si está utilizando un proxy HTTP y aún no está configurado, ingrese la información del proxy HTTP para los hosts locales y remotos.

   Se recomienda que utilice un servidor proxy diferente para cada par del clúster.

5. Opcional: si es necesario instalar un certificado CA raíz en ONTAP, especialmente cuando se utiliza un servidor proxy, pegue el certificado en el cuadro de texto provisto.
6. Seleccione **Agregar**.
7. Vaya a **Protección > Descripción general** y verifique el estado de la relación entre los clústeres de sincronización activa de SnapMirror y ONTAP Cloud Mediator.

CLI

1. Configurar ONTAP Cloud Mediator:
   `snapmirror mediator add -peer-cluster <peerClusterName> -type cloud -bluexp -org-id <NetApp Console Organization ID> -service-account-client-id <Service Account Client ID> -use-http-proxy-local <true|false> -use-http -proxy-remote <true|false>`
2. Comprobar el estado del mediador de ONTAP Cloud:
   `snapmirror mediator show`

   Ejemplo:

```
C1_cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
0.0.0.0          C2_cluster       connected         true
cloud
```

Protéjase con la sincronización activa de ONTAP SnapMirror

SnapMirror active sync ofrece protección asimétrica y, a partir de ONTAP 9.15.1, protección activo-activo simétrica.

Configurar la protección asimétrica

La configuración de la protección asimétrica mediante SnapMirror Active Sync implica seleccionar las LUN en el clúster de origen de ONTAP y añadirlas a un grupo de coherencia.

Antes de empezar

- Debe tener una licencia síncrona de SnapMirror.
- Debe ser un administrador de clústeres o máquinas virtuales de almacenamiento.
- Todos los volúmenes constituyentes de un grupo de coherencia deben estar en una única máquina virtual de almacenamiento (SVM).
  - Los LUN pueden residir en distintos volúmenes.
- Los clústeres de origen y destino no pueden ser los mismos.
- No es posible establecer relaciones de grupos de consistencia de sincronización activa de SnapMirror entre clústeres de ASA y clústeres no-ASA.
- El espacio IP predeterminado es necesario en la sincronización activa de SnapMirror para las relaciones entre iguales de clústeres. No se admite el espacio IP personalizado.
- El nombre del grupo de coherencia debe ser único.
- Los volúmenes en el clúster secundario (de destino) deben ser del tipo DP.
- Las SVM principales y secundarias deben estar en una relación entre iguales.

Pasos

Puede configurar un grupo de coherencia con la CLI de ONTAP o System Manager.

A partir de ONTAP 9.10.1, ONTAP ofrece un punto final de grupo de consistencia y un menú en el Administrador del sistema, con utilidades de administración adicionales. Si utiliza ONTAP 9.10.1 o posterior, consulte "Configurar un grupo de consistencia" entonces "configure la protección" para crear una relación de sincronización activa de SnapMirror .

Desde ONTAP 9.14.1 hasta 9.8, la sincronización activa de SnapMirror se conoce como SnapMirror Business Continuity (SM-BC).

System Manager

1. En el clúster principal, navegue hasta **Protección > Descripción general > Proteger para continuidad empresarial > Proteger LUN**.
2. Seleccione las LUN que desea proteger y añádalas a un grupo de protección.
3. Seleccione el clúster y la SVM de destino.
4. **La opción inicializar relación** está seleccionada de forma predeterminada. Haga clic en **Guardar** para comenzar la protección.
5. Vaya a **Consola > rendimiento** para verificar la actividad de IOPS de las LUN.
6. En el clúster de destino, utilice System Manager para comprobar que la protección de la relación de continuidad de negocio está sincronizada: **Protección > Relaciones**.

CLI

1. Cree una relación de grupo de coherencia a partir del clúster de destino.
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   Puede asignar hasta 12 volúmenes constituyentes con `cg-item-mappings` el parámetro en el `snapmirror create` comando.

   En el siguiente ejemplo se crean dos grupos de consistencia: `cg_src_ on the source with` `vol1` Y `vol2` un grupo de coherencia de destino reflejado, `cg_dst`.

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOverDuplex
   ```

2. Desde el clúster de destino, inicialice el grupo de coherencia.

   `destination::>snapmirror initialize -destination-path` *`destination-consistency-group`*

3. Confirme que la operación de inicialización se ha realizado correctamente. El estado debe ser `InSync`.

   ```
   snapmirror show
   ```

4. En cada clúster, cree un igroup para poder asignar las LUN al iniciador en el host de la aplicación.
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator` *`initiator_name`*

   Obtenga más información sobre `lun igroup create` en el "Referencia de comandos del ONTAP".

5. En cada clúster, asigne las LUN al igroup:

   `lun map -path` *`path_name`* `-igroup` *`igroup_name`*

6. Compruebe que la asignación de LUN se ha completado correctamente con `lun map` el comando. Luego, puede detectar las nuevas LUN en el host de la aplicación.

Configurar la protección activo-activo simétrica

Puede establecer una protección simétrica mediante System Manager o la interfaz de línea de comandos de ONTAP. En ambas interfaces, hay diferentes pasos para configuraciones uniformes y no uniformes.

Antes de empezar

- Ambos clústeres deben ejecutar ONTAP 9.15.1 o una versión posterior.
- Las configuraciones activo-activo simétricas requieren `AutomatedFailoverDuplex` la política de protección. Alternativamente, usted puede Crear una política de SnapMirror personalizada siempre que el `-type` IS `automated-failover-duplex`.
- En ONTAP 9.15.1, el activo-activo simétrico solo se admite en clústeres de 2 nodos.
- A partir de ONTAP 9.16.1 GA, la sincronización activa de SnapMirror admite configuraciones activo-activo simétricas en clústeres de cuatro nodos.
  - Para utilizar la sincronización activa de SnapMirror en un clúster de cuatro nodos, debe ejecutar ONTAP 9.16.1 GA o una versión posterior.
  - Antes de implementar una configuración de cuatro nodos, cree una relación de paridad entre clústeresdebe .
  - límitesRevise la para ver clústeres de cuatro nodos.
  - Si revierte a un clúster de dos nodos, debe eliminar las relaciones de sincronización activa de SnapMirror del clúster antes de revertir.
  - La configuración de cuatro nodos se puede usar para actualizar el almacenamiento y las controladoras. Este proceso no produce interrupciones y amplía el clúster mientras traslada los volúmenes a los nuevos nodos. Para obtener más información, consulte "actualice un clúster".
- A partir de ONTAP 9.17.1, puede configurar la protección activa/activa simétrica en espacios de nombres NVMe solo cuando ambos clústeres ejecutan ONTAP 9.17.1 o posterior.

Configurar la protección activa/activa simétrica mediante una configuración de sincronización activa SCSI SnapMirror

Pasos

Puede utilizar el Administrador del sistema o la CLI de ONTAP para configurar la protección activa/activa simétrica mediante asignaciones de host del protocolo SCSI.

System Manager

Pasos para una configuración uniforme

1. En el sitio principal, "Cree un grupo de consistencia mediante nuevas LUN."
   a. Al crear el grupo de consistencia, especifique iniciadores de host para crear iGroups.
   b. Seleccione la casilla de verificación **Activar SnapMirror** y luego elija la `AutomatedFailoverDuplex` política.
   c. En el cuadro de diálogo que aparece, seleccione la casilla **Replicar iGroups** para replicar iGroups. En **Editar ajustes de proximidad**, establezca SVM proximales para sus hosts.
   d. Selecciona **Guardar**.

Pasos para una configuración no uniforme

1. En el sitio principal, "Cree un grupo de consistencia mediante nuevas LUN."
   a. Al crear el grupo de consistencia, especifique iniciadores de host para crear iGroups.
   b. Seleccione la casilla de verificación **Activar SnapMirror** y luego elija la `AutomatedFailoverDuplex` política.
   c. Seleccione **Guardar** para crear las LUN, el grupo de consistencia, el igroup, la relación de SnapMirror y el mapa del igroup.
2. En el sitio secundario, cree un igroup y asigne las LUN.
   a. Vaya a **HOSTS** > **SAN Initiator Groups**.
   b. Seleccione **+Add** para crear un igroup nuevo.
   c. Proporcione un **Nombre**, seleccione el **Sistema Operativo del Host** y, a continuación, elija **Miembros del Grupo Iniciador**.
   d. Seleccione **Guardar** para inicializar la relación.
3. Asigne el nuevo igroup a las LUN de destino.
   a. Vaya a **Almacenamiento** > **LUN**.
   b. Seleccione todas las LUN que desea asignar al igroup.
   c. Seleccione **Más** y luego **Asignar a grupos de iniciadores**.

CLI

Pasos para una configuración uniforme

1. Cree una nueva relación de SnapMirror que agrupe todos los volúmenes en la aplicación. Asegúrese de designar la `AutomatedFailOverDuplex` política para establecer la replicación de sincronización bidireccional.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   Ejemplo: El siguiente ejemplo crea dos grupos de consistencia: cg_src en el origen con vol1 y vol2, y un grupo de consistencia reflejado en el destino, cg_dst.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
AutomatedFailOverDuplex
```

2. Inicialice la relación de SnapMirror:
`snapmirror initialize -destination-path <destination-consistency-group>`
3. Para confirmar que la operación se ha realizado correctamente, espere a que `Mirrored State` se muestre `SnapMirrored` como y el `Relationship Status Insync` como .

   `snapmirror show -destination-path <destination_path>`
4. En el host, configure la conectividad de host con acceso a cada clúster de acuerdo con sus necesidades.
5. Establezca la configuración del igroup. Establezca las rutas preferidas para los iniciadores en el clúster local. Especifique la opción para replicar la configuración en el cluster peer para afinidad inversa.

   ```
   SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
   <igroup_name> -replication-peer <peer_svm_name> -initiator <host>
   ```

   > A partir de ONTAP 9.16.1, utilice `-proximal-vserver local` el parámetro en este comando.

   ```
   SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
   <os_type> -initiator <host>
   ```

   > A partir de ONTAP 9.16.1, utilice `-proximal-vserver peer` el parámetro en este comando.
6. Desde el host, detecte las rutas y verifique que los hosts tengan una ruta activa/optimizada hacia el LUN de almacenamiento desde el clúster preferido.
7. Ponga en marcha la aplicación y distribuya las cargas de trabajo de los equipos virtuales entre los clusters para lograr el equilibrio de carga necesario.

Pasos para una configuración no uniforme

1. Cree una nueva relación de SnapMirror que agrupe todos los volúmenes en la aplicación. Asegúrese de designar la `AutomatedFailOverDuplex` política para establecer la replicación de sincronización bidireccional.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   Ejemplo: El siguiente ejemplo crea dos grupos de consistencia: cg_src en el origen con vol1 y vol2, y un grupo de consistencia reflejado en el destino, cg_dst.

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
AutomatedFailOverDuplex
```

2. Inicialice la relación de SnapMirror:
`snapmirror initialize -destination-path <destination-consistency-group>`
3. Para confirmar que la operación se ha realizado correctamente, espere a que `Mirrored State` se muestre `SnapMirrored` como y el `Relationship Status Insync` como .

   `snapmirror show -destination-path <destination_path>`
4. En el host, configure la conectividad de host con acceso a cada clúster de acuerdo con sus necesidades.
5. Establezca las configuraciones de igroups en los clústeres de origen y destino.

   ```
   # primary site
   SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_1_name_>

   # secondary site
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_2_name>
   ```
6. Desde el host, detecte las rutas y verifique que los hosts tengan una ruta activa/optimizada hacia el LUN de almacenamiento desde el clúster preferido.
7. Ponga en marcha la aplicación y distribuya las cargas de trabajo de los equipos virtuales entre los clusters para lograr el equilibrio de carga necesario.

Configurar la protección activa/activa simétrica mediante una configuración de sincronización activa de NVMe SnapMirror

Antes de empezar

Además de los requisitos para configurar la protección activa/activa simétrica, debe tener en cuenta las configuraciones compatibles y no compatibles al utilizar el protocolo NVMe.

- Los grupos de consistencia pueden tener uno o más subsistemas.
- Los volúmenes dentro del grupo de consistencia pueden tener mapas de espacios de nombres de múltiples subsistemas.
- Los subsistemas no pueden tener mapas de espacios de nombres que pertenezcan a más de un grupo de consistencia.
- Los subsistemas no pueden tener algunos mapas de espacios de nombres que pertenezcan a un grupo de consistencia y algunos mapas de espacios de nombres que no pertenezcan a un grupo de consistencia.
- Los subsistemas deben tener mapas de espacios de nombres que sean parte del mismo grupo de consistencia.

Pasos

A partir de ONTAP 9.17.1, puede usar el Administrador del sistema o la CLI de ONTAP para crear un grupo de consistencia y configurar la protección activa/activa simétrica mediante asignaciones de host del protocolo NVMe.

System Manager

1. En el sitio principal, "crear un grupo de consistencia utilizando nuevos volúmenes o espacios de nombres NVMe."
2. Seleccione **+Agregar** y elija **Usar nuevos espacios de nombres NVMe**.
3. Introduzca el nombre del grupo de consistencia.
4. Seleccione **Más**.
5. En la sección **Protección**, seleccione **Habilitar SnapMirror** y luego elija la opción `AutomatedFailoverDuplex` política.
6. En la sección **Mapeo de host**, elija **Subsistema NVMe existente** o **Nuevo subsistema NVMe**.
7. Seleccione "En proximidad a" para cambiar el SVM proximal. El SVM de origen está seleccionado por defecto.
8. Si es necesario, agregue otro subsistema NVMe.

CLI

1. Cree una nueva relación SnapMirror que agrupe todos los volúmenes que contienen todos los espacios de nombres NVMe utilizados por la aplicación. Asegúrese de designar el `AutomatedFailOverDuplex` Política para establecer replicación de sincronización bidireccional.

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   Ejemplo:

   ```
   DST::> snapmirror create -source-path vs_src:/cg/cg_src_1
   -destination-path vs_dst:/cg/cg_dst_1 -cg-item-mappings
   vs_src_vol1:@vs_dst_vol1,vs_src_vol2:@vs_dst_vol2 -policy
   AutomatedFailOverDuplex
   ```

2. Inicialice la relación de SnapMirror:
   `snapmirror initialize -destination-path <destination-consistency-group>`

   Ejemplo:

   ```
   DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
   ```

3. Para confirmar que la operación se ha realizado correctamente, espere a que `Mirrored State` se muestre `SnapMirrored` como y el `Relationship Status` `Insync` como .

   ```
   snapmirror show -destination-path <destination_path>
   ```

   Los subsistemas NVMe asociados con los espacios de nombres NVMe en los volúmenes principales se replican automáticamente en el clúster secundario.

4. En el host, configure la conectividad de host con acceso a cada clúster de acuerdo con sus

necesidades.

5. Especifique la SVM próxima a cada uno de sus hosts. Esto permite que el host acceda al espacio de nombres NVMe mediante una ruta desde el clúster preferido. Esta podría ser la SVM del clúster principal o la SVM del clúster de recuperación ante desastres.

   El siguiente comando indica que SVM VS_A es proximal al host H1 y establece VS_A como SVM proximal:

   ```
   SiteA::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H1_NQN>
   -proximal-vservers <VS_A>
   ```

   El siguiente comando indica que SVM VS_B es proximal al host H2 y establece VS_B como SVM proximal:

   ```
   SiteB::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H2_NQN>
   -proximal-vservers <VS_B>
   ```

6. Desde el host, descubra las rutas y verifique que los hosts tengan una ruta activa/optimizada al almacenamiento desde el clúster preferido.
7. Ponga en marcha la aplicación y distribuya las cargas de trabajo de los equipos virtuales entre los clusters para lograr el equilibrio de carga necesario.

Información relacionada

- "snapmirror create"
- "inicializar snapmirror"
- "espectáculo de Snapmirror"

Convertir una relación SnapMirror de ONTAP existente en una relación de sincronización activa de SnapMirror

Si ha configurado la protección de SnapMirror, puede convertir la relación a sincronización activa de SnapMirror. A partir de ONTAP 9.15.1, puede convertir la relación para utilizar protección activo-activo simétrica.

Convierte una relación SnapMirror iSCSI o FC existente en una relación de sincronización activa SnapMirror asimétrica

Si ya tiene una relación síncrona de SnapMirror iSCSI o FC entre un clúster de origen y uno de destino, puede convertirla en una relación de sincronización activa asimétrica de SnapMirror . Esto le permite asociar los volúmenes reflejados con un grupo de consistencia, lo que garantiza un RPO cero en una carga de trabajo multivolumen. Además, puede conservar las instantáneas de SnapMirror existentes si necesita volver a un punto en el tiempo anterior a la sincronización activa de SnapMirror .

Acerca de esta tarea

- Debe ser un administrador de clústeres y de SVM en los clústeres principales y secundarios.
- No se puede convertir un objetivo de punto de recuperación de cero en una sincronización de objetivo de tiempo de recuperación de cero cambiando la política de SnapMirror.
- Debe asegurarse de que se quita la asignación de las LUN antes de emitir `snapmirror create` el comando.

  Si los LUN existentes en el volumen secundario se asignan y se `AutomatedFailover` configura la

política, `snapmirror create` el comando activa un error.

Antes de empezar

- Debe existir una relación sincrónica SnapMirror de RPO cero entre el clúster primario y el secundario.
- Se deben anular la asignación de todas las LUN del volumen de destino antes de crear la relación de SnapMirror con objetivo de tiempo de recuperación cero.
- La sincronización activa de SnapMirror solo admite protocolos SAN (no NFS/CIFS). Asegúrese de que no hay ningún componente del grupo de consistencia montado para el acceso NAS.
- "Mediador ONTAP" Debe configurarse para la sincronización activa de SnapMirror .

Pasos

1. Desde el clúster secundario, realice una actualización de SnapMirror en la relación existente:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Compruebe que la actualización de SnapMirror se ha realizado correctamente:

   ```
   SiteB::>snapmirror show
   ```

3. Pausar cada una de las relaciones síncronas de objetivo de punto de recuperación cero:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Elimine cada una de las relaciones síncronas de RPO cero:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1

   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Liberar la relación de SnapMirror de origen, pero conservar las snapshots comunes:

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Cree una relación síncrona de SnapMirror con un objetivo de tiempo de recuperación cero:

   ```
   SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
   vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailover
   ```

7. Resincronice el grupo de consistencia:

   ```
   SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

8. Vuelva a analizar las rutas de I/o del LUN del host para restaurar todas las rutas a los LUN.

Convierte una relación SnapMirror iSCSI o FC existente en una relación simétrica activa/activa

A partir de ONTAP 9.15.1, puede convertir una relación SnapMirror iSCSI o FC existente en una relación activa/activa simétrica de sincronización activa de SnapMirror .

Antes de empezar

- Debe ejecutar ONTAP 9.15.1 o una versión posterior.
- Debe existir una relación sincronizada de SnapMirror con objetivo de punto de recuperación cero entre el clúster primario y el secundario.
- Se deben anular la asignación de todas las LUN del volumen de destino antes de crear la relación de SnapMirror con objetivo de tiempo de recuperación cero.
- La sincronización activa de SnapMirror solo admite protocolos SAN (no NFS/CIFS). Asegúrese de que no hay ningún componente del grupo de consistencia montado para el acceso NAS.
- "Mediador ONTAP" Debe configurarse para la sincronización activa de SnapMirror .

Pasos

1. Desde el clúster secundario, realice una actualización de SnapMirror en la relación existente:

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. Compruebe que la actualización de SnapMirror se ha realizado correctamente:

   ```
   SiteB::>snapmirror show
   ```

3. Pausar cada una de las relaciones síncronas de objetivo de punto de recuperación cero:

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. Elimine cada una de las relaciones síncronas de RPO cero:

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1

   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. Liberar la relación de SnapMirror de origen, pero conservar las snapshots comunes:

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. Cree una relación síncrona de RTO SnapMirror cero con la política AutomatedFailoverDuplex:

   ```
   SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
   vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailoverDuplex
   ```

7. Si los hosts existentes son locales en el clúster primario, añada el host al clúster secundario y establezca la conectividad con el respectivo acceso a cada clúster.

8. En el sitio secundario, elimine los mapas de LUN de los iGroups asociados con hosts remotos.

   Asegúrese de que el igroup no contiene mapas de LUN no replicadas.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

9. En el sitio primario, modifique la configuración del iniciador para los hosts existentes para establecer la ruta proximal de los iniciadores en el clúster local.

   ```
   SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
   <host> -proximal-vserver <server>
   ```

10. Añada un igroup y un iniciador nuevos para los hosts nuevos y configure la proximidad de host para la afinidad de host con su sitio local. Replicación de igroup ennable para replicar la configuración e invertir la localidad de host en el clúster remoto.

    ```
    SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
    SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
    -proximal-vserver vsB
    ```

11. Detecte las rutas en los hosts y compruebe que los hosts tengan una ruta de activo/optimizada al LUN de almacenamiento desde el clúster preferido
12. Ponga en marcha la aplicación y distribuya las cargas de trabajo de los equipos virtuales entre los clústeres.
13. Resincronice el grupo de consistencia:

    ```
    SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
    ```

14. Vuelva a analizar las rutas de I/o del LUN del host para restaurar todas las rutas a los LUN.

Información relacionada

- "snapmirror create"
- "snapmirror elimina"
- "Snapmirror en reposo"
- "versión de snapmirror"
- "resincronización de SnapMirror"
- "espectáculo de Snapmirror"

Convertir el tipo de relación de sincronización activa de ONTAP SnapMirror

A partir de ONTAP 9.15.1, se puede convertir entre tipos de protección de sincronización activa de SnapMirror: De asimétrica a activo-activo simétrico y viceversa.

Convertir a una relación activo-activo simétrica

Puede convertir una relación de sincronización activa iSCSI o FC SnapMirror con protección asimétrica para utilizar activa/activa simétrica.

Antes de empezar

- Ambos clústeres deben ejecutar ONTAP 9.15.1 o una versión posterior.
- Las configuraciones activo-activo simétricas requieren `AutomatedFailoverDuplex` la política de protección. Alternativamente, usted puede Crear una política de SnapMirror personalizada siempre que el `-type` IS `automated-failover-duplex`.

System Manager

Pasos para una configuración uniforme

1. Quite el igroup de destino:
   a. En el clúster de destino, vaya a **Hosts** > **Grupos de iniciadores de SAN**.
   b. Seleccione el igroup con la relación SnapMirror y, a continuación, **Eliminar**.
   c. En el cuadro de diálogo, seleccione el cuadro **Desasignar las LUN asociadas** y luego **Eliminar**.
2. Edite la relación de sincronización activa de SnapMirror.
   a. Navegue hasta **Protección** > **Relaciones**.
   b. Seleccione el menú de kabob junto a la relación que desea modificar y luego **Editar**.
   c. Modifique la **Política de Protección** a AutomatedFailoverDuplex.
   d. Al seleccionar `AutoMatedFailoverDuplex` se muestra un cuadro de diálogo para modificar la configuración de proximidad del host. Para los iniciadores, seleccione la opción apropiada para **Iniciador proximal a** y luego **Guardar**.
   e. Selecciona **Guardar**.
3. En el menú **Protección**, confirme que la operación se ha realizado correctamente cuando la relación se muestre como `InSync`.

Pasos para una configuración no uniforme

1. Quite el igroup de destino:
   a. En el sitio secundario, vaya a **HOSTS** > **Grupos de iniciadores SAN**.
   b. Seleccione el igroup con la relación SnapMirror y, a continuación, **Eliminar**.
   c. En el cuadro de diálogo, seleccione el cuadro **Desasignar las LUN asociadas** y luego **Eliminar**.
2. Cree un nuevo igroup:
   a. En el menú **Grupos de iniciadores de SAN** del sitio de destino, seleccione **Agregar**.
   b. Proporcione un **Nombre**, seleccione el **Sistema Operativo del Host** y, a continuación, elija **Miembros del Grupo Iniciador**.
   c. Selecciona **Guardar**.
3. Asigne el nuevo igroup a las LUN de destino.
   a. Vaya a **Almacenamiento** > **LUN**.
   b. Seleccione todas las LUN que desea asignar al igroup.
   c. Seleccione **Más** y luego **Asignar a grupos de iniciadores**.
4. Edite la relación de sincronización activa de SnapMirror.
   a. Navegue hasta **Protección** > **Relaciones**.
   b. Seleccione el menú de kabob junto a la relación que desea modificar y luego **Editar**.
   c. Modifique la **Política de Protección** a AutomatedFailoverDuplex.
   d. Al seleccionar AutoMatedFailoverDuplex, se inicia la opción de modificar la configuración de proximidad del host. Para los iniciadores, seleccione la opción apropiada para **Iniciador proximal a** y luego **Guardar**.
   e. Selecciona **Guardar**.

5. En el menú **Protección**, confirme que la operación se ha realizado correctamente cuando la relación se muestre como `InSync`.

CLI

Pasos para una configuración uniforme

1. Modifique la política de SnapMirror de `AutomatedFailover` a `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path <destination_path> -policy
   AutomatedFailoverDuplex
   ```

2. Al modificar la política se desencadena una resincronización. Espere a que la resincronización finalice y confirme que la relación es `Insync`:

   ```
   snapmirror show -destination-path <destination_path>
   ```

3. Si los hosts existentes son locales en el clúster primario, añada el host al segundo clúster y establezca la conectividad con el respectivo acceso a cada clúster.
4. En el sitio secundario, elimine los mapas de LUN de los iGroups asociados con hosts remotos.

   Asegúrese de que el igroup no contiene mapas de LUN no replicadas.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

5. En la ubicación principal, defina el nivel de privilegio en `advanced`:

   ```
   SiteA::> set -privilege advanced
   ```

6. Modifique la configuración del iniciador para los hosts existentes a fin de establecer la ruta proximal de los iniciadores en el clúster local.

   ```
   SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>
   -initiator <host> -proximal-vserver <server>
   ```

   Puede volver a establecer el nivel de privilegio en admin después de completar este paso.

7. Añada un igroup y un iniciador nuevos para los hosts nuevos y configure la proximidad de host para la afinidad de host con su sitio local. Replicación de igroup ennable para replicar la configuración e invertir la localidad de host en el clúster remoto.

   ```
   SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
   SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
   host2 -proximal-vserver vsB
   ```

8. Detecte las rutas en los hosts y compruebe que los hosts tengan una ruta de activo/optimizada al LUN de almacenamiento desde el clúster preferido
9. Ponga en marcha la aplicación y distribuya las cargas de trabajo de los equipos virtuales entre los clústeres.

Pasos para una configuración no uniforme

1. Modifique la política de SnapMirror de `AutomatedFailover` a `AutomatedFailoverDuplex`:

   ```
   snapmirror modify -destination-path <destination_path> -policy
   AutomatedFailoverDuplex
   ```

2. Al modificar la política se desencadena una resincronización. Espere a que la resincronización finalice y confirme que la relación es `Insync`:

   ```
   snapmirror show -destination-path <destination_path>
   ```

3. Si los hosts existentes son locales en el clúster primario, añada el host al segundo clúster y establezca la conectividad con el respectivo acceso a cada clúster.
4. En el sitio secundario, añada un nuevo igroup e iniciador para los nuevos hosts y establezca la proximidad de host para la afinidad del host con su sitio local. Asigne las LUN al igroup.

   ```
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup>
   SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator
   <host_name>
   SiteB::> lun mapping create -igroup <igroup> -path <path_name>
   ```

5. Detecte las rutas en los hosts y compruebe que los hosts tengan una ruta de activo/optimizada al LUN de almacenamiento desde el clúster preferido
6. Ponga en marcha la aplicación y distribuya las cargas de trabajo de los equipos virtuales entre los clústeres.

Convertir de una relación simétrica activa/activa a una asimétrica iSCSI o FC

Si ha configurado la protección activa/activa simétrica mediante iSCSI o FC, puede convertir la relación a protección asimétrica mediante la CLI de ONTAP .

Pasos

1. Mueva todas las cargas de trabajo de la máquina virtual al host local al clúster de origen.
2. Quite la configuración del igroup para los hosts que no gestionan las instancias de la máquina virtual y, a continuación, modifique la configuración del igroup para finalizar la replicación de igroup.

   ```
   igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
   ```

3. En el sitio secundario, desasigne las LUN.

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

4. En el sitio secundario, elimine la relación activo-activo simétrica.

   ```
   SiteB::> snapmirror delete -destination-path <destination_path>
   ```

5. En el sitio principal, libere la relación activo-activo simétrica.
   ```
   SiteA::> snapmirror release -destination-path <destination_path> -relationship
   -info-only true
   ```

6. Desde el sitio secundario, cree una relación con el mismo conjunto de volúmenes con `AutomatedFailover` la política para volver a sincronizar la relación.

```
SiteB::> snapmirror create -source-path <source_path> -destination-path
<destination_path> -cg-item-mappings <source:@destination> -policy
AutomatedFailover
SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy
<policy_type>
```

> El grupo de coherencia en el sitio secundario debe "se debe eliminar"volver a crear la relación. Los volúmenes de destino "Se debe convertir a tipo DP". Para convertir los volúmenes en DP, ejecute `snapmirror resync` el comando con una política `MirrorAndVault` que no sea-`AutomatedFailover`: , `MirrorAllSnapshots` O `Sync`.

7. Confirme que la relación Mirror State es `Snapmirrored` el Estado de la relación es `Insync`.

```
snapmirror show -destination-path destination_path
```

8. Vuelva a detectar las rutas desde el host.

Información relacionada

- "snapmirror elimina"
- "modificar snapmirror"
- "versión de snapmirror"
- "resincronización de SnapMirror"
- "espectáculo de Snapmirror"

Gestione la sincronización activa de SnapMirror y proteja los datos

Crear una instantánea común entre los grupos de consistencia de ONTAP

Además de las operaciones Snapshot programadas regularmente, puede crear manualmente un recurso común "snapshot" entre los volúmenes del grupo de coherencia de SnapMirror primario y los volúmenes en el grupo de coherencia de SnapMirror secundario.

Acerca de esta tarea

El intervalo de creación de la snapshot programada es de 12 horas.

Antes de empezar

- La relación de grupo SnapMirror debe estar sincronizada.

Pasos

1. Cree una instantánea común:

```
destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
```

2. Supervise el progreso de la actualización:

```
destination::>snapmirror show -fields newest-snapshot
```

Información relacionada

- "espectáculo de Snapmirror"

Realizar una conmutación por error planificada de clústeres de ONTAP en una relación de sincronización activa de SnapMirror

En una conmutación al respaldo planificada de los clústeres de ONTAP en una relación de sincronización de SnapMirror activo, debe cambiar los roles de los clústeres principal y secundario, de modo que el clúster secundario asuma el control del clúster principal. Durante una conmutación por error, lo que normalmente funciona el clúster secundario procesa las solicitudes de entrada y salida localmente sin interrumpir las operaciones del cliente.

Quizás desee realizar una conmutación al respaldo planificada para probar el estado de la configuración de recuperación de desastres o realizar tareas de mantenimiento del clúster principal.

Acerca de esta tarea

El administrador del clúster secundario inicia una conmutación al respaldo planificada. La operación requiere cambiar los roles primario y secundario de manera que el clúster secundario asuma el control del primario. Después, el nuevo clúster principal puede comenzar a procesar solicitudes de entrada y salida de forma local sin interrumpir las operaciones del cliente.

Antes de empezar

- La relación de sincronización activa de SnapMirror debe estar sincronizada.
- No puede iniciar una conmutación al respaldo planificada cuando hay una operación no disruptiva en proceso. Las operaciones no disruptivas incluyen traslados de volúmenes, reubicaciones de agregados y recuperación tras fallos de almacenamiento.
- El mediador ONTAP debe estar configurado, conectado y en quórum.

Pasos

Puede realizar una conmutación al respaldo planificada con la interfaz de línea de comandos de ONTAP o System Manager.

System Manager

Desde ONTAP 9.14.1 hasta 9.8, la sincronización activa de SnapMirror se conoce como SnapMirror Business Continuity (SM-BC).

1. En System Manager, seleccione **Protección > Descripción general > Relaciones**.
2. Identificar la relación de sincronización activa de SnapMirror que desea conmutar por error. Junto a su nombre, seleccione el … junto al nombre de la relación y luego seleccione **Failover**.
3. Para supervisar el estado de la conmutación al nodo de respaldo, utilice `snapmirror failover show` en la CLI de ONTAP.

CLI

1. Desde el clúster de destino, inicie la operación de conmutación por error:

   ```
   destination::>snapmirror failover start -destination-path
   vs1_dst:/cg/cg_dst
   ```

2. Supervise el progreso de la conmutación por error:

   ```
   destination::>snapmirror failover show
   ```

3. Cuando finalice la operación de conmutación por error, puede supervisar el estado de la relación de protección síncrona de SnapMirror desde el destino:

   ```
   destination::>snapmirror show
   ```

Información relacionada

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

Recuperarse de operaciones de conmutación por error automáticas no planificadas del clúster ONTAP

Una conmutación por error automática no planificada (AUFO) se produce cuando el clúster principal está inactivo o aislado. El mediador de ONTAP detecta cuando ocurre una conmutación por error y ejecuta una conmutación por error automática no planificada al clúster secundario. Esta operación se realiza únicamente con la ayuda del Mediador ONTAP . El clúster secundario se convierte en el principal y comienza a atender a los clientes. Esta operación sólo se realiza con la ayuda de ONTAP Mediator.

Después de la conmutación automática al respaldo no planificada, es importante volver a analizar las rutas de I/o del LUN del host para que no se pierda las rutas de I/O.

Restablecer la relación de protección tras una conmutación al respaldo no planificada

Puede volver a establecer la relación de protección mediante System Manager o la CLI de ONTAP.

System Manager

Pasos

Desde ONTAP 9.14.1 hasta 9.8, la sincronización activa de SnapMirror se conoce como SnapMirror Business Continuity (SM-BC).

1. Vaya a **Protección > Relaciones** y espere hasta que el estado de la relación muestre "InSync".
2. Para reanudar las operaciones en el clúster de origen original, haga clic en ⋮ y seleccione **Failover**.

CLI

Puede supervisar el estado de la conmutación automática al respaldo no planificada con `snapmirror failover show` el comando.

Por ejemplo:

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Consulte el "Referencia EMS" para obtener más información acerca de los mensajes de eventos y las acciones correctivas.

Reanude la protección en una configuración ramificada después de una conmutación al nodo de respaldo

A partir de ONTAP 9.15.1, la sincronización activa de SnapMirror admite la reconfiguración automática en la sección de distribución ramificada tras un evento de conmutación por error. El tramo de distribución ramificada asíncrona puede ser una relación de grupo de coherencia o una relación de volumen independiente. Para obtener más información, consulte "configuraciones de dispersión".

Si usa ONTAP 9.14.1 o una versión anterior y experimenta una conmutación al nodo de respaldo en el clúster secundario en la relación de sincronización activa de SnapMirror, el destino asíncrono de SnapMirror cambia a estado incorrecto. Debe restaurar manualmente la protección eliminando y volviendo a crear la relación con el extremo asíncrono de SnapMirror.

Pasos

1. Compruebe que el failover se ha completado correctamente:
   `snapmirror failover show`
2. En el extremo asíncrono de SnapMirror, elimine el extremo de fan-out:
   `snapmirror delete -destination-path` *`destination_path`*

3. En el tercer sitio, cree una relación asíncrona de SnapMirror entre el nuevo volumen primario de sincronización activa de SnapMirror y el volumen de destino asíncrono de distribución ramificada:
`snapmirror create -source-path source_path -destination-path destination_path -policy MirrorAllSnapshots -schedule schedule`
4. Resincronice la relación:
`snapmirror resync -destination-path destination_path`
5. Compruebe el estado y el estado de la relación:
`snapmirror show`

Información relacionada

- "snapmirror create"
- "snapmirror elimina"
- "espectáculo de conmutación por error de SnapMirror"
- "resincronización de SnapMirror"
- "espectáculo de Snapmirror"

Supervisar las operaciones de sincronización activa de ONTAP SnapMirror

Puede supervisar las siguientes operaciones de sincronización activa de SnapMirror para garantizar el estado de la configuración de sincronización activa de SnapMirror:

- Mediador ONTAP
- Operaciones de conmutación por error planificadas
- Operaciones automáticas de conmutación al respaldo no planificadas
- Disponibilidad de sincronización activa de SnapMirror

> A partir de ONTAP 9.15.1, System Manager muestra el estado de su relación de sincronización activa de SnapMirror en cualquier clúster. También puede supervisar el estado de los mediadores de ONTAP desde cualquier clúster en System Manager.

Mediador ONTAP

Durante las operaciones normales, el estado Mediador de ONTAP debe estar conectado. Si está en cualquier otro estado, esto podría indicar una condición de error. Es posible revisar el "Mensajes del sistema de gestión de eventos (EMS)" para determinar el error y las acciones correctivas adecuadas.

Operaciones de conmutación por error planificadas

Puede supervisar el estado y el progreso de una operación de conmutación al respaldo planificada mediante `snapmirror failover show` el comando. Por ejemplo:

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

Una vez finalizada la operación de conmutación por error, puede supervisar el estado de protección de SnapMirror desde el nuevo clúster de destino. Por ejemplo:

```
ClusterA::> snapmirror show
```

Consulte el "Referencia EMS" para obtener más información acerca de los mensajes de eventos y las acciones correctivas.

Operaciones automáticas de conmutación al respaldo no planificadas

Durante una conmutación al respaldo automática no planificada, puede supervisar el estado de la operación con `snapmirror failover show` el comando.

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

Consulte el "Referencia EMS" para obtener más información acerca de los mensajes de eventos y las acciones correctivas.

Disponibilidad de sincronización activa de SnapMirror

Puede comprobar la disponibilidad de la relación de sincronización activa de SnapMirror mediante una serie de comandos, ya sea en el clúster principal, el clúster secundario o en ambos.

Los comandos que utilice incluyen `snapmirror mediator show` el comando en el cluster primario y secundario para comprobar el estado de la conexión y del quórum, el `snapmirror show` comando y el `volume show` comando. Por ejemplo:

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                      Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                       No-consensus
```

Información relacionada

- "espectáculo de conmutación por error de SnapMirror"
- "inicio de conmutación por error de snapmirror"
- "Programa de mediación de Snapmirror"

Agregar o eliminar volúmenes a un grupo de consistencia de ONTAP

A medida que cambian los requisitos de carga de trabajo de la aplicación, es posible que deba añadir o quitar volúmenes de un grupo de coherencia para garantizar la continuidad del negocio. El proceso de añadir y quitar volúmenes en una relación de sincronización

activa de SnapMirror depende de la versión de ONTAP que esté utilizando.

En la mayoría de los casos, este es un proceso disruptivo que requiere que elimine la relación de SnapMirror, modifique el grupo de consistencia y reanude la protección. A partir de ONTAP 9.13.1, añadir volúmenes a un grupo de consistencia con una relación de SnapMirror activa es una operación no disruptiva.

Acerca de esta tarea

- En ONTAP 9,9.1, puede añadir o quitar volúmenes a un grupo de consistencia mediante la CLI de ONTAP.
- A partir de ONTAP 9.10,1, se recomienda gestionar "grupos de consistencia" mediante System Manager o con la API DE REST DE ONTAP.

  Si desea cambiar la composición del grupo de coherencia. Para ello, añada o quite un volumen, primero debe eliminar la relación original y, a continuación, volver a crear el grupo de coherencia con la nueva composición.

- A partir de ONTAP 9.13.1, puede agregar volúmenes sin interrupciones a un grupo de consistencia con una relación SnapMirror activa desde el origen o el destino. Esta acción no es compatible con el protocolo NVMe.

  Eliminar volúmenes es una operación disruptiva. Debe eliminar la relación de SnapMirror antes de eliminar los volúmenes.

ONTAP 9,9.1-9.13.0

Antes de empezar

- No puede comenzar a modificar el grupo de consistencia mientras está en el `InSync` estado.
- El volumen de destino debe ser del tipo DP.
- El volumen nuevo que añade para expandir el grupo de coherencia debe tener una pareja de copias de Snapshot comunes entre los volúmenes de origen y de destino.

Pasos

Los ejemplos se muestran en dos asignaciones de volúmenes: `vol_src1` ←- `vol_dst1>` y `vol_src2` ←→ `vol_dst2`, en una relación de grupo de coherencia entre los puntos finales `vs1_src:/cg/cg_src` y `vs1_dst:/cg/cg_dst`.

1. En los clústeres de origen y destino, compruebe que hay una snapshot común entre los clústeres de origen y destino con el comando `snapshot show -vserver` *`svm_name`* `-volume` *`volume_name`* `-snapshot` *`snapmirror`*

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*

   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. Si no existe ninguna instantánea común, cree e inicialice una relación de FlexVol SnapMirror:

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. Elimine la relación del grupo de consistencia:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

4. Liberar la relación de SnapMirror de origen y conservar las snapshots comunes:

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. Desasigne las LUN y elimine la relación de grupo de consistencia existente:

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   > Se anula la asignación de las LUN de destino, mientras que las LUN de la copia principal siguen sirviendo la I/o del host

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. **Si utiliza ONTAP 9.10.1 a 9.13.0,** elimine y vuelva a crear el grupo de consistencia en el origen con

la composición correcta. Siga los pasos en"Eliminar un grupo de consistencia" y luego"Configure un único grupo de consistencia". ONTAP realizar las operaciones de eliminación y creación en el Administrador del sistema o con la API REST de ONTAP ; no hay ningún procedimiento CLI.

Si está utilizando ONTAP 9,9.1, pase al siguiente paso.

7. Cree el nuevo grupo de consistencia en el destino con la nueva composición:

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. Resincronice la relación del grupo de consistencia de objetivo de tiempo de recuperación cero para garantizar que está sincronizada:

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. Reasigne las LUN no asignadas en el paso 5:

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. Vuelva a analizar las rutas de I/o del LUN del host para restaurar todas las rutas a los LUN.

ONTAP 9.13.1 y versiones posteriores

A partir de ONTAP 9.13.1, es posible añadir volúmenes a un grupo de coherencia con una relación de sincronización activa de SnapMirror activa sin interrupciones. La sincronización activa de SnapMirror admite la adición de volúmenes de origen o destino.

> Desde ONTAP 9.14.1 hasta 9.8, la sincronización activa de SnapMirror se conoce como SnapMirror Business Continuity (SM-BC).

Para obtener detalles sobre cómo añadir volúmenes del grupo de coherencia de origen, consulte Modificar un grupo de consistencia.

Añada un volumen desde el clúster de destino

1. En el clúster de destino, seleccione **Protección** > **Relaciones**.
2. Busque la configuración de SnapMirror a la que desea añadir volúmenes. Seleccione ⋮ y luego **Expandir**.
3. Seleccione las relaciones de volumen cuyos volúmenes se añadirán al grupo de coherencia
4. Seleccione **Expandir**.

Información relacionada

- "snapmirror elimina"
- "inicializar snapmirror"
- "versión de snapmirror"
- "resincronización de SnapMirror"

Actualice y revierta con la sincronización activa de ONTAP SnapMirror

La sincronización activa de SnapMirror es compatible a partir de ONTAP 9,9.1. Actualizar y revertir el clúster o las controladoras de ONTAP puede afectar a las relaciones de sincronización activa de SnapMirror según la versión de ONTAP a la que actualice o revierta.

Actualice un clúster

A partir de ONTAP 9.16.1, SnapMirror active Sync admite clústeres de cuatro nodos en configuraciones activo-activo simétricas. El clúster de cuatro nodos se puede utilizar para actualizar las controladoras y el almacenamiento.

Antes de empezar

- Revise la "requisitos para clústeres de cuatro nodos".
- Puede crear configuraciones asimétricas durante el proceso de actualización tecnológica; sin embargo, debe volver a una configuración simétrica después de completar la actualización.
- Estas instrucciones se aplican a una configuración existente de cuatro nodos con 50 o menos grupos de consistencia y 400 o menos extremos de volumen.

Pasos

1. "Mueva todos los volúmenes de sincronización activa de SnapMirror a un par *único* de alta disponibilidad (HA)".
2. "Quite los nodos no utilizados del clúster".
3. "Añada los nodos nuevos al clúster".
4. "Mueva todos los volúmenes" en los nodos nuevos.
5. "Quite los nodos no utilizados del clúster" a continuación, reemplácelos "con los nodos nuevos".

Actualice ONTAP con sincronización activa de SnapMirror

Para usar la sincronización activa de SnapMirror, todos los nodos de los clústeres de origen y de destino deben ejecutar ONTAP 9.9.1 o una versión posterior.

Al actualizar ONTAP con relaciones de sincronización activa de SnapMirror activas, debe utilizar Actualización automatizada no disruptiva (ANDU). El uso de ANDU garantiza que las relaciones de sincronización activa de SnapMirror estén sincronizadas y en buen estado durante el proceso de actualización.

No hay pasos de configuración necesarios para preparar las implementaciones de sincronización activa de SnapMirror para las actualizaciones de ONTAP. Sin embargo, se recomienda que antes y después de la actualización, compruebe que:

- Las relaciones de sincronización activa de SnapMirror están sincronizadas.
- No hay errores relacionados con SnapMirror en el registro de eventos.
- El Mediador está en línea y en buen estado desde ambos clusters.
- Todos los hosts pueden ver todas las rutas correctamente para proteger los LUN.

Cuando actualiza clústeres de ONTAP 9.9,1 o 9.9.1 a ONTAP 9.10,1 y versiones posteriores, ONTAP crea nuevos grupos de consistencia en los clústeres de origen y de destino para las relaciones de sincronización activa de SnapMirror que se pueden configurar mediante System Manager.

`snapmirror quiesce` `snampirror resume`Los comandos y no se admiten con la sincronización activa de SnapMirror.

Vuelva a ONTAP 9.9.1 desde ONTAP 9.10.1

Para revertir las relaciones de la 9.10.1 a la 9,9.1, deben eliminarse las relaciones de sincronización activa de SnapMirror, seguidas de la instancia del grupo de consistencia 9.10.1. Los grupos de consistencia con una relación de sincronización activa de SnapMirror activa no se pueden eliminar. Todos los volúmenes de FlexVol que se hayan actualizado a 9.10.1 asociados previamente con otro contenedor inteligente o aplicación empresarial en la versión 9.9.1 o anterior ya no se asociarán al revertir. Al eliminar grupos de consistencia no se eliminan los volúmenes constituyentes ni las snapshots granulares de volúmenes. Consulte "Eliminar un grupo de consistencia"para obtener más información sobre esta tarea en ONTAP 9.10,1 y versiones posteriores.

Revertir desde ONTAP 9.9.1

La sincronización activa de SnapMirror no es compatible con clústeres mixtos de ONTAP que incluyan versiones anteriores a ONTAP 9,9.1.

Al revertir de ONTAP 9.9.1 a una versión anterior de ONTAP, debe tener en cuenta lo siguiente:

- Si el clúster aloja un destino de SnapMirror de sincronización activa, no se podrá revertir a ONTAP 9,8 o una versión anterior hasta que la relación se rompa y se elimine.
- Si el clúster aloja un origen de sincronización activa de SnapMirror, no se podrá revertir a ONTAP 9,8 o una versión anterior hasta que se publique la relación.
- Es necesario eliminar todas las políticas de sincronización activa de SnapMirror personalizadas creadas por el usuario antes de volver a ONTAP 9,8 o una versión anterior.

Para cumplir estos requisitos, consulte "Quitar una configuración de sincronización activa de SnapMirror".

Pasos

1. Confirme la preparación para la reversión introduciendo el siguiente comando de uno de los clústeres en la relación de sincronización activa de SnapMirror:

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   El siguiente resultado de ejemplo muestra un clúster que no está listo para revertir con instrucciones para la limpieza.

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   ```

```
all data LIFs down: network interface modify {-role data} -status-admin
down
Disable snapshot policies.
    Command to list snapshot policies: "snapshot policy show".
    Command to disable snapshot policies: "snapshot policy modify
-vserver
   * -enabled false"

   Break off the initialized online data-protection (DP) volumes and
delete
   Uninitialized online data-protection (DP) volumes present on the
local
   node.
    Command to list all online data-protection volumes on the local
node:
   volume show -type DP -state online -node <local-node-name>
    Before breaking off the initialized online data-protection volumes,
   quiesce and abort transfers on associated SnapMirror relationships
and
   wait for the Relationship Status to be Quiesced.
    Command to quiesce a SnapMirror relationship: snapmirror quiesce
    Command to abort transfers on a SnapMirror relationship: snapmirror
   abort
    Command to see if the Relationship Status of a SnapMirror
relationship
   is Quiesced: snapmirror show
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
```

```
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. Una vez que haya cumplido los requisitos de la comprobación de reversión, consulte "Revierte ONTAP".

Información relacionada

- "interfaz de red"
- "rotura de snapmirror"
- "eliminar política de snapmirror"
- "Mostrar política de Snapmirror"
- "Snapmirror en reposo"
- "espectáculo de Snapmirror"

Eliminar una configuración de sincronización activa de ONTAP SnapMirror

Si ya no necesita una protección síncrona de SnapMirror con objetivo de tiempo de recuperación cero, puede eliminar su relación de sincronización activa de SnapMirror.

Eliminar una configuración asimétrica

- Antes de eliminar la relación de sincronización activa de SnapMirror, deben quitarse la asignación de todas las LUN del clúster de destino.
- Una vez que se anula la asignación de las LUN y se vuelve a analizar el host, el destino SCSI notifica a los hosts que ha cambiado el inventario de LUN. Las LUN existentes en los volúmenes secundarios con objetivo de tiempo de recuperación cero cambian para reflejar una identidad nueva después de eliminar la relación con objetivo de tiempo de recuperación cero. Los hosts detectan los LUN del volumen secundario como nuevos LUN que no tienen relación con los LUN del volumen de origen.
- Los volúmenes secundarios permanecen en los volúmenes de recuperación ante desastres una vez que se elimina la relación. Puede emitir `snapmirror break` el comando para convertirlos a lectura/escritura.
- No se permite eliminar la relación en el estado fallido cuando no se invierte la relación.

Pasos

1. En el clúster secundario, quite la relación del grupo de consistencia de sincronización activa de SnapMirror entre el extremo de origen y el extremo de destino:

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. En el clúster principal, libere la relación del grupo de coherencia y las copias de Snapshot creadas para la relación:

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. Realice una detección repetida del host para actualizar el inventario de LUN.

4. A partir de ONTAP 9.10.1, al eliminar la relación SnapMirror no se elimina el grupo de consistencia. Si desea eliminar el grupo de coherencia, debe usar System Manager o la API DE REST de ONTAP. Consulte Eliminar un grupo de consistencia para obtener más información.

Eliminar la configuración activa/activa simétrica de iSCSI o FC

Es posible quitar una configuración simétrica mediante System Manager o la interfaz de línea de comandos de ONTAP. En ambas interfaces, hay diferentes pasos para configuraciones uniformes y no uniformes.

System Manager

Pasos para una configuración uniforme

1. En el sitio primario, elimine los hosts remotos del igroup y finalice la replicación.
   a. Vaya a **Hosts** > **Grupos de iniciadores SAN**.
   b. Seleccione el igroup que desea modificar y luego **Editar**.
   c. Quite el iniciador remoto y finalice la replicación de igroup. Selecciona **Guardar**.
2. En el sitio secundario, elimine la relación replicada desasignando las LUN.
   a. Vaya a **HOSTS** > **SAN Initiator Groups**.
   b. Seleccione el igroup con la relación SnapMirror y, a continuación, **Eliminar**.
   c. En el cuadro de diálogo, seleccione el cuadro **Desasignar las LUN asociadas** y luego **Eliminar**.
   d. Navegue hasta **Protección** > **Relaciones**.
   e. Seleccione la relación de sincronización activa de SnapMirror y, a continuación, **Versión** para eliminar las relaciones.

Pasos para una configuración no uniforme

1. En el sitio primario, elimine los hosts remotos del igroup y finalice la replicación.
   a. Vaya a **Hosts** > **Grupos de iniciadores SAN**.
   b. Seleccione el igroup que desea modificar y luego **Editar**.
   c. Quite el iniciador remoto y finalice la replicación de igroup. Selecciona **Guardar**.
2. En el sitio secundario, quite la relación de sincronización activa de SnapMirror.
   a. Navegue hasta **Protección** > **Relaciones**.
   b. Seleccione la relación de sincronización activa de SnapMirror y, a continuación, **Versión** para eliminar las relaciones.

CLI

Pasos para una configuración uniforme

1. Mueva todas las cargas de trabajo de la máquina virtual al host local al clúster de origen de la sincronización activa de SnapMirror.
2. En el clúster de origen, quite los iniciadores del igroup y modifique la configuración del iGroup para finalizar la replicación de igroup.

   ```
   SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
   <os_type> -initiator <host2>
   SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
   <os_type> -replication-peer "-"
   ```

3. En el sitio secundario, elimine el mapa de LUN y quite la configuración de igroup:

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
   <>
   SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
   ```

4. En el sitio secundario, elimine la relación de sincronización activa de SnapMirror.

   ```
   SiteB::> snapmirror delete -destination-path destination_path
   ```

5. En el sitio principal, publicar la relación de sincronización activa de SnapMirror del sitio principal.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Vuelva a detectar las rutas para verificar que solo la ruta local esté disponible para el host.

Pasos para una configuración no uniforme

1. Mueva todas las cargas de trabajo de la máquina virtual al host local al clúster de origen de la sincronización activa de SnapMirror.
2. En el clúster de origen, quite los iniciadores del igroup.

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
<host2>
```

3. En el sitio secundario, elimine el mapa de LUN y quite la configuración de igroup:

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. En el sitio secundario, elimine la relación de sincronización activa de SnapMirror.

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. En el sitio principal, publicar la relación de sincronización activa de SnapMirror del sitio principal.

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. Vuelva a detectar las rutas para verificar que solo la ruta local esté disponible para el host.

Eliminar una configuración activa/activa simétrica NVMe

System Manager

Pasos

1. En el clúster de origen, navegue a **Protección > Replicación**.
2. Localice la relación que desea eliminar, seleccione ⋮ y seleccione **Eliminar**.

CLI

1. Desde el clúster de destino, elimine la relación de sincronización activa de SnapMirror .

   ```
   snapmirror delete -destination-path <destination_path> -unmap-namespace
   true
   ```

   Ejemplo:

   ```
   DST::> snapmirror delete -destination-path vs1:/cg/cg_dst_1 -force
   true
   ```

   El subsistema y sus espacios de nombres se eliminan del clúster secundario.

2. Desde el clúster de origen, libere la relación de sincronización activa de SnapMirror desde el sitio principal.

   ```
   snapmirror release -destination-path <destination_path>
   ```

   Ejemplo:

   ```
   SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
   ```

3. Vuelva a detectar las rutas para verificar que solo la ruta local esté disponible para el host.

Información relacionada

- "rotura de snapmirror"
- "snapmirror elimina"
- "versión de snapmirror"

Eliminar ONTAP Mediator o ONTAP Cloud Mediator

Si desea eliminar una configuración existente de ONTAP Mediator o ONTAP Cloud Mediator de sus clústeres de ONTAP , puede hacerlo mediante el `snapmirror mediator remove` Comando. Por ejemplo, solo se puede usar un tipo de Mediador a la vez, por lo que se debe eliminar una instancia antes de instalar la otra.

Pasos

Puede eliminar ONTAP Mediator o ONTAP Cloud Mediator completando uno de los siguientes pasos.

Mediador ONTAP

1. Eliminar Mediador ONTAP:

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   Ejemplo:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

Mediador de la nube de ONTAP

1. Eliminar ONTAP Cloud Mediator:

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   Ejemplo:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

Información relacionada

- "eliminar mediador de snapmirror"

Solucionar problemas

La operación de eliminación de SnapMirror de ONTAP falla en el estado de toma

Utilice la siguiente información si `snapmirror delete` El comando falla cuando una relación de grupo de consistencia de sincronización activa de SnapMirror está en estado de toma de control.

Tema:

Cuando ONTAP 9.9.1 está instalado en un clúster, al ejecutar el comando `snapmirror delete` El comando falla cuando una relación de grupo de consistencia de sincronización activa de SnapMirror está en estado de toma de control.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

Solución

Cuando los nodos en una relación de sincronización activa de SnapMirror están en estado de toma de control, realice la operación de eliminación y liberación de SnapMirror con la opción "-force" establecida en verdadera.

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

Información relacionada

- "snapmirror elimina"

Error al crear una relación SnapMirror de ONTAP e inicializar un grupo de consistencia

Utilice la siguiente información si falla la creación de una relación SnapMirror y la inicialización del grupo de consistencia.

Tema:

Se produce un error en la creación de la relación de SnapMirror y en la inicialización del grupo de consistencia.

Solución:

Asegúrese de no haber superado el límite de grupos de consistencia por clúster. Los límites del grupo de coherencia en la sincronización activa de SnapMirror son independientes de la plataforma y difieren en función de la versión de ONTAP. Consulte "Límites de objeto" para obtener orientación específica sobre su versión de ONTAP.

Error

Si el grupo de coherencia está atascado inicializando, compruebe el estado de las inicializaciones del grupo de consistencia con la API de REST DE ONTAP, System Manager o el comando `sn show -expand`.

> Desde ONTAP 9.14.1 hasta 9.8, la sincronización activa de SnapMirror se conoce como SnapMirror Business Continuity (SM-BC).

Solución:

Si no se pueden inicializar los grupos de consistencia, elimine la relación de sincronización activa de SnapMirror, elimine el grupo de consistencia y, a continuación, vuelva a crear la relación e inicialícelo. Este flujo de trabajo varía en función de la versión de ONTAP que se utilice.

Si utiliza ONTAP 9.9.1	Si utiliza ONTAP 9.10.1 o una versión posterior

1. "Quite la configuración de SnapMirror Active Sync" 2. "Cree una relación de grupo de consistencia y luego inicialice la relación del grupo de consistencia"	1. En **Protection > Relationships**, busque la relación de sincronización activa de SnapMirror en el grupo de consistencia. Seleccione ⋮, y luego * Eliminar * para eliminar la relación de sincronización activa de SnapMirror. 2. "Elimine el grupo de consistencia" 3. "Configure el grupo de consistencia"

La conmutación por error planificada del clúster ONTAP no tuvo éxito

Utilice la siguiente información si la operación de conmutación por error planificada no tiene éxito.

Tema:

Tras ejecutar `snapmirror failover start` el comando, el resultado del `snapmirror failover show` comando muestra un mensaje indica que hay una operación no disruptiva en curso.

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                                  08:35:04
08:35:04
```

Causa:

Una conmutación al respaldo planificada no puede comenzar cuando exista una operación no disruptiva en curso, incluyendo el movimiento de volúmenes, la reubicación de agregados y la conmutación al respaldo de almacenamiento.

Solución:

Se debe esperar a que finalice la operación no disruptiva y volver a intentar la operación de conmutación al nodo de respaldo.

Información relacionada

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

No se puede acceder a ONTAP Mediator o ONTAP Cloud Mediator o el estado del quórum del mediador es falso

Utilice la siguiente información si no se puede acceder a ONTAP Mediator o ONTAP Cloud Mediator o si el estado del quórum del mediador es falso.

Tema:

Después de ejecutar el `snapmirror failover start` comando, la salida para el `snapmirror failover show` El comando muestra un mensaje que indica que ONTAP Mediator o ONTAP Cloud Mediator no está configurado.

Ver "Configurar el mediador de ONTAP y los clústeres para la sincronización activa de snapmirror" o "Configurar ONTAP Cloud Mediator para la sincronización activa de SnapMirror" .

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

Causa:

Mediador no está configurado o existen problemas de conectividad de red.

Solución:

Si no se configura ONTAP Mediator, debe configurar ONTAP Mediator antes de poder establecer una relación de sincronización activa de SnapMirror. Solucione cualquier problema de conectividad de red. Asegúrese de que Mediator está conectado y que el estado de quórum es verdadero en el sitio de origen y de destino mediante el comando snapmirror mediador show. Para obtener más información, consulte "Configure el Mediador ONTAP".

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

Información relacionada

- "espectáculo de conmutación por error de SnapMirror"
- "inicio de conmutación por error de snapmirror"
- "Programa de mediación de Snapmirror"

Se puede acceder a ONTAP Cloud Mediator, pero responde lentamente

Utilice la siguiente información si ONTAP Cloud Meditor falla con un error que indica que la latencia de ping es mayor que la latencia recomendada.

Tema:

Administrador del sistema: El servicio Cloud Mediator está disponible pero responde lentamente.

CLI: El `mediator add` El comando falla con el error:
`Error: command failed: The ping latency of the BlueXP cloud server is <x> ms which is higher than twice the recommended latency of 200 ms.`

Causa:

Es posible que los clústeres no estén ubicados cerca de la nube de la consola de NetApp o que haya cuellos de botella en la ruta de red.

Solución:

- Verifique la ubicación geográfica y la proximidad a la nube de la consola NetApp (EE. UU. Este).
- Optimice la ruta de red o aborde los cuellos de botella.
- Mida el tiempo de ida y vuelta (RTT) utilizando herramientas de red y reduzca la latencia dentro de los límites recomendados.
- Utilice un proxy HTTP para mejorar el rendimiento.

Ver "Configurar ONTAP Cloud Mediator y los clústeres para la sincronización activa de SnapMirror" .

Recuperación tras fallos no planificada automática no activada en el sitio B

Utilice la siguiente información si una falla en el Sitio A no desencadena una conmutación por error no planificada en el Sitio B.

Tema:

Un error en el sitio A no activa una conmutación por error no planificada en el sitio B.

Posible causa n.o 1:

El Mediador de ONTAP o el Mediador de ONTAP Cloud no están configurados. Para determinar si esta es la causa, emita el `snapmirror mediator show` comando en el clúster del Sitio B.

```
Cluster2::> snapmirror mediator show
This table is currently empty.
```

Este ejemplo indica que el Mediador no está configurado en el Sitio B.

Solución:

Asegúrese de que Mediator esté configurado en ambos clústeres, que el estado esté conectado y que el quórum esté establecido en Verdadero.

Posible causa n.o 2:

El grupo de consistencia de SnapMirror no está sincronizado. Para determinar si esta es la causa, consulte el registro de eventos para ver si el grupo de consistencia estaba sincronizado durante el momento en el que se produjo un error en el sitio.

```
cluster::> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- ------------
--------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

Solución:

Realice los pasos siguientes para realizar una conmutación por error forzada en el sitio B.

1. Desasigne todas las LUN que pertenecen al grupo de consistencia desde el sitio B.
2. Elimine la relación del grupo de coherencia de SnapMirror mediante la `force` opción.
3. Introduzca el `snapmirror break` comando en los volúmenes constituyentes del grupo de coherencia para convertir los volúmenes de DP a R/W, para habilitar I/O del sitio B.
4. Arranque los nodos del sitio A para crear una relación de objetivo de tiempo de recuperación cero desde el sitio B al sitio A.
5. Libere el grupo de consistencia con `relationship-info-only` en la ubicación A para conservar la snapshot común y desasignar las LUN que pertenecen al grupo de consistencia.
6. Convierta los volúmenes en el sitio A de R/W a DP mediante la configuración de una relación de nivel de volumen con la política de sincronización o la política asíncrona.
7. Emita el `snapmirror resync` para sincronizar las relaciones.
8. Elimine las relaciones de SnapMirror con la política de sincronización en el sitio A.
9. Libere las relaciones de SnapMirror con la política de sincronización mediante `relationship-info-only true` en el sitio B.
10. Cree una relación de grupo de consistencia del Sitio B al Sitio A.
11. Realice una resincronización del grupo de consistencia del sitio A y, a continuación, compruebe que el grupo de consistencia está sincronizado.
12. Vuelva a analizar las rutas de I/o del LUN del host para restaurar todas las rutas a los LUN.

Información relacionada

- "rotura de snapmirror"
- "Programa de mediación de Snapmirror"
- "resincronización de SnapMirror"

Enlace entre el Sitio B y el Mediador ONTAP inactivo y el Sitio A inactivo

Para comprobar la conexión del ONTAP Mediator o del ONTAP Cloud Mediator, utilice el `snapmirror mediator show` Comando. Si el estado de conexión es inaccesible y el Sitio B no puede comunicarse con el Sitio A, obtendrá un resultado similar al siguiente.

Siga los pasos de la solución para restablecer la conexión.

Ejemplo:

Usando el comando `snapmirror mediator show` de ONTAP Cloud Mediator:

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status Type
--------------- ---------------- ----------------- ------------- -------
0.0.0.0         C1_cluster       unreachable       true          cloud
```

Usando el comando `snapmirror mediator show` de salida del Mediador ONTAP :

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
--------------- ---------------- ----------------- -------------
10.237.86.17    C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

Solución

Fuerce una conmutación por error para habilitar E/S desde el sitio B y, a continuación, establezca una relación de RTO cero desde el sitio B al sitio A. Complete los siguientes pasos para realizar una conmutación por error forzada en el sitio B.

1. Anule la asignación de todos los LUN que pertenecen al grupo de consistencia del Sitio B. Esto fallará, por lo que primero debe modificar el igroup para eliminar el par de replicación SVM y luego eliminar el mapa de LUN.

Ejemplo:

```
C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_1                        igroup1       0
mixed
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
2 entries were displayed.

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_5 -igroup igroup1
Error: command failed: The peer cluster is unreachable and a SnapMirror
       Mediator is not configured. The configuration is locked for
replicated
       objects in this Vserver peer relationship on both clusters. The
only
       supported configuration change is to manually disable replication
on
       both sides of the relationship, after which configuration changes
are
       supported.
C1_cluster::> igroup modify -igroup igroup1 -replication-peer -

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_1 -igroup igroup1

C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
1 entries were displayed.
```

1. Elimine la relación del grupo de coherencia SnapMirror con la opción force.

2. Introduzca el comando SnapMirror break (`snapmirror break -destination_path svm:_volume_`) en los volúmenes constituyentes del grupo de coherencia para convertir los volúmenes de DP a RW, para habilitar la I/O del sitio B.

   Debe emitir el comando snapmirror break para cada relación del grupo de coherencia. Por ejemplo, si hay tres volúmenes en el grupo de coherencia, emitirá el comando para cada volumen.

3. Arranque los nodos del sitio A para crear una relación de objetivo de tiempo de recuperación cero desde el sitio B al sitio A.
4. Libere el grupo de consistencia con Relationship-info-only en el sitio A para conservar una Snapshot común y desasignar las LUN que pertenecen al grupo de consistencia.
5. Convierta los volúmenes en el sitio A de RW a DP configurando una relación de nivel de volumen mediante una política de sincronización o una política asíncrona.
6. Emita el `snapmirror resync` comando para sincronizar las relaciones.
7. Elimine las relaciones de SnapMirror con la política de sincronización en el sitio A.
8. Lance las relaciones de SnapMirror con la política Sync mediante la relación-info-only true en el sitio B.
9. Cree una relación de grupo de consistencia entre el sitio B y el sitio A.
10. En el clúster de origen, resincronice el grupo de consistencia. Compruebe que el estado del grupo de consistencia esté sincronizado.
11. Vuelva a analizar las rutas de I/O del LUN del host para restaurar todas las rutas a las LUN.

Información relacionada

- "rotura de snapmirror"
- "Programa de mediación de Snapmirror"
- "resincronización de SnapMirror"
- "espectáculo de Snapmirror"

Enlace entre el Sitio A y el Mediador ONTAP inactivo y el Sitio B inactivo

Cuando use SnapMirror, puede perder conectividad entre ONTAP Mediator o los clústeres con conexión entre iguales. Puede diagnosticar el problema si se comprueba la conexión, la disponibilidad y el estado de consenso de las distintas partes de la relación de sincronización activa de SnapMirror y, a continuación, se reanuda la conexión forzosamente.

Qué comprobar	Comando CLI	Indicador
Mediador del Sitio A	`snapmirror mediator show`	El estado de conexión se muestra como `unreachable`
Conectividad del centro B.	`cluster peer show`	Disponibilidad se muestra como `unavailable`
El estado de consenso del volumen de sincronización activa de SnapMirror	`volume show volume_name -fields smbc-consensus`	`sm-bc consensus`Aparece el campo `Awaiting-consensus`

Para obtener información adicional sobre cómo diagnosticar y resolver este problema, consulte la"Base de conocimientos de NetApp : El vínculo entre el Sitio A y el Mediador está inactivo y el Sitio B está inactivo al

usar la sincronización activa de SnapMirror" .

Información relacionada

- "espectáculo de pares de clúster"
- "Programa de mediación de Snapmirror"

La operación de eliminación de ONTAP SnapMirror falla cuando se establece una valla en el volumen de destino

Utilice la siguiente información si la operación de eliminación de SnapMirror falla cuando alguno de los volúmenes de destino tiene una barrera de redirección configurada.

Tema:

Se produce un error en la operación de eliminación de SnapMirror cuando alguno de los volúmenes de destino tiene un conjunto de cerca de redirección.

Solución

Realizar las siguientes operaciones para volver a intentar la redirección y eliminar la cerca del volumen de destino.

- Resincronización de SnapMirror
- Actualización de SnapMirror

La operación de movimiento de volumen se bloquea cuando el servidor principal de ONTAP está inactivo

Utilice la siguiente información si una operación de movimiento de volumen queda bloqueada indefinidamente en un estado de transferencia diferida cuando el sitio principal está inactivo en una relación de sincronización activa de SnapMirror .

Tema:

Una operación de movimiento de volúmenes se detiene de forma indefinida en un estado de transición diferido cuando el sitio principal está inactivo en una relación de sincronización activa de SnapMirror. Cuando el sitio primario está inactivo, el sitio secundario realiza una conmutación por error automática no planificada (AUFO). Cuando hay una operación de movimiento de volumen en curso cuando se activa el AUFO, el movimiento de volumen se queda atascado.

Solución:

Cancele la instancia de movimiento de volumen que está bloqueada y reinicie la operación de movimiento de volumen.

La versión de ONTAP SnapMirror falla cuando no se puede eliminar la instantánea

Utilice la siguiente información si la operación de liberación de SnapMirror falla cuando no se puede eliminar la instantánea.

Tema:

Se produce un error en la operación de versión de SnapMirror cuando no se puede eliminar la copia de Snapshot.

Solución:

La Snapshot contiene una etiqueta transitoria. Utilice `snapshot delete` el comando con `-ignore-owners` la opción para quitar la snapshot transitoria.

```
snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners
true -force true
```

Vuelva a intentar `snapmirror release` el comando.

Información relacionada

- "versión de snapmirror"

La instantánea de referencia de movimiento de volumen se muestra como la más reciente para la relación SnapMirror de ONTAP

Utilice la siguiente información si la instantánea de referencia de movimiento de volumen se muestra como la más nueva para la relación SnapMirror después de una operación de movimiento de volumen.

Tema:

Después de realizar una operación de movimiento de volumen en un volumen de grupo de coherencia, es posible que la Snapshot de referencia de movimiento de volúmenes se muestre incorrectamente como la más reciente para la relación de SnapMirror.

La snapshot más reciente se puede ver con el siguiente comando:

```
snapmirror show -fields newest-snapshot status -expand
```

Solución:

Realice manualmente una `snapmirror resync` o espere a que finalice la siguiente operación de resincronización automática.

Información relacionada

- "resincronización de SnapMirror"
- "espectáculo de Snapmirror"

Mediador de ONTAP para la sincronización activa de MetroCluster y SnapMirror

Más información sobre ONTAP Mediator

Esta documentación se refiere a la versión local de ONTAP Mediator. Para obtener información sobre ONTAP Cloud Mediator, disponible a partir de ONTAP 9.17.1, consulte "Documentación de sincronización activa de SnapMirror" .

ONTAP Mediator proporciona varias funciones para las características de ONTAP:

- Proporciona un almacén persistente y cercado para metadatos de alta disponibilidad.
- Funciona como proxy ping para la vida útil de la controladora.
- Proporciona funcionalidad de consulta de estado de nodo síncrono para ayudar a determinar el quórum.

ONTAP Mediator proporciona dos servicios systemctl adicionales:

- **`ontap_mediator.service`**

  Mantiene el servidor API REST para administrar las relaciones ONTAP.

- **`mediator-scst.service`**

  Controla el inicio y el apagado del módulo iSCSI (SCST).

Herramientas proporcionadas para el administrador del sistema

Herramientas proporcionadas para el administrador del sistema:

- **`/usr/local/bin/mediator_change_password`**

  Establece una nueva contraseña de API cuando se proporcionan el nombre de usuario y la contraseña actuales de la API.

- **`/usr/local/bin/mediator_change_user`**

  Establece un nuevo nombre de usuario de API cuando se proporcionan el nombre de usuario y la contraseña actuales de la API.

- **`/usr/local/bin/mediator_generate_support_bundle`**

  Genera un archivo tgz local con toda la información de soporte útil necesaria para la comunicación con el soporte al cliente de NetApp. Esto incluye la configuración de la aplicación, los registros y cierta información del sistema. Los paquetes se generan en el disco local y se pueden transferir manualmente, según sea necesario. Ubicación de almacenamiento: /Opt/netapp/data/support_bundles/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  Elimina el paquete ONTAP Mediator y el módulo del núcleo SCST. Esto incluye todos los datos de configuración, registros y buzón de correo.

- **`/usr/local/bin/mediator_unlock_user`**

  Libera un bloqueo en la cuenta de usuario de la API si se alcanzó el límite de reintentos de autenticación. Esta función se utiliza para evitar la derivación de contraseña de fuerza bruta. Solicita al usuario el nombre de usuario y la contraseña correctos.

- **`/usr/local/bin/mediator_add_user`**

  (Solo soporte) Se utiliza para agregar el usuario de la API durante la instalación.

Notas especiales

ONTAP Mediator confía en SCST para proporcionar iSCSI (consulte http://scst.sourceforge.net/index.html). Este paquete es un módulo del núcleo que se compila durante la instalación específicamente para el núcleo. Es posible que cualquier actualización del núcleo requiera la reinstalación de SCST. Como alternativa, desinstale y vuelva a instalar ONTAP Mediator y luego reconfigure la relación de ONTAP.

Cualquier actualización del kernel del sistema operativo del servidor se debe coordinar con una ventana de mantenimiento de ONTAP.

Nuevas funciones en ONTAP Mediator

Con cada versión se proporcionan nuevas mejoras de ONTAP Mediator. Esto es lo nuevo.

Mejoras

Para obtener información sobre la versión de SCST, consulte la Matriz de soporte SCST.

Versión de ONTAP Mediator	Mejoras
1,11	• Compatibilidad con RHEL: ◦ Compatible: 9.5. ◦ Recomendado: 10.1, 10.0, 9.7, 9.6, 9.4 y 8.10. • Soporte para Rocky Linux 10.1, 9.7 y 8,10. • Compatibilidad con Oracle Linux 10.0 y 9.6. • Agrega soporte para IPv6 para configuraciones IP de MetroCluster . • Agrega soporte para fapolicyd.
1,10	• Compatibilidad con RHEL: ◦ Compatible: 9.5. ◦ Recomendado: 10.0, 9.6, 9.4 y 8,10. • Soporte para Rocky Linux 10.0, 9.6 y 8,10. • Actualiza la versión base de Python de Python 3.9 a Python 3.12.
1.9.1	• Compatibilidad con RHEL: ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 y 8.4. ◦ Recomendados: 9.5, 9.4, 9.2, 9.0, 8.10 y 8.8. • Soporte para Rocky Linux 9.5 y 8.10. • Agrega nuevos certificados para la verificación de firmas de código. • Se agregó soporte para omitir las verificaciones de firma de código mediante el `-skip-code-signature-check` bandera. • El instalador muestra advertencias cuando detecta certificados de firma de código caducados.

1,9	• Compatibilidad con RHEL: ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 y 8.4. ◦ Recomendados: 9.5, 9.4, 9.2, 9.0, 8.10 y 8.8. • Soporte para Rocky Linux 9.5 y 8.10. • Compatibilidad de FIPS para RHEL y Rocky Linux. • Mejoras de rendimiento añadidas para una mayor escalabilidad. • Nombres de archivo mejorados para simplificar la configuración de certificados firmados por PKI.
1,8	• Compatibilidad con RHEL: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4. ◦ Recomendados: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 y 8.8. • Soporte para Rocky Linux 9.4 y 8.10.
1,7	• Compatibilidad con RHEL: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4. ◦ Recomendado: 9.3, 9.2, 9.1, 9.0, 8.9 y 8.8. • Soporte para Rocky Linux 9.3 y 8.9. • Compatibilidad con datos SAN (nombre alternativo del sujeto) en certificados autofirmados y certificados firmados por terceros.
1,6	• Actualizaciones de Python 3,9. • Compatibilidad con RHEL: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4. ◦ Recomendado: 9.2, 9.1, 9.0 y 8,8. • Soporte para Rocky Linux 9.2 y 8.8. • Interrupción del soporte para RHEL 7.x / CentOS todas las versiones.
1,5	• Compatibilidad con RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6. • Soporte para CentOS 7.9, 7.8, 7.7 y 7.6. • Incluye advertencias de amortización para RHEL 7.x / CentOS 7.x. • Optimiza la velocidad para sistemas de sincronización activa de SnapMirror a gran escala. • Se añadió una firma de código criptográfica al instalador.
1,4	• Compatibilidad con RHEL 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6. • Soporte para CentOS 7.9, 7.8, 7.7 y 7.6. • Se ha añadido soporte para Secure Boot (SB) del firmware basado en UFEI.

1,3	• Compatibilidad con RHEL 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6. • Soporte para CentOS 7.9, 7.8, 7.7 y 7.6.
1,2	• Compatibilidad con RHEL 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6. • Soporte para CentOS 7.9, 7.8, 7.7 y 7.6. • Compatibilidad con buzones HTTPS. • Para usar con ONTAP 9,8+ MCC-IP AUSO y SnapMirror ACTIVE SYNC ZRTO.
1,1	• Compatibilidad con RHEL 8.0 y 7.6. • Soporte para CentOS 7,6. • Elimina las dependencias de Perl.
1,0	• Compatibilidad con buzones de correo iSCSI. • Para uso con ONTAP 9,7+ MCC-IP AUSO. • Compatibilidad con RHEL/CentOS 7,6.

Matriz de compatibilidad de SO

OS for ONTAP Mediator	1,11	1,10	1.9.1	1,9	1,8	1,7	1,6	1,5	1,4	1,3	1,2	1,1	1,0
RHEL 10.1	Sí	No	No	No	No	No	No	No	No	No	No	No	No
RHEL 10.0	Sí	Sí	Sí	No	No	No	No	No	No	No	No	No	No
RHEL 9.7	Sí	No	No	No	No	No	No	No	No	No	No	No	No
RHEL 9.6	Sí	Sí	Sí	No	No	No	No	No	No	No	No	No	No
RHEL 9,5	Compatible	Compatible	Sí	Sí	No	No	No	No	No	No	No	No	No
RHEL 9,4	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No	No
RHEL 9,3	No	No	Compatible	Compatible	Sí	Sí	No	No	No	No	No	No	No

RHEL 9,2	No	No	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No
RHEL 9,1	No	No	Compatible	Compatible	Sí	Sí	Sí	No	No	No	No	No	No
RHEL 9,0	No	No	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No
RHEL 8,10	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No	No	No
RHEL 8,9	No	No	Compatible	Compatible	Sí	Sí	No	No	No	No	No	No	No
RHEL 8,8	No	No	Sí	Sí	Sí	Sí	Sí	No	No	No	No	No	No
RHEL 8,7	No	No	Compatible	Compatible	Sí	Sí	Sí	No	No	No	No	No	No
RHEL 8,6	No	No	Compatible	Compatible	Sí	Sí	Sí	No	No	No	No	No	No
RHEL 8,5	No	No	Compatible	Compatible	Sí	Sí	Sí	Sí	Sí	No	No	No	No
RHEL 8,4	No	No	Compatible	Compatible	Sí	Sí	Sí	Sí	Sí	No	No	No	No
RHEL 8,3	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sí	Sí	Sí	No	No	No
RHEL 8,2	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sí	Sí	Sí	No	No	No
RHEL 8,1	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	No	No
RHEL 8,0	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	Sí	No
RHEL y CentOS 7.9	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sí	Sí	Sí	Compatible	No	No

RHEL y CentOS 7.8	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	No	No
RHEL y CentOS 7.7	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	No	No
RHEL y CentOS 7.6	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Obsoleto	Sí	Sí	Sí	Sí	Sí	Sí (solo RHEL)
CentOS 8 y STREAM	No	No	No	No	No	No	No	No	No	No	N / A	N / A	N / A
Rocky Linux 10,0	Sí	Sí	No	No	No	No	No	No	No	No	No	No	No
Rocky Linux 9	Sí	Sí	Sí	Sí	Sí	Sí	Sí	N / A	N / A	N / A	N / A	N / A	N / A
Rocky Linux 8	Sí	Sí	Sí	Sí	Sí	Sí	Sí	N / A	N / A	N / A	N / A	N / A	N / A
Oracle Linux 10,0	Sí	No	No	No	No	No	No	No	No	No	No	No	No
Oracle Linux 9	Sí	No	No	No	No	No	No	No	No	No	No	No	No

- «Sí» significa que el sistema operativo se recomienda para la instalación de ONTAP Mediator, y es totalmente compatible con él.
- “No” significa que el sistema operativo y el Mediador ONTAP no son compatibles.
- "Compatible" significa que Red Hat ya no admite estas versiones de RHEL, pero ONTAP Mediator aún se puede instalar en ellas.
- ONTAP Mediator 1.6 agrega soporte para Rocky Linux 9 y 8.

- ONTAP Mediator 1,5 fue la última versión admitida para los sistemas operativos de sucursal RHEL 7.x.
- CentOS 8 se eliminó para todas las versiones debido a su reramificación. CentOS Stream no se consideró un sistema operativo de destino de producción adecuado. No se ha planificado ningún soporte.

Matriz de soporte SCST

La siguiente tabla muestra la versión de SCST admitida para cada versión de ONTAP Mediator.

Versión de ONTAP Mediator	Versión de SCST compatible
Mediador ONTAP 1.11	scst-3.9.tar.gz
Mediador ONTAP 1.10	scst-3.9.tar.gz
Mediador ONTAP 1.9.1	scst-3,8.0.tar.bz2
Mediador ONTAP 1,9	scst-3,8.0.tar.bz2
Mediador ONTAP 1,8	scst-3,8.0.tar.bz2
Mediador ONTAP 1,7	scst-3,7.0.tar.bz2
Mediador ONTAP 1,6	scst-3,7.0.tar.bz2
Mediador ONTAP 1,5	scst-3,6.0.tar.bz2
Mediador ONTAP 1,4	scst-3,6.0.tar.bz2
Mediador ONTAP 1,3	scst-3,5.0.tar.bz2
Mediador ONTAP 1,2	scst-3,4.0.tar.bz2
Mediador ONTAP 1,1	scst-3,4.0.tar.bz2
Mediador ONTAP 1,0	scst-3,3.0.tar.bz2

Instale o actualice

Resumen del flujo de trabajo de instalación de ONTAP Mediator

La instalación de ONTAP Mediator incluye la preparación de la instalación, proporcionar acceso a los repositorios, descargar el paquete de instalación, verificar la firma del código, instalar el paquete de ONTAP Mediator y realizar tareas de configuración posteriores a la instalación.

1. **"Prepárese para instalar o actualizar ONTAP Mediator"**

Para instalar o actualizar ONTAP Mediator, debe asegurarse de que se cumplan todos los requisitos previos.

2. **"Actualizar el SO del host y Mediator"**

Si está actualizando una versión existente de ONTAP Mediator, primero debe desinstalar la versión anterior y luego instalar la nueva. Si es la primera vez que instala ONTAP Mediator, puede omitir este paso.

3 **"Proporcionar acceso al repositorio"**

Debe habilitar el acceso a los repositorios para que ONTAP Mediator pueda acceder a los paquetes necesarios durante el proceso de instalación.

4 **"Descargue el paquete de instalación de ONTAP Mediator"**

Descargue el paquete de instalación de ONTAP Mediator desde la página de descarga de ONTAP Mediator.

5 **"Verifique la firma del código del paquete de instalación de ONTAP Mediator"**

NetApp recomienda verificar la firma del código de ONTAP Mediator antes de instalar el paquete de instalación de ONTAP Mediator.

6 **"Instalar ONTAP Mediator"**

Para instalar ONTAP Mediator, debe obtener el paquete de instalación y ejecutar el instalador en el host.

7 **"Verificar la instalación de ONTAP Mediator"**

Después de instalar ONTAP Mediator, verifique que se esté ejecutando correctamente.

8 **"Realizar tareas de configuración posteriores a la instalación"**

Una vez instalado y en funcionamiento ONTAP Mediator, se deben realizar tareas de configuración adicionales para utilizar las funciones de ONTAP Mediator.

Instalar o actualizar ONTAP Mediator

Para instalar o actualizar ONTAP Mediator, debe cumplir con todos los requisitos previos, descargar el paquete de instalación y ejecutar el instalador en el host.

- A partir de ONTAP 9,8, puede usar cualquier versión de ONTAP Mediator para supervisar una relación de sincronización activa de SnapMirror.
- Puede utilizar cualquier versión de ONTAP Mediator para supervisar una configuración IP de MetroCluster .

Consideraciones sobre la instalación y la actualización

Revise estos puntos antes de actualizar o instalar ONTAP Mediator.

ONTAP Mediator 1.8 y versiones anteriores no son compatibles con el modo FIPS de Red Hat Enterprise Linux (RHEL) e impiden su correcta instalación. Puede comprobar si el modo FIPS está habilitado utilizando el `fips-mode-setup --check` dominio. Puede desactivar el modo FIPS utilizando el `fips-modesetup --disable` dominio. Reinicie después de deshabilitar el modo FIPS para instalar con éxito ONTAP Mediator 1.8 o anterior.

- Debe actualizar ONTAP Mediator a la última versión. Las versiones anteriores siguen funcionando con todas las versiones de ONTAP , pero las versiones más recientes incluyen parches de seguridad para componentes de terceros.
- Cuando se actualiza a una nueva versión de ONTAP Mediator, el instalador se actualiza automáticamente a la versión de SCST recomendada a menos que haya disponible una versión superior. Para obtener instrucciones sobre la instalación manual de una versión SCST superior, consulte "Gestionar Mediador ONTAP". Para ver las versiones compatibles, consulte la "Matriz de soporte SCST".

> - Si la instalación falla, es posible que deba actualizar a una versión más reciente de ONTAP Mediator.
> - A partir del 15 de junio de 2025, no podrás instalar ni actualizar ONTAP Mediator 1.9 y 1.8 porque sus certificados de firma de código han expirado. Si la instalación o actualización falla, utilice en su lugar la versión de parche ONTAP Mediator 1.9.1.

- Si instala `yum-utils` el paquete, puede usar `needs-restarting` el comando.
- A partir de ONTAP Mediator 1.11, se admite IPv6 para las configuraciones IP de MetroCluster .

Requisitos del host

Siga estos requisitos al instalar RHEL o Rocky Linux y configurar los repositorios asociados.

> Si modifica el proceso de instalación o configuración, es posible que deba realizar otros pasos.

Requisitos de distribución de Linux

- Instale RHEL o Rocky Linux siguiendo las mejores prácticas de Red Hat. Debido a que CentOS 8.x ha llegado al final de su ciclo de vida, no se recomiendan versiones compatibles de CentOS 8.x.
- Al instalar ONTAP Mediator, asegúrese de que el sistema tenga acceso al repositorio requerido para que el programa de instalación pueda recuperar e instalar todas las dependencias de software necesarias.
- Para permitir que el instalador yum encuentre software dependiente en los repositorios de RHEL, registre el sistema durante la instalación o después mediante una suscripción válida a Red Hat.

> Consulte la documentación de Red Hat Subscription Manager para obtener más información.

Requisitos de red

Asegúrese de que los siguientes puertos están disponibles y no se utilizan para ONTAP Mediator:

Puerto/servicios	Origen	Dirección	Destino	Específico
22 tcp	Host de gestión	Entrada	Mediador ONTAP	(Opcional) Gestión de SSH / ONTAP Mediator
31784 tcp	cluster-mgmt y node-mgmt LIFs	Entrada	Servidor web de Mediador ONTAP	API DE REST (REQUERIDA) (HTTPS)

3260/tcp	LIF de gestión de nodos	Entrada	Destinos iSCSI del mediador de ONTAP	(Requerido para configuraciones IP de MetroCluster) Conexión de datos iSCSI para buzones de correo

Para los clientes de SMBC, ONTAP no requiere que el puerto 3260 esté habilitado o conectado.

- Si utiliza un cortafuegos de terceros, consulte"Requisitos de firewall para ONTAP Mediator" .
- Para hosts Linux sin acceso a Internet, asegúrese de que los paquetes requeridos estén disponibles en un repositorio local.

  Si utiliza el protocolo de control de agregación de enlaces (LACP) en un entorno Linux, configure el núcleo y establezca `sysctl net.ipv4.conf.all.arp_ignore` el en `2`.

Requisitos de OS

Su sistema operativo debe cumplir los siguientes requisitos:

- instalación física de 64 bits o máquina virtual
- 8 GB DE MEMORIA RAM
- 1 GB de espacio en disco (utilizado para la instalación de aplicaciones, registros del servidor y la base de datos)
- Usuario: Acceso raíz

En la siguiente tabla se muestran los sistemas operativos admitidos para cada versión de ONTAP Mediator.

Versión de ONTAP Mediator	Versiones de Linux compatibles
1,11	• Red Hat Enterprise Linux ◦ Compatible: 9.5 [1] ◦ Recomendado: 10.1, 10.0, 9.7, 9.6, 9.4 y 8.10 • Rocky Linux 10,1, 9.7 y 8,10 • Oracle Linux 10.0 y 9.6
1,10	• Red Hat Enterprise Linux ◦ Compatible: 9.5 [1] ◦ Recomendado: 10.0, 9.6, 9.4 y 8,10 • Rocky Linux 10,0, 9.6 y 8,10
1.9.1	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendados: 9.5, 9.4, 9.2, 9.0, 8.10 y 8.8 • Rocky Linux 9.5 y 8.10

1,9	• Red Hat Enterprise Linux ◦ Compatible: 9.3, 9.1, 8.9, 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendados: 9.5, 9.4, 9.2, 9.0, 8.10 y 8.8 • Rocky Linux 9.5 y 8.10
1,8	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendados: 9.4, 9.3, 9.2, 9.1, 9.0, 8.10, 8.9 y 8.8 • Rocky Linux 9.4 y 8.10
1,7	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendado: 9.3, 9.2, 9.1, 9.0, 8.9 y 8.8 • Rocky Linux 9.3 y 8.9
1,6	• Red Hat Enterprise Linux: ◦ Compatible: 8.7, 8.6, 8.5 y 8.4 [1] ◦ Recomendado: 9.2, 9.1, 9.0 y 8,8 • Rocky Linux 9.2 y 8.8
1,5	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6 • CentOS: 7.9, 7.8, 7.7 y 7.6
1,4	• Red Hat Enterprise Linux: 8.5, 8.4, 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6 • CentOS: 7.9, 7.8, 7.7 y 7.6
1,3	• Red Hat Enterprise Linux: 8.3, 8.2, 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6 • CentOS: 7.9, 7.8, 7.7 y 7.6
1,2	• Red Hat Enterprise Linux: 8.1, 8.0, 7.9, 7.8, 7.7 y 7.6 • CentOS: 7.9, 7.8, 7.7 y 7.6

1. Compatible significa que Red Hat ya no admite estas versiones de RHEL, pero ONTAP Mediator aún se puede instalar en ellas.

Paquetes requeridos del sistema operativo

Los siguientes paquetes son requeridos por ONTAP Mediator:

Los paquetes están preinstalados o instalados automáticamente por el instalador de ONTAP Mediator.

Todas las versiones RHEL/CentOS	Paquetes adicionales para RHEL 10.x / Rocky Linux 10	Paquetes adicionales para RHEL 9.x / Rocky Linux 9	Paquetes adicionales para RHEL 8.x / Rocky Linux 8
• openssl • openssl • kernel-devel-$ (uname -r) • gcc • marca • libselinux-utils • parche • bzip2 • perl-Data-Dumper • perl-Extls-MakeMaker • efibootmgr • mokutil	• python3.12 • desarrollo de Python 3.12	• elfutils-libelf-devel • policcoreutils-python-utils • python3 • python3-devel	• elfutils-libelf-devel • policcoreutils-python-utils • redhat-lsb-core • python39 • python39-devel

El paquete de instalación de Mediator es un archivo tar comprimido autoextraíble que incluye:

- Un archivo RPM que contiene todas las dependencias que no pueden obtenerse del repositorio de la versión compatible.
- Una secuencia de comandos de instalación.

Se recomienda utilizar un certificado SSL válido.

Consideraciones sobre la actualización del sistema operativo y compatibilidad de kernel

- Puedes actualizar todos los paquetes de biblioteca excepto el kernel, pero es posible que tengas que reiniciar para aplicar los cambios en ONTAP Mediator. Programe un tiempo de inactividad si necesita reiniciar.
- Debes mantener actualizado el núcleo del sistema operativo. Actualiza el núcleo del kernel a una versión compatible que figure en la lista."Matriz de versiones de ONTAP Mediator" . Debe reiniciar el sistema, así que planifique una ventana de mantenimiento para la interrupción del servicio.
  - Desinstale el módulo del kernel SCST antes de reiniciar y, a continuación, vuelva a instalarlo.
  - Prepare una versión compatible de SCST para reinstalarla antes de iniciar la actualización del sistema operativo del kernel.

- La versión del kernel debe coincidir con la versión del sistema operativo.
- No actualice el kernel a una versión posterior a la del sistema operativo compatible con su versión de ONTAP Mediator, ya que es probable que el módulo SCST probado no funcione.

Instale ONTAP Mediator cuando el inicio seguro de UEFI esté activado

ONTAP Mediator se puede instalar en un sistema con o sin arranque seguro UEFI activado.

Acerca de esta tarea

Puede optar por deshabilitar el inicio seguro de UEFI antes de instalar ONTAP Mediator si no es necesario o si está solucionando problemas de instalación de ONTAP Mediator. Desactive la opción UEFI Secure Boot en la configuración de su máquina.

Para obtener instrucciones detalladas sobre cómo deshabilitar UEFI Secure Boot, consulte la documentación del sistema operativo del host.

Para instalar ONTAP Mediator con UEFI Secure Boot habilitado, debe registrar una clave de seguridad antes de que pueda iniciarse el servicio. La clave se genera durante el paso de compilación de la instalación SCST y se guarda como un par de claves público-privado en su máquina. Utilice la `mokutil` utilidad para agregar la clave pública como una clave de propietario de la máquina (MOK) a su firmware UEFI, lo que permite que el sistema confíe y cargue el módulo firmado. Guarde la `mokutil` frase de contraseña en una ubicación segura, ya que es necesario al reiniciar el sistema para activar el MOK.

Pasos

1. Compruebe si UEFI Secure Boot está habilitado en su sistema:

   ```
   mokutil --sb-state
   ```

   Los resultados indican si UEFI Secure Boot está activado en este sistema.

Si…	Vaya a…
El arranque seguro de UEFI está activado	
El arranque seguro UEFI está deshabilitado	"Actualice el sistema operativo del host y luego ONTAP Mediator"

   - Se le pedirá que cree una frase de acceso que debe almacenar en una ubicación segura. Necesitará esta frase de contraseña para habilitar la clave en el Administrador de inicio UEFI.
   - ONTAP Mediator 1.2.0 y versiones anteriores no admiten este modo.

2. Si la `mokutil` utilidad no está instalada, ejecute el siguiente comando:

   ```
   yum install mokutil
   ```

Actualice el sistema operativo host y ONTAP Mediator

Para actualizar el sistema operativo host para ONTAP Mediator a una versión posterior, primero debe desinstalar ONTAP Mediator.

Acerca de esta tarea

Antes de actualizar el sistema operativo host para ONTAP Mediator con la herramienta leapp-upgrade, desinstale ONTAP Mediator. La herramienta comprueba si hay nuevas versiones de RPM en los repositorios registrados.

El instalador de ONTAP Mediator instala un archivo .rpm, que la herramienta leapp-upgrade incluye en la

búsqueda. Debido a que el instalador descomprime el archivo en lugar de descargarlo de un repositorio registrado, la herramienta no puede encontrar una actualización. Debe utilizar la herramienta leapp-upgrade para desinstalar el paquete.

Pasos

1. Realiza una copia de seguridad de los archivos de registro:

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. Realice la actualización con la herramienta leapp-upgrade:

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. Reinstale el mediador ONTAP :

Realice el resto de los pasos inmediatamente después de volver a instalar ONTAP Mediator para evitar la pérdida de archivos de registro.

```
[rootmediator-host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. Detener ontap_mediator:

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. Reemplazar los archivos de registro:

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. Iniciar ontap_mediator:

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. Vuelva a conectar todos los clústeres ONTAP al mediador ONTAP actualizado:

MetroCluster sobre IP

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It may
take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

SnapMirror síncrono activo

Para la sincronización activa de SnapMirror , no es necesario reinstalar los certificados TLS almacenados fuera de /opt/netapp. Realiza copias de seguridad y restaura los certificados almacenados en /opt/netapp.

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                          ONTAPMediatorCA                        server-
ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
```

```
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer
-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true

peer1::>
```

Información relacionada

- "eliminar certificado de seguridad"
- "instalación del certificado de seguridad"
- "Mostrar certificado de seguridad"
- "añadir mediador de snapmirror"
- "eliminar mediador de snapmirror"
- "almacenamiento iscsi-initiator show"

Proporcione acceso al repositorio para la instalación de ONTAP Mediator

Debe habilitar el acceso a los repositorios para que ONTAP Mediator pueda acceder a los paquetes necesarios durante el proceso de instalación.

Pasos

1. Determine a qué repositorios se debe acceder, como se muestra en la siguiente tabla:

Si su sistema operativo es…	Debe proporcionar acceso a estos repositorios…
RHEL 10.x	• rhel-10-para-x86_64-baseos-rpm • rhel-10-para-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64-baseos-rpms • rhel-9-for-x86_64-appstream-rpms
RHEL 8.x	• rhel-8-for-x86_64-baseos-rpms • rhel-8-for-x86_64-appstream-rpms
RHEL 7.x	• rhel-7-server-optional-rpms
CentOS 7.x	• C7.6.1810 - repositorio base
Rocky Linux 10	• flujo de aplicación • baseos
Rocky Linux 9	• flujo de aplicación • baseos
Rocky Linux 8	• flujo de aplicación • baseos

2. Utilice uno de los siguientes procedimientos para habilitar el acceso a los repositorios enumerados anteriormente para que ONTAP Mediator pueda acceder a los paquetes necesarios durante el proceso de instalación.

Si ONTAP Mediator tiene dependencias en módulos Python presentes en los repositorios "extras" y "opcionales", es posible que necesite acceder a los `rhel-X-for-x86_64-extras-rpms` y `rhel-X-for-x86_64-optional-rpms` archivos.

Procedimiento para el sistema operativo RHEL 10.x

Utilice este procedimiento si su sistema operativo es **RHEL 10.x** para habilitar el acceso a los repositorios:

Pasos

1. Suscríbase al repositorio deseado:

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
```

En el ejemplo siguiente se muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this system.
```

2. Ejecute `yum repolist` el comando.

Los repositorios recientemente suscritos deben aparecer en la lista.

Procedimiento para el sistema operativo RHEL 9.x.

Utilice este procedimiento si su sistema operativo es **RHEL 9.x** para permitir el acceso a los repositorios:

Pasos

1. Suscríbase al repositorio deseado:

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

   En el ejemplo siguiente se muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Ejecute `yum repolist` el comando.

   Los repositorios recientemente suscritos deben aparecer en la lista.

Procedimiento para el sistema operativo RHEL 8.x.

Utilice este procedimiento si su sistema operativo es **RHEL 8.x** para permitir el acceso a los repositorios:

Pasos

1. Suscríbase al repositorio deseado:

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

   En el ejemplo siguiente se muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. Ejecute `yum repolist` el comando.

   Los repositorios recientemente suscritos deben aparecer en la lista.

Procedimiento para el sistema operativo RHEL 7.x.

Utilice este procedimiento si su sistema operativo es **RHEL 7.x** para permitir el acceso a los repositorios:

Pasos

1. Suscríbase al repositorio deseado:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

En el ejemplo siguiente se muestra la ejecución de este comando:

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. Ejecute `yum repolist` el comando.

En el siguiente ejemplo, se muestra la ejecución de este comando. El repositorio "rhel-7-Server-optional-rpms" debe aparecer en la lista.

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
|  26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                    repo name
status
rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
Linux 7 Server - Optional (RPMs)   19,447
rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
Linux 7 Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#
```

Procedimiento para el sistema operativo CentOS 7.x.

Utilice este procedimiento si su sistema operativo es **CentOS 7.x** para permitir el acceso a los repositorios:

> Los siguientes ejemplos muestran un repositorio para CentOS 7,6 y es posible que no funcione para otras versiones de CentOS. Utilice el repositorio base para su versión de CentOS.

Pasos

1. Agregue el repositorio base C7.6.1810. El repositorio de almacén base C7,6.1810 contiene el paquete «kernel-devel» necesario para ONTAP Mediator.
2. Agregue las siguientes líneas a /etc/yum.repos.d/CentOS-Vault.repo.

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. Ejecute `yum repolist` el comando.

   En el siguiente ejemplo, se muestra la ejecución de este comando. El repositorio de CentOS-7.6.1810 - base debería aparecer en la lista.

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz         | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db       | 6.0 MB  00:00:04
repo id                    repo name                status
C7.6.1810-base/x86_64      CentOS-7.6.1810 - Base   10,019
base/7/x86_64              CentOS-7 - Base          10,097
extras/7/x86_64            CentOS-7 - Extras        307
updates/7/x86_64           CentOS-7 - Updates       1,010
repolist: 21,433
[root@localhost ~]#
```

Procedimiento para sistemas operativos Rocky Linux 10, 9 o 8

Utilice este procedimiento si su sistema operativo es **Rocky Linux 10**, **Rocky Linux 9** o **Rocky Linux 8** para habilitar el acceso a los repositorios:

Pasos

1. Suscríbase a los repositorios requeridos:

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

2. Realice una `clean` operación:

```
dnf clean all
```

3. Verifique la lista de repositorios:

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 10 - AppStream
baseos                          Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 8 - AppStream
baseos                          Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

Descargue el paquete de instalación de ONTAP Mediator

Descargue el paquete de instalación de ONTAP Mediator e instálelo.

Pasos

1. Descargue el paquete de instalación de ONTAP Mediator desde la página de descarga de ONTAP Mediator.

   "Página de descarga de Mediador ONTAP"

2. Asegúrese de haber colocado el paquete de instalación de Mediator en el directorio de trabajo actual:

   ```
   [root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.11.0.tgz
   ```

   ```
   ontap-mediator-1.11.0.tgz
   ```

   Para las versiones 1,4 y anteriores de ONTAP Mediator, el instalador se denomina `ontap-mediator`.

   Si su sistema no tiene acceso a Internet, asegúrese de que el instalador pueda acceder a los paquetes necesarios.

3. Si es necesario, mueva el paquete de instalación de Mediator al directorio de instalación.
4. Descomprima el paquete del instalador:

   ```
   tar xvfz ontap-mediator-1.11.0.tgz
   ```

```
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
```

Verifique la firma del código del Mediador ONTAP

NetApp recomienda verificar la firma del código del mediador ONTAP antes de la instalación. Este paso es opcional.

Antes de empezar

Asegúrese de que su sistema cumple con estos requisitos antes de verificar la firma de código del mediador ONTAP .

- A partir del 15 de junio de 2025, no podrá instalar ni actualizar a ONTAP Mediator 1.9 ni 1.8 porque los certificados de verificación de firma de código han caducado. En su lugar, instale o actualice a ONTAP Mediator 1.11 o 1.10.
- Si el sistema no cumple con los siguientes requisitos, el proceso de verificación no es necesario y puede ir directamente a "Instale el paquete de instalación del Mediador ONTAP".

- versiones de openssl 1.0.2 a 3.0 para verificación básica
- la versión de openssl 1.1.0 o posterior para las operaciones de la Autoridad de fijación temporal (TSA)
- Acceso público a Internet para verificación OCSP

El paquete de descarga incluye los siguientes archivos:

Archivo	Descripción
`ONTAP-Mediator-production.pub`	Clave pública utilizada para verificar la firma
`csc-prod-chain-ONTAP-Mediator.pem`	La cadena de confianza de CA de certificación pública
`csc-prod-ONTAP-Mediator.pem`	El certificado utilizado para generar la clave
`ontap-mediator-1.11.0`	El ejecutable de instalación del producto para la versión 1.11

`ontap-mediator-1.11.0.sig`	El SHA-256 hash, luego RSA-firmado usando la clave csc-prod, firma para el instalador
`ontap-mediator-1.11.0.sig.tsr`	La solicitud de revocación para el uso por parte de OCSCP para la firma del instalador
`ontap-mediator-1.11.0.tsr`	Archivo de solicitud de firma de marca de hora
`tsa-prod-ONTAP-Mediator.pem`	El certificado público para la TSR
`tsa-prod-chain-ONTAP-Mediator.pem`	El certificado público CA Chain para la TSR

Pasos

1. Realice la comprobación de revocación `csc-prod-ONTAP-Mediator.pem` mediante el protocolo de estado de certificado en línea (OCSP).
   a. Localice la URL OCSP del certificado. Los certificados de desarrollador podrían no proporcionar un URI:

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. Genere una solicitud OCSP para el certificado.

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
   -reqout req.der
   ```

   c. Conéctese al administrador de OCSP para enviar la solicitud OCSP:

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
   ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
   chain-ONTAP-Mediator.pem
   ```

2. Verifique la cadena de confianza del CSC y las fechas de vencimiento con respecto al host local:

   `openssl verify`

   > `openssl`La versión de LA RUTA DE ACCESO debe tener un valor válido `cert.pem` (no autofirmado).

```
openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
Signature-Check certificate has expired or is invalid. Download a newer
version of the ONTAP Mediator.
openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
Stamp certificate has expired or is invalid. Download a newer version of
the ONTAP Mediator.
```

3. Verifique el `ontap-mediator-1.11.0.sig.tsr` y `ontap-mediator-1.11.0.tsr` archivos que utilizan los certificados asociados:

OpenSSL 3.x

```
openssl ts -verify -data ontap-mediator-1.11.0.sig -in ontap-mediator-
1.11.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-
prod-ONTAP-Mediator.pem
```

OpenSSL 1.x

```
openssl ts -verify -data ontap-mediator-1.11.0 -in ontap-mediator-
1.11.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```

`.tsr`Los archivos contienen la marca de tiempo de la respuesta asociada con el instalador y la firma del código. El procesamiento confirma que la marca de tiempo tiene una firma válida de la TSA y que su archivo de entrada no ha cambiado. Tu máquina realiza la verificación localmente. No necesitas acceder a los servidores de la TSA.

4. Verificar firmas con respecto a la clave:

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature
ontap-mediator-1.11.0.sig ontap-mediator-1.11.0
```

Instale el paquete de instalación del Mediador ONTAP

Para instalar ONTAP Mediator, debe obtener el paquete de instalación y ejecutar el instalador en el host.

Pasos

1. Ejecute el instalador y responda a las indicaciones según sea necesario:

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

Para omitir la comprobación de firma durante la instalación, utilice este comando: `./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y --skip-code -signature-check`

El instalador crea las cuentas necesarias e instala los paquetes requeridos. Si el Mediador ya está instalado, le solicitará que lo actualice.

Ejemplo de instalación de ONTAP Mediator (salida de la consola)

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.11.0.tgz
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
[root@mediator_host ~]#./ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
   WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
   Continue without code signature checking (only recommended if
integrity has been established manually)? yes/no: yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Would you like to use the default account names: netapp +
mediatoradmin? (Y(es)/n(o)): yes



Enter ONTAP Mediator user account (mediatoradmin) password:
```

```
Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.


+ Checking for default Linux firewall


+ Installing required packages.


Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025
01:28:32 AM EDT.
Package openssl-1:3.2.2-16.el10.x86_64 is already installed.
Package libselinux-utils-3.8-1.el10.x86_64 is already installed.
Package perl-Data-Dumper-2.189-512.el10.x86_64 is already installed.
Package bzip2-1.0.8-25.el10.x86_64 is already installed.
Package efibootmgr-18-8.el10.x86_64 is already installed.
Package mokutil-2:0.6.0-11.el10.x86_64 is already installed.
Package policycoreutils-python-utils-3.8-1.el10.noarch is already
installed.
Package python3-3.12.9-1.el10.x86_64 is already installed.
Dependencies resolved.
================================================================================
================================================================================
================================================================================
=========================
 Package
Architecture                                        Version
Repository                                              Size
================================================================================
================================================================================
================================================================================
=========================
Installing:
 elfutils-libelf-devel
x86_64                                              0.192-5.el10
```

```
AppStream                                              50 k
 gcc
x86_64                                          14.2.1-7.el10
AppStream                                              37 M
 kernel-devel
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                              22 M
 make
x86_64                                          1:4.4.1-9.el10
BaseOS                                                591 k
 openssl-devel
x86_64                                          1:3.2.2-16.el10
AppStream                                             3.9 M
 patch
x86_64                                          2.7.6-26.el10
AppStream                                             134 k
 perl-ExtUtils-MakeMaker
noarch                                          2:7.70-513.el10
AppStream                                              297 k
 python3-devel
x86_64                                          3.12.9-1.el10
AppStream
 334 k
 python3-pip
noarch                                          23.3.2-7.el10
AppStream                                             3.2 M
Installing dependencies:
 annobin-docs
noarch                                          12.92-1.el10
AppStream                                              94 k
 annobin-plugin-gcc
x86_64                                          12.92-1.el10
AppStream                                             985 k
 bison
x86_64                                          3.8.2-9.el10
AppStream                                             1.0 M
 cmake-filesystem
x86_64                                          3.30.5-2.el10
AppStream                                              29 k
 cpp
x86_64                                          14.2.1-7.el10
AppStream                                              12 M
 dwz
x86_64                                          0.15-7.el10
AppStream                                             139 k
 efi-srpm-macros
```

```
noarch                                          6-6.el10
AppStream                                          25 k
 flex
x86_64                                          2.6.4-19.el10
AppStream                                         303 k
 fonts-srpm-macros
noarch                                          1:2.0.5-18.el10
AppStream                                          29 k
 forge-srpm-macros
noarch                                          0.4.0-6.el10
AppStream                                          23 k
 gcc-plugin-annobin
x86_64                                          14.2.1-7.el10
AppStream                                          62 k
 glibc-devel
x86_64                                          2.39-37.el10
AppStream                                         641 k
 go-srpm-macros
noarch                                          3.6.0-4.el10
AppStream                                          29 k
 kernel-headers
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                         2.3 M
 kernel-srpm-macros
noarch                                          1.0-25.el10
AppStream                                          11 k
 libxcrypt-devel
x86_64                                          4.4.36-10.el10
AppStream                                          33 k
 libzstd-devel
x86_64                                          1.5.5-9.el10
AppStream
  53 k
 lua-srpm-macros
noarch                                          1-15.el10
AppStream                                          10 k
 m4
x86_64                                          1.4.19-11.el10
AppStream                                         309 k
 ocaml-srpm-macros
noarch                                          10-4.el10
AppStream                                          10 k
 openblas-srpm-macros
noarch                                          2-19.el10
AppStream                                         9.0 k
 package-notes-srpm-macros
```

```
noarch                                          0.5-13.el10
AppStream                                          11 k
 perl-AutoSplit
noarch                                          5.74-512.el10
AppStream                                          23 k
 perl-Benchmark
noarch                                          1.25-512.el10
AppStream                                          28 k
 perl-CPAN-Meta-Requirements
noarch                                          2.143-11.el10
AppStream                                          39 k
 perl-CPAN-Meta-YAML
noarch                                          0.018-512.el10
AppStream                                          29 k
 perl-Devel-PPPort
x86_64                                          3.72-512.el10
AppStream                                         223 k
 perl-ExtUtils-Command
noarch                                          2:7.70-513.el10
AppStream                                          16 k
 perl-ExtUtils-Constant
noarch                                          0.25-512.el10
AppStream                                          47 k
 perl-ExtUtils-Install
noarch                                          2.22-511.el10
AppStream                                          47 k
 perl-ExtUtils-Manifest
noarch                                          1:1.75-511.el10
AppStream                                          37 k
 perl-ExtUtils-ParseXS
noarch                                          1:3.51-512.el10
AppStream                                         190 k
 perl-File-Compare
noarch                                          1.100.800-512.el10
AppStream                                          15 k
 perl-File-Copy
noarch                                          2.41-512.el10
AppStream                                          22 k
 perl-I18N-Langinfo
x86_64                                          0.24-512.el10
AppStream                                          28 k
 perl-JSON-PP
noarch                                          1:4.16-512.el10
AppStream                                          69 k
 perl-Test-Harness
noarch                                          1:3.48-512.el10
```

```
AppStream                                          288 k
 perl-lib
x86_64                                          0.65-512.el10
AppStream                                           16 k
 perl-srpm-macros
noarch                                          1-57.el10
AppStream                                          9.7 k
 perl-version
x86_64                                          8:0.99.32-4.el10
AppStream                                           68 k
 pyproject-srpm-macros
noarch                                          1.16.2-1.el10
AppStream                                           16 k
 python-srpm-macros
noarch                                          3.12-9.1.el10
AppStream                                           26 k
 python3-pyparsing
noarch                                          3.1.1-7.el10
BaseOS                                             273 k
 qt6-srpm-macros
noarch                                          6.8.1-3.el10
AppStream
 11 k
 redhat-rpm-config
noarch                                          288-1.el10
AppStream                                           83 k
 rust-toolset-srpm-macros
noarch                                          1.84.1-1.el10
AppStream                                           13 k
 systemtap-sdt-devel
x86_64                                          5.2-2.el10
AppStream                                           78 k
 systemtap-sdt-dtrace
x86_64                                          5.2-2.el10
AppStream                                           72 k
 zlib-ng-compat-devel
x86_64                                          2.2.3-1.el10
AppStream                                           41 k
Installing weak dependencies:
 perl-CPAN-Meta
noarch                                          2.150010-511.el10
AppStream                                          202 k
 perl-Encode-Locale
noarch                                          1.05-31.el10
AppStream                                           21 k
 perl-Time-HiRes
```

```
x86_64                                                 4:1.9777-511.el10
AppStream                                                  62 k
 perl-devel
x86_64                                                 4:5.40.1-512.el10
AppStream                                                 772 k
 perl-doc
noarch                                                 5.40.1-512.el10
AppStream                                                 4.9 M

Transaction Summary
================================================================================
================================================================================
================================================================================
=========================
Install  63 Packages

Total size: 94 M
Installed size: 282 M
Downloading Packages:
BaseOS Packages Red Hat Enterprise Linux 10
439 kB/s | 3.7 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
 Userid     : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
  Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Installing       : perl-version-8:0.99.32-4.el10.x86_64
1/63
  Installing       : perl-File-Copy-2.41-512.el10.noarch
2/63
  Installing       : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
3/63
  Installing       : perl-Time-HiRes-4:1.9777-511.el10.x86_64
4/63
```

```
  Installing       : perl-JSON-PP-1:4.16-512.el10.noarch
5/63
  Installing       : perl-File-Compare-1.100.800-512.el10.noarch
6/63
  Installing       : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
  Installing       : m4-1.4.19-11.el10.x86_64
8/63
  Installing       : make-1:4.4.1-9.el10.x86_64
9/63
  Installing       : bison-3.8.2-9.el10.x86_64
10/63
  Installing       : flex-2.6.4-19.el10.x86_64
11/63
  Installing       : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
  Installing       : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
  Installing       : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
  Installing       : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
  Installing       : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
  Installing       : python3-pip-23.3.2-7.el10.noarch
17/63
  Installing       : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
  Installing       : perl-srpm-macros-1-57.el10.noarch
19/63
  Installing       : perl-lib-0.65-512.el10.x86_64
20/63
  Installing       : perl-doc-5.40.1-512.el10.noarch
21/63
  Installing       : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
  Installing       : perl-Encode-Locale-1.05-31.el10.noarch
23/63
  Installing       : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
  Installing       : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
  Installing       : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
  Installing       : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
```

```
  Installing       : perl-Benchmark-1.25-512.el10.noarch
28/63
  Installing       : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
  Installing       : perl-AutoSplit-5.74-512.el10.noarch
30/63
  Installing       : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
  Installing       : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
  Installing       : openblas-srpm-macros-2-19.el10.noarch
33/63
  Installing       : ocaml-srpm-macros-10-4.el10.noarch
34/63
  Installing       : lua-srpm-macros-1-15.el10.noarch
35/63
  Installing       : libzstd-devel-1.5.5-9.el10.x86_64
36/63
  Installing       : kernel-srpm-macros-1.0-25.el10.noarch
37/63
  Installing       : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
  Installing       : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
  Installing       : glibc-devel-2.39-37.el10.x86_64
40/63
  Installing       : efi-srpm-macros-6-6.el10.noarch
41/63
  Installing       : dwz-0.15-7.el10.x86_64
42/63
  Installing       : cpp-14.2.1-7.el10.x86_64
43/63
  Installing       : gcc-14.2.1-7.el10.x86_64
44/63
  Installing       : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
  Installing       : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
  Installing       : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
  Installing       : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
  Installing       : annobin-docs-12.92-1.el10.noarch
49/63
  Installing       : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
```

```
  Installing       : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/63
  Installing       : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
  Installing       : go-srpm-macros-3.6.0-4.el10.noarch
53/63
  Installing       : python-srpm-macros-3.12-9.1.el10.noarch
54/63
  Installing       : redhat-rpm-config-288-1.el10.noarch
55/63
  Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
  Installing       : python3-pyparsing-3.1.1-7.el10.noarch
56/63
  Installing       : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
  Installing       : perl-devel-4:5.40.1-512.el10.x86_64
58/63
  Installing       : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
  Installing       : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
  Installing       : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Installing       : python3-devel-3.12.9-1.el10.x86_64
62/63
  Installing       : patch-2.7.6-26.el10.x86_64
63/63
  Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch              annobin-plugin-gcc-
12.92-1.el10.x86_64            bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64           cpp-14.2.1-
7.el10.x86_64
  dwz-0.15-7.el10.x86_64                        efi-srpm-macros-6-
6.el10.noarch                  elfutils-libelf-devel-0.192-
5.el10.x86_64   flex-2.6.4-19.el10.x86_64                       fonts-
srpm-macros-1:2.0.5-18.el10.noarch
  forge-srpm-macros-0.4.0-6.el10.noarch         gcc-14.2.1-
7.el10.x86_64                          gcc-plugin-annobin-14.2.1-
7.el10.x86_64     glibc-devel-2.39-37.el10.x86_64               go-
```

```
srpm-macros-3.6.0-4.el10.noarch
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64        kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64           libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch              m4-1.4.19-
11.el10.x86_64                          make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch              openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64          package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch             perl-Benchmark-1.25-
512.el10.noarch
  perl-CPAN-Meta-2.150010-511.el10.noarch       perl-CPAN-Meta-
Requirements-2.143-11.el10.noarch  perl-CPAN-Meta-YAML-0.018-
512.el10.noarch   perl-Devel-PPPort-3.72-512.el10.x86_64          perl-
Encode-Locale-1.05-31.el10.noarch
  perl-ExtUtils-Command-2:7.70-513.el10.noarch  perl-ExtUtils-Constant-
0.25-512.el10.noarch       perl-ExtUtils-Install-2.22-511.el10.noarch
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch  perl-ExtUtils-Manifest-
1:1.75-511.el10.noarch
  perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch  perl-File-Compare-
1.100.800-512.el10.noarch       perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.x86_64         perl-JSON-PP-1:4.16-
512.el10.noarch
  perl-Test-Harness-1:3.48-512.el10.noarch      perl-Time-HiRes-
4:1.9777-511.el10.x86_64          perl-devel-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch                 perl-lib-0.65-
512.el10.x86_64
  perl-srpm-macros-1-57.el10.noarch             perl-version-8:0.99.32-
4.el10.x86_64              pyproject-srpm-macros-1.16.2-1.el10.noarch
python-srpm-macros-3.12-9.1.el10.noarch         python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch              python3-pyparsing-
3.1.1-7.el10.noarch             qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch             rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64         systemtap-sdt-dtrace-
5.2-2.el10.x86_64            zlib-ng-compat-devel-2.2.3-1.el10.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.vdizgQ/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20250715160240.log)
    This step takes several minutes. View progress in the log file.
    Sudoer config verified
```

```
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that a reboot is
needed.
     SCST does not start automatically when Secure Boot is enabled and
not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
root@mediator_host:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
 Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 28759 (python)
      Tasks: 1 (limit: 22990)
     Memory: 66.8M (peak: 68.8M)
        CPU: 2.865s
```

```
     CGroup: /system.slice/ontap_mediator.service
             └─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
15s ago
 Invocation: f1d3be6ca1f9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
     CGroup: /system.slice/mediator-scst.service
             └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#
```

Registre la clave de seguridad para el arranque seguro UEFI.

A partir de ONTAP Mediator 1.4, el mecanismo de arranque seguro está habilitado en los sistemas UEFI. Cuando el Arranque Seguro está habilitado, debe tomar pasos adicionales para registrar la clave de seguridad después de la instalación.

Pasos

1. Siga las instrucciones del archivo README para firmar el módulo del kernel SCST:

   ```
   /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
   signing
   ```

2. Localice las claves que desee:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

> Tras la instalación, la salida del sistema proporciona los archivos README y la ubicación de la clave.

3. Agregue la clave pública a la lista MOK:

```
mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

> Puedes dejar la clave privada en su ubicación predeterminada o moverla a una ubicación segura. Debes mantener la clave pública en su ubicación actual para que el Administrador de arranque pueda usarla. Para obtener más información, consulte el archivo README.module-signing:
>
> ```
> [root@hostname ~]# ls
> /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
> README.module-signing scst_module_key.der scst_module_key.priv
> ```

4. Reinicie el host y utilice el Administrador de arranque UEFI de su dispositivo para aprobar el nuevo MOK. Necesitarás la contraseña proporcionada para el `mokutil` utilidad en"Instale ONTAP Mediator cuando el inicio seguro de UEFI esté activado" .

Firma de módulos del kernel SCST

Tras instalar ONTAP Mediator, si systemctl status `mediator-scst` Si aparece como fallido (inactivo), siga estos pasos para firmar el módulo del kernel SCST.

Pasos

1. Durante el proceso de compilación se genera un par de claves pública/privada en el `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/` directorio, utilizando el siguiente comando:

```
[root@mediator-host ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
[root@mediator-host ~]#
```

2. Inicie el proceso de importación de la clave pública al repositorio de claves UEFI ejecutando los siguientes comandos:

```
[root@mediator-host ~]# mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
input password:
input password again:

[root@mediator-host ~]#
```

3. El software mokutil solicita una contraseña temporal para esta clave durante el proceso de importación.
4. Verifique si el proceso de importación ha comenzado con el `mokutil --list-new` y luego reinicie el sistema. El gestor de arranque inicia el administrador EFI MOK.
5. Utilice los menús en pantalla para activar la clave del módulo del kernel SCST. Tras el arranque, ejecute `systemctl status mediator-scst` . Una vez iniciado el servicio, se firman los módulos del kernel SCST.

Compruebe el estado de instalación de ONTAP Mediator

Después de instalar ONTAP Mediator, verifique que se esté ejecutando correctamente.

Pasos

1. Ver el estado del Mediador de ONTAP:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme los puertos que utiliza ONTAP Mediator:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp    0    0 0.0.0.0:31784    0.0.0.0:*       LISTEN

         tcp    0    0 0.0.0.0:3260     0.0.0.0:*       LISTEN

         tcp6   0    0 :::3260          :::*            LISTEN
```

Configuración posterior a la instalación de ONTAP Mediator

Una vez instalado y en funcionamiento ONTAP Mediator, se deben realizar tareas de configuración adicionales en el sistema de almacenamiento ONTAP para utilizar las funciones de ONTAP Mediator:

- Para utilizar ONTAP Mediator en una configuración IP de MetroCluster, consulte "Configurar ONTAP Mediator desde una configuración IP de MetroCluster" .
- Para utilizar la sincronización activa de SnapMirror, consulte "Instale ONTAP Mediator y confirme la configuración del clúster ONTAP".

Configurar las políticas de seguridad de ONTAP Mediator

ONTAP Mediator admite varias configuraciones de seguridad configurables. Los valores predeterminados para todas las configuraciones se proporcionan en un `low_space_threshold_mib: 10` archivo de sólo lectura:

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

Todos los valores colocados en el `ontap_mediator.user_config.yaml` sustituirán los valores predeterminados y se mantendrán en todas las actualizaciones de ONTAP Mediator.

Después de modificar `ontap_mediator.user_config.yaml` , reinicie ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Modificar los atributos de ONTAP Mediator

Los atributos de Mediador de ONTAP descritos en esta sección se pueden modificar si es necesario.

> No se deben cambiar otros valores por defecto en el `ontap_mediator.config.yaml` porque los valores modificados no se mantienen durante las actualizaciones de ONTAP Mediator.

Puede modificar los atributos de ONTAP Mediator copiando las variables necesarias en el `ontap_mediator.user_config.yaml` archivo para sustituir la configuración predeterminada.

Instale certificados SSL de terceros

Si necesita reemplazar los certificados autofirmados predeterminados por certificados SSL de terceros, modifique ciertos atributos en los siguientes archivos:

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

Las variables en estos archivos se utilizan para controlar los archivos de certificado utilizados por ONTAP Mediator.

ONTAP Mediator 1,9 y posteriores

Las variables predeterminadas que aparecen en la siguiente tabla se incluyen en el `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` archivo.

Variable	Ruta
`cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`
`ca_key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key`
`ca_serial_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl`
`cert_valid_days`	`1095`
`x509_passin_pwd`	`pass:ontap`

- `cert_valid_days` se utiliza para establecer la caducidad de los certificados de cliente. El valor máximo es de tres años (1095 días).
- `x509_passin_pwd` es la frase de acceso del certificado de cliente firmado.

Las variables predeterminadas que aparecen en la siguiente tabla se incluyen en el `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` archivo.

Variable	Ruta
`mediator_cert`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`mediator_key`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`

ONTAP Mediator 1,8 y anteriores

Las variables predeterminadas que aparecen en la siguiente tabla se incluyen en el `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` archivo.

Variable	Ruta
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days` se utiliza para establecer la caducidad de los certificados de cliente. El valor máximo es de tres años (1095 días).
- `x509_passin_pwd` es la frase de acceso del certificado de cliente firmado.

Las variables predeterminadas que aparecen en la siguiente tabla se incluyen en el `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` archivo.

Variable	Ruta
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

Si modifica estos atributos, reinicie ONTAP Mediator para aplicar los cambios. Para obtener instrucciones detalladas sobre cómo sustituir certificados predeterminados por certificados de terceros, consulte "Sustituya los certificados autofirmados por certificados de terceros de confianza".

Protección contra ataques con contraseña

Las siguientes configuraciones proporcionan protección contra ataques de adivinación de contraseñas de fuerza bruta.

Para activar la función, configure un valor para `window_seconds` y la `retry_limit`.

Ejemplos:

- Proporcione un intervalo de 5 minutos para las conjeturas y, a continuación, restablezca el recuento a cero fallos:

  ```
  authentication_lock_window_seconds: 300
  ```

- Bloquee la cuenta si se producen cinco fallos dentro del marco temporal de la ventana:

  ```
  authentication_retry_limit: 5
  ```

- Reduzca el impacto de los ataques de adivinación de contraseñas de fuerza bruta estableciendo un retraso que se produce antes de rechazar cada intento, lo que ralentiza los ataques.

  ```
  authentication_failure_delay_seconds: 5
  ```

  ```
  authentication_failure_delay_seconds: 0   # seconds (float) to delay
  failed auth attempts prior to response, 0 = no delay
  authentication_lock_window_seconds: null  # seconds (int) since the
  oldest failure before resetting the retry counter, null = no window
  authentication_retry_limit: null          # number of retries to allow
  before locking API access, null = unlimited
  ```

Reglas de complejidad de contraseñas

Los siguientes campos controlan las reglas de complejidad de la contraseña de la cuenta de usuario de la API de ONTAP Mediator.

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

Control del espacio libre

Existen ajustes que controlan el espacio libre necesario en el `/opt/netapp/lib/ontap_mediator` disco.

Si el espacio es inferior al umbral establecido, el servicio emitirá un evento de advertencia.

```
low_space_threshold_mib: 10
```

Control del espacio de registro de reserva

La RESERVA_LOG_SPACE se controla mediante valores específicos. De forma predeterminada, la instalación de ONTAP Mediator crea un espacio de disco independiente para los registros. El instalador crea un nuevo archivo de tamaño fijo con un total de 700 MB de espacio de disco para el registro de ONTAP Mediator.

Para desactivar esta función y utilizar el espacio en disco predeterminado, realice los siguientes pasos:

1. Cambie el valor de RESERVE_LOG_SPACE de 1 a 0 en el siguiente archivo:

   `/opt/netapp/lib/ontap_mediator/tools/mediator_env`

2. Reinicie Mediator:

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

      ```
      RESERVE_LOG_SPACE=0
      ```

   b. `systemctl restart ontap_mediator`

Para volver a habilitar la función, cambie el valor de 0 a 1 y reinicie Mediator.

> Al alternar entre espacios de disco no se depuran los logs existentes. Se realiza una copia de seguridad de todos los registros anteriores y, a continuación, se mueve al espacio de disco actual después de alternar y reiniciar Mediator.

Gestionar Mediador ONTAP

Administrar ONTAP Mediator, lo que incluye cambiar las credenciales de usuario, detener y volver a habilitar el servicio, verificar su estado e instalar o desinstalar SCST para el mantenimiento del host. También es posible gestionar certificados, como regenerar certificados autofirmados, reemplazarlos por certificados de terceros de confianza y solucionar problemas relacionados con los certificados.

Cambie el nombre de usuario

Puede cambiar el nombre de usuario mediante el siguiente procedimiento.

Acerca de esta tarea

Realice esta tarea en el host Linux donde instaló ONTAP Mediator.

Si no puede alcanzar este comando, puede que deba ejecutar el comando con la ruta completa como se muestra en el ejemplo siguiente:

`/usr/local/bin/mediator_username`

Pasos

Cambie el nombre de usuario eligiendo una de las siguientes opciones:

- **Opción (A)**: Ejecute el comando `mediator_change_user` y responda a las indicaciones como se muestra en el siguiente ejemplo:

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- **Opción (b)**: Ejecuta el siguiente comando:

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

Cambie la contraseña

Puede cambiar la contraseña mediante el siguiente procedimiento.

Acerca de esta tarea

Realice esta tarea en el host Linux donde instaló ONTAP Mediator.

Si no puede alcanzar este comando, puede que deba ejecutar el comando con la ruta completa como se muestra en el ejemplo siguiente:

```
/usr/local/bin/mediator_change_password
```

Pasos

Cambie la contraseña eligiendo una de las siguientes opciones:

- **Opción (A)**: Ejecute `mediator_change_password` el comando y responda a las indicaciones como se muestra en el siguiente ejemplo:

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
              Old Password:
              New Password:
          Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- **Opción (b)**: Ejecuta el siguiente comando:

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

El ejemplo muestra que la contraseña se cambia de “mediator1” a “mediator2”.

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
The password has been updated successfully.
[root@mediator-host ~]#
```

Detener el mediador de ONTAP

Para detener ONTAP Mediator, realice los siguientes pasos:

Pasos

1. Detener el mediador de ONTAP:

```
systemctl stop ontap_mediator
```

2. Detener SCST:

```
systemctl stop mediator-scst
```

3. Deshabilitar ONTAP Mediator y SCST:

```
systemctl disable ontap_mediator mediator-scst
```

Volver a habilitar el mediador de ONTAP

Para volver a habilitar ONTAP Mediator, realice los siguientes pasos:

Pasos

1. Habilitar ONTAP Mediator y SCST:

```
systemctl enable ontap_mediator mediator-scst
```

2. Iniciar SCST:

```
systemctl start mediator-scst
```

3. Iniciar Mediador ONTAP:

```
systemctl start ontap_mediator
```

Verificar que ONTAP Mediator esté en buen estado

Después de instalar ONTAP Mediator, verifique que se esté ejecutando correctamente.

Pasos

1. Ver el estado del Mediador de ONTAP:
   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. Confirme los puertos que utiliza ONTAP Mediator:

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

Desinstalar ONTAP Mediator

Si es necesario, puede eliminar ONTAP Mediator.

Antes de empezar

Debe desconectar ONTAP Mediator de ONTAP antes de eliminarlo.

Acerca de esta tarea

Realice esta tarea en el host Linux donde instaló ONTAP Mediator.

Si no puede alcanzar este comando, puede que deba ejecutar el comando con la ruta completa como se muestra en el ejemplo siguiente:

`/usr/local/bin/uninstall_ontap_mediator`

Paso

1. Desinstalar ONTAP Mediator:

   `uninstall_ontap_mediator`

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

Vuelva a generar un certificado autofirmado temporal

A partir de ONTAP Mediator 1,7, puede regenerar un certificado autofirmado temporal mediante el siguiente procedimiento.

Este procedimiento solo se admite en sistemas que ejecuten ONTAP Mediator 1,7 o posterior.

Acerca de esta tarea

- Realice esta tarea en el host Linux donde instaló ONTAP Mediator.
- Puede realizar esta tarea solo si los certificados autofirmados generados quedaron obsoletos debido a cambios en el nombre de host o la dirección IP del host después de instalar ONTAP Mediator.
- Una vez que el certificado autofirmado temporal ha sido reemplazado por un certificado de terceros de confianza, *NOT* use esta tarea para regenerar un certificado. La ausencia de un certificado autofirmado provocará que falle este procedimiento.

Paso

Para regenerar un nuevo certificado autofirmado temporal para el host actual, realice el siguiente paso:

1. Reiniciar ONTAP Mediator:

   ```
   ./make_self_signed_certs.sh overwrite
   ```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

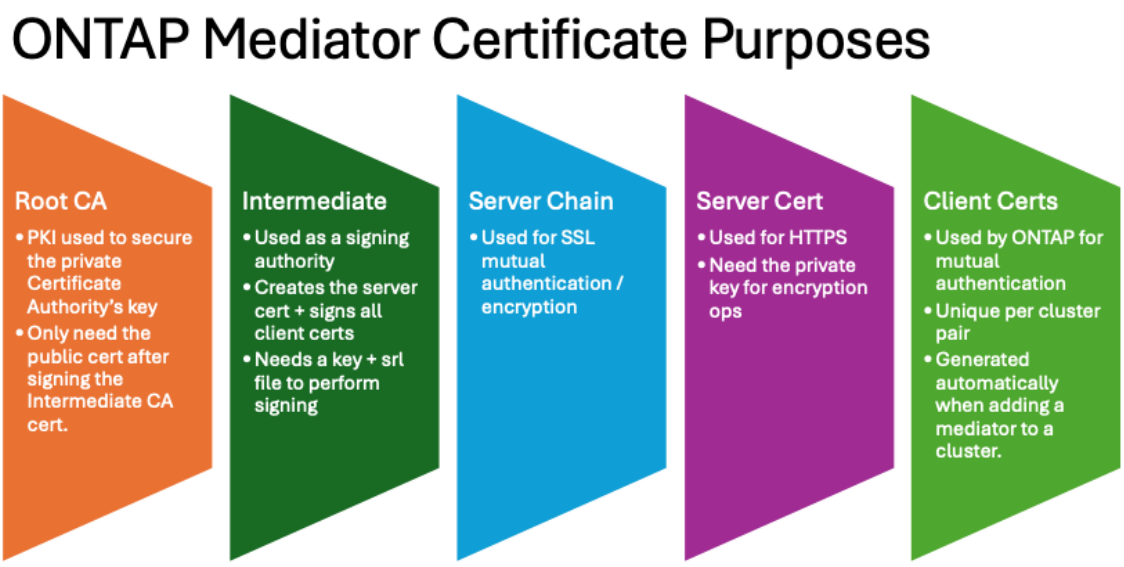
Sustituya los certificados autofirmados por certificados de terceros de confianza

Si es compatible, puede reemplazar los certificados autofirmados por certificados de terceros de confianza.

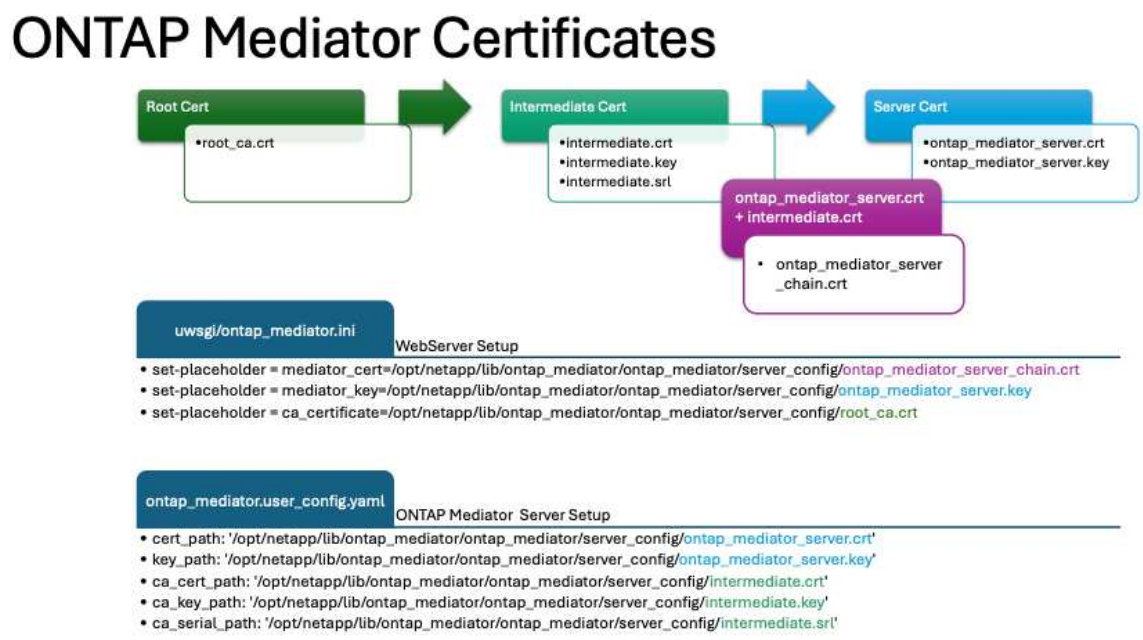
- Los certificados de terceros solo se admiten a partir de ONTAP 9.16,1 y en algunas versiones de parches anteriores de ONTAP. Consulte "ID de error de NetApp Bugs Online CONTAP-243278".
- Los certificados de terceros solo son compatibles con los sistemas que ejecutan ONTAP Mediator 1,7 o posterior.

Acerca de esta tarea

- Realice esta tarea en el host Linux donde instaló ONTAP Mediator.
- Puede realizar esta tarea si los certificados autofirmados generados deben ser reemplazados por certificados obtenidos de una entidad de certificación (CA) subordinada de confianza. Para lograr esto, debe tener acceso a una autoridad de infraestructura de clave pública (PKI) de confianza.
- La siguiente imagen muestra las finalidades de cada certificado ONTAP Mediator.



- La siguiente imagen muestra la configuración del servidor web y de ONTAP Mediator.



Paso 1: Obtenga un certificado de un tercero que emita un certificado de CA

Puede obtener un certificado de una autoridad de PKI mediante el siguiente procedimiento.

El siguiente ejemplo demuestra la sustitución de los actores de certificados autofirmados por los actores de certificados de terceros ubicados en

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`.

> El ejemplo ilustra los criterios necesarios para los certificados requeridos para ONTAP Mediator. Puede obtener los certificados de una autoridad PKI de una manera que pueda ser diferente a este procedimiento. Ajuste el procedimiento de acuerdo a su necesidad de negocio.

ONTAP Mediator 1,9 y posteriores

1. Cree una clave privada `intermediate.key` y un archivo de configuración `openssl_ca.cnf` que consumirá la autoridad PKI para generar un certificado.

   a. Generar la clave privada `intermediate.key` :

      ejemplo

```
openssl genrsa -aes256 -out intermediate.key 4096
```

   a. El archivo de configuración `openssl_ca.cnf` (ubicado en `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) define las propiedades que debe tener el certificado generado.

2. Utilice la clave privada y el archivo de configuración para crear una solicitud de firma de certificado `intermediate.csr`:

   Ejemplo:

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key intermediate.key
-new -config openssl_ca.cnf -out intermediate.csr
Enter pass phrase for intermediate.key:
[root@scs000216655 server_config]# cat intermediate.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. Envíe la solicitud de firma de certificado `intermediate.csr` a una autoridad de PKI para su firma.

   La autoridad PKI verifica la solicitud y firma la `.csr` , generando el certificado `intermediate.crt` . Además, es necesario obtener la `root_ca.crt` certificado que firmó el `intermediate.crt` certificado de la autoridad PKI.

   Para los clústeres de SnapMirror Business Continuity (SM-BC), debe agregar el `intermediate.crt` y `root_ca.crt` certificados a un clúster ONTAP .
   Ver"Configurar ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror" .

ONTAP Mediator 1,8 y anteriores

1. Cree una clave privada `ca.key` y un archivo de configuración `openssl_ca.cnf` que consumirá la autoridad PKI para generar un certificado.

   a. Generar la clave privada `ca.key` :

      ejemplo

```
openssl genrsa -aes256 -out ca.key 4096
```

a. El archivo de configuración `openssl_ca.cnf` (ubicado en `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`) define las propiedades que debe tener el certificado generado.

2. Utilice la clave privada y el archivo de configuración para crear una solicitud de firma de certificado `ca.csr`:

Ejemplo:

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key ca.key -new
-config openssl_ca.cnf -out ca.csr
Enter pass phrase for ca.key:
[root@scs000216655 server_config]# cat ca.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. Envíe la solicitud de firma de certificado `ca.csr` a una autoridad de PKI para su firma.

La autoridad de PKI verifica la solicitud y firma la , generando el `.csr`certificado `ca.crt`. Además, debe obtener `root_ca.crt that signed the `ca.crt` el certificado de la autoridad PKI.

> Para los clústeres de continuidad del negocio de SnapMirror (SM-BC), es necesario añadir `ca.crt` los certificados y `root_ca.crt` a un clúster de ONTAP. Consulte "Configurar ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror".

Paso 2: Genere un certificado de servidor firmando con una certificación de CA de terceros

ONTAP Mediator 1,9 y posteriores

Un certificado de servidor debe estar firmado por la clave privada `intermediate.key` y el certificado de terceros `intermediate.crt` . Además, el archivo de configuración `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contiene ciertos atributos que especifican las propiedades necesarias para los certificados de servidor emitidos por OpenSSL.

Los siguientes comandos pueden generar un certificado de servidor.

Pasos

1. Para generar una solicitud de firma de certificación (CSR) del servidor, ejecute el siguiente comando en `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` la carpeta:

   ```
   openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
   rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
   ontap_mediator_server.csr
   ```

2. Para generar un certificado de servidor a partir de la CSR, ejecute el siguiente comando desde el `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` carpeta:

   > Estos archivos se obtuvieron de una autoridad PKI. Si utiliza un nombre de certificado diferente, sustituya `intermediate.crt` y `intermediate.key` por los nombres de archivo correspondientes.

   ```
   openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA
   intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095
   -req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
   ```

   - La `-CAcreateserial` opción se utiliza para generar `intermediate.srl` los archivos.

ONTAP Mediator 1,8 y anteriores

Un certificado de servidor debe estar firmado por la clave privada `ca.key` y el certificado de terceros `ca.crt` . Además, el archivo de configuración `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf` contiene ciertos atributos que especifican las propiedades necesarias para los certificados de servidor emitidos por OpenSSL.

Los siguientes comandos pueden generar un certificado de servidor.

Pasos

1. Para generar una solicitud de firma de certificación (CSR) del servidor, ejecute el siguiente comando en `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` la carpeta:

   ```
   openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
   rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
   ontap_mediator_server.csr
   ```

2. Para generar un certificado de servidor a partir de la CSR, ejecute el siguiente comando desde el `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` carpeta:

Estos archivos se obtuvieron de una autoridad PKI. Si utiliza un nombre de certificado diferente, sustituya `ca.crt` y `ca.key` por los nombres de archivo correspondientes.

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- La `-CAcreateserial` opción se utiliza para generar `ca.srl` los archivos.

Paso 3: Reemplace el nuevo certificado de CA de terceros y el certificado de servidor en la configuración de ONTAP Mediator

ONTAP Mediator 1.10 y posteriores

La configuración del certificado se suministra a ONTAP Mediator en el archivo de configuración ubicado en `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . El archivo incluye los siguientes atributos:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` y `key_path` son variables de certificado de servidor.
- `ca_cert_path`, `ca_key_path`, Y `ca_serial_path` son variables de certificado CA.

Pasos

1. Reemplace todos `intermediate.*` los archivos con los certificados de terceros.
2. Cree una cadena de certificados desde los `intermediate.crt` certificados y `ontap_mediator_server.crt` :

   ```
   cat ontap_mediator_server.crt intermediate.crt >
   ontap_mediator_server_chain.crt
   ```

3. Actualizar el `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` archivo.

   Actualizar los valores de `ssl_keyfile` , `ssl_certfile` , y `ssl_ca_certs` :

   ```
   ssl_keyfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key

   ssl_certfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt

   ssl_ca_certs:
   ```

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt`

- El `ssl_keyfile` El valor es la ruta clave en el `ontap_mediator_server.crt` archivo, que es `ontap_mediator_server.key` .
- El `ssl_certfile` El valor es el camino de la `ontap_mediator_server_chain.crt` archivo.
- El `ssl_ca_certs` El valor es el camino de la `root_ca.crt` archivo.

4. Compruebe que los siguientes atributos de los certificados recién generados se han definido correctamente:
   - Propietario del Grupo Linux: `netapp:netapp`
   - Permisos de Linux: `600`
5. Reiniciar ONTAP Mediator:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.9.1 y 1.9

La configuración del certificado se suministra a ONTAP Mediator en el archivo de configuración ubicado en `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . El archivo incluye los siguientes atributos:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` y `key_path` son variables de certificado de servidor.
- `ca_cert_path`, `ca_key_path`, Y `ca_serial_path` son variables de certificado CA.

Pasos

1. Reemplace todos `intermediate.*` los archivos con los certificados de terceros.
2. Cree una cadena de certificados desde los `intermediate.crt` certificados y `ontap_mediator_server.crt` :

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. Actualice `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` el archivo.

   Actualizar los valores de `mediator_cert`, `mediator_key`y `ca_certificate`:

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - `mediator_cert`El valor es la ruta del `ontap_mediator_server_chain.crt` archivo.
   - `mediator_key value`Es la ruta de acceso clave del `ontap_mediator_server.crt` archivo, que es `ontap_mediator_server.key`.
   - `ca_certificate`El valor es la ruta del `root_ca.crt` archivo.

4. Compruebe que los siguientes atributos de los certificados recién generados se han definido correctamente:
   - Propietario del Grupo Linux: `netapp:netapp`
   - Permisos de Linux: `600`

5. Reiniciar ONTAP Mediator:

   ```
   systemctl restart ontap_mediator
   ```

ONTAP Mediator 1,8 y anteriores

La configuración del certificado se suministra a ONTAP Mediator en el archivo de configuración ubicado en `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` . El archivo incluye los siguientes atributos:

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- `cert_path` y `key_path` son variables de certificado de servidor.
- `ca_cert_path`, `ca_key_path`, Y `ca_serial_path` son variables de certificado CA.

Pasos

1. Reemplace todos `ca.*` los archivos con los certificados de terceros.
2. Cree una cadena de certificados desde los `ca.crt` certificados y `ontap_mediator_server.crt` :

   ```
   cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
   ```

3. Actualice `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` el archivo.

   Actualizar los valores de `mediator_cert`, `mediator_key`y `ca_certificate`:

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - `mediator_cert`El valor es la ruta del `ontap_mediator_server_chain.crt` archivo.
   - `mediator_key value`Es la ruta de acceso clave del `ontap_mediator_server.crt` archivo, que es `ontap_mediator_server.key`.
   - `ca_certificate`El valor es la ruta del `root_ca.crt` archivo.
4. Compruebe que los siguientes atributos de los certificados recién generados se han definido correctamente:
   - Propietario del Grupo Linux: `netapp:netapp`

- Permisos de Linux: `600`

5. Reiniciar ONTAP Mediator:

```
systemctl restart ontap_mediator
```

Paso 4: Opcionalmente, utilice una ruta o un nombre diferente para sus certificados de terceros

ONTAP Mediator 1.10 y posteriores

Puede utilizar certificados de terceros con un nombre diferente `intermediate.*` o almacenar los certificados de terceros en una ubicación diferente.

Pasos

1. Configure el `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` archivo para sustituir los valores de variables por defecto en el `ontap_mediator.config.yaml` archivo.

   Si ha obtenido `intermediate.crt` de una autoridad PKI y almacena su clave privada `intermediate.key` en la ubicación `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, el `ontap_mediator.user_config.yaml` archivo debe tener el siguiente ejemplo:

   > Si utilizó `intermediate.crt` para firmar el `ontap_mediator_server.crt` certificado, `intermediate.srl` se genera el archivo. Consulte Paso 2: Genere un certificado de servidor firmando con una certificación de CA de terceros para obtener más información.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. Si está utilizando una estructura de certificado donde `root_ca.crt` El certificado proporciona una `intermediate.crt` certificado que firma el `ontap_mediator_server.crt` certificado, crear una cadena de certificados a partir de `intermediate.crt` y `ontap_mediator_server.crt` certificados:

> Debe haber obtenido los `intermediate.crt` certificados y `ontap_mediator_server.crt` de una autoridad PKI anteriormente en el procedimiento.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. Actualizar el `/opt/netapp/lib/ontap_mediator/uvicorn/config.json` archivo.

   Actualizar los valores de `ssl_keyfile` , `ssl_certfile` , y `ssl_ca_certs` :

   ```
   ssl_keyfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
   or_server.key

   ssl_certfile:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
   or_server_chain.crt

   ssl_ca_certs:
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - El `ssl_keyfile` El valor es la ruta clave en el `ontap_mediator_server.crt` archivo, que es `ontap_mediator_server.key` .
   - El `ssl_certfile` El valor es el camino de la `ontap_mediator_server_chain.crt` archivo.
   - El `ssl_ca_certs` El valor es el camino de la `root_ca.crt` archivo.

   > Para los clústeres de SnapMirror Business Continuity (SM-BC), debe agregar el `intermediate.crt` y `root_ca.crt` certificados a un clúster ONTAP . Ver"Configurar ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror" .

c. Compruebe que los siguientes atributos de los certificados recién generados se han definido correctamente:

   - Propietario del Grupo Linux: `netapp:netapp`
   - Permisos de Linux: `600`

2. Reinicie ONTAP Mediator cuando los certificados se actualicen en el archivo de configuración:

   ```
   systemctl restart ontap_mediator
   ```

ONTAP Mediator 1.9.1 y 1.9

Puede utilizar certificados de terceros con un nombre diferente `intermediate.*` o almacenar los certificados de terceros en una ubicación diferente.

Pasos

1. Configure el `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` archivo para sustituir los valores de variables por defecto en el `ontap_mediator.config.yaml` archivo.

   Si ha obtenido `intermediate.crt` de una autoridad PKI y almacena su clave privada `intermediate.key` en la ubicación `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, el `ontap_mediator.user_config.yaml` archivo debe tener el siguiente ejemplo:

Si utilizó `intermediate.crt` para firmar el `ontap_mediator_server.crt` certificado, `intermediate.srl` se genera el archivo. Consulte Paso 2: Genere un certificado de servidor firmando con una certificación de CA de terceros para obtener más información.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. Si está utilizando una estructura de certificado donde `root_ca.crt` El certificado proporciona una `intermediate.crt` certificado que firma el `ontap_mediator_server.crt` certificado, crear una cadena de certificados a partir de `intermediate.crt` y `ontap_mediator_server.crt` certificados:

Debe haber obtenido los `intermediate.crt` certificados y `ontap_mediator_server.crt` de una autoridad PKI anteriormente en el procedimiento.

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. Actualice `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` el archivo.

Actualizar los valores de `mediator_cert`, `mediator_key`y `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`El valor es la ruta del `ontap_mediator_server_chain.crt` archivo.
- `mediator_key`El valor es la ruta de acceso clave del `ontap_mediator_server.crt` archivo, que es `ontap_mediator_server.key`.
- `ca_certificate`El valor es la ruta del `root_ca.crt` archivo.

Para los clústeres de SnapMirror Business Continuity (SM-BC), debe agregar el `intermediate.crt` y `root_ca.crt` certificados a un clúster ONTAP . Ver"Configurar ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror" .

c. Compruebe que los siguientes atributos de los certificados recién generados se han definido correctamente:

- Propietario del Grupo Linux: `netapp:netapp`
- Permisos de Linux: `600`

2. Reinicie ONTAP Mediator cuando los certificados se actualicen en el archivo de configuración:

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1,8 y anteriores

Puede utilizar certificados de terceros con un nombre diferente `ca.*` o almacenar los certificados de terceros en una ubicación diferente.

Pasos

1. Configure el `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.`

`user_config.yaml` archivo para sustituir los valores de variables por defecto en el `ontap_mediator.config.yaml` archivo.

Si ha obtenido `ca.crt` de una autoridad PKI y almacena su clave privada `ca.key` en la ubicación `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`, el `ontap_mediator.user_config.yaml` archivo debe tener el siguiente ejemplo:

> Si utilizó `ca.crt` para firmar el `ontap_mediator_server.crt` certificado, `ca.srl` se genera el archivo. Consulte Paso 2: Genere un certificado de servidor firmando con una certificación de CA de terceros para obtener más información.

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

a. Si está utilizando una estructura de certificados donde el `root_ca.crt` certificado proporciona un `ca.crt` certificado que firma el `ontap_mediator_server.crt` certificado, cree una cadena de certificados a partir de los `ca.crt` certificados y. `ontap_mediator_server.crt`

Debe haber obtenido los `ca.crt` certificados y `ontap_mediator_server.crt` de una autoridad PKI anteriormente en el procedimiento.

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

b. Actualice `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` el archivo.

Actualizar los valores de `mediator_cert`, `mediator_key`y `ca_certificate`:

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`El valor es la ruta del `ontap_mediator_server_chain.crt` archivo.
- `mediator_key`El valor es la ruta de acceso clave del `ontap_mediator_server.crt` archivo, que es `ontap_mediator_server.key`.
- `ca_certificate`El valor es la ruta del `root_ca.crt` archivo.

Para los clústeres de continuidad del negocio de SnapMirror (SM-BC), es necesario añadir `ca.crt` los certificados y `root_ca.crt` a un clúster de ONTAP. Consulte "Configurar ONTAP Mediator y los clústeres para la sincronización activa de SnapMirror".

c. Compruebe que los siguientes atributos de los certificados recién generados se han definido correctamente:

- Propietario del Grupo Linux: `netapp:netapp`
- Permisos de Linux: `600`

2. Reinicie ONTAP Mediator cuando los certificados se actualicen en el archivo de configuración:

```
systemctl restart ontap_mediator
```

Solucionar problemas relacionados con los certificados

Puede comprobar ciertas propiedades de los certificados.

Verifique el vencimiento del certificado

Utilice el siguiente comando para identificar el rango de validez del certificado.

ONTAP Mediator 1,9 y posteriores

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP Mediator 1,8 y anteriores

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

Verifique las extensiones X509v3 en la certificación CA

Utilice el siguiente comando para verificar las extensiones X509v3 en la certificación CA.

ONTAP Mediator 1,9 y posteriores

Las propiedades definidas en **v3_ca** en `openssl_ca.cnf` se muestran como `X509v3 extensions` en `intermediate.crt`.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAP Mediator 1,8 y anteriores

Las propiedades definidas en **v3_ca** en `openssl_ca.cnf` se muestran como `X509v3 extensions` en `ca.crt`.

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

Verifique las extensiones X509v3 en el certificado del servidor y los nombres alternativos del asunto

`v3_req`Las propiedades definidas en `openssl_server.cnf` el archivo de configuración se muestran como `X509v3 extensions` en el certificado.

En el siguiente ejemplo, puedes obtener las variables en el `alt_names` secciones ejecutando los comandos `hostname -A` y `hostname -I` en la máquina virtual Linux en la que está instalado ONTAP Mediator.

Consulte con el administrador de red los valores correctos de las variables.

ONTAP Mediator 1,9 y posteriores

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP Mediator 1,8 y anteriores

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

Verifique que una clave privada coincida con un certificado

Puede verificar si una clave privada concreta coincide con un certificado.

Utilice los siguientes comandos OpenSSL en la clave y el certificado respectivamente.

ONTAP Mediator 1,9 y posteriores

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP Mediator 1,8 y anteriores

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

Si el `-modulus` atributo para ambos coincide, indica que la clave privada y el par de certificados son compatibles y pueden trabajar entre sí.

Compruebe que un certificado de servidor se crea a partir de un certificado de CA particular

Puede utilizar el siguiente comando para verificar que el certificado de servidor se cree a partir de un certificado de CA particular.

ONTAP Mediator 1,9 y posteriores

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt
--untrusted intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
[root@mediator_host server_config]#
```

ONTAP Mediator 1,8 y anteriores

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

Si se está utilizando la validación del protocolo de estado de certificado en línea (OCSP), utilice el comando "openssl-verify".

Mantenga el SO del host para ONTAP Mediator

Asegúrese de que el sistema operativo host para ONTAP Mediator reciba mantenimiento regular para lograr un rendimiento óptimo.

Reinicie el host

Reinicie el host solo cuando los clústeres estén en buen estado. Los clústeres no pueden responder a fallas mientras ONTAP Mediator está fuera de línea. Programa un horario para el mantenimiento antes de reiniciar.

ONTAP Mediator se reanuda automáticamente durante un reinicio y vuelve a ingresar a las relaciones configuradas previamente con los clústeres de ONTAP .

Actualizaciones del paquete de host

Actualice cualquier biblioteca o paquete yum excepto el kernel. Reinicie el host si es necesario para que los cambios surtan efecto. Programe una ventana de servicio antes de reiniciar el host.

Si instala `yum-utils` el paquete, utilice el `needs-restarting` comando para detectar si algún cambio de paquete requiere un reinicio.

Reinicie después de actualizar las dependencias de ONTAP Mediator porque los cambios no tienen efecto inmediato.

Actualizar el kernel del sistema operativo anfitrión

SCST debe compilarse para el kernel que esté utilizando. Para actualizar el sistema operativo, es necesario programar un tiempo para el mantenimiento.

Pasos

Siga estos pasos para actualizar el kernel del sistema operativo host.

> Antes de actualizar el kernel, verifique que el sistema operativo y la versión de ONTAP Mediator sean compatibles. Para conocer las versiones compatibles, consulte la"Matriz de compatibilidad de SO" .

1. Detener el mediador de ONTAP.
2. Desinstale el paquete SCST, consulteRealizar mantenimiento del host . (SCST no proporciona un mecanismo de actualización).
3. Actualice el sistema operativo y reinicie.
4. Vuelva a instalar el paquete SCST.
5. Vuelva a habilitar ONTAP Mediator.

Realizar mantenimiento del host

Actualizar el kernel de la máquina virtual puede causar problemas de compatibilidad con los módulos SCST. Desinstale y vuelva a instalar SCST manualmente.

Paso 1: Desinstalar SCST

Para desinstalar SCST, utilice el paquete tar correspondiente a su versión de ONTAP Mediator.

Pasos

1. Descargue el paquete SCST apropiado (como se muestra en la siguiente tabla) y extráigalo.

Para esta versión…	Usar este paquete tar…
Mediador ONTAP 1.11	scst-3.9.tar.gz
Mediador ONTAP 1.10	scst-3.9.tar.gz
Mediador ONTAP 1.9.1	scst-3,8.0.tar.bz2
Mediador ONTAP 1,9	scst-3,8.0.tar.bz2
Mediador ONTAP 1,8	scst-3,8.0.tar.bz2
Mediador ONTAP 1,7	scst-3,7.0.tar.bz2
Mediador ONTAP 1,6	scst-3,7.0.tar.bz2
Mediador ONTAP 1,5	scst-3,6.0.tar.bz2
Mediador ONTAP 1,4	scst-3,6.0.tar.bz2
Mediador ONTAP 1,3	scst-3,5.0.tar.bz2
Mediador ONTAP 1,1	scst-3,4.0.tar.bz2
Mediador ONTAP 1,0	scst-3,3.0.tar.bz2

   a. Acceda al paquete de código abierto desde"Descargas de sourceforge de SCST" .
   b. Seleccione **Descargar versiones lanzadas**.
   c. Extraiga el paquete a su máquina virtual.

2. Ejecute los siguientes comandos de desinstalación en el `scst` directorio:
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

Paso 2: Instalar SCST

Para instalar SCST manualmente, necesita el paquete tar de SCST que se utiliza para la versión instalada de ONTAP Mediator (consulte laTabla SCST).

Realice este paso antes de instalar ONTAP Mediator. Si la versión de SCST que está utilizando es más nueva que la versión incluida con el instalador de ONTAP Mediator, el instalador omite este paso.

1. Ejecute los siguientes comandos de instalación en el `scst` directorio:
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`

      Si está realizando una instalación por primera vez y desea preinstalar ONTAP Mediator, ejecute el siguiente comando antes de continuar con el siguiente paso:

      ```
      mkdir -p
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
      ```

   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
   h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

      Si preinstala SCST antes de ONTAP Mediator durante una primera instalación, omita este paso. El instalador aplica los parches SCST relevantes.

2. Opcionalmente, si Secure Boot está activado, antes de reiniciar, realice los siguientes pasos:
   a. Determinar cada nombre de archivo para el `scst_vdisk` , `scst` , y `iscsi_scst` módulos:

      ```
      [root@localhost ~]# modinfo -n scst_vdisk
      [root@localhost ~]# modinfo -n scst
      [root@localhost ~]# modinfo -n iscsi_scst
      ```

   b. Determine la versión del kernel:

      ```
      [root@localhost ~]# uname -r
      ```

   c. Firme cada archivo de módulo con el kernel:

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

d. Instale la clave UEFI con el firmware.

Las instrucciones para instalar la clave UEFI se encuentran en:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

La clave UEFI generada se encuentra en:

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. Reiniciar el sistema:

```
reboot
```

El host cambia al nombre de host o IP

Acerca de esta tarea

- Realice esta tarea en el host Linux donde instaló ONTAP Mediator.
- Haga esto solo si los certificados autofirmados ya no son válidos porque el nombre de host o la dirección IP cambian después de instalar ONTAP Mediator.
- Una vez que el certificado autofirmado temporal haya sido reemplazado por un certificado de terceros confiable, *no* utilice esta tarea para regenerar un certificado. Si no tiene un certificado autofirmado, no puede utilizar este procedimiento.

Paso

Cree un certificado autofirmado temporal para el host actual:

1. Reiniciar ONTAP Mediator:

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

Obtenga más información sobre la administración de sitios IP de MetroCluster con ONTAP System Manager

Las configuraciones de MetroCluster reflejan de forma síncrona los datos y la configuración entre dos clústeres de ONTAP en ubicaciones separadas. A partir de ONTAP 9.8, puede usar System Manager como una interfaz simplificada para gestionar una configuración de IP de MetroCluster.

> Solo puede ejecutar operaciones de MetroCluster mediante System Manager en una configuración de IP de MetroCluster. En una configuración FC de MetroCluster, puede seguir usando System Manager para gestionar cada nodo de la configuración de MetroCluster, pero no se puede ejecutar ninguna operación específica de MetroCluster.

Normalmente, debe instalar y configurar clústeres en una configuración de MetroCluster en dos sitios geográficos diferentes. A continuación, debe configurar entre iguales entre los clústeres de modo que se sincronicen y compartan los datos. Los dos clústeres de la red de conexión entre iguales proporcionan

recuperación ante desastres bidireccional, donde cada clúster puede ser el origen y el backup del otro clúster. En configuraciones IP de MetroCluster de ocho o cuatro nodos, cada sitio consta de controladoras de almacenamiento configuradas como uno o dos pares de alta disponibilidad (HA).

Puede "instalar ONTAP Mediator" en una tercera ubicación para supervisar el estado de los nodos y sus partners de recuperación ante desastres. ONTAP Mediator puede implementar una conmutación no planificada asistida por mediador (MAUSO) en caso de desastre.

También puede realizar una conmutación de sitios negociada para restablecer uno de los clústeres para el mantenimiento planificado. El clúster de partners se encarga de todas las operaciones de I/O de datos para ambos clústeres hasta que se abre el clúster en el que realizó el mantenimiento y se ejecuta una operación de conmutación de estado.

Encontrará procedimientos para configurar y gestionar una configuración de IP de MetroCluster mediante System Manager en "Documentación de MetroCluster".

Protección de datos mediante backup en cinta

Obtenga información sobre la copia de seguridad en cinta de los volúmenes ONTAP FlexVol

ONTAP es compatible con los procesos de backup y restauración a cinta mediante el protocolo de gestión de datos de red (NDMP). NDMP le permite realizar backups de datos en sistemas de almacenamiento directamente en cinta, lo cual resulta en un uso más eficiente del ancho de banda de la red. ONTAP es compatible con los motores de volcado y SMTape para backups a cinta.

Puede realizar backups o restauraciones de volcado o SMTape mediante aplicaciones de backup compatibles con NDMP. Solo se admite la versión 4 de NDMP.

Copia de seguridad en cinta mediante volcado

Dump es una copia de seguridad basada en instantáneas en la que se realizan copias de seguridad de los datos del sistema de archivos en cinta. El motor de volcado ONTAP realiza copias de seguridad de los archivos, directorios y la información de la lista de control de acceso (ACL) aplicable a la cinta. Puede realizar un backup de un volumen completo, de un qtree completo o de un subárbol que no sea un volumen completo o un qtree completo. El volcado admite copias de seguridad de línea base, diferencial e incrementales.

Backup en cinta con SMTape

SMTape es una solución de recuperación ante desastres basada en Snapshot de ONTAP que realiza backups de bloques de datos a cinta. Puede usar SMTape para realizar backups de volúmenes a las cintas. Sin embargo, no puede realizar un backup en el nivel qtree o subárbol. SMTape admite copias de seguridad de línea base, diferenciales e incrementales.

A partir de ONTAP 9.13.1, el backup en cinta con SMTape es compatible con SnapMirror síncrono activo.

Flujo de trabajo de copia de seguridad y restauración de cintas de ONTAP

Es posible realizar operaciones de backup y restauración a cinta con una aplicación de backup habilitada para NDMP.

Acerca de esta tarea

El flujo de trabajo de backup y restauración a cinta ofrece información general de las tareas relacionadas con las operaciones de backup y restauración en cinta. Para obtener información detallada sobre cómo realizar una operación de backup y restauración, consulte la documentación de la aplicación de backup.

Pasos

1. Configure una biblioteca de cintas eligiendo una topología de cinta compatible con NDMP.
2. Active los servicios NDMP en el sistema de almacenamiento.

   Puede habilitar los servicios NDMP en el nivel del nodo o en el nivel de la máquina virtual de almacenamiento (SVM). Esto depende del modo NDMP en el que elija ejecutar las operaciones de backup y restauración a cinta.

3. Utilice las opciones NDMP para gestionar NDMP en su sistema de almacenamiento.

   Puede usar las opciones de NDMP a nivel de nodo o de SVM. Esto depende del modo NDMP en el que elija ejecutar las operaciones de backup y restauración a cinta.

   Puede modificar las opciones de NDMP en el nivel de nodo mediante `system services ndmp modify` el comando y en el nivel de SVM mediante `vserver services ndmp modify` el comando. Obtenga más información sobre `system services ndmp modify` y `vserver services ndmp modify` en el "Referencia de comandos del ONTAP".

4. Realizar un backup a cinta o una restauración de datos mediante una aplicación de backup compatible con NDMP.

   ONTAP es compatible con los motores de volcado y SMTape para backup y restauración a cinta.

   Para obtener más información acerca del uso de la aplicación de copia de seguridad (también denominada *Data Management Applications* o *DMAs*) para realizar operaciones de copia de seguridad o restauración, consulte la documentación de la aplicación de copia de seguridad.

Información relacionada

Topologías habituales de backup en cinta NDMP

Motor de volcado para volúmenes FlexVol

Casos de uso para motores de copia de seguridad de volcado y SMTape de ONTAP

ONTAP admite dos motores de respaldo: SMTape y dump. Debe conocer los casos de uso de los motores de copia de seguridad SMTape y de volcado para ayudarle a elegir el motor de copia de seguridad para realizar operaciones de copia de seguridad en cinta y restauración.

El volcado se puede utilizar en los siguientes casos:

- Recuperación de acceso directo (DAR) de ficheros y directorios
- Copia de seguridad de un subconjunto de subdirectorios o archivos en una ruta de acceso específica
- Exclusión de archivos y directorios específicos durante las copias de seguridad
- Conservación del backup a largo plazo

SMTape se puede utilizar en los siguientes casos:

- Solución de recuperación tras siniestros
- Conservación del ahorro de la deduplicación y de la configuración de deduplicación en los datos de backup durante la operación de restauración
- Backup de grandes volúmenes

Gestión de unidades de cinta

Obtenga información sobre la administración de unidades de cinta ONTAP

Puede verificar las conexiones de la biblioteca de cintas y ver la información de la unidad de cinta antes de realizar una operación de backup o restauración de cinta. Puede utilizar una unidad de cinta no cualificada emulando esta unidad a una unidad de cinta cualificada. También puede asignar y eliminar alias de cinta además de ver los alias existentes.

Cuando se realiza el backup de los datos en cinta, estos se almacenan en archivos de cinta. Las marcas de archivo separan los archivos de cinta y los archivos no tienen nombres. Especifique un archivo de cinta por su posición en la cinta. Se escribe un archivo de cinta mediante un dispositivo de cinta. Cuando lea el archivo de cinta, debe especificar un dispositivo que tenga el mismo tipo de compresión que utilizó para escribir ese archivo de cinta.

Comandos de ONTAP para administrar unidades de cinta, cambiadores de medios y operaciones de unidades de cinta

Hay comandos para ver información acerca de las unidades de cinta y los intercambiadores de medios en un clúster, conectar una unidad de cinta y desconectarla, modificar la posición del cartucho de la unidad de cinta, configurar y borrar el nombre del alias de la unidad de cinta y restablecer una unidad de cinta. También es posible ver y restablecer las estadísticas de la unidad de cinta.

Si desea…	Se usa este comando…
Conectar una unidad de cinta	`storage tape online`
Borre un nombre de alias para la unidad de cinta o el cambiador de medios	`storage tape alias clear`
Activar o desactivar una operación de rastreo de cinta para una unidad de cinta	`storage tape trace`
Modifique la posición del cartucho de la unidad de cinta	`storage tape position`

Si desea…	Se usa este comando…
Restablezca una unidad de cinta	`storage tape reset` Este comando solo está disponible en el nivel de privilegios avanzados.
Defina un nombre de alias para la unidad de cinta o el cambiador de medios	`storage tape alias set`
Desconectar una unidad de cinta	`storage tape offline`
Ver información acerca de todas las unidades de cinta e intercambiadores de medios	`storage tape show`
Ver información acerca de las unidades de cinta conectadas al clúster	• `storage tape show-tape-drive` • `system node hardware tape drive show`
Ver información acerca de los cambiadores de medios conectados al clúster	`storage tape show-media-changer`
Ver información de errores sobre las unidades de cinta conectadas al clúster	`storage tape show-errors`
Ver todas las unidades de cinta cualificadas y compatibles de ONTAP conectadas a cada nodo del clúster	`storage tape show-supported-status`
Vea alias de todas las unidades de cinta e intercambiadores de medios conectados a cada nodo del clúster	`storage tape alias show`
Restablece la lectura de estadísticas de una unidad de cinta a cero	`storage stats tape zero tape_name` Debe utilizar este comando en el nodeshell.
Vea las unidades de cinta compatibles con ONTAP	`storage show tape supported [-v]` Debe utilizar este comando en el nodeshell. Puede utilizar `-v` la opción para ver más detalles sobre cada unidad de cinta.
Vea las estadísticas de dispositivos de cinta para comprender el rendimiento de la cinta y comprobar los patrones de uso	`storage stats tape tape_name` Debe utilizar este comando en el nodeshell.

Información relacionada

- "cinta de almacenamiento"
- "espectáculo de cintas de almacenamiento"
- "cinta de almacenamiento mostrar-estado-compatible"
- "unidad de cinta de almacenamiento"
- "alias de cinta de almacenamiento claro"
- "conjunto de alias de cinta de almacenamiento"
- "Mostrar alias de cinta de almacenamiento"
- "rastro de cinta de almacenamiento"

Utilice una unidad de cinta no calificada para la copia de seguridad en cinta ONTAP

Puede utilizar una unidad de cinta no cualificada en un sistema de almacenamiento si puede emular una unidad de cinta cualificada. Luego se trata como una unidad de cinta cualificada. Para utilizar una unidad de cinta no cualificada, primero debe determinar si emula cualquiera de las unidades de cinta cualificadas.

Acerca de esta tarea

Una unidad de cinta no cualificada es una unidad conectada al sistema de almacenamiento, pero que ONTAP no admite ni reconoce.

Pasos

1. Ver las unidades de cinta no cualificadas conectadas a un sistema de almacenamiento mediante `storage tape show-supported-status` el comando.

   El siguiente comando muestra las unidades de cinta conectadas al sistema de almacenamiento y el estado de soporte y cualificación de cada unidad de cinta. También se muestran las unidades de cinta no cualificadas. `tape_drive_vendor_name` Es una unidad de cinta no cualificada conectada al sistema de almacenamiento pero no compatible con ONTAP.

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                    Is
          Tape Drive                Supported  Support Status
          --------------------      ---------  --------------
          "tape_drive_vendor_name"  false      Nonqualified tape drive
          Hewlett-Packard C1533A    true       Qualified
          Hewlett-Packard C1553A    true       Qualified
          Hewlett-Packard Ultrium 1 true       Qualified
          Sony SDX-300C             true       Qualified
          Sony SDX-500C             true       Qualified
          StorageTek T9840C         true       Dynamically Qualified
          StorageTek T9840D         true       Dynamically Qualified
          Tandberg LTO-2 HH         true       Dynamically Qualified
```

2. Emular la unidad de cinta cualificada.

   "Descargas de NetApp: Archivos de configuración de dispositivo de cinta"

Información relacionada

- Qué son las unidades de cinta adecuadas
- "cinta de almacenamiento mostrar-estado-compatible"

Asignar alias de cinta a una unidad de cinta o cambiador de medios para la copia de seguridad en cinta ONTAP

Para facilitar la identificación del dispositivo, puede asignar alias de cinta a una unidad de cinta o a un cambiador de medios. Los alias proporcionan una correspondencia entre los nombres lógicos de los dispositivos de copia de seguridad y un nombre asignado permanentemente a la unidad de cinta o al cambiador de medios.

Pasos

1. Asigne un alias a una unidad de cinta o a un cambiador de medios mediante el `storage tape alias set` comando.

   Obtenga más información sobre `storage tape alias set` en el "Referencia de comandos del ONTAP".

   Puede ver la información del número de serie (SN) sobre las unidades de cinta mediante el `system node hardware tape drive show` comando y sobre las bibliotecas de cintas mediante los `system node hardware tape library show` comandos.

   El siguiente comando establece un nombre de alias en una unidad de cinta con el número de serie SN[123456]L4 conectado al nodo, cluster1-01:

   ```
   cluster-01::> storage tape alias set  -node cluster-01 -name st3
   -mapping SN[123456]L4
   ```

   El siguiente comando establece un nombre de alias en un cambiador de medios con el número de serie SN[65432] conectado al nodo, cluster1-01:

   ```
   cluster-01::> storage tape alias set  -node cluster-01 -name mc1
   -mapping SN[65432]
   ```

Información relacionada

- Qué es el solapamiento de cinta
- Eliminación de alias de cinta
- "conjunto de alias de cinta de almacenamiento"

Eliminar alias de cinta a una unidad de cinta o cambiador de medio para la copia de seguridad en cinta ONTAP

Puede eliminar alias mediante el `storage tape alias clear` comando cuando ya no se necesitan alias persistentes para una unidad de cinta o un cambiador de medios.

Pasos

1. Elimine un alias de una unidad de cinta o de un cambiador de medios mediante el `storage tape alias clear` comando.

   Obtenga más información sobre `storage tape alias clear` en el "Referencia de comandos del ONTAP".

   El siguiente comando elimina los alias de todas las unidades de cinta especificando el ámbito de la operación de borrado de alias en `tape`:

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

Después de terminar

Si va a realizar una operación de backup o restauración de cinta mediante NDMP, después de eliminar un alias de una unidad de cinta o un cambiador de medios, debe asignar un nuevo nombre de alias a la unidad de cinta o al cambiador de medios para continuar accediendo al dispositivo de cinta.

Información relacionada

- Qué es el solapamiento de cinta
- Asignación de alias de cinta
- "alias de cinta de almacenamiento claro"

Habilitar o deshabilitar las reservas de cinta ONTAP

Puede controlar el modo en que ONTAP gestiona las reservas de dispositivos de cinta con `tape.reservations` la opción. De forma predeterminada, la reserva de cinta está desactivada.

Acerca de esta tarea

La activación de la opción de reservas de cintas puede ocasionar problemas si las unidades de cinta, los cambiadores de medios, los puentes o las bibliotecas no funcionan correctamente. Si los comandos de cinta indican que el dispositivo está reservado cuando no hay otros sistemas de almacenamiento que utilicen el dispositivo, esta opción debería estar desactivada.

Pasos

1. Para utilizar el mecanismo de reserva/liberación SCSI o la reserva persistente SCSI para desactivar las reservas en cinta, introduzca el siguiente comando en el clustershell:

   `options -option-name tape.reservations -option-value {scsi | persistent | off}`

   `scsi` Selecciona el mecanismo de reserva/liberación SCSI.

   `persistent` Selecciona Reservas persistentes SCSI.

`off` desactiva las reservas de cinta.

Información relacionada

Qué reservas de cinta son

Comandos ONTAP para verificar las conexiones de la biblioteca de cintas

Puede ver información acerca de la ruta de conexión entre un sistema de almacenamiento y una configuración de biblioteca de cintas conectada al sistema de almacenamiento. Puede utilizar esta información para verificar la ruta de conexión a la configuración de la biblioteca de cintas o para solucionar problemas relacionados con las rutas de conexión.

Puede ver los siguientes detalles de la biblioteca de cintas para verificar las conexiones de la biblioteca de cintas después de agregar o crear una biblioteca de cintas nueva, o después de restaurar una ruta de acceso fallida en una ruta única o acceso multivía a una biblioteca de cintas. También puede utilizar esta información al solucionar errores relacionados con la ruta de acceso o si el acceso a una biblioteca de cintas falla.

- Nodo al que está conectada la biblioteca de cintas
- ID del dispositivo
- Ruta NDMP
- Nombre de la biblioteca de cintas
- ID de puerto de destino e puerto de iniciador
- Acceso de ruta única o multivía a una biblioteca de cintas para cada puerto iniciador FC o de destino
- Detalles de la integridad de los datos relacionados con la ruta, como «'errores de ruta'» y «'Manual de ruta'».
- Los grupos LUN y el número de LUN

Si desea…	Se usa este comando…
Ver información sobre una biblioteca de cintas en un clúster	`system node hardware tape library show`
Ver información de ruta de una biblioteca de cintas	`storage tape library path show`
Vea la información de ruta de una biblioteca de cintas para cada puerto iniciador	`storage tape library path show-by-initiator`
Vea la información de conectividad entre una biblioteca de cinta de almacenamiento y un clúster	`storage tape library config show`

Información relacionada

- "Mostrar configuración de la biblioteca de cintas de almacenamiento"
- "biblioteca de cintas de hardware del nodo del sistema mostrar"
- "Mostrar ruta de la biblioteca de cintas de almacenamiento"

- "Ruta de la biblioteca de cintas de almacenamiento mostrada por iniciador"

Acerca de las unidades de cinta

Obtenga más información sobre las unidades de cinta ONTAP calificadas

Debe utilizar una unidad de cinta cualificada que se haya probado y encontrado para funcionar correctamente en un sistema de almacenamiento. Puede seguir el solapamiento de cintas y activar reservas de cinta para asegurarse de que sólo un sistema de almacenamiento accede a una unidad de cinta en un momento determinado.

Una unidad de cinta cualificada es una unidad de cinta que se ha probado y que funciona correctamente en sistemas de almacenamiento. Puede calificar las unidades de cinta para las versiones de ONTAP existentes mediante el archivo de configuración de cinta.

Formato del archivo de configuración de cinta ONTAP

El formato de archivo de configuración de cinta consta de campos como el ID de proveedor, el ID de producto y los detalles de los tipos de compresión de una unidad de cinta. Este archivo también consta de campos opcionales para activar la función de carga automática de una unidad de cinta y cambiar los valores de tiempo de espera de comando de una unidad de cinta.

La siguiente tabla muestra el formato del archivo de configuración de cinta:

Elemento	Tamaño	Descripción
`vendor_id` (cadena)	hasta 8 bytes	El ID de proveedor según lo informado por `SCSI Inquiry` el comando.
`product_id`(cadena)	hasta 16 bytes	El ID de producto según lo informado por `SCSI Inquiry` el comando.
`id_match_size`(número)		El número de bytes del ID de producto que se va a utilizar para la coincidencia para detectar la unidad de cinta que se va a identificar, comenzando por el primer carácter del ID de producto en los datos de consulta.
`vendor_pretty` (cadena)	hasta 16 bytes	Si este parámetro está presente, se especifica mediante la cadena mostrada por el comando, `storage tape show -device -names`; de lo contrario, se muestra INQ_VENDOR_ID.

Elemento	Tamaño	Descripción
`product_pretty`(cadena)	hasta 16 bytes	Si este parámetro está presente, se especifica mediante la cadena mostrada por el comando, `storage tape show -device -names`; de lo contrario, se muestra INQ_PRODUCT_ID.

Los `vendor_pretty` `product_pretty` campos y son opcionales, pero si uno de estos campos tiene un valor, el otro también debe tener un valor.

En la siguiente tabla se explica la descripción, el código de densidad y el algoritmo de compresión para los distintos tipos de compresión, como `l` , , `m` `h` y `a`:

Elemento	Tamaño	Descripción
`{l	m	h
a}_description=(string)`	hasta 24 bytes	Cadena que se va a imprimir para el comando nodeshell `sysconfig -t` , que describe las características de la configuración de densidad concreta.
`{l	m	h
a}_density=(hex codes)`		El código de densidad que se va a establecer en el descriptor de bloque de página del modo SCSI correspondiente al código de densidad deseado para l, m, h o a..
`{l	m	h
a}_algorithm=(hex codes)`		El algoritmo de compresión que se establecerá en la página del modo de compresión SCSI correspondiente al código de densidad y la característica de densidad deseada.

En la siguiente tabla se describen los campos opcionales disponibles en el archivo de configuración de cinta:

Campo	Descripción
`autoload=(Boolean yes/no)`	Este campo se establece en `yes` si la unidad de cinta tiene una función de carga automática; es decir, después de insertar el cartucho de cinta, la unidad de cinta se prepara sin necesidad de ejecutar un `SCSI load` comando (unidad de inicio/parada). El valor por defecto de este campo es `no`.
`cmd_timeout_0x`	Valor de tiempo de espera individual. Debe utilizar este campo sólo si desea especificar un valor de tiempo de espera diferente del que está utilizando como valor predeterminado el controlador de cinta. El archivo de ejemplo enumera los valores de tiempo de espera predeterminados del comando SCSI que utiliza la unidad de cinta. El valor de tiempo de espera puede expresarse en minutos (m), segundos (s) o milisegundos (ms). No debe cambiar este campo.

Puede descargar y ver el archivo de configuración de cinta desde el sitio de soporte de NetApp.

Ejemplo de formato de archivo de configuración de cinta

El formato de archivo de configuración de cinta para la unidad de cinta HP LTO5 ULTRIUM es el siguiente:

`vendor_id`= «HP»

`product_id`= «Ultrium 5-SCSI»

`id_match_size`= 9

`vendor_pretty`= «Hewlett-Packard»

`product_pretty`= LTO-5

`l_description`= LTO-3(ro)/4 4/800GB pulg.

`l_density`=0x00

`l_algorithm`=0x00

`m_description`= LTO-3(ro)/4 8/1600GB cmp

`m_density`=0x00

`m_algorithm`=0x01

`h_description`= LTO-5 1600GB

`h_density`=0x58

`h_algorithm`=0x00

`a_description`= LTO-5 3200GB cmp

`a_density`=0x58

`a_algorithm`=0x01

`autoload`= sí

Información relacionada

- "Herramientas de NetApp: Archivos de configuración de dispositivos de cinta"
- "espectáculo de cintas de almacenamiento"

Cómo el sistema de almacenamiento ONTAP califica dinámicamente una unidad de cinta

El sistema de almacenamiento califica una unidad de cinta de forma dinámica emparejando su ID de proveedor y su ID de producto con la información contenida en la tabla de calificación de cinta.

Cuando conecta una unidad de cinta al sistema de almacenamiento, busca una identificación del proveedor y una coincidencia de ID de producto entre la información obtenida durante la detección de cinta y la información de la tabla de calificación de cinta interna. Si el sistema de almacenamiento detecta una coincidencia, Marca la unidad de cinta como cualificada y puede acceder a la unidad de cinta. Si el sistema de almacenamiento no encuentra una coincidencia, la unidad de cinta permanece en estado no cualificado y no se accede a ella.

Descripción general de los dispositivos de cinta

Obtenga más información sobre los dispositivos de cinta ONTAP

Un dispositivo de cinta es una representación de una unidad de cinta. Es una combinación específica de tipo de rebobinado y capacidad de compresión de una unidad de cinta.

Se crea un dispositivo de cinta para cada combinación de tipo de rebobinado y capacidad de compresión. Por tanto, una unidad de cinta o una biblioteca de cintas pueden tener asociados varios dispositivos de cinta. Debe especificar un dispositivo de cinta para mover, escribir o leer cintas.

Al instalar una unidad de cinta o una biblioteca de cintas en un sistema de almacenamiento, ONTAP crea dispositivos de cinta asociados con la unidad de cinta o la biblioteca de cintas.

ONTAP detecta unidades de cinta y bibliotecas de cintas y asigna números lógicos y dispositivos de cinta a ellos. ONTAP detecta las bibliotecas y unidades de cinta SCSI paralelas, SAS y Fibre Channel cuando están conectadas a los puertos de interfaz. ONTAP detecta estas unidades cuando sus interfaces están habilitadas.

Formato de un nombre de dispositivo de cinta ONTAP

Cada dispositivo de cinta tiene un nombre asociado que aparece en un formato definido. El formato incluye información acerca del tipo de dispositivo, el tipo de rebobinado, el alias y el tipo de compresión.

El formato de un nombre de dispositivo de cinta es el siguiente:

`rewind_type st alias_number compression_type`

`rewind_type` es el tipo de rebobinado.

En la siguiente lista se describen los distintos valores de tipo de rebobinado:

- **r**

  ONTAP rebobina la cinta después de que termine de escribir el archivo de cinta.

- **no**

  ONTAP no rebobinará la cinta después de que termine de escribir el archivo de cinta. Debe utilizar este tipo de rebobinado cuando desee escribir varios archivos de cinta en la misma cinta.

- **ur**

  Este es el tipo de rebobinado de descarga/recarga. Cuando se utiliza este tipo de rebobinado, la biblioteca de cintas descarga la cinta cuando llega al final de un archivo de cinta y, a continuación, carga la cinta siguiente, si existe una.

  Debe utilizar este tipo de rebobinado sólo en las siguientes circunstancias:

  - La unidad de cinta asociada con este dispositivo se encuentra en una biblioteca de cintas o en un cambiador de medios que se encuentra en el modo de biblioteca.
  - La unidad de cinta asociada con este dispositivo está conectada a un sistema de almacenamiento.
  - Las cintas suficientes para la operación que está realizando están disponibles en la secuencia de cintas de biblioteca definida para esta unidad de cinta.

Si graba una cinta con un dispositivo de no rebobinado, debe rebobinar la cinta antes de leerla.

`st` es la designación estándar para una unidad de cinta.

`alias_number` Es el alias que ONTAP asigna a la unidad de cinta. Cuando ONTAP detecta una nueva unidad de cinta, ONTAP asigna un alias a la unidad de cinta.

`compression_type` es un código específico de la unidad para la densidad de los datos de la cinta y el tipo de compresión.

La lista siguiente describe los diversos valores de `compression_type`:

- **a**

  Mayor compresión

- **h**

  Alta compresión

- **m**

  Compresión media

- **l**

  Baja compresión

Ejemplos

`nrst0a` especifica un dispositivo sin rebobinado en la unidad de cinta 0 utilizando la compresión más alta.

Ejemplo de una lista de dispositivos de cinta

En el siguiente ejemplo se muestran los dispositivos de cinta asociados con HP Ultrium 2-SCSI:

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,        format is: HP (200GB)
nrst0l -  no rewind device,     format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,        format is: HP (200GB)
nrst0m -  no rewind device,     format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,        format is: HP (200GB)
nrst0h -  no rewind device,     format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,        format is: HP (400GB w/comp)
nrst0a -  no rewind device,     format is: HP (400GB w/comp)
urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

En la siguiente lista se describen las abreviaturas del ejemplo anterior:

- GB—Gigabytes; esta es la capacidad de la cinta.
- con compresión; esto muestra la capacidad de cinta con compresión.

Número admitido de dispositivos de cinta ONTAP simultáneos

ONTAP admite un máximo de 64 conexiones simultáneas de unidad de cinta, 16 cambiadores de soporte y 16 dispositivos de puente o router para cada sistema de almacenamiento (por nodo) en cualquier combinación de conexiones Fibre Channel, SCSI o SAS.

Las unidades de cinta o los cambiadores de medios pueden ser dispositivos en bibliotecas de cintas físicas o virtuales o dispositivos independientes.

> Aunque un sistema de almacenamiento puede detectar 64 conexiones a unidades de cinta, la cantidad máxima de sesiones de backup y restauración que pueden realizarse de forma simultánea depende de los límites de escalabilidad del motor de backup.

Información relacionada

Límites de escalabilidad para sesiones de backup y restauración de volcado

Solapamiento de cinta

Descripción general de solapamiento de cinta

Aliasing simplifica el proceso de identificación del dispositivo. Aliasing enlaza un nombre de ruta física (PPN) o un número de serie (SN) de una cinta o un cambiador de soporte a un nombre de alias persistente pero modificable.

La siguiente tabla describe cómo el aliasing de cinta le permite asegurarse de que una unidad de cinta (o biblioteca de cintas o cambiador de medios) está siempre asociada con un único nombre de alias:

Situación	Reasignar el alias
Cuando se reinicia el sistema	La unidad de cinta se reasigna automáticamente su alias anterior.
Cuando un dispositivo de cinta se mueve a otro puerto	El alias se puede ajustar para que apunte a la nueva dirección.
Cuando más de un sistema utiliza un dispositivo de cinta concreto	El usuario puede configurar el alias para que sea el mismo en todos los sistemas.

Al actualizar de Data ONTAP 8.1.x a Data ONTAP 8.2.x, la función de alias de cinta de Data ONTAP 8.2.x modifica los nombres de alias de cinta existentes. En tal caso, es posible que tenga que actualizar los nombres de alias de cinta en la aplicación de copia de seguridad.

La asignación de alias de cinta proporciona una correspondencia entre los nombres lógicos de los dispositivos de copia de seguridad (por ejemplo, st0 o mc1) y un nombre asignado permanentemente a un puerto, una unidad de cinta o un cambiador de medios.

st0 y st00 son nombres lógicos diferentes.

Los nombres lógicos y números de serie se utilizan sólo para acceder a un dispositivo. Después de acceder al dispositivo, devuelve todos los mensajes de error utilizando el nombre de ruta física.

Hay dos tipos de nombres disponibles para el solapamiento: Nombre de ruta física y número de serie.

Aprenda sobre los nombres de las rutas físicas

Los nombres de rutas físicas (PNP) son las secuencias de direcciones numéricas que ONTAP asigna a unidades de cinta y bibliotecas de cintas basadas en el adaptador o switch SCSI-2/3 (ubicación específica) que están conectados al sistema de almacenamiento. Los PPNS también se conocen como nombres eléctricos.

Los PPNS de los dispositivos de conexión directa utilizan el siguiente formato `host_adapter`: . `device_id_lun`

El valor de LUN se muestra solo para dispositivos de cambio de cinta y medio cuyos valores de LUN no son cero; es decir, si el valor de LUN es cero, `lun` no se muestra la parte de PPN.

Por ejemplo, PPN 8.6 indica que el número de adaptador de host es 8, el ID de dispositivo es 6 y el número de unidad lógica (LUN) es 0.

Los dispositivos de cinta SAS también son dispositivos de conexión directa. Por ejemplo, el PPN 5c.4 indica que en un sistema de almacenamiento, el SAS HBA está conectado en la ranura 5, la cinta SAS está conectada al puerto C del SAS HBA y el identificador de dispositivo es 4.

Los PPNS de los dispositivos conectados por switch Fibre Channel utilizan el siguiente formato `switch:port_id:.device_id_lun`

Por ejemplo, el PPN MY_SWITCH:5.3L2 indica que la unidad de cinta conectada al puerto 5 de un switch llamado MY_SWITCH está establecida con el ID de dispositivo 3 y tiene el LUN 2.

La unidad determina el LUN (número de unidad lógica). Fibre Channel, bibliotecas y unidades de cinta SCSI, así como discos, tienen VPN.

Los PPNS de unidades de cinta y bibliotecas no cambian a menos que cambie el nombre del conmutador, se mueva la unidad de cinta o la biblioteca o se reconfigure la unidad de cinta o la biblioteca. Los PPNS permanecen sin cambios después del reinicio. Por ejemplo, si se retira una unidad de cinta denominada MY_SWITCH:5.3L2 y SE conecta una nueva unidad de cinta con el mismo ID de dispositivo y LUN al puerto 5 del conmutador MY_SWITCH, se podrá acceder a la nueva unidad de cinta mediante MY_SWITCH:5.3L2.

Aprenda sobre los números de serie

Un número de serie (SN) es un identificador único para una unidad de cinta o un cambiador de medios. ONTAP genera alias basados en SN en lugar de WWN.

Dado que el SN es un identificador único para una unidad de cinta o un cambiador de medios, el alias permanece igual independientemente de las múltiples rutas de conexión a la unidad de cinta o al cambiador de medios. Esto ayuda a los sistemas de almacenamiento a realizar un seguimiento de la misma unidad de cinta o cambiador de medios en una configuración de biblioteca de cintas.

El número de serie de una unidad de cinta o un cambiador de medios no cambia aunque cambie el nombre del conmutador Fibre Channel al que está conectada la unidad de cinta o el cambiador de medios. Sin embargo, en una biblioteca de cintas si reemplaza una unidad de cinta existente con una nueva, ONTAP genera nuevos alias porque cambia el número de serie de la unidad de cinta. Además, si mueve una unidad de cinta existente a una nueva ranura de una biblioteca de cintas o reasigna el LUN de la unidad de cinta, ONTAP genera un nuevo alias para esa unidad de cinta.

Debe actualizar las aplicaciones de backup con los alias recién generados.

El número de serie de un dispositivo de cinta utiliza el siguiente formato: `SN[xxxxxxxxxx]L[X]`

`x` Es un carácter alfanumérico y L`X` es el LUN del dispositivo de cinta. Si la LUN es 0,`X` no se muestra la parte L de la cadena.

Cada SN consta de hasta 32 caracteres; el formato para el SN no distingue entre mayúsculas y minúsculas.

Consideraciones al configurar el acceso a cinta multiruta de ONTAP

Puede configurar dos rutas desde el sistema de almacenamiento para acceder a las unidades de cinta de una biblioteca de cintas. Si falla una ruta, el sistema de almacenamiento puede utilizar las otras rutas para acceder a las unidades de cinta sin

tener que reparar inmediatamente la ruta con error. Esto garantiza que se puedan reiniciar las operaciones de cinta.

Al configurar el acceso a cinta multivía desde el sistema de almacenamiento, debe tener en cuenta lo siguiente:

- En bibliotecas de cintas que admiten la asignación de LUN, para acceder de varias rutas a un grupo LUN, la asignación de LUN debe ser simétrica en cada ruta.

  Las unidades de cinta e intercambiadores de medios se asignan a grupos de LUN (conjunto de LUN que comparten el mismo conjunto de rutas del iniciador) en una biblioteca de cintas. Todas las unidades de cinta de un grupo LUN deben estar disponibles para las operaciones de backup y restauración en todas las rutas múltiples.

- Se puede configurar un máximo de dos rutas desde el sistema de almacenamiento para acceder a las unidades de cinta de una biblioteca de cintas.
- El acceso a cinta multivía es compatible con el equilibrio de carga. El equilibrio de carga está deshabilitado de forma predeterminada.

En el ejemplo siguiente, el sistema de almacenamiento accede al grupo LUN 0 a través de dos rutas de iniciador: 0b y 0d. En estas dos rutas, el grupo de LUN tiene el mismo número de LUN, 0 y el número de LUN, 5. El sistema de almacenamiento accede al grupo LUN 1 a través de solo una ruta de iniciador, 3d.

```
STSW-3070-2_cluster::> storage tape library config show

Node                    LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
----------------------- ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01        0      5         IBM 3573-TL_1
510a09800000412d     0b

0d
                              1      2         IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

Información relacionada

- "Mostrar configuración de la biblioteca de cintas de almacenamiento"

Aprenda a agregar unidades de cinta y bibliotecas a los sistemas de almacenamiento ONTAP

Puede agregar bibliotecas y unidades de cinta al sistema de almacenamiento de forma dinámica (sin desconectar el sistema).

Al añadir un nuevo cambiador de medios, el sistema de almacenamiento detecta su presencia y la añade a la configuración. Si ya se hace referencia al cambiador de medios en la información del alias, no se crea ningún nombre lógico nuevo. Si no se hace referencia a la biblioteca, el sistema de almacenamiento crea un nuevo

alias para el cambiador de medios.

En una configuración de biblioteca de cintas, debe configurar una unidad de cinta o un cambiador de medios en el LUN 0 de un puerto de destino para ONTAP para descubrir todos los cambiadores de medios y unidades de cinta en ese puerto de destino.

Obtenga más información sobre las reservas de cintas de ONTAP

Múltiples sistemas de almacenamiento pueden compartir el acceso a unidades de cinta, cambiadores de medio, puentes o bibliotecas de cintas. Las reservas de cintas garantizan que sólo un sistema de almacenamiento pueda acceder a un dispositivo en cualquier momento, ya sea habilitando el mecanismo de reserva/versión SCSI o las reservas persistentes SCSI para todas las unidades de cinta, cambiadores medianos, puentes y bibliotecas de cintas.

Todos los sistemas que comparten dispositivos en una biblioteca, incluidos o no conmutadores, deben utilizar el mismo método de reserva.

El mecanismo de reserva/liberación SCSI para reservar dispositivos funciona bien en condiciones normales. Sin embargo, durante los procedimientos de recuperación de errores de interfaz, se pueden perder las reservas. Si esto sucede, los iniciadores que no son el propietario reservado pueden acceder al dispositivo.

Las reservas realizadas con reservas persistentes SCSI no se ven afectadas por mecanismos de recuperación de errores, como el restablecimiento de bucle o el restablecimiento de objetivos; sin embargo, no todos los dispositivos implementan correctamente las reservas persistentes SCSI.

Transferir datos entre sistemas de almacenamiento

Transferir datos de ONTAP usando ndmpcopy

El `ndmpcopy` comando nodeshell transfiere datos entre sistemas de almacenamiento compatibles con NDMP v4. Puede realizar transferencias de datos completas e incrementales. Puede transferir volúmenes completos o parciales, qtrees, directorios o archivos individuales.

Acerca de esta tarea

Gracias al uso de ONTAP 8.x y versiones anteriores, las transferencias incrementales están limitadas a un máximo de dos niveles (uno completo y hasta dos backups incrementales).

A partir de ONTAP 9.0 y versiones posteriores, las transferencias incrementales están limitadas a un máximo de nueve niveles (uno completo y hasta nueve backups incrementales).

Puede ejecutarse `ndmpcopy` en la línea de comandos nodeshell de los sistemas de almacenamiento de origen y de destino, o en un sistema de almacenamiento que no sea ni el origen ni el destino de la transferencia de datos. También puede ejecutarse `ndmpcopy` en un único sistema de almacenamiento que sea tanto el origen como el destino de la transferencia de datos.

Puede usar las direcciones IPv4 o IPv6 de los sistemas de almacenamiento de origen y destino en el `ndmpcopy` comando. El formato de ruta es `/vserver_name/volume_name \[path\]`.

Pasos

1. Active el servicio NDMP en los sistemas de almacenamiento de origen y destino:

Si realiza transferencia de datos en el origen o el destino en…	Usar el siguiente comando…
Modo de NDMP con ámbito SVM	`vserver services ndmp on` Para la autenticación NDMP en la SVM de administración, la cuenta de usuario es `admin` y el rol de usuario es `admin` o `backup`. En la SVM de datos, la cuenta de usuario es `vsadmin` y el rol de usuario es `vsadmin` o `vsadmin-backup` el rol.
Modo de NDMP con ámbito del nodo	`system services ndmp on`

2. Transferir datos dentro de un sistema de almacenamiento o entre sistemas de almacenamiento mediante `ndmpcopy` el comando en el infierno de nodos:

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

Los nombres DNS no son compatibles con ndmpcopy. Debe proporcionar la dirección IP del origen y del destino. La dirección de bucle invertido (127.0.0.1) no es compatible con la dirección IP de origen ni con la dirección IP de destino.

- `ndmpcopy`El comando determina el modo de dirección para las conexiones de control de la siguiente manera:
  - El modo de dirección para la conexión de control corresponde a la dirección IP proporcionada.
  - Puede sustituir estas reglas mediante las `-mcs` `-mcd` opciones y.
- Si el origen o el destino son el sistema ONTAP, entonces según el modo NDMP (ámbito del nodo o ámbito de la SVM), utilice una dirección IP que permita el acceso al volumen de destino.
- `source_path` y `destination_path` son los nombres absolutos de la ruta hasta el nivel granular de volumen, qtree, directorio o archivo.
- `-mcs` especifica el modo de direccionamiento preferido para la conexión de control al sistema de almacenamiento de origen.

  `inet` Indica un modo de dirección IPv4 e `inet6` indica un modo de dirección IPv6.

- `-mcd` especifica el modo de direccionamiento preferido para la conexión de control con el sistema de almacenamiento de destino.

  `inet` Indica un modo de dirección IPv4 e `inet6` indica un modo de dirección IPv6.

- `-md` especifica el modo de direcciones preferido para la transferencia de datos entre los sistemas de almacenamiento de origen y destino.

`inet` Indica un modo de dirección IPv4 e `inet6` indica un modo de dirección IPv6.

Si no utiliza la `-md` opción en el `ndmpcopy` comando, el modo de direccionamiento para la conexión de datos se determina de la siguiente manera:

- Si alguna de las direcciones especificadas para las conexiones de control es una dirección IPv6, el modo de dirección para la conexión de datos es IPv6.
- Si las dos direcciones especificadas para las conexiones de control son direcciones IPv4, el `ndmpcopy` comando intenta primero un modo de dirección IPv6 para la conexión de datos.

  Si no es así, el comando utiliza un modo de dirección IPv4.

  Una dirección IPv6, si se especifica, debe escribirse entre corchetes.

  Este comando de ejemplo migra datos de una ruta de origen (`source_path`) a una ruta de destino)(`destination_path`.

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+
Este comando de ejemplo establece explícitamente las conexiones de control y la conexión de datos para utilizar el modo de dirección IPv6:

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Opciones para el comando ndmpcopy

Debe comprender las opciones disponibles para que el `ndmpcopy` comando nodeshell tenga éxito"transferencia de datos".

En la siguiente tabla se enumeran las opciones disponibles.

Opción	Descripción
`-sa username:[password]`	Esta opción configura el nombre de usuario y la contraseña de autenticación de origen para conectarse con el sistema de almacenamiento de origen. Esta es una opción obligatoria. Para un usuario sin privilegios de administrador, debe especificar la contraseña específica de NDMP generada por el sistema del usuario. La contraseña que genera el sistema es obligatoria tanto para los usuarios administradores como para los que no son de administrador.
`-da username:[password]`	Esta opción establece el nombre de usuario y la contraseña de autenticación de destino para conectarse al sistema de almacenamiento de destino. Esta es una opción obligatoria.
`-st {md5`	`text}`
Esta opción establece el tipo de autenticación de origen que se utilizará al conectarse al sistema de almacenamiento de origen. Esta es una opción obligatoria y, por lo tanto, el usuario debe proporcionar `text md5` la opción o.	`-dt {md5`
`text}`	Esta opción establece el tipo de autenticación de destino que se utilizará al conectarse al sistema de almacenamiento de destino.
`-l`	Esta opción define el nivel de volcado utilizado para la transferencia al valor especificado de LEVEL.Los valores válidos son `0 1` , a , `9` donde `0` indica una transferencia completa y `1 9` especifica una transferencia incremental. El valor predeterminado es `0`.
`-d`	Esta opción permite la generación de mensajes de registro de depuración ndmpcopy. Los archivos de registro de depuración ndmpcopy se encuentran en el `/mroot/etc/log` volumen raíz. Los nombres de los archivos de registro de depuración ndmpcopy tienen `ndmpcopy.yyyymmdd` formato.
`-f`	Esta opción activa el modo forzado. Este modo permite sobrescribir los archivos del sistema `/etc` en el directorio raíz del volumen 7-Mode.

Opción	Descripción
`-h`	Esta opción imprime el mensaje de ayuda.
`-p`	Esta opción le pide que introduzca la contraseña para la autorización de origen y destino. Esta contraseña sustituye la contraseña especificada para `-sa -da` las opciones y. Esta opción solo se puede utilizar cuando el comando se ejecuta en una consola interactiva.
`-exclude`	Esta opción excluye los archivos o directorios especificados de la ruta de acceso especificada para la transferencia de datos. El valor puede ser una lista separada por comas de nombres de directorio o de archivo como **`.pst`** `o .txt`. El número máximo de patrones de exclusión admitidos es 32 y el número máximo de caracteres admitidos es 255.

NDMP para volúmenes FlexVol

Obtenga información sobre NDMP para volúmenes ONTAP FlexVol

El protocolo de gestión de datos de red (NDMP) es un protocolo estandarizado para controlar el backup, la recuperación y otros tipos de transferencia de datos entre dispositivos de almacenamiento primarios y secundarios, como sistemas de almacenamiento y bibliotecas de cintas.

Al habilitar la compatibilidad con NDMP en un sistema de almacenamiento, permite que ese sistema de almacenamiento se comunique con aplicaciones de backup conectadas a la red compatibles con NDMP (también denominadas *Data Management Applications* o *DMAs*), servidores de datos y servidores de cinta que participan en operaciones de backup o recuperación. Todas las comunicaciones de red se producen a través de la red TCPIP o TCP/IPv6. NDMP también proporciona un control de bajo nivel de unidades de cinta e intercambiadores de tamaño medio.

Puede realizar operaciones de backup y restauración de cinta en el modo NDMP de ámbito del nodo o en el modo NDMP de la máquina virtual de almacenamiento (SVM) con ámbito.

Debe saber cuáles son las consideraciones que debe tener en cuenta a la hora de utilizar NDMP, la lista de variables de entorno y las topologías de backup en cinta de NDMP admitidas. También puede habilitar o deshabilitar la funcionalidad DAR mejorada. Los dos métodos de autenticación compatibles con ONTAP para autenticar el acceso NDMP a un sistema de almacenamiento son: Sin formato y sin reto.

Información relacionada

Variables de entorno compatibles con ONTAP

Acerca de los modos de funcionamiento de NDMP

Conozca los modos de funcionamiento de ONTAP NDMP

Puede optar por realizar operaciones de backup y restauración a cinta, ya sea en el nivel de nodo o en el nivel de la máquina virtual de almacenamiento (SVM). Para ejecutar estas operaciones correctamente en el nivel de SVM, el servicio NDMP debe estar habilitado en la SVM.

Si actualiza de Data ONTAP 8.2 a Data ONTAP 8.3, seguirá reteniendo el modo de funcionamiento NDMP usado en 8.2 después de la actualización de 8.2 a 8.3.

Si instala un clúster nuevo con Data ONTAP 8.2 o posterior, NDMP se encuentra en el modo NDMP de ámbito SVM de manera predeterminada. Para realizar operaciones de backup y restauración de cinta en el modo de NDMP de ámbito del nodo, debe habilitar explícitamente el modo de NDMP de ámbito del nodo.

Obtenga información sobre el modo NDMP de ONTAP con ámbito de nodo

En el modo NDMP de ámbito del nodo, puede realizar operaciones de backup y restauración a cinta en el nivel del nodo. Se seguirá reteniendo el modo de funcionamiento NDMP usado en Data ONTAP 8.2 después de la actualización de 8.2 a 8.3.

En el modo NDMP de ámbito del nodo, puede realizar operaciones de backup y restauración de cinta en un nodo que posea el volumen. Para realizar estas operaciones, debe establecer conexiones de control NDMP en una LIF alojada en el nodo propietario de los dispositivos de volumen o cinta.

Este modo quedó obsoleto y se quitará en un lanzamiento principal futuro.

Obtenga información sobre el modo NDMP de ONTAP con ámbito SVM

Se pueden ejecutar operaciones de backup y restauración de cinta en el nivel de máquina virtual de almacenamiento (SVM) correctamente si el servicio NDMP está habilitado en la SVM. Puede realizar backups y restauraciones de todos los volúmenes alojados en diferentes nodos en la SVM de un clúster si la aplicación de backup admite la extensión CAB.

Se puede establecer una conexión de control NDMP en diferentes tipos de LIF. En el modo NDMP con ámbito SVM, estas LIF pertenecen a la SVM de datos o a la SVM de administrador. La conexión puede establecerse en un LIF solo si el servicio NDMP está habilitado en la SVM propietaria de este LIF.

Una LIF de datos pertenece a la SVM de datos y la LIF entre clústeres, la LIF de gestión de nodos y la LIF de gestión de clúster pertenecen a la SVM de administrador.

En el modo NDMP de ámbito SVM, la disponibilidad de volúmenes y dispositivos de cinta para operaciones de backup y restauración depende del tipo de LIF en el que se establezca la conexión de control NDMP y el estado de la extensión CAB. Si su aplicación de backup admite la extensión CAB y un volumen y el dispositivo de cinta comparten la misma afinidad, la aplicación de backup puede realizar una operación de backup o restauración local, en lugar de una operación de backup o restauración triple.

Información relacionada

Comandos para gestionar el modo NDMP de ámbito de nodo

Consideraciones al utilizar el servicio NDMP de ONTAP

Debe tener en cuenta una serie de consideraciones que se deben tener en cuenta al iniciar el servicio NDMP en el sistema de almacenamiento.

- Cada nodo admite un máximo de 16 backups, restauraciones o combinación simultáneas de los dos mediante unidades de cinta conectadas.
- Los servicios NDMP pueden generar datos del historial de ficheros si así lo solicitan las aplicaciones de backup NDMP.

  El historial de archivos se utiliza en las aplicaciones de copia de seguridad para permitir la recuperación optimizada de subconjuntos seleccionados de datos de una imagen de copia de seguridad. La generación y el procesamiento del historial de archivos pueden requerir mucho tiempo y requerir gran cantidad de CPU tanto en el sistema de almacenamiento como en la aplicación de backup.

  SMTape no admite el historial de archivos.

  Si la protección de datos está configurada para la recuperación ante desastres, donde se recuperará toda la imagen de copia de seguridad, puede deshabilitar la generación del historial de archivos para reducir el tiempo de copia de seguridad. Consulte la documentación de la aplicación de copia de seguridad para determinar si es posible desactivar la generación del historial de archivos NDMP.

- La política de firewall para NDMP está habilitada de forma predeterminada en todos los tipos de LIF.
- En el modo NDMP de ámbito del nodo, el backup de un volumen FlexVol requiere que utilice la aplicación de backup para iniciar un backup en un nodo propietario del volumen.

  Sin embargo, no puede realizar backups de un volumen raíz de nodo.

- Puede realizar un backup NDMP desde cualquier LIF de la forma permitida por las políticas de firewall.

  Si utiliza una LIF de datos, debe seleccionar una LIF que no esté configurada para la conmutación por error. Si una LIF de datos conmuta al nodo de respaldo durante una operación de NDMP, la operación de NDMP falla y debe volver a ejecutarse.

- En el modo NDMP de ámbito del nodo y la máquina virtual de almacenamiento (SVM) en modo NDMP sin soporte de extensión CAB, la conexión de datos NDMP usa la misma LIF que la conexión de control NDMP.
- Durante la migración de LIF, las operaciones de backup y restauración continuas se interrumpen.

  Debe iniciar las operaciones de backup y restauración después de la migración de LIF.

- La ruta de acceso de copia de seguridad NDMP tiene el formato *`/vserver_name/volume_name/path_name`*.

  `path_name` es opcional y especifica la ruta del directorio, el archivo o la instantánea.

- Cuando se realiza un backup de un destino de SnapMirror a cinta mediante el motor de volcado, solo se realiza un backup de los datos del volumen.

  Sin embargo, si se realiza un backup de un destino de SnapMirror en cinta con SMTape, también se realiza el backup de los metadatos. Las relaciones de SnapMirror y los metadatos asociados no se realizan en un backup a cinta. Por lo tanto, durante la restauración, solo se restauran los datos de ese volumen, pero no se restauran las relaciones de SnapMirror asociadas.

Información relacionada

Qué hace la extensión Cluster Aware Backup

"Administración del sistema"

Variable de entorno

Conozca las variables de entorno compatibles con ONTAP NDMP

Las variables de entorno se utilizan para comunicar información sobre una operación de backup o restauración entre una aplicación de backup habilitada para NDMP y un sistema de almacenamiento.

Por ejemplo, si un usuario especifica que una aplicación de copia de seguridad debe realizar una copia de `/vserver1/vol1/dir1` seguridad , la aplicación de copia de seguridad define la variable de entorno DEL SISTEMA DE ARCHIVOS en `/vserver1/vol1/dir1`. Del mismo modo, si un usuario especifica que una copia de seguridad debe ser una copia de seguridad de nivel 1, la aplicación de copia de seguridad establece la variable DE entorno DE NIVEL en 1 (una).

La configuración y examen de las variables de entorno suelen ser transparentes para los administradores de backup, es decir, la aplicación de backup las establece automáticamente.

Un administrador de backup rara vez especifica variables de entorno; no obstante, se puede cambiar el valor de una variable de entorno de la cual establece la aplicación de backup para caracterizar o trabajar en torno a un problema funcional o de rendimiento. Por ejemplo, es posible que un administrador desee deshabilitar temporalmente la generación del historial de archivos para determinar si el procesamiento de la información del historial de archivos de la aplicación de copia de seguridad está contribuyendo a problemas de rendimiento o de funcionamiento.

Muchas aplicaciones de backup proporcionan un medio para anular o modificar variables de entorno o especificar variables de entorno adicionales. Para obtener información, consulte la documentación de la aplicación de copia de seguridad.

Variables de entorno compatibles con ONTAP

ONTAP admite variables de entorno, que tienen un valor predeterminado asociado. Sin embargo, puede modificar manualmente estos valores predeterminados.

Si modifica manualmente los valores establecidos por la aplicación de backup, la aplicación podría comportarse de forma impredecible. Esto se debe a que las operaciones de backup o restauración podrían no estar haciendo lo que la aplicación de backup esperaba que hicieran, pero en algunos casos, una modificación sensata puede ayudar a identificar o solucionar problemas.

En las tablas siguientes se enumeran las variables de entorno cuyo comportamiento es común para el volcado y SMTape y las variables que sólo se admiten para el volcado y SMTape. Estas tablas también contienen descripciones de cómo funcionan las variables de entorno compatibles con ONTAP si se utilizan:

En la mayoría de los casos, las variables que tienen el valor, `Y` también aceptan `T` y `N` también aceptan `F`.

Variables de entorno compatibles para volcado y SMTape

Variable de entorno	Valores válidos	Predeterminado	Descripción
DEPURAR	`Y` o. `N`	`N`	Especifica que se imprime la información de depuración.
SISTEMA DE ARCHIVOS	`string`	`none`	Especifica el nombre de la ruta de acceso de la raíz de los datos de los que se va a realizar una copia de seguridad.
VERSIÓN_NDMP	`return_only`	`none`	No debe modificar la variable NDMP_VERSION. Creada por la operación de backup, la variable NDMP_VERSION devuelve la versión de NDMP. ONTAP establece la variable NDMP_VERSION durante un backup para uso interno y para pasar a una aplicación de backup con fines informativos. La versión NDMP de una sesión NDMP no está configurada con esta variable.
SEPARADOR_NOMBRE_RUTA	`return_value`	`none`	Especifica el carácter separador del nombre de ruta de acceso. Este carácter depende del sistema de archivos del que se va a realizar el backup. En el caso de ONTAP, el carácter «»/» se asignará a esta variable. El servidor NDMP configura esta variable antes de iniciar una operación de backup a cinta.

Variable de entorno	Valores válidos	Predeterminado	Descripción
TIPO	`dump` o. `smtape`	`dump`	Especifica el tipo de backup admitido para realizar operaciones de backup y restauración a cinta.
VERBOSE	`Y` o. `N`	`N`	Aumenta los mensajes de registro mientras se realiza una operación de copia de seguridad o restauración de cinta.

Variables de entorno compatibles con el volcado

Variable de entorno	Valores válidos	Predeterminado	Descripción
ACL_START	`return_only`	`none`	Creada por la operación de backup, la variable ACL_START es un valor de desplazamiento que utilizan una operación de restauración de acceso directo o de backup NDMP reiniciable. El valor de desplazamiento es el desplazamiento de bytes en el archivo de volcado donde comienzan los datos de ACL (pase V) y se devuelven al final de una copia de seguridad. Para que una operación de restauración de acceso directo restaure correctamente los datos de los que se ha realizado un backup, el valor de ACL_START debe pasarse a la operación de restauración cuando se inicia. Una operación de backup reiniciable de NDMP utiliza el valor ACL_START para comunicarse con la aplicación de backup donde comienza la parte no reiniciable del flujo de backup.

Variable de entorno	Valores válidos	Predeterminado	Descripción
FECHA_BASE	`0`, , `-1`, o `DUMP_DATE` valor	`-1`	Especifica la fecha de inicio de las copias de seguridad incrementales. Cuando se define en `-1`, el especificador incremental BASE_DATE está desactivado. Cuando se configura en `0` una copia de seguridad de nivel 0, se activan las copias de seguridad incrementales. Después de la copia de seguridad inicial, el valor de la variable DUMP_DATE de la copia de seguridad incremental anterior se asigna a la variable BASE_DATE. Estas variables son una alternativa a las copias de seguridad incrementales basadas en NIVEL/ACTUALIZACIÓN.
DIRECTO	`Y` o. `N`	`N`	Especifica que una restauración se debe reenviar directamente a la ubicación de la cinta en la que residen los datos del archivo en lugar de analizar la cinta completa. Para que la recuperación de acceso directo funcione, la aplicación de backup debe proporcionar información de posicionamiento. Si esta variable se define en `Y`, la aplicación de copia de seguridad especifica los nombres de archivo o directorio y la información de posicionamiento.

Variable de entorno	Valores válidos	Predeterminado	Descripción
NOMBRE_DMP	`string`	`none`	Especifica el nombre de una copia de seguridad de varios subárboles. Esta variable es obligatoria para varias copias de seguridad de subárbol.
FECHA_DE_VOLCADO	`return_value`	`none`	No se cambia esta variable directamente. La copia de seguridad la crea si la variable BASE_DATE se define en un valor distinto de `-1`. LA variable DUMP_DATE se deriva prependiente el valor de nivel de 32 bits a un valor de tiempo de 32 bits calculado por el software de volcado. El nivel se incrementa desde el valor del último nivel pasado a la variable BASE_DATE. El valor resultante se utiliza como valor BASE_DATE en un backup incremental posterior.

Variable de entorno	Valores válidos	Predeterminado	Descripción
MEJORADO_DAR_HABILITADO	`Y` o. `N`	`N`	Especifica si la funcionalidad DAR mejorada está activada. La funcionalidad DAR mejorada es compatible con DAR de directorios y DAR de ficheros con secuencias NT. Proporciona mejoras de rendimiento. Las mejoras DE DAR durante la restauración solo son posibles si se cumplen las siguientes condiciones: • ONTAP admite DAR mejorado. • El historial de archivos está activado (HIST=y) durante la copia de seguridad. • `ndmpd.offset_map.enable`La opción se establece en `on. • La variable ENHANCED_DAR_ENABLED está definida en `Y` Durante la restauración.

Variable de entorno	Valores válidos	Predeterminado	Descripción
EXCLUIR	`pattern_string`	`none`	Especifica los archivos o directorios que se excluyen al realizar una copia de seguridad de los datos. La lista de exclusión es una lista de nombres de archivos o directorios separados por comas. Si el nombre de un archivo o directorio coincide con uno de los nombres de la lista, se excluye de la copia de seguridad. Las siguientes reglas se aplican al especificar nombres en la lista excluir: • Debe utilizarse el nombre exacto del archivo o directorio. • El asterisco (*), un carácter comodín, debe ser el primer carácter o el último de la cadena. Cada cadena puede tener hasta dos asteriscos. • Una coma en un nombre de archivo o directorio debe ir precedida de una barra invertida. • La lista de exclusión puede contener hasta 32 nombres.

Variable de entorno	Valores válidos	Predeterminado	Descripción
EXTRAER	`Y`, , `N` o. `E`	`N`	Especifica que se van a restaurar los subárboles de un conjunto de datos de copia de seguridad. La aplicación de copia de seguridad especifica los nombres de los subárboles que se van a extraer. Si un archivo especificado coincide con un directorio cuyo contenido se hizo una copia de seguridad, el directorio se extrae recursivamente. Para cambiar el nombre de un archivo, un directorio o un qtree durante la restauración sin utilizar DAR, se debe configurar la variable de entorno de EXTRACCIÓN en `E`.
EXTRAER_ACL	`Y` o. `N`	`Y`	Especifica que las ACL del archivo de copia de seguridad se restauran en una operación de restauración. El valor predeterminado es restaurar las ACL cuando se restauran los datos, excepto para DARS (DIRECT=y).

Variable de entorno	Valores válidos	Predeterminado	Descripción
FUERZA	`Y` o. `N`	`N`	Determina si la operación de restauración debe comprobar la disponibilidad de espacio de volumen y de nodos de información en el volumen de destino. Si se configura esta variable `Y`, la operación de restauración omite las comprobaciones de espacio del volumen y la disponibilidad de nodos de información en la ruta de destino. Si no hay suficiente espacio o inodos en el volumen de destino, la operación de restauración recupera la cantidad de datos permitidos por el espacio del volumen de destino y la disponibilidad de nodos de información. La operación de restauración se detiene cuando el espacio del volumen o los inodos no están disponibles.

Variable de entorno	Valores válidos	Predeterminado	Descripción
HIST	`Y` o. `N`	`N`	Especifica que la información del historial de archivos se envía a la aplicación de copia de seguridad. La mayoría de las aplicaciones de copia de seguridad comerciales establecen la variable HIST en `Y`. Si desea aumentar la velocidad de una operación de copia de seguridad o desea solucionar un problema con la recopilación de historial de archivos, puede establecer esta variable en `N`. No debe establecer la variable HIST en `Y` si la aplicación de copia de seguridad no admite el historial de archivos.

Variable de entorno	Valores válidos	Predeterminado	Descripción
IGNORE_CTIME	`Y` o. `N`	`N`	Especifica que no se realiza una copia de seguridad incremental de un archivo si sólo ha cambiado su valor ctime desde la copia de seguridad incremental anterior. Algunas aplicaciones, como el software de análisis de virus, cambian el valor de ctime de un archivo dentro del inodo, aunque el archivo o sus atributos no hayan cambiado. Como resultado, una copia de seguridad incremental puede hacer una copia de seguridad de los archivos que no han cambiado. `IGNORE_CTIME`La variable debe especificarse sólo si las copias de seguridad incrementales están tomando una cantidad inaceptable de tiempo o espacio porque se modificó el valor ctime.

Variable de entorno	Valores válidos	Predeterminado	Descripción
IGNORE_QTREES	`Y` o. `N`	`N`	Especifica que la operación de restauración no restaura la información de qtree a partir de qtrees de los que se ha realizado un backup.
NIVEL	`0-31`	`0`	Especifica el nivel de backup. El nivel 0 copia todo el conjunto de datos. Niveles de copia de seguridad incrementales, especificados por valores superiores a 0, copie todos los archivos (nuevos o modificados) desde la última copia de seguridad incremental. Por ejemplo, un nivel 1 realiza una copia de seguridad de los archivos nuevos o modificados desde la copia de seguridad de nivel 0, un nivel 2 realiza una copia de seguridad de los archivos nuevos o modificados desde la copia de seguridad de nivel 1, etc.
LISTA	`Y` o. `N`	`N`	Enumera los nombres de los archivos de backup y los números de nodos de información sin restaurar los datos realmente.
QTREES_DE_LISTAS	`Y` o. `N`	`N`	Enumera los qtrees de los que se ha realizado backup sin restaurar realmente los datos.

```
ient
e
pérd
ida
de
dato
s:
```

Variable de entorno	Valores válidos	Predeterminado	Descripción
NOMBRES DE MULTIÁRBOL_	`string`	`none`	Especifica que la copia de seguridad es una copia de seguridad de varios subárboles. Se especifican varios subárboles en la cadena, que es una lista de nombres de subárboles separados por nuevas líneas y terminados en nulo. Los subárboles se especifican mediante nombres de ruta relativos a su directorio raíz común, que deben especificarse como último elemento de la lista. Si se usa esta variable, también se debe usar la variable DMP_NAME.
NDMP_UNICODE_ FH	`Y` o. `N`	`N`	Especifica que se incluye un nombre Unicode además del nombre NFS del archivo en la información del historial de archivos. Esta opción no la utilizan la mayoría de las aplicaciones de copia de seguridad y no debe establecerse a menos que la aplicación de copia de seguridad esté diseñada para recibir estos nombres de archivo adicionales. También se debe establecer la variable HIST.
NO_ACL	`Y` o. `N`	`N`	Especifica que las ACL no se deben copiar al realizar copias de seguridad de datos.

s, que se mueven entre qtrees en origen durante

Variable de entorno	Valores válidos	Predeterminado	Descripción
ÁRBOL_NO_CUOTA	`Y` o. `N`	`N`	Especifica que los archivos y directorios en qtrees deben ignorarse al realizar una copia de seguridad de los datos. Cuando se define en `Y`, los elementos de qtrees del conjunto de datos especificado por la variable FILESYSTEM no se realizan copias de seguridad. Esta variable solo tiene un efecto si la variable FILESYSTEM especifica un volumen completo. La variable NON_QUOTA_TREE sólo funciona en una copia de seguridad de nivel 0 y no funciona si se especifica la variable MULTI_SUBTREE_NAMES. Los archivos o directorios especificados para excluirse para la copia de seguridad no se excluyen si define NON_QUOTA_TREE en `Y` simultáneamente.
NOWRITE	`Y` o. `N`	`N`	Especifica que la operación de restauración no debe escribir datos en el disco. Esta variable se utiliza para la depuración.

Variable de entorno	Valores válidos	Predeterminado	Descripción
RECURSIVA	`Y` o. `N`	`Y`	Especifica que se amplíen las entradas de directorio durante una restauración DE DAR. Las variables de entorno DIRECT y ENFOTED_DAR_ENABLED `Y` también deben estar activadas (definidas en). Si la variable RECURSIVA está desactivada (establecida en `N`), sólo los permisos y las ACL de todos los directorios de la ruta de origen original se restauran de la cinta, no del contenido de los directorios. Si la variable RECURSIVA se define en `N` o la variable RECOVER_FULL_PATH se define en `Y`, la ruta de recuperación debe terminar con la ruta de acceso original. Si la variable RECURSIVA está deshabilitada y hay más de una ruta de recuperación, todas las rutas de recuperación deben estar contenidas en el más largo de las rutas de recuperación. De lo contrario, se mostrará un mensaje de error. Por ejemplo, las siguientes son rutas de

Variable de entorno	Valores válidos	Predeterminado	Descripción
RECUPERE_FULL_PATHS	`Y` o. `N`	`N`	Especifica que la ruta de recuperación completa tendrá sus permisos y ACL restaurados después del DAR. DIRECT y ENHANCED_DAR_ENABLED `Y` también deben estar activados (definido en). Si RECOVER_FULL_PATHS está definido en `Y`, la ruta de recuperación debe terminar en la ruta original. Si ya hay directorios en el volumen de destino, sus permisos y ACL no se restaurarán a partir de la cinta.
ACTUALIZAR	`Y` o. `N`	`Y`	Actualiza la información de los metadatos para permitir la realización de backups incrementales basados EN NIVELES.

Variables de entorno compatibles con SMTape

Variable de entorno	Valores válidos	Predeterminado	Descripción
FECHA_BASE	`DUMP_DATE`	`-1`	Especifica la fecha de inicio de las copias de seguridad incrementales. `BASE_DATE` es una representación en cadena de los identificadores de instantánea de referencia. Con la `BASE_DATE` cadena, SMTape localiza la instantánea de referencia. `BASE_DATE` no es necesaria para backups de base. Para una copia de seguridad incremental, el valor de `DUMP_DATE` la variable de la línea base anterior o la copia de seguridad incremental se asigna a la `BASE_DATE` variable. La aplicación de copia de seguridad asigna `DUMP_DATE` el valor de una copia de seguridad inicial o incremental de SMTape anterior.

Variable de entorno	Valores válidos	Predeterminado	Descripción
FECHA_DE_VOLCADO	`return_value`	`none`	Al final de una copia de seguridad SMTape, DUMP_DATE contiene un identificador de cadena que identifica la instantánea utilizada para esa copia de seguridad. Esta instantánea se puede utilizar como instantánea de referencia para una copia de seguridad incremental posterior. El valor resultante de DUMP_DATE se utiliza como valor BASE_DATE para las copias de seguridad incrementales subsiguientes.
SMTAPE_BACKUP_SET_ID	`string`	`none`	Identifica la secuencia de backups incrementales asociados con el backup de referencia. El ID del conjunto de backup es un ID exclusivo de 128 bits que se genera durante una copia de seguridad de línea de base. La aplicación de copia de seguridad asigna este ID como entrada a `SMTAPE_BACKUP_SET_ID` la variable durante una copia de seguridad incremental.

Variable de entorno	Valores válidos	Predeterminado	Descripción
SMTAPE_SNAPSHOT_NAME	Cualquier snapshot válida que esté disponible en el volumen	`Invalid`	Cuando la variable SMTAPE_SNAPSHOT_NAME se define en una instantánea, esa instantánea y sus instantáneas más antiguas se realizan copias de seguridad en cinta. Para la copia de seguridad incremental, esta variable especifica la instantánea incremental. La variable BASE_DATE proporciona la instantánea de línea base.
SMTAPE_DELETE_SNAPSHOT	`Y` o. `N`	`N`	Para una instantánea creada automáticamente por SMTape, cuando la variable SMTAPE_DELETE_SNAPSHOT se define en `Y`, después de que se complete la operación de copia de seguridad, SMTape suprime esta instantánea. Sin embargo, no se eliminará una copia de Snapshot creada por la aplicación de backup.
SMTAPE_BREAK_MIRROR	`Y` o. `N`	`N`	Cuando la variable SMTAPE_BREAK_MIRROR se establece en `Y`, el volumen de tipo `DP` se cambia a un `RW` volumen después de una restauración correcta.

Obtenga información sobre las topologías comunes de respaldo en cinta NDMP de ONTAP

NDMP admite una serie de topologías y configuraciones entre aplicaciones de backup y sistemas de almacenamiento u otros servidores NDMP que proporcionan datos (sistemas de archivos) y servicios de cinta.

Del sistema de almacenamiento a la cinta local

En la configuración más simple, una aplicación de copia de seguridad realiza una copia de seguridad de los datos de un sistema de almacenamiento a un subsistema de cinta conectado al sistema de almacenamiento. La conexión de control NDMP existe en el límite de la red. La conexión de datos NDMP que existe dentro del sistema de almacenamiento entre los servicios de datos y cinta se denomina configuración local NDMP.

Sistema de almacenamiento a cinta conectado a otro sistema de almacenamiento

Una aplicación de backup también puede realizar backups de datos de un sistema de almacenamiento en una librería de cintas (un cambiador medio con una o varias unidades de cinta) conectada a otro sistema de almacenamiento. En este caso, la conexión de datos NDMP entre los servicios de datos y la cinta se proporciona mediante una conexión de red TCP o TCP/IPv6. Esto se denomina configuración de sistema de almacenamiento triple NDMP.

Librería de cintas conectada a la red y del sistema de almacenamiento

Las bibliotecas de cinta compatibles con NDMP proporcionan una variación de la configuración triple. En este caso, la biblioteca de cintas se conecta directamente a la red TCP/IP y se comunica con la aplicación de backup y el sistema de almacenamiento a través de un servidor NDMP interno.

Almacenamiento del sistema al servidor de datos, a cinta o servidor de datos al sistema de almacenamiento a cinta

NDMP también admite configuraciones triples de sistemas de almacenamiento para servidores de datos y sistemas de datos-servidor-almacenamiento, aunque estas variantes se implementan menos en gran medida. El sistema de almacenamiento al servidor permite realizar backups de los datos del sistema de almacenamiento en una biblioteca de cintas conectada al host de aplicaciones de backup o a otro sistema servidor de datos. La configuración de servidor a sistema de almacenamiento permite realizar copias de seguridad de los datos del servidor en una biblioteca de cintas conectada al sistema de almacenamiento.

Métodos de autenticación NDMP compatibles con ONTAP

Puede especificar un método de autenticación para permitir solicitudes de conexión NDMP. ONTAP es compatible con dos métodos para autenticar el acceso NDMP a un sistema de almacenamiento: Texto sin formato y el reto.

En el modo NDMP de ámbito nodo, tanto el reto como el texto sin formato están habilitados de forma predeterminada. Sin embargo, no puede desactivar el desafío. Puede activar y desactivar texto sin formato. En el método de autenticación de texto sin formato, la contraseña de inicio de sesión se transmite como texto sin cifrar.

En el modo NDMP de ámbito de la máquina virtual de almacenamiento (SVM), el método de autenticación es el reto de forma predeterminada. A diferencia del modo NDMP de ámbito de nodo, en este modo puede habilitar y deshabilitar los métodos de autenticación de texto sin formato y de desafío.

Información relacionada

Autenticación de usuario en un modo NDMP de ámbito de nodo

Autenticación de usuario en el modo NDMP con ámbito de SVM

Extensiones NDMP compatibles con ONTAP

NDMP v4 proporciona un mecanismo para crear extensiones de protocolo NDMP v4 sin tener que modificar el protocolo NDMP v4 de núcleo. Debe conocer las extensiones de

NDMP v4 compatibles con ONTAP.

Las siguientes extensiones de NDMP v4 son compatibles con ONTAP:

- Respaldo para clúster (CAB)

  Esta extensión solo es compatible con el modo NDMP con el ámbito de la SVM.

- Extensión de dirección de conexión (cae) para compatibilidad con IPv6
- Clase de extensión 0x2050

  Esta extensión admite operaciones de backup reiniciables y extensiones de administración de Snapshot.

  El `NDMP_SNAP_RECOVER` mensaje, que forma parte de las extensiones de gestión de Snapshot, se usa para iniciar una operación de recuperación y para transferir los datos recuperados de un snapshot local a una ubicación de sistema de archivos local. En ONTAP, este mensaje solo permite la recuperación de volúmenes y archivos normales.

  El `NDMP_SNAP_DIR_LIST` mensaje le permite explorar las snapshots de un volumen. Si se realiza una operación no disruptiva mientras hay una operación de exploración en curso, la aplicación de backup debe volver a iniciar la operación de exploración.

- Extensión de copia de seguridad reiniciable NDMP

  Puede utilizar la funcionalidad de extensión de backup reiniciable (RBE) de NDMP para reiniciar un backup desde un punto de control conocido en el flujo de datos antes del fallo.

Obtenga información sobre la funcionalidad DAR mejorada para ONTAP NDMP

Puede utilizar la funcionalidad DE recuperación DE acceso directo (DAR) mejorada para DAR de directorios y DAR de ficheros y secuencias NT. De forma predeterminada, la función DAR mejorada está activada.

Habilitar una funcionalidad DAR mejorada puede tener un impacto en el rendimiento de backup, ya que es necesario crear y escribir un mapa offset en cinta. Puede habilitar o deshabilitar EL DAR mejorado en los modos NDMP de ámbito de nodos y de máquinas virtuales de almacenamiento (SVM).

Límites de escalabilidad de ONTAP para sesiones NDMP

Debe tener en cuenta el número máximo de sesiones NDMP que se pueden establecer de manera simultánea en sistemas de almacenamiento de diferentes capacidades de memoria del sistema. Este número máximo depende de la memoria del sistema de un sistema de almacenamiento.

Los límites mencionados en la siguiente tabla son para el servidor NDMP. Los límites mencionados en la sección "límites de disponibilidad para sesiones de copia de seguridad y restauración de volcado" corresponden a la sesión de descarga y restauración.

Límites de escalabilidad para sesiones de backup y restauración de volcado

Memoria del sistema de un sistema de almacenamiento	Número máximo de sesiones NDMP
Menos de 16 GB	8
Mayor o igual que 16 GB pero menor que 24 GB	20
Mayor o igual que 24 GB	36

Puede obtener la memoria del sistema de su sistema de almacenamiento mediante `sysconfig -a` el comando (disponible en el infierno de nodo). Obtenga más información sobre `sysconfig -a` en el "Referencia de comandos del ONTAP".

Obtenga información sobre la compatibilidad de NDMP con volúmenes ONTAP FlexGroup

A partir de ONTAP 9.7, NDMP es compatible con los volúmenes FlexGroup.

A partir de ONTAP 9.7, se admite el comando ndmpcopy para la transferencia de datos entre volúmenes FlexVol y FlexGroup.

Si se revierte de ONTAP 9.7 a una versión anterior, la información de transferencia incremental de las transferencias anteriores no se conserva y, por lo tanto, se debe realizar una copia básica después de revertir.

A partir de ONTAP 9.8, las siguientes funciones NDMP son compatibles con los volúmenes FlexGroup:

- El mensaje NDMP_SNAP_RECOVER de la clase de extensión 0x2050 se puede utilizar para recuperar archivos individuales de un volumen FlexGroup.
- Se admite la extensión de backup NDMP restartable (RBE) para los volúmenes de FlexGroup.
- Las variables de entorno EXCLUDE y MULTI_SUBTREE_NAMES son compatibles con los volúmenes FlexGroup.

Obtenga información sobre NDMP con volúmenes SnapLock de ONTAP

La creación de varias copias de datos regulados le proporciona escenarios de recuperación redundantes y, al utilizar el volcado y la restauración NDMP, es posible conservar las características DE escritura única y lectura múltiple (WORM) de los archivos de origen en un volumen SnapLock.

Los atributos WORM de los archivos de un volumen de SnapLock se conservan al realizar backups, restaurar y copiar datos; sin embargo, los atributos WORM solo se aplican al restaurar a un volumen de SnapLock. Si se restaura un backup de un volumen SnapLock en un volumen distinto a un volumen SnapLock, se conservan los atributos WORM, pero se ignoran y ONTAP no los aplica.

Gestione el modo NDMP de ámbito del nodo para volúmenes FlexVol

Obtenga información sobre cómo administrar el modo NDMP con ámbito de nodo de ONTAP para volúmenes FlexVol

Puede administrar NDMP en el nivel de nodo mediante los comandos y las opciones de

NDMP. Puede modificar las opciones de NDMP mediante `options` el comando. Es necesario usar credenciales específicas de NDMP para acceder a un sistema de almacenamiento a fin de ejecutar operaciones de backup y restauración a cinta.

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

Comandos para administrar el modo NDMP con ámbito de nodo de ONTAP

Puede usar `system services ndmp` los comandos para gestionar NDMP a nivel de nodo. Algunos de estos comandos quedan obsoletos y se quitarán en una versión principal futura.

Puede utilizar los siguientes comandos NDMP solamente en el nivel de privilegio avanzado:

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`
- `system services ndmp log stop`

Si desea…	Se usa este comando…
Active el servicio NDMP	`system services ndmp on*`
Desactive el servicio NDMP	`system services ndmp off*`
Mostrar la configuración de NDMP	`system services ndmp show*`
Modifique la configuración de NDMP	`system services ndmp modify*`
Muestra la versión predeterminada de NDMP	`system services ndmp version*`
Mostrar la configuración del servicio NDMP	`system services ndmp service show`
Modifique la configuración del servicio NDMP	`system services ndmp service modify`
Mostrar todas las sesiones de NDMP	`system services ndmp status`
Mostrar información detallada acerca de todas las sesiones NDMP	`system services ndmp probe`
Finalice la sesión NDMP especificada	`system services ndmp kill`
Finalice todas las sesiones NDMP	`system services ndmp kill-all`

Si desea…	Se usa este comando…
Cambie la contraseña NDMP	`system services ndmp password*`
Habilite el modo de NDMP de ámbito del nodo	`system services ndmp node-scope-mode on*`
Deshabilite el modo NDMP de ámbito del nodo	`system services ndmp node-scope-mode off*`
Muestra el estado del modo NDMP de ámbito del nodo	`system services ndmp node-scope-mode status*`
Cierre todas las sesiones NDMP con fuerza	`system services ndmp service terminate`
Inicie el demonio del servicio NDMP	`system services ndmp service start`
Detenga el demonio del servicio NDMP	`system services ndmp service stop`
Inicie el registro para la sesión NDMP especificada	`system services ndmp log start*`
Detenga el registro de la sesión NDMP especificada	`system services ndmp log stop*`

- Estos comandos quedaron obsoletos y se quitarán en una versión principal futura.

Obtenga más información sobre `system services ndmp` en el "Referencia de comandos del ONTAP".

Autenticación de usuario en un modo NDMP de ámbito de nodo

En el modo NDMP de ámbito del nodo, debe utilizar credenciales específicas de NDMP para acceder a un sistema de almacenamiento a fin de realizar operaciones de backup y restauración a cinta.

El ID de usuario predeterminado es "'root'". Antes de usar NDMP en un nodo, debe asegurarse de cambiar la contraseña de NDMP predeterminada asociada con el usuario NDMP. También es posible cambiar el ID de usuario predeterminado de NDMP.

Información relacionada

Comandos para gestionar el modo NDMP de ámbito de nodo

Lo que es el modo NDMP de ámbito del nodo

Gestione el modo NDMP de ámbito SVM para volúmenes FlexVol

Obtenga información sobre cómo administrar el modo NDMP con ámbito SVM de ONTAP para volúmenes FlexVol

Puede gestionar NDMP por SVM usando las opciones y los comandos de NDMP. Puede modificar las opciones de NDMP mediante `vserver services ndmp modify` el comando. En el modo NDMP con ámbito SVM, la autenticación del usuario está

integrada con el mecanismo de control de acceso basado en roles.

Puede agregar NDMP en la lista de protocolos permitidos o no permitidos mediante `vserver modify` el comando. De forma predeterminada, NDMP se encuentra en la lista de protocolos permitidos. Si se agrega NDMP a la lista de protocolos no permitidos, no se podrán establecer sesiones NDMP.

Puede controlar el tipo de LIF en el que se establece una conexión de datos NDMP mediante `-preferred-interface-role` la opción. Durante una conexión de datos NDMP, NDMP elige una dirección IP que pertenece al tipo de LIF tal como especifica esta opción. Si las direcciones IP no pertenecen a ninguno de estos tipos de LIF, no se puede establecer la conexión de datos NDMP. Obtenga más información sobre `vserver services ndmp modify` en el "Referencia de comandos del ONTAP".

Comandos para administrar el modo NDMP con ámbito SVM de ONTAP

Puede utilizar `vserver services ndmp` los comandos para gestionar NDMP en cada máquina virtual de almacenamiento (SVM, antes denominada Vserver).

Si desea…	Se usa este comando…
Active el servicio NDMP	`vserver services ndmp on` El servicio NDMP siempre debe estar habilitado en todos los nodos de un clúster. Puede habilitar el servicio NDMP en un nodo mediante `system services ndmp on` el comando. De manera predeterminada, el servicio NDMP siempre está habilitado en un nodo.
Desactive el servicio NDMP	`vserver services ndmp off`
Mostrar la configuración de NDMP	`vserver services ndmp show`
Modifique la configuración de NDMP	`vserver services ndmp modify`
Muestra la versión NDMP predeterminada	`vserver services ndmp version`
Mostrar todas las sesiones de NDMP	`vserver services ndmp status`
Mostrar información detallada acerca de todas las sesiones NDMP	`vserver services ndmp probe`
Terminar una sesión NDMP especificada	`vserver services ndmp kill`
Finalice todas las sesiones NDMP	`vserver services ndmp kill-all`
Genere la contraseña NDMP	`vserver services ndmp generate-password`

Si desea…	Se usa este comando…
Mostrar el estado de la extensión NDMP	`vserver services ndmp extensions show` Este comando solo está disponible en el nivel de privilegios avanzado.
Modifique el estado de la extensión NDMP (enable o disable)	`vserver services ndmp extensions modify` Este comando solo está disponible en el nivel de privilegios avanzado.
Inicie el registro para la sesión NDMP especificada	`vserver services ndmp log start` Este comando solo está disponible en el nivel de privilegios avanzado.
Detenga el registro de la sesión NDMP especificada	`vserver services ndmp log stop` Este comando solo está disponible en el nivel de privilegios avanzado.

Obtenga más información sobre `vserver services ndmp` en el "Referencia de comandos del ONTAP".

Información relacionada

Comandos para gestionar el modo NDMP con ámbito de la SVM

Qué hace la extensión Cluster Aware Backup

Qué es el modo NDMP con ámbito SVM

"Administración del sistema"

Obtenga información sobre la extensión Cluster Aware Backup para ONTAP NDMP

CAB (Backup para Cluster Aware) es una extensión del protocolo NDMP v4. Esta extensión permite que el servidor NDMP establezca una conexión de datos en un nodo propietario de un volumen. Esto también permite a la aplicación de backup determinar si hay volúmenes y dispositivos de cinta ubicados en el mismo nodo de un clúster.

Para permitir que el servidor NDMP identifique el nodo propietario de un volumen y establezca una conexión de datos en dicho nodo, la aplicación de backup debe admitir la extensión CAB. La extensión CAB requiere que la aplicación de copia de seguridad informe al servidor NDMP del volumen que se va a realizar una copia de seguridad o restaurar antes de establecer la conexión de datos. Esto permite que el servidor NDMP determine el nodo que aloja el volumen y establezca la conexión de datos correctamente.

Con la extensión CAB que admite la aplicación de backup, el servidor NDMP proporciona información de afinidad acerca de los volúmenes y los dispositivos de cinta. Con esta información de afinidad, la aplicación de backup puede realizar un backup local en lugar de un backup triple si un volumen y un dispositivo de cinta están ubicados en el mismo nodo de un clúster.

Disponibilidad de volúmenes ONTAP y dispositivos de cinta para realizar copias de seguridad y restaurar en diferentes tipos de LIF

Puede configurar una aplicación de backup para establecer una conexión de control NDMP en cualquiera de los tipos de LIF de un clúster. En el modo NDMP de la máquina virtual de almacenamiento (SVM), puede determinar la disponibilidad de volúmenes y dispositivos de cinta para las operaciones de backup y restauración, en función de estos tipos de LIF y el estado de la extensión CAB.

En las siguientes tablas, se muestra la disponibilidad de volúmenes y dispositivos de cinta para los tipos de LIF de conexión de control NDMP y el estado de la extensión CAB:

La disponibilidad de volúmenes y dispositivos de cinta cuando la aplicación de backup no admite la extensión CAB

Tipo de LIF de conexión de control NDMP	Volúmenes disponibles para backup o restauración	Dispositivos de cinta disponibles para backup o restauración
LIF de gestión de nodos	Todos los volúmenes alojados por un nodo	Los dispositivos de cinta conectados al nodo que aloja el LIF de gestión del nodo
LIF de datos	Solo los volúmenes que pertenecen a la SVM alojada por un nodo que aloja la LIF de datos	Ninguno
LIF de gestión de clústeres	Todos los volúmenes alojados por un nodo que aloja el LIF de gestión de clústeres	Ninguno
LIF de interconexión de clústeres	Todos los volúmenes alojados por un nodo que aloja la LIF de interconexión de clústeres	Los dispositivos de cinta conectados al nodo que aloja la LIF de interconexión de clústeres

Disponibilidad de volúmenes y dispositivos de cinta cuando la aplicación de backup admite la extensión CAB

Tipo de LIF de conexión de control NDMP	Volúmenes disponibles para backup o restauración	Dispositivos de cinta disponibles para backup o restauración
LIF de gestión de nodos	Todos los volúmenes alojados por un nodo	Los dispositivos de cinta conectados al nodo que aloja el LIF de gestión del nodo
LIF de datos	Todos los volúmenes que pertenecen a la SVM que aloja la LIF de datos	Ninguno
LIF de gestión de clústeres	Todos los volúmenes del clúster	Todos los dispositivos de cinta del cluster

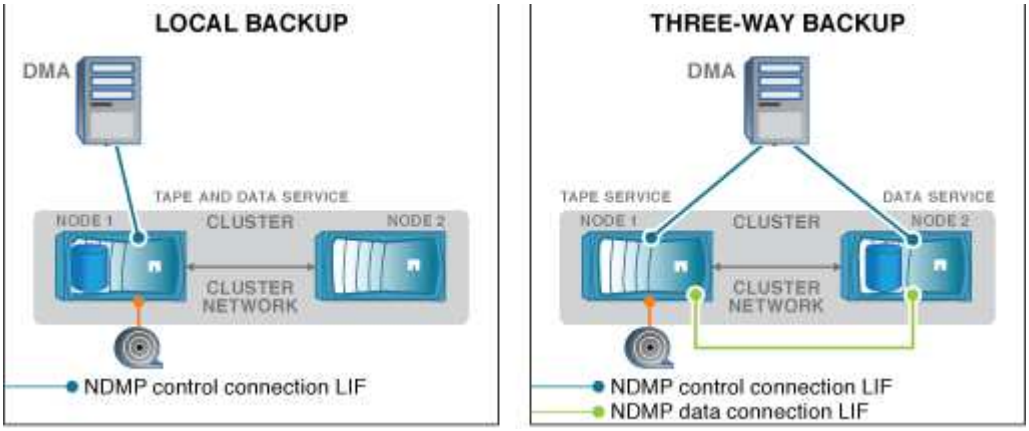
Tipo de LIF de conexión de control NDMP	Volúmenes disponibles para backup o restauración	Dispositivos de cinta disponibles para backup o restauración
LIF de interconexión de clústeres	Todos los volúmenes del clúster	Todos los dispositivos de cinta del cluster

Obtenga información sobre la afinidad de ONTAP NDMP

Una vez que la aplicación de backup se detecta EN CABINA, el servidor NDMP proporciona información única sobre la ubicación de los volúmenes y los dispositivos de cinta. Mediante el uso de esta información de afinidad, la aplicación de backup puede realizar un backup local en lugar de un backup triple si un volumen y un dispositivo de cinta comparten la misma afinidad.

Si la conexión de control NDMP se establece en una LIF de gestión de nodos, LIF de gestión de clústeres, O mediante LIF de interconexión de clústeres, la aplicación de backup puede usar la información de afinidad para determinar si un volumen y un dispositivo de cinta están ubicados en el mismo nodo y, a continuación, realizar una operación de backup o restauración local o triple. Si la conexión del control NDMP se establece en una LIF de datos, la aplicación de backup siempre realiza un backup triple.

Backup NDMP local y backup NDMP triple



Mediante la información de afinidad con los volúmenes y los dispositivos de cinta, DMA (aplicación de backup) realiza un backup NDMP local en el volumen y el dispositivo de cinta ubicados en el nodo 1 del clúster. Si el volumen se mueve del nodo 1 al nodo 2, cambia la información de afinidad sobre el volumen y el dispositivo de cinta. Por lo tanto, para un backup posterior, DMA realiza una operación de backup NDMP triple. De este modo se garantiza la continuidad de la política de backup del volumen independientemente del nodo al que se traslade el volumen.

Información relacionada

Qué hace la extensión Cluster Aware Backup

El servidor NDMP admite conexiones de control ONTAP seguras en modo de ámbito SVM

Se puede establecer una conexión de control segura entre la aplicación de administración de datos (DMA) y el servidor NDMP utilizando sockets seguros (SSL/TLS) como mecanismo de comunicación. Esta comunicación SSL se basa en los certificados del servidor. El servidor NDMP escucha en el puerto 30000 (asignado por IANA para el

servicio "'ndmps'").

Tras establecer la conexión desde el cliente en este puerto, el protocolo de enlace SSL estándar se produce cuando el servidor presenta el certificado al cliente. Cuando el cliente acepta el certificado, se completa el apretón de manos SSL. Una vez completado este proceso, toda la comunicación entre el cliente y el servidor se cifra. El flujo de trabajo del protocolo NDMP sigue siendo exactamente igual que antes. La conexión NDMP segura sólo requiere autenticación de certificado del servidor. Un DMA puede optar por establecer una conexión mediante la conexión al servicio NDMP seguro o al servicio NDMP estándar.

De manera predeterminada, el servicio NDMP seguro está deshabilitado para una máquina virtual de almacenamiento (SVM). Puede habilitar o deshabilitar el servicio NDMP seguro en una SVM determinada mediante `vserver services ndmp modify -vserver vserver -is-secure-control -connection-enabled [true|false]` el comando.

Tipos de conexión de datos NDMP ONTAP

En el modo NDMP de la máquina virtual de almacenamiento (SVM), los tipos de conexión de datos NDMP admitidos dependen del tipo de LIF de conexión de control NDMP y el estado de la extensión CAB. Este tipo de conexión de datos NDMP indica si se puede ejecutar una operación de backup o restauración NDMP local o triple.

Puede realizar un backup o una operación de restauración NDMP triple a través de una red TCP o TCP/IPv6. En las siguientes tablas, se muestran los tipos de conexión de datos NDMP según el tipo de LIF de conexión de control NDMP y el estado de la extensión CAB.

Tipo de conexión de datos NDMP cuando la aplicación de backup admite una extensión CAB

Tipo de LIF de conexión de control NDMP	Tipo de conexión de datos NDMP
LIF de gestión de nodos	LOCAL, TCP Y TCP/IPV6
LIF de datos	TCP/TCP
LIF de gestión de clústeres	LOCAL, TCP Y TCP/IPV6
LIF de interconexión de clústeres	LOCAL, TCP Y TCP/IPV6

Tipo de conexión de datos NDMP cuando la aplicación de backup no admite la extensión CAB

Tipo de LIF de conexión de control NDMP	Tipo de conexión de datos NDMP
LIF de gestión de nodos	LOCAL, TCP Y TCP/IPV6
LIF de datos	TCP/TCP
LIF de gestión de clústeres	TCP/TCP
LIF de interconexión de clústeres	LOCAL, TCP Y TCP/IPV6

Información relacionada

Qué hace la extensión Cluster Aware Backup

"Gestión de redes"

Autenticación de usuarios de ONTAP en el modo NDMP con ámbito SVM

En el modo NDMP de la máquina virtual de almacenamiento (SVM), la autenticación de usuario NDMP está integrada con el control de acceso basado en roles. En el contexto de la SVM, el usuario NDMP debe tener el rol "'vsadmin'" o "'vsadmin-backup'". En un contexto de cluster, el usuario NDMP debe tener el rol «'admin'» o «'backup'».

Además de estas funciones predefinidas, una cuenta de usuario asociada a una función personalizada también puede utilizarse para la autenticación NDMP siempre y cuando la función personalizada tenga la carpeta «'vserver Services ndmp'» en su directorio de comandos y el nivel de acceso de la carpeta no sea «'none'». En este modo, debe generar una contraseña NDMP para una cuenta de usuario determinada, que se crea mediante el control de acceso basado en roles. Los usuarios de clúster con un rol de administrador o backup pueden acceder a una LIF de gestión de nodos, una LIF de gestión de clústeres o una LIF de interconexión de clústeres. Los usuarios de un rol de vsadmin o de vsadmin pueden acceder solo a la LIF de datos para esa SVM. Por lo tanto, según la función de un usuario, la disponibilidad de volúmenes y dispositivos de cinta para las operaciones de backup y restauración varía.

Este modo también admite la autenticación de usuario para usuarios NIS y LDAP. Por lo tanto, los usuarios NIS y LDAP pueden acceder a varias SVM con un ID de usuario y una contraseña comunes. Sin embargo, la autenticación NDMP no admite usuarios de Active Directory.

En este modo, una cuenta de usuario debe estar asociada a la aplicación SSH y al método de autenticación «'Contraseña de usuario'».

Información relacionada

Comandos para gestionar el modo NDMP con ámbito de la SVM

"Administración del sistema"

Generar una contraseña específica de NDMP para los usuarios de ONTAP NDMP

En el modo NDMP de la máquina virtual de almacenamiento (SVM), debe generar una contraseña para un ID de usuario específico. La contraseña generada se basa en la contraseña de inicio de sesión real para el usuario NDMP. Si cambia la contraseña de inicio de sesión real, deberá generar de nuevo la contraseña específica de NDMP.

Pasos

1. Utilice `vserver services ndmp generate-password` el comando para generar una contraseña específica de NDMP.

   Puede utilizar esta contraseña en cualquier operación NDMP actual o futura que requiera la introducción de la contraseña.

   Desde el contexto de la máquina virtual de almacenamiento (SVM, antes denominada Vserver), puede generar contraseñas de NDMP para usuarios que solo pertenecen a esa SVM.

El ejemplo siguiente muestra cómo generar una contraseña específica de NDMP para un ID de usuario usuario1:

```
cluster1::vserver services ndmp> generate-password -vserver vs1 -user
user1

Vserver: vs1
User: user1
Password: jWZiNt57huPOoD8d
```

2. Si cambia la contraseña a su cuenta de sistema de almacenamiento normal, repita este procedimiento para obtener su nueva contraseña específica de NDMP.

Cómo se ven afectadas las operaciones de copia de seguridad y restauración en cinta durante la recuperación ante desastres en las configuraciones de ONTAP MetroCluster

Se pueden ejecutar operaciones de backup y restauración a cinta simultáneamente durante la recuperación ante desastres en una configuración de MetroCluster. Debe entender cómo se ven afectadas estas operaciones durante la recuperación de desastres.

Si las operaciones de backup y restauración de cinta se llevan a cabo en un volumen de anSVM en una relación de recuperación ante desastres, puede continuar con las operaciones de backup y restauración de cinta incrementales después de una conmutación de sitios y conmutación de estado.

Acerca del motor de volcado para volúmenes FlexVol

Obtenga información sobre el motor de volcado ONTAP para volúmenes FlexVol

Dump es una solución de copia de seguridad y recuperación basada en instantáneas de ONTAP que le ayuda a realizar copias de seguridad de archivos y directorios desde una instantánea a un dispositivo de cinta y restaurar los datos de los que se ha realizado la copia de seguridad en un sistema de almacenamiento.

Puede realizar una copia de seguridad de los datos del sistema de archivos, como directorios, archivos y su configuración de seguridad asociada, en un dispositivo de cinta mediante la copia de seguridad de volcado. Puede realizar backup de un volumen completo, de un qtree completo o de un subárbol que no sea ni un volumen completo ni un qtree completo.

Puede realizar un backup o una restauración de volcado utilizando aplicaciones de backup compatibles con NDMP.

Al realizar una copia de seguridad de volcado, puede especificar la instantánea que se utilizará para una copia de seguridad. Si no se especifica una instantánea para la copia de seguridad, el motor de volcado crea una instantánea para la copia de seguridad. Una vez finalizada la operación de copia de seguridad, el motor de volcado elimina esta instantánea.

Puede realizar copias de seguridad de nivel 0, incrementales o diferenciales en cinta utilizando el motor de descarga.

Después de revertir a una versión anterior a Data ONTAP 8.3, debe ejecutar una operación de backup base antes de realizar una operación de backup incremental.

Información relacionada

"Actualización, reversión o degradación"

Cómo funciona una copia de seguridad de volcado con ONTAP NDMP

Una copia de seguridad de volcado escribe los datos del sistema de archivos del disco a la cinta mediante un proceso predefinido. Puede realizar un backup de un volumen, un qtree o un subárbol que no sea ni un volumen completo ni un qtree completo.

En la siguiente tabla se describe el proceso que ONTAP utiliza para realizar un backup del objeto indicado por la ruta de volcado:

Etapa	Acción
1	Para un volumen completo menor que los backups qtree o los backups completos de qtree, ONTAP atraviesa directorios para identificar los archivos en los que se va a realizar el backup. Si va a realizar el backup de un volumen o qtree completo, ONTAP combina esta fase con la fase 2.
2	Para un backup de volumen completo o de qtree completo, ONTAP identifica los directorios en los volúmenes o qtrees de los que se va a realizar un backup.
3	ONTAP escribe los directorios en la cinta.
4	ONTAP escribe los archivos en la cinta.
5	ONTAP escribe la información de ACL (si corresponde) en la cinta.

La copia de seguridad de volcado utiliza una instantánea de los datos para la copia de seguridad. Por lo tanto, no es necesario desconectar el volumen antes de iniciar el backup.

La copia de seguridad de volcado asigna un nombre a cada instantánea que crea `snapshot_for_backup.n`, donde `n` es un entero que comienza en 0. Cada vez que la copia de seguridad de volcado crea una instantánea, aumenta el entero en 1. El entero se restablece a 0 después de reiniciar el sistema de almacenamiento. Una vez finalizada la operación de copia de seguridad, el motor de volcado elimina esta instantánea.

Cuando ONTAP realiza varios backups de volcado de forma simultánea, el motor de volcado crea varias instantáneas. Por ejemplo, si ONTAP ejecuta dos backups de volcado simultáneamente, encontrará las siguientes snapshots en los volúmenes de los cuales se realizan backups de datos: `snapshot_for_backup.0` Y `snapshot_for_backup.1`.

Cuando se realiza una copia de seguridad desde una instantánea, el motor de volcado no crea una instantánea adicional.

Tipos de datos de los que el motor de descarga realiza una copia de seguridad

El motor de volcado permite lanzar backups de los datos a cinta como protección ante desastres o interrupciones en la controladora. Además de realizar backups de objetos de datos como archivos, directorios, qtrees o volúmenes completos, el motor de volcado puede realizar backups de muchos tipos de información acerca de cada archivo. Conocer los tipos de datos que el motor de volcado puede realizar y las restricciones que se deben tener en cuenta puede ayudarle a planificar su método de recuperación ante desastres.

Además de realizar una copia de seguridad de los datos de los archivos, el motor de volcado puede realizar una copia de seguridad de la siguiente información acerca de cada archivo, según corresponda:

- GID de UNIX, UID del propietario y permisos de archivo
- Acceso UNIX, creación y tiempo de modificación
- Tipo de archivo
- Tamaño de archivo
- Nombre dos, atributos dos y hora de creación
- Listas de control de acceso (ACL) con 1,024 entradas de control de acceso (ACE)
- Información de Qtree
- Rutas de unión

Las rutas de unión se copian como enlaces simbólicos.

- Clones LUN y LUN

  Puede realizar backups de un objeto de LUN completo; sin embargo, no puede realizar backups de un único archivo dentro del objeto LUN. De igual modo, puede restaurar un objeto de LUN completo, pero no un solo archivo dentro de la LUN.

  > El motor de volcado realiza una copia de seguridad de los clones de LUN como LUN independientes.

- Archivos alineados con equipos virtuales

  Las versiones anteriores a Data ONTAP 8.1.2 no admiten la copia de seguridad de archivos alineados con equipos virtuales.

> Cuando se realiza la transición de un clon de LUN respaldado por snapshots de Data ONTAP operativo en 7-Mode a ONTAP, se convierte en una LUN inconsistente. El motor de volcado no realiza copias LUN incoherentes.

Cuando restaura datos en un volumen, las operaciones de I/o del cliente están restringidas en las LUN que se restauran. La restricción de LUN se elimina solo cuando se completa la operación de restauración de volcado. De forma similar, durante una operación de restauración de archivos o LUN únicos de SnapMirror, las I/o del cliente están restringidas a ambos archivos y LUN que se van a restaurar. Esta restricción se elimina solo cuando se completa la operación de restauración de archivos o LUN. Si se realiza un backup de volcado en un volumen en el que se está realizando una operación de restauración de volcado o restauración de archivo único de SnapMirror o LUN, los archivos o LUN que tienen restricción de I/o del cliente no se incluyen en el backup. Estos archivos o LUN se incluyen en una operación de copia de seguridad posterior si la restricción de I/o del cliente se elimina.

Una LUN que se ejecute en Data ONTAP 8.3 y que se realice un backup a cinta solo se podrá restaurar a las versiones 8.3 y posteriores, y no a una versión anterior. Si la LUN se restaura a una versión anterior, la LUN se restaura como un archivo.

Cuando se realiza un backup de un volumen secundario de SnapVault o de un destino de SnapMirror para volúmenes a cinta, solo se realiza un backup de los datos del volumen. No se realiza un backup de los metadatos asociados. Por lo tanto, cuando intenta restaurar el volumen, solo se restauran los datos de ese volumen. La información sobre las relaciones de SnapMirror para volúmenes no está disponible en el backup y, por lo tanto, no se restaura.

Si vuelca un archivo que sólo tiene permisos de Windows NT y lo restaura a un qtree o volumen de estilo UNIX, el archivo obtiene los permisos UNIX predeterminados para ese qtree o volumen.

Si vuelca un archivo que solo tiene permisos de UNIX y lo restaura a un qtree o volumen de estilo NTFS, el archivo obtiene los permisos de Windows predeterminados para ese qtree o volumen.

Otros volcados y restauraciones conservan los permisos.

Puede realizar backups de los archivos alineados con la máquina virtual y la `vm-align-sector` opción. Para obtener más información sobre los archivos alineados con VM, consulte "Gestión de almacenamiento lógico".

Obtenga información sobre las cadenas de incremento y ONTAP NDMP

Una cadena de incremento es una serie de copias de seguridad incrementales de la misma ruta. Como puede especificar cualquier nivel de backup en cualquier momento, debe comprender las cadenas de incremento para poder realizar backups y restauraciones de manera efectiva. Es posible ejecutar 31 niveles de operaciones de backup incrementales.

Existen dos tipos de cadenas de incremento:

- Una cadena de incremento consecutiva, que es una secuencia de backups incrementales que comienza con el nivel 0 y se eleva por 1 en cada backup posterior.
- Una cadena de incremento no consecutiva, donde las copias de seguridad incrementales omiten niveles o tienen niveles que están fuera de secuencia, como 0, 2, 3, 1, 4 o más comúnmente 0, 1, 1, 1 o 0, 1, 2, 1, 2.

Los backups incrementales se basan en los backups más recientes de bajo nivel. Por ejemplo, la secuencia de niveles de backup 0, 2, 3, 1, 4 proporciona dos cadenas de incremento: 0, 2, 3 y 0, 1, 4. La siguiente tabla explica las bases de los backups incrementales:

Orden de copia de seguridad	Incrementar el nivel	Cadena de incremento	Base	Archivos de copia de seguridad
1	0	Ambas	De los archivos del sistema de almacenamiento	Todos los archivos de la ruta de copia de seguridad

Orden de copia de seguridad	Incrementar el nivel	Cadena de incremento	Base	Archivos de copia de seguridad
2	2	0, 2, 3	Backup de nivel 0	Archivos en la ruta de copia de seguridad creada desde la copia de seguridad de nivel 0
3	3	0, 2, 3	Backup de nivel 2	Archivos en la ruta de copia de seguridad creada desde la copia de seguridad de nivel 2
4	1	0, 1, 4	Backup de nivel 0, porque es el nivel más reciente inferior al backup de nivel 1	Archivos en la ruta de copia de seguridad creados desde la copia de seguridad de nivel 0, incluidos los archivos que se encuentran en las copias de seguridad de nivel 2 y nivel 3
5	4	0, 1, 4	El backup de nivel 1, porque es un nivel inferior y es más reciente que los backups de nivel 0, nivel 2 o nivel 3	Archivos creados desde la copia de seguridad de nivel 1

Obtenga más información sobre el factor de bloqueo y ONTAP NDMP

Un bloque de cinta es 1,024 bytes de datos. Durante un backup o una restauración de cinta, es posible especificar la cantidad de bloques de cinta que se transfieren en cada operación de lectura/escritura. Este número se llama el *factor de bloqueo*.

Puede utilizar un factor de bloqueo de 4 a 256. Si tiene previsto restaurar una copia de seguridad en un sistema distinto al del que hizo la copia de seguridad, el sistema de restauración debe admitir el factor de bloqueo que se utilizó para la copia de seguridad. Por ejemplo, si se utiliza un factor de bloqueo de 128, el sistema en el que se restaura ese backup debe admitir un factor de bloqueo de 128.

Durante una copia de seguridad NDMP, EL OBJETO MOVER_RECORD_SIZE determina el factor de bloqueo. ONTAP permite un valor máximo de 256 KB para MOVER_RECORD_SIZE.

Cuándo reiniciar una copia de seguridad de volcado de ONTAP

En ocasiones, un backup de volcado no finaliza a causa de errores internos o externos, como errores de escritura en cinta, interrupciones del suministro eléctrico, interrupciones

accidentales de los usuarios o incoherencias internas en el sistema de almacenamiento. Si falla el backup por uno de estos motivos, puede reiniciarlo.

Puede optar por interrumpir y reiniciar un backup para evitar periodos de gran tráfico en el sistema de almacenamiento o competir por otros recursos limitados del sistema de almacenamiento, como una unidad de cinta. Puede interrumpir una copia de seguridad larga y reiniciarla más tarde si una restauración (o copia de seguridad) más urgente requiere la misma unidad de cinta. Los backups reiniciables persisten durante los reinicios. Sólo puede reiniciar una copia de seguridad anulada en cinta si se cumplen las siguientes condiciones:

- La copia de seguridad anulada se encuentra en la fase IV
- Todas las instantáneas asociadas bloqueadas por el comando dump están disponibles.
- El historial de archivos debe estar activado.

Cuando dicha operación de volcado se anula y se deja en un estado reiniciable, las instantáneas asociadas se bloquean. Estas copias de Snapshot se liberan una vez que se elimina el contexto de backup. Puede ver la lista de contextos de copia de seguridad mediante el `vserver services ndmp restartable backup show` comando.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                   Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Auto-created?: true
                    Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                    Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

Cómo funciona una restauración de volcado con ONTAP NDMP

Una restauración de volcado escribe los datos del sistema de archivos de una cinta a un disco mediante un proceso predefinido.

El proceso de la siguiente tabla muestra el funcionamiento de la restauración de volcado:

Etapa	Acción
1	ONTAP cataloga los archivos que deben extraerse de la cinta.
2	ONTAP crea directorios y archivos vacíos.

Etapa	Acción
3	ONTAP lee un archivo desde una cinta, lo escribe en el disco y establece los permisos (incluidas las ACL) en él.
4	ONTAP repite las fases 2 y 3 hasta que todos los archivos especificados se copien de la cinta.

Tipos de datos que restaura el motor de volcado

Cuando se produce un desastre o una interrupción de la controladora, el motor de volcado ofrece diversos métodos para recuperar todos los datos de los que se hizo backup, desde archivos individuales a atributos de archivo, a directorios completos. Conocer los tipos de datos que el motor de volcado puede restaurar y cuándo utilizar qué método de recuperación puede ayudar a minimizar el tiempo de inactividad.

Puede restaurar datos a una LUN asignada en línea. Sin embargo, las aplicaciones host no pueden acceder a esta LUN hasta que se complete la operación de restauración. Una vez finalizada la operación de restauración, la caché del host de los datos de LUN se debe vaciar para ofrecer coherencia con los datos restaurados.

El motor de descarga puede recuperar los siguientes datos:

- Contenido de los archivos y directorios
- Permisos de archivos UNIX
- ACL

  Si restaura un archivo que solo tiene permisos de archivo UNIX a un qtree o volumen NTFS, el archivo no tiene ACL de Windows NT. El sistema de almacenamiento utiliza sólo los permisos de archivo UNIX en este archivo hasta que se crea una ACL de Windows NT en él.

  > Si restaura ACL respaldados de sistemas de almacenamiento que ejecutan Data ONTAP 8.2 a sistemas de almacenamiento que ejecutan Data ONTAP 8.1.x y versiones anteriores que tienen un límite de ACE inferior a 1,024, se restaura una ACL predeterminada.

- Información de Qtree

  La información de qtree se utiliza solo si un qtree se restaura en la raíz de un volumen. La información de qtree no se utiliza si se restaura un qtree en un directorio inferior, `/vs1/vol1/subdir/lowerdir` como , y deja de ser un qtree.

- Todos los demás atributos de archivo y directorio
- Secuencias de Windows NT
- LUN
  - Es necesario restaurar una LUN a nivel de volumen o un nivel de qtree para que permanezca como una LUN.

    Si se restaura a un directorio, se restaura como un archivo porque no contiene metadatos válidos.

  - Un LUN de 7-Mode se restaura como LUN en un volumen ONTAP.
- Un volumen de 7-Mode se puede restaurar en un volumen de ONTAP.

- Los archivos alineados con máquinas virtuales restaurados en un volumen de destino heredan las propiedades de alineación de máquinas virtuales del volumen de destino.
- El volumen de destino de una operación de restauración puede tener archivos con bloqueos obligatorios o de asesoramiento.

  Mientras se realiza una operación de restauración en dicho volumen de destino, el motor de volcado ignora estos bloqueos.

Consideraciones antes de restaurar datos con ONTAP NDMP

Puede restaurar los datos de los que se ha realizado una copia de seguridad en su ruta original o en otro destino. Si va a restaurar datos con un backup en otro destino, debe preparar el destino para la operación de restauración.

Antes de restaurar datos en su ruta original o en un destino diferente, debe disponer de la siguiente información y cumplir los requisitos siguientes:

- El nivel de la restauración
- La ruta a la que se van a restaurar los datos
- El factor de bloqueo utilizado durante el backup
- Si realiza una restauración incremental, todas las cintas deben estar en la cadena de backup
- Una unidad de cinta disponible y compatible con la cinta a restaurar

Antes de restaurar los datos en otro destino, debe ejecutar las operaciones siguientes:

- Si va a restaurar un volumen, debe crear un volumen nuevo.
- Si va a restaurar un qtree o un directorio, debe cambiar el nombre de los archivos que probablemente tengan los mismos nombres que los archivos que va a restaurar.

> En ONTAP 9, los nombres de qtree admiten el formato Unicode. Las versiones anteriores de ONTAP no admiten este formato. Si un qtree con nombres Unicode en ONTAP 9 se copia en una versión anterior de ONTAP `ndmpcopy` mediante el comando o mediante la restauración de una imagen de backup en una cinta, el qtree se restaura como un directorio normal y no como un qtree con formato Unicode.

> Si un archivo restaurado tiene el mismo nombre que un archivo existente, el archivo existente se sobrescribe con el archivo restaurado. Sin embargo, los directorios no se sobrescriben.

Para cambiar el nombre de un archivo, un directorio o un qtree durante la restauración sin utilizar DAR, se debe configurar la variable de entorno de EXTRACCIÓN en `E`.

Espacio requerido en el sistema de almacenamiento de destino

Necesita aproximadamente 100 MB de espacio en el sistema de almacenamiento de destino que la cantidad de datos que se van a restaurar.

La operación de restauración comprueba la disponibilidad de espacio de los volúmenes y de nodos de información en el volumen de destino cuando se inicia la operación de restauración. Configurar la variable de entorno FORCE como `Y` provoca que la operación de restauración omita las comprobaciones de espacio del volumen y de disponibilidad de nodos en la ruta de destino. Si no hay suficiente espacio o inodos disponibles en el volumen de destino, la operación de restauración recupera la cantidad de datos permitidos por el espacio del volumen de destino y la disponibilidad del inodo. La operación de restauración se detiene cuando no queda más espacio del volumen o inodos.

Límites de escalabilidad para sesiones de copia de seguridad y restauración de volcado de ONTAP

Es necesario conocer la cantidad máxima de sesiones de backup y restauración de volcado que se pueden ejecutar simultáneamente en sistemas de almacenamiento de diferentes capacidades de memoria del sistema. Este número máximo depende de la memoria del sistema de un sistema de almacenamiento.

Los límites mencionados en la tabla siguiente son para el motor de descarga o restauración. Los límites mencionados en los límites de escalabilidad para las sesiones NDMP son para el servidor NDMP, que son más altos que los límites del motor.

Memoria del sistema de un sistema de almacenamiento	Cantidad total de sesiones de backup y restauración de volcado
Menos de 16 GB	4
Mayor o igual que 16 GB pero menor que 24 GB	16
Mayor o igual que 24 GB	32

Si se utiliza `ndmpcopy` el comando para copiar datos dentro de los sistemas de almacenamiento, se establecen dos sesiones NDMP: Una para el backup de volcado y otra para la restauración de volcado.

Puede obtener la memoria del sistema de su sistema de almacenamiento mediante `sysconfig -a` el comando (disponible en el infierno de nodo). Obtenga más información sobre `sysconfig -a` en el "Referencia de comandos del ONTAP".

Información relacionada

Límites de escalabilidad para sesiones NDMP

Elimine los contextos reiniciables proporcionando el nombre de ONTAP SVM y el ID del contexto

Si desea iniciar un backup en lugar de reiniciar un contexto, puede eliminar el contexto.

Acerca de esta tarea

Puede suprimir un contexto reiniciable mediante el `vserver services ndmp restartable-backup delete` comando proporcionando el nombre de SVM y el identificador de contexto.

Pasos

1. Eliminar un contexto reiniciable:

   vserver services ndmp restartable-backup delete -vserver *vserver-name* -context -id *context_identifier*.

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                  Is Cleanup Pending?
----------- ----------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                  Is Cleanup Pending?
----------- ----------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

Cómo funciona el volcado en un volumen secundario de ONTAP SnapVault

Es posible realizar operaciones de backup a cinta en datos que estén reflejados en el volumen secundario de SnapVault. Puede realizar un backup únicamente de los datos que se reflejan en el volumen secundario de SnapVault a cinta, y no los metadatos de la relación de SnapVault.

Cuando (`snapmirror break`se interrumpe la relación de reflejo de protección de datos) o cuando se produce una resincronización de SnapMirror, siempre debe ejecutar un backup de referencia.

Información relacionada

- "rotura de snapmirror"

Cómo funciona el volcado con la conmutación por error del almacenamiento de ONTAP y las operaciones ARL

Antes de ejecutar operaciones de backup de volcado o restauración, debe comprender cómo funcionan estas operaciones con las operaciones de conmutación por error (toma de control y devolución) de almacenamiento o reubicación de agregados (ARL). `-override-vetoes`La opción determina el comportamiento del motor de volcado durante una operación de failover de almacenamiento o ARL.

Cuando se está ejecutando una operación de copia de seguridad o restauración de volcado y la `-override-vetoes` opción se define en `false`, se detiene una operación de conmutación por error de almacenamiento iniciada por el usuario o ARL. Sin embargo, si la `-override-vetoes` opción está definida en `true`, la operación de failover de almacenamiento o ARL continuará y se anulará la operación de copia de seguridad o restauración de volcado. Cuando el sistema de almacenamiento inicia automáticamente una conmutación por error o una operación de ARL del almacenamiento, siempre se cancela una operación de backup o restauración de volcado activa. No es posible reiniciar las operaciones de volcado de backup y restauración incluso después de la conmutación por error de almacenamiento o de la finalización de las operaciones de ARL.

Operaciones de descarga cuando se admite la extensión DE LA CABINA

Si la aplicación de backup admite la extensión CAB, puede seguir realizando operaciones de backup de volcado y restauración incrementales sin tener que volver a configurar las políticas de backup tras una conmutación por error del almacenamiento o una operación ARL.

Operaciones de volcado cuando la extensión DE LA CABINA no es compatible

Si la aplicación de backup no admite la extensión CAB, puede seguir realizando operaciones de backup y restauración de volcado incrementales si migra la LIF configurada en la política de backup al nodo que aloja el agregado de destino. De lo contrario, una vez realizada la conmutación por error del almacenamiento y la operación ARL, debe realizar un backup básico antes de realizar la operación de backup incremental.

> Para las operaciones de recuperación tras fallos de almacenamiento, el LIF configurado en la política de backup se debe migrar al nodo compañero.

Información relacionada

"Alta disponibilidad"

Cómo funciona el volcado con el movimiento de volumen de ONTAP

El sistema de almacenamiento puede ejecutar en paralelo las operaciones de backup y restauración de cinta y el movimiento de volúmenes hasta que el sistema de almacenamiento intente la fase final de transposición. Una vez completada esta fase, no se permiten nuevas operaciones de backup y restauración en cinta en el volumen que se mueve. No obstante, las operaciones actuales siguen en ejecución hasta que se complete.

En la siguiente tabla se describe el comportamiento de las operaciones de backup a cinta y restauración después de la operación de movimiento de volúmenes:

Si realiza operaciones de backup y restauración en cinta en…	Realice lo siguiente…
La aplicación de backup admite la extensión CAB del modo NDMP de las máquinas virtuales de almacenamiento (SVM)	Puede seguir realizando operaciones incrementales de backup a cinta y restauración en volúmenes de lectura/escritura y solo lectura sin tener que reconfigurar las políticas de backup.

Si realiza operaciones de backup y restauración en cinta en…	Realice lo siguiente…
El modo NDMP con ámbito SVM cuando la aplicación de backup no admite la extensión CAB	Puede seguir realizando operaciones incrementales de backup a cinta y restauración en volúmenes de lectura/escritura y solo lectura si migra la LIF configurada en la política de backup al nodo que aloja el agregado de destino. De lo contrario, después del movimiento de volumen, debe ejecutar un backup básico antes de ejecutar la operación de backup incremental.

Cuando se produce un movimiento de volúmenes, si el volumen que pertenece a una SVM diferente del nodo de destino tiene el mismo nombre que el del volumen movido, no se pueden ejecutar operaciones de backup incrementales del volumen movido.

Cómo funciona el volcado cuando un FlexVol volume ONTAP FlexVol está lleno

Antes de realizar una operación de backup de volcado incremental, debe asegurarse de que haya suficiente espacio libre en el volumen FlexVol.

Si se produce un error en la operación, debe aumentar el espacio libre del volumen Flex Vol aumentando su tamaño o eliminando las snapshots. A continuación, vuelva a realizar la operación de copia de seguridad incremental.

Cómo funciona el volcado cuando cambia el tipo de acceso a un volumen ONTAP

Cuando un volumen de destino de SnapMirror o un volumen secundario de SnapVault cambian el estado de lectura/escritura a solo lectura o de solo lectura a lectura/escritura, se debe ejecutar una operación de backup o restauración de cinta de referencia.

Los volúmenes secundarios de destino de SnapMirror y SnapVault son volúmenes de solo lectura. Si realiza operaciones de backup y restauración de cinta en dichos volúmenes, se debe ejecutar una operación de backup o restauración de línea base siempre que el volumen cambie el estado de solo lectura a lectura/escritura o de lectura/escritura a solo lectura.

Cómo funciona el volcado con una restauración de un solo archivo o LUN de ONTAP SnapMirror

Antes de realizar operaciones de volcado de backup o restauración en un volumen en el que se restaura un solo archivo o LUN mediante la tecnología SnapMirror, debe entender cómo funcionan las operaciones de volcado con una sola operación de restauración de archivos o LUN.

Durante una operación de restauración de un único archivo o LUN de SnapMirror, las I/o del cliente están restringidas en el archivo o LUN que se van a restaurar. Cuando la operación de restauración de archivos o LUN individuales finaliza, se elimina la restricción de I/o del archivo o LUN. Si se realiza un backup de volcado en un volumen para el que se restaura un solo archivo o LUN, el archivo o el LUN que tiene restricción de I/o del cliente no se incluye en el backup de volcado. En una operación de copia de seguridad posterior, se realiza una copia de seguridad de este archivo o LUN en cinta después de eliminar la restricción de E/S.

No se puede realizar una restauración de volcado y una operación de restauración de archivos o LUN de

SnapMirror simultáneamente en el mismo volumen.

Cómo se ven afectadas las operaciones de copia de seguridad y restauración de volcado en las configuraciones de ONTAP MetroCluster

Antes de llevar a cabo operaciones de backup de volcado y restauración en una configuración de MetroCluster, debe comprender cómo se ven afectadas las operaciones de volcado cuando se produzca una operación de conmutación de sitios o conmutación de estado.

Operación de copia de seguridad o restauración de volcado seguida de la conmutación

Considere dos clústeres: El clúster 1 y el clúster 2. Durante una operación de backup de volcado o restauración en el clúster 1, si se inicia una conmutación por error desde el clúster 1 al clúster 2, se produce lo siguiente:

- Si el valor de `override-vetoes` la opción es `false`, el switchover se anula y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, la operación de copia de seguridad de volcado o restauración se anula y el switchover continúa.

Operación de copia de seguridad o restauración de volcado seguida de una conmutación de estado

Una conmutación de sitios se realiza desde el clúster 1 al clúster 2 y se inicia una operación de backup de volcado o restauración en el clúster 2. La operación de volcado realiza un backup o restaura un volumen ubicado en el clúster 2. En este punto, si se inicia una conmutación de estado del clúster 2 al clúster 1, sucede lo siguiente:

- Si el valor de `override-vetoes` la opción es `false`, el cambio se cancela y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, la operación de copia de seguridad o restauración se anula y la conmutación continúa.

La operación de backup o restauración de volcado se inició durante una conmutación de sitios o una conmutación de estado

Durante una conmutación de sitios del clúster 1 al clúster 2, si se inicia una operación de backup de volcado o restauración en el clúster 1, las operaciones de backup o restauración fallan y la conmutación continúa.

Durante una conmutación de estado del clúster 2 al clúster 1, si se inicia una operación de backup o restauración de volcado desde el clúster 2, la operación de backup o restauración dará error y esta continuará.

Acerca del motor SMTape para volúmenes de FlexVol

Obtenga información sobre el motor SMTape de ONTAP para volúmenes FlexVol

SMTape es una solución de recuperación ante desastres de ONTAP que realiza backup de bloques de datos a cinta. Puede usar SMTape para realizar backups de volúmenes a las cintas. Sin embargo, no puede realizar un backup en el nivel qtree o subárbol. SMTape admite copias de seguridad de línea base, diferenciales e incrementales. SMTape no requiere una licencia.

Puede realizar una operación de backup y restauración de SMTape mediante una aplicación de backup compatible con NDMP. Puede elegir SMTape para realizar operaciones de backup y restauración solo en el modo de NDMP de las máquinas virtuales de almacenamiento (SVM) con ámbito.

> No se admite el proceso de reversión cuando hay una sesión de copia de seguridad o restauración de SMTape en curso. Debe esperar hasta que finalice la sesión o debe anular la sesión NDMP.

Con SMTape, puede realizar backups de 255 snapshots. Para los siguientes backups de línea base, incrementales o diferenciales, debe eliminar las snapshots antiguas respaldadas.

Antes de realizar una restauración base, el volumen al cual se restauran los datos debe ser de tipo `DP` y este volumen debe estar en estado restringido. Después de una restauración correcta, este volumen está en línea automáticamente. Se pueden realizar restauraciones posteriores incrementales o diferenciales en este volumen en el orden en que se ejecutaron los backups.

Obtenga información sobre el uso de instantáneas de ONTAP durante la copia de seguridad de SMTape

Debe comprender cómo se usan las snapshots durante un backup de referencia de SMTape y un backup incremental. También hay que tener en cuenta al realizar un backup con SMTape.

Backup de línea de base

Al realizar un backup de línea base, es posible especificar el nombre de la snapshot que se copiará en cinta. Si no se especifica ninguna instantánea, según el tipo de acceso del volumen (lectura/escritura o solo lectura), se crea automáticamente una instantánea o se utilizan instantáneas existentes. Cuando se especifica una instantánea para la copia de seguridad, también se realiza una copia de seguridad de todas las instantáneas anteriores a la instantánea especificada en cinta.

Si no se especifica una snapshot para el backup, se producirá lo siguiente:

- Para un volumen de lectura/escritura, se crea automáticamente una copia Snapshot.

  La copia Snapshot recién creada y todas las instantáneas más antiguas se realizan backups en cinta.

- Para un volumen de solo lectura, se realizan backups en cinta de todas las copias Snapshot, incluida la última.

  No se realiza un backup de las copias de Snapshot nuevas que se creen después de iniciar el backup.

Backup incremental

Para las operaciones de backup diferenciales o incrementales de SMTape, las aplicaciones de backup compatibles con NDMP crean y gestionan las copias snapshot.

Siempre debe especificar una snapshot mientras realiza una operación de backup incremental. Para que la operación de backup incremental se realice correctamente, la snapshot de backup realizada durante la operación de backup anterior (base de referencia o incremental) debe estar en el volumen desde el que se realiza el backup. Para asegurarse de utilizar esta instantánea con backup, debe tener en cuenta la política de Snapshot asignada en este volumen al configurar la política de backup.

Consideraciones sobre backups de SMTape en destinos de SnapMirror

- Una relación de mirroring de protección de datos crea snapshots temporales en el volumen de destino para la replicación.

  No se deben usar estas snapshots para la copia de seguridad de SMTape.

- Si se produce una actualización de SnapMirror en un volumen de destino en una relación de reflejo de protección de datos durante una operación de backup de SMTape en el mismo volumen, no debe eliminarse en el volumen de origen la copia de Snapshot del backup de SMTape.

  Durante la operación de backup, SMTape bloquea la snapshot en el volumen de destino y, si se elimina la snapshot correspondiente en el volumen de origen, se producirá un error en la operación de actualización de SnapMirror subsiguiente.

- No se deben usar estas snapshots durante un backup incremental.

Capacidades de SMTape para optimizar las operaciones de copia de seguridad y restauración de cintas ONTAP

Las funciones de SMTape, como la copia de seguridad de instantáneas, los backups incrementales y diferenciales, la conservación de las funciones de deduplicación y compresión en volúmenes restaurados y la propagación de cintas, ayudan a optimizar las operaciones de copia de seguridad en cinta y restauración.

SMTape ofrece las siguientes capacidades:

- Ofrece una solución de recuperación tras siniestros
- Permite backups incrementales y diferenciales
- Realiza un backup de las snapshots
- Permite realizar backups y restauraciones de volúmenes deduplicados y mantiene la deduplicación en los volúmenes restaurados
- Realiza backups de volúmenes comprimidos y mantiene la compresión en los volúmenes restaurados
- Permite siembra de cintas

SMTape admite el factor de bloqueo en múltiplos de 4 KB, dentro del intervalo de 4 KB a 256 KB.

> Es posible restaurar datos en volúmenes creados solo en dos versiones principales consecutivas de ONTAP.

Límites de escalabilidad de ONTAP para sesiones de copia de seguridad y restauración de SMTape

Al ejecutar operaciones de backup y restauración de SMTape mediante NDMP o interfaz de línea de comandos (propagación de cintas), debe tener en cuenta la cantidad máxima de sesiones de backup y restauración de SMTape que pueden realizarse de manera simultánea en sistemas de almacenamiento con diferentes capacidades de memoria del sistema. Este número máximo depende de la memoria del sistema de un sistema de almacenamiento.

Los límites de escalabilidad de las sesiones de backup y restauración de SMTape son diferentes de los límites de sesiones de NDMP y los límites de sesiones de volcado.

Memoria del sistema de almacenamiento	Cantidad total de sesiones de backup y restauración de SMTape
Menos de 16 GB	6
Mayor o igual que 16 GB pero menor que 24 GB	16
Mayor o igual que 24 GB	32

Puede obtener la memoria del sistema de su sistema de almacenamiento mediante `sysconfig -a` el comando (disponible en el infierno de nodo). Obtenga más información sobre `sysconfig -a` en el "Referencia de comandos del ONTAP".

Información relacionada

- Límites de escalabilidad para sesiones NDMP
- Límites de escalabilidad para sesiones de backup y restauración de volcado

Obtenga más información sobre la siembra de cintas ONTAP

La propagación de cintas es una funcionalidad SMTape que ayuda a inicializar un volumen de FlexVol de destino en una relación de mirroring de protección de datos.

La propagación de cintas permite establecer una relación de mirroring para la protección de datos entre un sistema de origen y un sistema de destino a través de una conexión de ancho de banda bajo.

El mirroring incremental de instantáneas del origen al destino es posible en una conexión de bajo ancho de banda. Sin embargo, una duplicación inicial de la instantánea base lleva mucho tiempo en una conexión de bajo ancho de banda. En estos casos, se puede realizar una copia de seguridad SMTape del volumen de origen a una cinta y usar la cinta para transferir la snapshot base inicial al destino. A continuación, puede configurar las actualizaciones incrementales de SnapMirror en el sistema de destino mediante la conexión con un ancho de banda bajo.

Cómo funciona SMTape con la conmutación por error de almacenamiento de ONTAP y las operaciones ARL

Antes de ejecutar operaciones de backup o restauración de SMTape, debe comprender cómo funcionan estas operaciones con la operación de conmutación al nodo de respaldo (toma de control y retorno al nodo primario) de almacenamiento o la operación de reubicación de agregados (ARL). `-override-vetoes`La opción determina el comportamiento del motor de SMTape durante una operación de recuperación tras fallos de almacenamiento o ARL.

Cuando se está ejecutando una operación de copia de seguridad o restauración de SMTape y la `-override-vetoes` opción se define en `false`, se detiene una operación de recuperación por error o ARL de almacenamiento iniciada por el usuario y se completa la operación de copia de seguridad o restauración. Si la aplicación de backup admite la extensión CAB, puede seguir realizando operaciones incrementales de backup y restauración de datos SMTape sin tener que reconfigurar las políticas de backup. Sin embargo, si la

`-override-vetoes` opción está definida en `true`, la operación de failover de almacenamiento o ARL continúa y se cancela la operación de copia de seguridad o restauración de SMTape.

Información relacionada

"Gestión de redes"

"Alta disponibilidad"

Cómo funciona SMTape con el movimiento de volumen de ONTAP

Las operaciones de backup de SMTape y las operaciones de movimiento de volúmenes se pueden ejecutar en paralelo hasta que el sistema de almacenamiento intente la fase final de la transición. Una vez pasada esta fase, no se pueden ejecutar nuevas operaciones de backup de SMTape en el volumen que se va a mover. No obstante, las operaciones actuales siguen en ejecución hasta que se complete.

Antes de iniciar la fase de transición de un volumen, la operación de movimiento de volúmenes comprueba las operaciones de backup de SMTape activas en el mismo volumen. Si hay operaciones de backup de SMTape activas, la operación de movimiento de volúmenes pasa al estado de transposición diferida y permite que se completen las operaciones de backup de SMTape. Una vez completadas estas operaciones de backup, debe reiniciar manualmente la operación de movimiento de volúmenes.

Si la aplicación de backup admite la extensión CAB, puede seguir realizando operaciones incrementales de backup y restauración de cinta en volúmenes de lectura/escritura y solo lectura sin tener que reconfigurar las políticas de backup.

No se pueden ejecutar las operaciones de restauración básica y movimiento de volúmenes de forma simultánea; sin embargo, la restauración incremental puede ejecutarse en paralelo con las operaciones de movimiento de volúmenes, con un comportamiento similar al de las operaciones de backup de SMTape durante las operaciones de movimiento de volúmenes.

Cómo funciona SMTape con las operaciones de rehosting de volúmenes ONTAP

No se pueden iniciar las operaciones de SMTape cuando hay una operación de realojamiento de volumen en curso en un volumen. Cuando un volumen está implicado en una operación de realojamiento de volúmenes, no debe iniciarse la sesión de SMTape en ese volumen.

Si hay alguna operación de rehost de volumen en curso, se produce un error en el backup o la restauración de SMTape. Si hay un backup o una restauración de SMTape en curso, se producirá un error en las operaciones de rehost de volúmenes con el mensaje de error correspondiente. Esta condición se aplica tanto a las operaciones de backup o restauración basadas en NDMP como a las basadas en CLI.

Cómo se ve afectada una política de respaldo NDMP de ONTAP durante ADB

Cuando se habilita el equilibrador automático de datos (ADB), el equilibrador analiza las estadísticas de uso de agregados para identificar el agregado que ha superado el porcentaje de uso de umbral alto configurado.

Tras identificar el agregado que ha superado el umbral, el equilibrador identifica un volumen que se puede mover a agregados que residen en otro nodo del clúster e intenta mover dicho volumen. Esta situación afecta a la política de backup configurada para este volumen porque si la aplicación de gestión de datos (DMA) no

tiene en CUENTA LA CABINA, el usuario debe volver a configurar la política de backup y ejecutar la operación de backup de referencia.

> Si el DMA es compatible CON CAB y la política de respaldo se ha configurado utilizando una interfaz específica, el ADB no se ve afectado.

Cómo se ven afectadas las operaciones de copia de seguridad y restauración de SMTape en las configuraciones de ONTAP MetroCluster

Antes de ejecutar operaciones de backup y restauración de SMTape en una configuración de MetroCluster, debe comprender cómo se ven afectadas las operaciones de SMTape cuando se produce una operación de conmutación de sitios o conmutación de estado.

Operación de backup o restauración de SMTape seguida de una conmutación

Considere dos clústeres: El clúster 1 y el clúster 2. Durante una operación de backup o restauración de SMTape en el clúster 1, si se inicia una conmutación entre el clúster 1 y el clúster 2, se produce lo siguiente:

- Si el valor de `-override-vetoes` la opción es `false`, el proceso de switchover se anula y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, la operación de copia de seguridad o restauración de SMTape se anula y el proceso de switchover continúa.

Operación de copia de seguridad o restauración de SMTape seguida de una conmutación de estado

Se realiza una conmutación de sitios desde el clúster 1 al clúster 2 y se inicia una operación de backup o restauración de SMTape en el clúster 2. La operación SMTape realiza backups o restaura un volumen ubicado en el clúster 2. En este punto, si se inicia una conmutación de estado del clúster 2 al clúster 1, sucede lo siguiente:

- Si el valor de `-override-vetoes` la opción es `false`, el proceso de conmutación se anula y la operación de copia de seguridad o restauración continúa.
- Si el valor de la opción es `true`, la operación de copia de seguridad o restauración se anula y el proceso de conmutación continúa.

La operación de backup o restauración de SMTape se inició durante una conmutación de sitios o conmutación de estado

Durante un proceso de conmutación de sitios del clúster 1 al clúster 2, si se inicia una operación de backup o restauración de SMTape en el clúster 1, la operación de backup o restauración falla y la conmutación continúa.

Durante un proceso de conmutación de estado del clúster 2 al clúster 1, si se inicia una operación de backup o restauración SMTape desde el clúster 2, la operación de backup o restauración falla y la conmutación de estado continúa.

Supervisar las operaciones de backup y restauración a cinta para volúmenes de FlexVol

Supervisar las operaciones de copia de seguridad y restauración de cintas ONTAP para volúmenes FlexVol

Es posible ver los archivos de registro de eventos para supervisar las operaciones de backup a cinta y restauración. ONTAP registra automáticamente importantes eventos de backup y restauración, así como la hora en que se producen en un archivo de registro denominado `backup` en `/etc/log/` el directorio de la controladora. De forma predeterminada, el registro de eventos se establece en `on`.

Es posible que desee ver los archivos de registro de eventos por los siguientes motivos:

- Comprobar si un backup nocturno se ha realizado correctamente
- Recopilación de estadísticas sobre operaciones de backup
- Para usar la información de los archivos de registro de eventos anteriores con el fin de ayudar a diagnosticar problemas con las operaciones de backup y restauración

Una vez cada semana, los archivos de registro de eventos se rotan. `/etc/log/backup`El nombre del archivo se cambia a `/etc/log/backup.0`, `/etc/log/backup.0` el nombre del archivo se cambia a `/etc/log/backup.1`, etc. El sistema guarda los archivos de registro durante un máximo de seis semanas; por lo tanto, puede tener hasta siete archivos de mensajes (`/etc/log/backup.[0-5]`y el `/etc/log/backup` archivo actual).

Acceda a los archivos de registro de eventos de ONTAP para operaciones de copia de seguridad y restauración en cinta

Puede acceder a los archivos de registro de eventos para las operaciones de copia de seguridad y restauración en cinta en `/etc/log/ rdfile` el directorio mediante el comando en el infierno de nodos. Es posible ver estos archivos de registro de eventos para supervisar las operaciones de backup a cinta y restauración.

Acerca de esta tarea

Con configuraciones adicionales, como un rol de control de acceso con acceso al `spi` servicio web o una cuenta de usuario configurada con el `http` método de acceso, también puede utilizar un explorador web para acceder a estos archivos de registro.

Pasos

1. Para acceder a nodeshell, introduzca el siguiente comando:

   `node run -node *node_name*`

   `node_name` es el nombre del nodo.

2. Para acceder a los archivos del registro de eventos para las operaciones de backup a cinta y restauración, escriba el siguiente comando:

   `rdfile /etc/log/backup`

Información relacionada

"Administración del sistema"

Qué es el formato de mensaje de volcado y restauración del registro de eventos

Formato de mensaje de registro de eventos de volcado y restauración de ONTAP

Para cada evento de volcado y restauración, se escribe un mensaje en el archivo de registro de copia de seguridad.

El formato del mensaje de volcado y restauración del registro de eventos es el siguiente:

type timestamp identifier event (event_info)

En la lista siguiente se describen los campos en el formato de mensaje del registro de eventos:

- Cada mensaje de registro comienza con uno de los indicadores de tipo descritos en la siguiente tabla:

Tipo	Descripción
registro	Evento de registro
dmp	Evento de volcado
rst	Evento de restauración

- `timestamp` muestra la fecha y hora del evento.
- `identifier`El campo de un evento de volcado incluye la ruta de volcado y el identificador único del volcado. `identifier`El campo de un evento de restauración utiliza únicamente el nombre de la ruta de destino de restauración como identificador único. Los mensajes de eventos relacionados con el registro no incluyen ningún `identifier` campo.

Obtenga información sobre los eventos de registro de ONTAP

El campo de evento de un mensaje que comienza con un registro especifica el comienzo de un registro o el final de un registro.

Contiene uno de los eventos que se muestran en la siguiente tabla:

Evento	Descripción
Inicio_registro	Indica el comienzo del registro o que el registro se ha vuelto a activar después de estar desactivado.
Stop_Logging	Indica que se ha desactivado el registro.

Obtenga información sobre los eventos de volcado de ONTAP

El campo de evento de un evento de volcado contiene un tipo de evento seguido de información específica del evento entre paréntesis.

En la siguiente tabla se describen los eventos, sus descripciones y la información de eventos relacionada que puede registrarse para una operación de volcado:

Evento	Descripción	Información del evento
Comenzar	Se ha iniciado el volcado NDMP	Nivel de descarga y tipo de volcado
Fin	Volcados completados correctamente	Cantidad de datos procesados
Anular	Se cancela la operación	Cantidad de datos procesados
Opciones	Se muestran las opciones especificadas	Todas las opciones y sus valores asociados, incluidas las opciones NDMP
Tape_open	La cinta está abierta para lectura y escritura	Nombre del nuevo dispositivo de cinta
Tape_close	La cinta se cierra para lectura/escritura	El nombre del dispositivo de cinta
Cambio de fase	Un volcado está entrando en una nueva fase de procesamiento	El nombre de la nueva fase
Error	Un volcado ha encontrado un evento inesperado	Mensaje de error
Snapshot	Se crea o se ubica una instantánea	El nombre y la hora de la copia de Snapshot
Volcado_base	Se ha localizado una entrada de volcado base en el metarchivo interno	El nivel y la hora del volcado base (sólo para volcados incrementales)

Obtenga información sobre los eventos de restauración de ONTAP

El campo de evento de restauración contiene un tipo de evento seguido de información específica del evento entre paréntesis.

En la siguiente tabla, se proporciona información sobre los eventos, sus descripciones y la información de eventos relacionada que se puede registrar para una operación de restauración:

Evento	Descripción	Información del evento
Comenzar	Se ha iniciado la restauración NDMP	Nivel de restauración y tipo de restauración
Fin	Las restauraciones se completaron correctamente	Número de archivos y cantidad de datos procesados

Evento	Descripción	Información del evento
Anular	Se cancela la operación	Número de archivos y cantidad de datos procesados
Opciones	Se muestran las opciones especificadas	Todas las opciones y sus valores asociados, incluidas las opciones NDMP
Tape_open	La cinta está abierta para lectura y escritura	Nombre del nuevo dispositivo de cinta
Tape_close	La cinta se cierra para lectura/escritura	El nombre del dispositivo de cinta
Cambio de fase	Restore está entrando en una nueva fase de procesamiento	El nombre de la nueva fase
Error	La restauración encuentra un evento inesperado	Mensaje de error

Habilitar o deshabilitar el registro de eventos para operaciones de copia de seguridad y restauración en cinta ONTAP

Puede activar o desactivar el registro de eventos.

Pasos

1. Para habilitar o deshabilitar el registro de eventos, introduzca el siguiente comando en el clustershell:

   `options -option_name backup.log.enable -option-value {on | off}`

   `on` activa el registro de eventos.

   `off` desactiva el registro de eventos.

   El registro de eventos está activado de forma predeterminada.

Mensajes de error para backup y restauración a cinta de volúmenes de FlexVol

Mensajes de error de copia de seguridad y restauración

Limitación de recursos: No hay ningún subproceso disponible

- **Mensaje**

  `Resource limitation: no available thread`

- **Causa**

  El número máximo de subprocesos de E/S de cinta local activos está actualmente en uso. Puede tener un

máximo de 16 unidades de cinta locales activas.

- **Acción Correctiva**

  Espere a que finalicen algunos trabajos de cinta antes de iniciar una nueva tarea de copia de seguridad o restauración.

Reserva de cintas prehecha

- **Mensaje**

  `Tape reservation preempted`

- **Causa**

  La unidad de cinta está en uso por otra operación o la cinta se ha cerrado prematuramente.

- **Acción Correctiva**

  Asegúrese de que la unidad de cinta no esté en uso en otra operación y de que la aplicación DMA no haya cancelado el trabajo y vuelva a intentarlo.

No se pudo inicializar el medio

- **Mensaje**

  `Could not initialize media`

- **Causa**

  Puede obtener este error por uno de los siguientes motivos:

  - La unidad de cinta utilizada para la copia de seguridad está dañada o dañada.
  - La cinta no contiene la copia de seguridad completa o está dañada.
  - El número máximo de subprocesos de E/S de cinta local activos está actualmente en uso.

    Puede tener un máximo de 16 unidades de cinta locales activas.

- **Acción Correctiva**
  - Si la unidad de cinta está dañada o dañada, vuelva a intentar la operación con una unidad de cinta válida.
  - Si la cinta no contiene la copia de seguridad completa o está dañada, no podrá realizar la operación de restauración.
  - Si no hay recursos de cinta disponibles, espere a que finalicen algunos de los trabajos de backup o restauración y vuelva a intentar la operación.

Número máximo de volcados o restauraciones permitidos (límite máximo de sesión) en curso

- **Mensaje**

  `Maximum number of allowed dumps or restores` *`(maximum session limit)`* `in progress`

- **Causa**

  Ya se está ejecutando la cantidad máxima de trabajos de backup o restauración.

- **Acción Correctiva**

  Vuelva a intentar la operación después de que finalicen algunos de los trabajos en ejecución actualmente.

Error de soporte al escribir la cinta

- **Mensaje**

  ```
  Media error on tape write
  ```

- **Causa**

  La cinta utilizada para la copia de seguridad está dañada.

- **Acción Correctiva**

  Sustituya la cinta y vuelva a intentar la tarea de copia de seguridad.

Error al escribir en la cinta

- **Mensaje**

  ```
  Tape write failed
  ```

- **Causa**

  La cinta utilizada para la copia de seguridad está dañada.

- **Acción Correctiva**

  Sustituya la cinta y vuelva a intentar la tarea de copia de seguridad.

Error al escribir la cinta: La nueva cinta encontró un error de soporte

- **Mensaje**

  ```
  Tape write failed - new tape encountered media error
  ```

- **Causa**

  La cinta utilizada para la copia de seguridad está dañada.

- **Acción Correctiva**

  Sustituir la cinta y volver a intentar la copia de seguridad.

Error al escribir en la cinta: La nueva cinta está rota o está protegida contra escritura

- **Mensaje**

```
Tape write failed - new tape is broken or write protected
```

- **Causa**

  La cinta utilizada para el backup está dañada o protegida contra escritura.

- **Acción Correctiva**

  Sustituir la cinta y volver a intentar la copia de seguridad.

Error al escribir en cinta: La nueva cinta ya está al final del soporte

- **Mensaje**

```
Tape write failed - new tape is already at the end of media
```

- **Causa**

  No hay suficiente espacio en la cinta para completar la copia de seguridad.

- **Acción Correctiva**

  Sustituir la cinta y volver a intentar la copia de seguridad.

Error de escritura de cinta

- **Mensaje**

```
Tape write error - The previous tape had less than the required minimum
capacity, size MB, for this tape operation, The operation should be restarted
from the beginning
```

- **Causa**

  La capacidad de la cinta no es suficiente para contener los datos de copia de seguridad.

- **Acción Correctiva**

  Utilice cintas con mayor capacidad y vuelva a intentar realizar la tarea de backup.

Error de soporte en la cinta de lectura

- **Mensaje**

```
Media error on tape read
```

- **Causa**

  La cinta de la que se van a restaurar los datos está dañada y puede que no contenga los datos de copia de seguridad completos.

- **Acción Correctiva**

  Si está seguro de que la cinta tiene la copia de seguridad completa, vuelva a intentar la operación de

restauración. Si la cinta no contiene la copia de seguridad completa, no se puede ejecutar la operación de restauración.

Error de lectura de cinta

- **Mensaje**

  ```
  Tape read error
  ```

- **Causa**

  La unidad de cinta está dañada o la cinta no contiene la copia de seguridad completa.

- **Acción Correctiva**

  Si la unidad de cinta está dañada, utilice otra unidad de cinta. Si la cinta no contiene la copia de seguridad completa, no podrá restaurar los datos.

Ya al final de la cinta

- **Mensaje**

  ```
  Already at the end of tape
  ```

- **Causa**

  La cinta no contiene datos o debe rebobinarse.

- **Acción Correctiva**

  Si la cinta no contiene datos, utilice la cinta que contiene la copia de seguridad y vuelva a intentar la tarea de restauración. De lo contrario, rebobine la cinta y vuelva a intentar el trabajo de restauración.

El tamaño del registro de cinta es demasiado pequeño. Pruebe con un tamaño mayor.

- **Mensaje**

  ```
  Tape record size is too small. Try a larger size.
  ```

- **Causa**

  El factor de bloqueo especificado para la operación de restauración es menor que el factor de bloqueo que se utilizó durante el backup.

- **Acción Correctiva**

  Utilice el mismo factor de bloqueo que se especificó durante la copia de seguridad.

El tamaño del registro de cinta debe ser block_Siz1 y no Block_Size2

- **Mensaje**

  ```
  Tape record size should be block_size1 and not block_size2
  ```

- **Causa**

  El factor de bloqueo especificado para la restauración local es incorrecto.

- **Acción Correctiva**

  Vuelva a intentar el trabajo de restauración con `block_size1` como factor de bloqueo.

El tamaño del registro de la cinta debe estar comprendido entre 4 KB y 256 KB

- **Mensaje**

  ```
  Tape record size must be in the range between 4KB and 256KB
  ```

- **Causa**

  El factor de bloqueo especificado para la operación de backup o restauración no se encuentra dentro del rango permitido.

- **Acción Correctiva**

  Especifique un factor de bloqueo entre 4 KB y 256 KB.

Mensajes de error de NDMP

Error de comunicación de red

- **Mensaje**

  ```
  Network communication error
  ```

- **Causa**

  Se produjo un error en la comunicación a una cinta remota en una conexión triple NDMP.

- **Acción Correctiva**

  Compruebe la conexión de red al mando a distancia.

Mensaje de Read Socket: Error_string

- **Mensaje**

  ```
  Message from Read Socket: error_string
  ```

- **Causa**

  Restaurar la comunicación desde la cinta remota en la conexión NDMP 3-way tiene errores.

- **Acción Correctiva**

  Compruebe la conexión de red al mando a distancia.

Mensaje de Write Dirnet: Error_string

- **Mensaje**

  ```
  Message from Write Dirnet: error_string
  ```

- **Causa**

  Se produjo un error en la comunicación de backup a una cinta remota en una conexión triple NDMP.

- **Acción Correctiva**

  Compruebe la conexión de red al mando a distancia.

Leer el conector hembra EOF recibido

- **Mensaje**

  ```
  Read Socket received EOF
  ```

- **Causa**

  El intento de comunicarse con una cinta remota en una conexión triple NDMP ha alcanzado el fin de la Marca de archivo. Es posible que se intente realizar una restauración triple desde una imagen de backup con un tamaño de bloque mayor.

- **Acción Correctiva**

  Especifique el tamaño de bloque correcto y vuelva a intentar la operación de restauración.

ndmpd número de versión no válido: version_number "

- **Mensaje**

  ```
  ndmpd invalid version number: version_number
  ```

- **Causa**

  La versión NDMP especificada no es compatible con el sistema de almacenamiento.

- **Acción Correctiva**

  Especifique la versión 4 de NDMP.

Ndmpd session_ID no activo

- **Mensaje**

  ```
  ndmpd session session_ID not active
  ```

- **Causa**

  Es posible que la sesión NDMP no exista.

- **Acción Correctiva**

  Utilice `ndmpd status` el comando para ver las sesiones de NDMP activas.

No se puede obtener la referencia de volumen para Volume_name

- **Mensaje**

  ```
  Could not obtain vol ref for Volume vol_name
  ```

- **Causa**

  No se pudo obtener la referencia del volumen debido a que este puede estar en uso por parte de otras operaciones.

- **Acción Correctiva**

  Volver a intentar la operación más tarde.

El tipo de conexión de datos ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] no es compatible con las conexiones de control ["IPv6"|"IPv4"]

- **Mensaje**

  ```
  Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
  for ["IPv6"|"IPv4"] control connections
  ```

- **Causa**

  En el modo NDMP de ámbito de nodo, la conexión de datos NDMP establecida debe ser del mismo tipo de dirección de red (IPv4 o IPv6) que la conexión de control NDMP.

- **Acción Correctiva**

  Póngase en contacto con el proveedor de sus aplicaciones de backup.

ESCUCHA DE DATOS: Error de condición de preparación de la conexión DE datos DE LA CABINA

- **Mensaje**

  ```
  DATA LISTEN: CAB data connection prepare precondition error
  ```

- **Causa**

  Se produce un error en la escucha de datos NDMP cuando la aplicación de backup ha negociado la extensión CAB con el servidor NDMP y el tipo de dirección de conexión de datos NDMP especificado no coincide entre los mensajes NDMP_CAB_DATA_CONN_PREPARE y NDMP_DATA_LISTEN.

- **Acción Correctiva**

  Póngase en contacto con el proveedor de sus aplicaciones de backup.

CONEXIÓN DE DATOS: Error de condición de preparación de la conexión DE datos DE LA CABINA

- **Mensaje**

  ```
  DATA CONNECT: CAB data connection prepare precondition error
  ```

- **Causa**

  Se produce un error en la conexión de datos NDMP cuando la aplicación de backup ha negociado la extensión CAB con el servidor NDMP y el tipo de dirección de conexión de datos NDMP especificado no coincide entre los mensajes NDMP_CAB_DATA_CONN_PREPARE y NDMP_DATA_CONNECT.

- **Acción Correctiva**

  Póngase en contacto con el proveedor de sus aplicaciones de backup.

Error:error al mostrar: No se puede obtener la contraseña del usuario '<username>'

- **Mensaje**

  ```
  Error: show failed: Cannot get password for user '<username>'
  ```

- **Causa**

  Configuración de cuenta de usuario incompleta para NDMP

- **Acción Correctiva**

  Asegúrese de que la cuenta de usuario esté asociada con el método de acceso SSH y que el método de autenticación sea la contraseña de usuario.

Mensajes de error de volcado

El volumen de destino es de solo lectura

- **Mensaje**

  ```
  Destination volume is read-only
  ```

- **Causa**

  La ruta a la que se intenta realizar la operación de restauración es de solo lectura.

- **Acción Correctiva**

  Intente restaurar los datos en una ubicación diferente.

El qtree de destino es de solo lectura

- **Mensaje**

  ```
  Destination qtree is read-only
  ```

- **Causa**

El qtree al que se intenta restaurar es de solo lectura.

- **Acción Correctiva**

  Intente restaurar los datos en una ubicación diferente.

Vuelca temporalmente desactivado en el volumen, vuelva a intentarlo

- **Mensaje**

  ```
  Dumps temporarily disabled on volume, try again
  ```

- **Causa**

  El backup de volcado NDMP se intenta en un volumen de destino de SnapMirror que forma parte de una `snapmirror break` `snapmirror resync` operación o una.

- **Acción Correctiva**

  Espere a que `snapmirror break` `snapmirror resync` finalice la operación OR y, a continuación, realice la operación de volcado.

  > Siempre que el estado de un volumen de destino de SnapMirror cambie de lectura/escritura a solo lectura o de solo lectura a lectura/escritura, debe ejecutar un backup de referencia.

Información relacionada

- "rotura de snapmirror"
- "resincronización de SnapMirror"

Etiquetas de NFS no reconocidas

- **Mensaje**

  ```
  Error: Aborting: dump encountered NFS security labels in the file system
  ```

- **Causa**

  Las etiquetas de seguridad NFS son compatibles a partir de ONTAP 9.9.1 cuando NFSv4.2 está habilitado. Sin embargo, el motor de volcado no reconoce actualmente las etiquetas de seguridad NFS. Si encuentra alguna etiqueta de seguridad NFS en los archivos, directorios o cualquier archivo especial en cualquier formato de volcado, el volcado falla.

- **Acción Correctiva**

  Compruebe que ningún archivo o directorio tiene etiquetas de seguridad NFS.

No se crearon archivos

- **Mensaje**

  ```
  No files were created
  ```

- **Causa**

  Se intentó un DAR de directorio sin permitir la funcionalidad DAR mejorada.

- **Acción Correctiva**

  Active la funcionalidad DAR mejorada y vuelva a intentar DAR.

Error en la restauración del <file name> de archivo

- **Mensaje**

  ```
  Restore of the file file name failed
  ```

- **Causa**

  Cuando SE realiza UN DAR (recuperación de acceso directo) de un archivo cuyo nombre de archivo es el mismo que el de un LUN del volumen de destino, se produce un error EN EL DAR.

- **Acción Correctiva**

  Vuelva a intentar DAR del archivo.

Error de truncamiento para el inode <inode number> src…

- **Mensaje**

  ```
  Truncation failed for src inode <inode number>. Error <error number>. Skipping
  inode.
  ```

- **Causa**

  El inodo de un archivo se elimina cuando se restaura el archivo.

- **Acción Correctiva**

  Espere a que se complete la operación de restauración en un volumen antes de usar ese volumen.

No se puede bloquear una snapshot necesaria mediante el volcado

- **Mensaje**

  ```
  Unable to lock a snapshot needed by dump
  ```

- **Causa**

  La snapshot especificada para el backup no está disponible.

- **Acción Correctiva**

  Vuelva a intentar el backup con una copia Snapshot diferente.

  Utilice `snap list` el comando para ver la lista de instantáneas disponibles.

Obtenga más información sobre `snap list` en el "Referencia de comandos del ONTAP".

No se pueden localizar los archivos de mapa de bits

- **Mensaje**

  ```
  Unable to locate bitmap files
  ```

- **Causa**

  Es posible que se hayan eliminado los archivos de mapa de bits necesarios para la operación de copia de seguridad. En este caso, no se puede reiniciar el backup.

- **Acción Correctiva**

  Vuelva a ejecutar la copia de seguridad.

El volumen se encuentra temporalmente en estado transitorio

- **Mensaje**

  ```
  Volume is temporarily in a transitional state
  ```

- **Causa**

  El volumen del que se realiza el backup se encuentra temporalmente en el estado desmontado.

- **Acción Correctiva**

  Espere algún tiempo y vuelva a realizar la copia de seguridad.

Mensajes de error de SMTape

Trozos fuera de servicio

- **Mensaje**

  ```
  Chunks out of order
  ```

- **Causa**

  Las cintas de copia de seguridad no se restauran en el orden correcto.

- **Acción Correctiva**

  Vuelva a intentar la operación de restauración y cargue las cintas en la secuencia correcta.

Formato de fragmento no compatible

- **Mensaje**

  ```
  Chunk format not supported
  ```

- **Causa**

  La imagen de copia de seguridad no es de SMTape.

- **Acción Correctiva**

  Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tenga la copia de seguridad de SMTape.

Error al asignar memoria

- **Mensaje**

  ```
  Failed to allocate memory
  ```

- **Causa**

  El sistema se ha quedado sin memoria.

- **Acción Correctiva**

  Vuelva a intentar el trabajo más tarde cuando el sistema no esté demasiado ocupado.

Error al obtener el búfer de datos

- **Mensaje**

  ```
  Failed to get data buffer
  ```

- **Causa**

  El sistema de almacenamiento se agotó de los búferes.

- **Acción Correctiva**

  Espere a que algunas operaciones del sistema de almacenamiento finalicen y luego vuelva a intentar la tarea.

Error al encontrar la snapshot

- **Mensaje**

  ```
  Failed to find snapshot
  ```

- **Causa**

  La instantánea especificada para el backup no está disponible.

- **Acción Correctiva**

  Compruebe si la instantánea especificada está disponible. Si no es así, vuelva a intentarlo con la instantánea correcta.

No se puede crear la snapshot

- **Mensaje**

  `Failed to create snapshot`

- **Causa**

  El volumen ya contiene el número máximo de copias de Snapshot.

- **Acción Correctiva**

  Elimine algunas Snapshot y vuelva a intentar la operación de backup.

Error al bloquear la snapshot

- **Mensaje**

  `Failed to lock snapshot`

- **Causa**

  La instantánea está en uso o se ha eliminado.

- **Acción Correctiva**

  Si otra operación está utilizando la instancia de Snapshot, espere a que finalice esa operación y vuelva a intentar el backup. Si la snapshot se ha eliminado, no se puede realizar el backup.

Error al eliminar la snapshot

- **Mensaje**

  `Failed to delete snapshot`

- **Causa**

  No se ha podido eliminar la instantánea automática porque está en uso en otras operaciones.

- **Acción Correctiva**

  Utilice `snap` el comando para determinar el estado de la snapshot. Si la instantánea no es necesaria, elimínela manualmente.

Error al obtener la snapshot más reciente

- **Mensaje**

  `Failed to get latest snapshot`

- **Causa**

  Es posible que la instantánea más reciente no exista porque el volumen se está inicializando mediante SnapMirror.

- **Acción Correctiva**

  Vuelva a intentarlo una vez completada la inicialización.

No se pudo cargar la nueva cinta

- **Mensaje**

  ```
  Failed to load new tape
  ```

- **Causa**

  Error en unidad de cinta o soporte.

- **Acción Correctiva**

  Sustituya la cinta y vuelva a intentar la operación.

Error al inicializar la cinta

- **Mensaje**

  ```
  Failed to initialize tape
  ```

- **Causa**

  Puede obtener este mensaje de error por uno de los siguientes motivos:

  - La imagen de copia de seguridad no es de SMTape.
  - El factor de bloqueo de cinta especificado es incorrecto.
  - La cinta está dañada o dañada.
  - Se ha cargado una cinta incorrecta para la restauración.

- **Acción Correctiva**
  - Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tiene una copia de seguridad de SMTape.
  - Si el factor de bloqueo es incorrecto, especifique el factor de bloqueo correcto y vuelva a intentar la operación.
  - Si la cinta está dañada, no podrá realizar la operación de restauración.
  - Si se carga la cinta incorrecta, vuelva a intentar la operación con la cinta correcta.

Error al inicializar el flujo de restauración

- **Mensaje**

  ```
  Failed to initialize restore stream
  ```

- **Causa**

  Puede obtener este mensaje de error por uno de los siguientes motivos:

- La imagen de copia de seguridad no es de SMTape.
- El factor de bloqueo de cinta especificado es incorrecto.
- La cinta está dañada o dañada.
- Se ha cargado una cinta incorrecta para la restauración.

- **Acción Correctiva**
  - Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tenga la copia de seguridad de SMTape.
  - Si el factor de bloqueo es incorrecto, especifique el factor de bloqueo correcto y vuelva a intentar la operación.
  - Si la cinta está dañada, no podrá realizar la operación de restauración.
  - Si se carga la cinta incorrecta, vuelva a intentar la operación con la cinta correcta.

Error al leer la imagen de la copia de seguridad

- **Mensaje**

  ```
  Failed to read backup image
  ```

- **Causa**

  La cinta está dañada.

- **Acción Correctiva**

  Si la cinta está dañada, no podrá realizar la operación de restauración.

Falta el encabezado de la imagen o está dañado

- **Mensaje**

  ```
  Image header missing or corrupted
  ```

- **Causa**

  La cinta no contiene una copia de seguridad de SMTape válida.

- **Acción Correctiva**

  Vuelva a intentarlo con una cinta que contenga un backup válido.

Afirmación interna

- **Mensaje**

  ```
  Internal assertion
  ```

- **Causa**

  Hay un error interno de SMTape.

- **Acción Correctiva**

  Informe sobre el error y envíe `etc/log/backup` el archivo al soporte técnico.

Número mágico de imagen de copia de seguridad no válido

- **Mensaje**

  ```
  Invalid backup image magic number
  ```

- **Causa**

  La imagen de copia de seguridad no es de SMTape.

- **Acción Correctiva**

  Si la imagen de copia de seguridad no es de SMTape, vuelva a intentar la operación con una cinta que tenga la copia de seguridad de SMTape.

Suma de comprobación de imagen de backup no válida

- **Mensaje**

  ```
  Invalid backup image checksum
  ```

- **Causa**

  La cinta está dañada.

- **Acción Correctiva**

  Si la cinta está dañada, no podrá realizar la operación de restauración.

Cinta de entrada no válida

- **Mensaje**

  ```
  Invalid input tape
  ```

- **Causa**

  La firma de la imagen de copia de seguridad no es válida en el encabezado de la cinta. La cinta tiene datos dañados o no contiene una imagen de copia de seguridad válida.

- **Acción Correctiva**

  Vuelva a intentar el trabajo de restauración con una imagen de backup válida.

La ruta de volumen no es válida

- **Mensaje**

  ```
  Invalid volume path
  ```

- **Causa**

  No se encuentra el volumen especificado para la operación de backup o restauración.

- **Acción Correctiva**

  Vuelva a intentar el trabajo con una ruta de volumen y un nombre de volumen válidos.

El ID del conjunto de copia de seguridad no coincide

- **Mensaje**

  ```
  Mismatch in backup set ID
  ```

- **Causa**

  La cinta cargada durante un cambio de cinta no forma parte del conjunto de copia de seguridad.

- **Acción Correctiva**

  Cargue la cinta correcta y vuelva a intentar el trabajo.

No coincide con la Marca de tiempo de backup

- **Mensaje**

  ```
  Mismatch in backup time stamp
  ```

- **Causa**

  La cinta cargada durante un cambio de cinta no forma parte del conjunto de copia de seguridad.

- **Acción Correctiva**

  Utilice `smtape restore -h` el comando para verificar la información de cabecera de una cinta.

Trabajo anulado debido a cierre

- **Mensaje**

  ```
  Job aborted due to shutdown
  ```

- **Causa**

  El sistema de almacenamiento se está reiniciando.

- **Acción Correctiva**

  Vuelva a intentar el trabajo después de que se reinicie el sistema de almacenamiento.

Trabajo abortado debido a la eliminación automática de instantáneas

- **Mensaje**

```
Job aborted due to snapshot autodelete
```

- **Causa**

  El volumen no tiene espacio suficiente y se ha activado la eliminación automática de snapshots.

- **Acción Correctiva**

  Libere espacio en el volumen y vuelva a intentar el trabajo.

En la actualidad, la cinta se está utilizando en otras operaciones

- **Mensaje**

  ```
  Tape is currently in use by other operations
  ```

- **Causa**

  La unidad de cinta está en uso por otro trabajo.

- **Acción Correctiva**

  Se debe reintentar la copia de seguridad una vez finalizado el trabajo actualmente activo.

Las cintas están fuera de servicio

- **Mensaje**

  ```
  Tapes out of order
  ```

- **Causa**

  La primera cinta de la secuencia de cinta para la operación de restauración no tiene el encabezado de la imagen.

- **Acción Correctiva**

  Cargue la cinta con el encabezado de la imagen y vuelva a intentar el trabajo.

Error de transferencia (se canceló debido a una operación de MetroCluster)

- **Mensaje**

  ```
  Transfer failed (Aborted due to MetroCluster operation)
  ```

- **Causa**

  La operación SMTape se cancela debido a una operación de conmutación de sitios o conmutación de estado.

- **Acción Correctiva**

  Lleve a cabo la operación SMTape después de que finalice la operación de conmutación o conmutación de regreso.

Error en la transferencia (interrupción iniciada por ARL)

- **Mensaje**

  ```
  Transfer failed (ARL initiated abort)
  ```

- **Causa**

  Mientras se está realizando una operación SMTape si se inicia una reubicación de agregado, se cancela la operación SMTape.

- **Acción Correctiva**

  Realice la operación SMTape después de que finalice la operación de reubicación de agregados.

Error en la transferencia (interrupción iniciada por CFO)

- **Mensaje**

  ```
  Transfer failed (CFO initiated abort)
  ```

- **Causa**

  La operación SMTape se cancela debido a una operación de recuperación tras fallos (toma de control y retorno al nodo primario) del almacenamiento de un agregado CFO.

- **Acción Correctiva**

  Ejecutar la operación de SMTape tras la recuperación tras la recuperación tras fallos del agregado CFO de almacenamiento.

Error en la transferencia (interrupción iniciada por SFO)

- **Mensaje**

  ```
  Transfer failed (SFO initiated abort)
  ```

- **Causa**

  La operación SMTape se cancela debido a una operación de conmutación al nodo de respaldo (toma de control y retorno al nodo primario) del almacenamiento.

- **Acción Correctiva**

  Realice la operación SMTape después de que termine la operación de recuperación tras fallos (toma de control y devolución) del almacenamiento.

Agregado subyacente durante la migración

- **Mensaje**

  ```
  Underlying aggregate under migration
  ```

- **Causa**

Si se inicia una operación SMTape en un agregado que se está realizando la migración (conmutación por error del almacenamiento o reubicación de agregados), la operación SMTape falla.

- **Acción Correctiva**

  Realice la operación SMTape una vez finalizada la migración de agregado.

El volumen se encuentra actualmente en proceso de migración

- **Mensaje**

  ```
  Volume is currently under migration
  ```

- **Causa**

  La migración de volúmenes y el backup de SMTape no se pueden ejecutar simultáneamente.

- **Acción Correctiva**

  Vuelva a intentar el trabajo de backup después de completar la migración del volumen.

Volumen sin conexión

- **Mensaje**

  ```
  Volume offline
  ```

- **Causa**

  El volumen del cual se realiza el backup está sin conexión.

- **Acción Correctiva**

  Coloque el volumen en línea y vuelva a intentar el backup.

Volumen no restringido

- **Mensaje**

  ```
  Volume not restricted
  ```

- **Causa**

  No está restringido el volumen de destino al que se restauran los datos.

- **Acción Correctiva**

  Restrinja el volumen y vuelva a intentar la operación de restauración.

Configuración de NDMP

Obtenga más información sobre la configuración de NDMP de ONTAP

Puede configurar rápidamente un clúster ONTAP 9 para utilizar el protocolo de gestión de datos de red (NDMP) con el fin de realizar backups de los datos directamente en cinta mediante una aplicación de backup de terceros.

Si la aplicación de backup admite Cluster Aware Backup (CAB), puede configurar NDMP como *SVM-scoped* o *node-scoped*:

- Con el ámbito de SVM en el nivel del clúster (SVM de administrador), puede realizar backup de todos los volúmenes alojados en diferentes nodos del clúster. Siempre que sea posible, se recomienda utilizar NDMP con ámbito SVM.
- NDMP de ámbito de nodo le permite realizar backup de todos los volúmenes alojados en ese nodo.

Si la aplicación de backup no admite CAB, debe utilizar NDMP de ámbito de nodo.

El protocolo NDMP de ámbito SVM y el de ámbito de nodo son mutuamente exclusivos; no se pueden configurar en el mismo clúster.

NDMP de ámbito del nodo está obsoleto en ONTAP 9.

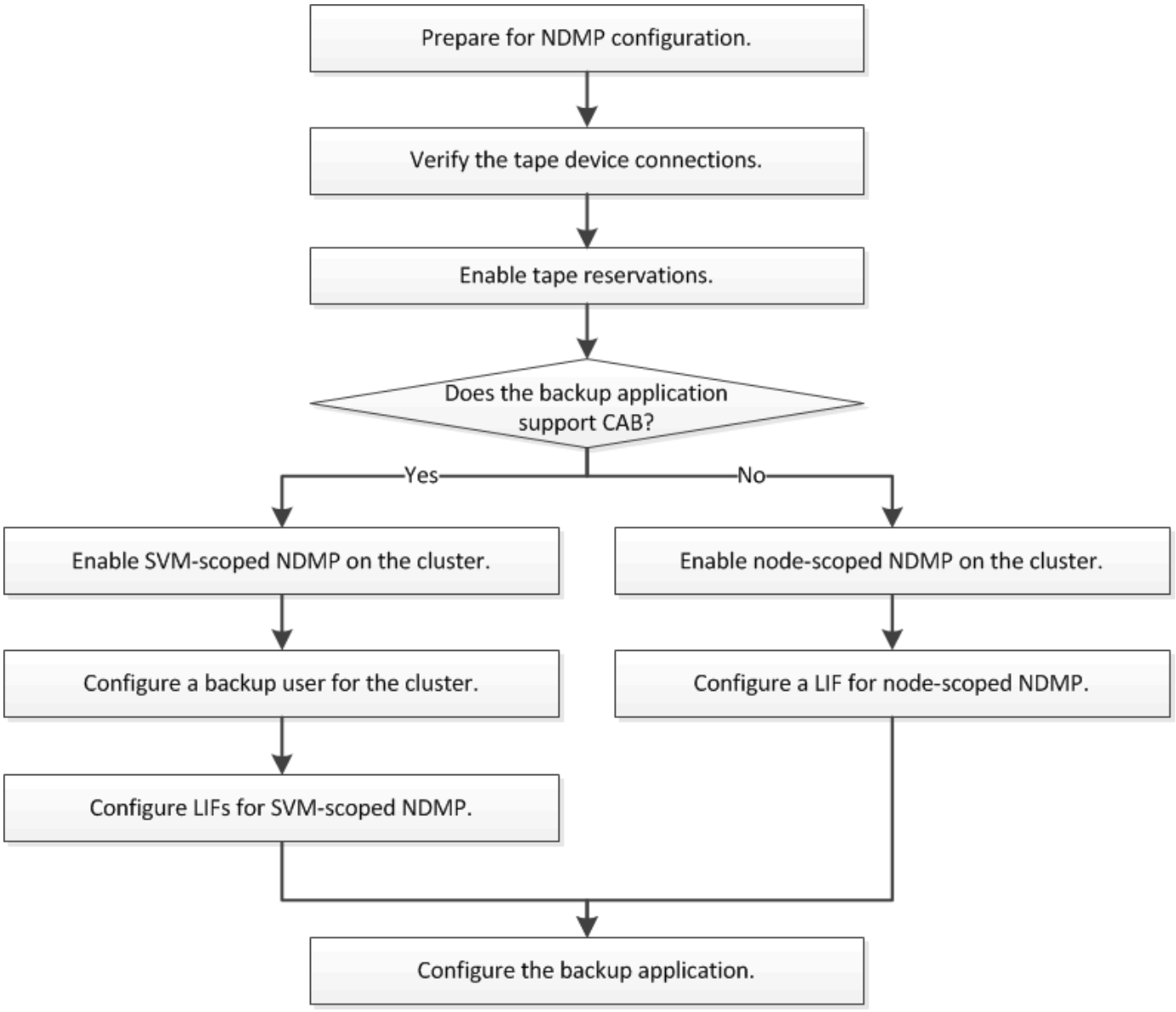
Más información sobre "Respaldo para clúster (CAB)".

Antes de configurar NDMP, compruebe lo siguiente:

- Tiene una aplicación de copia de seguridad de terceros (también llamada aplicación de administración de datos o DMA).
- Es un administrador de clúster.
- Se instalan dispositivos de cinta y un servidor multimedia opcional.
- Los dispositivos de cinta están conectados al clúster a través de un switch Fibre Channel (FC) o conectados localmente.
- Al menos un dispositivo de cinta tiene un número de unidad lógica (LUN) de 0.

Obtenga más información sobre el flujo de trabajo de configuración de NDMP de ONTAP

La configuración del backup en cinta mediante NDMP implica preparar la configuración NDMP, verificar las conexiones del dispositivo de cinta, habilitar las reservas en cinta, configurar NDMP en el nivel de SVM o nodo, habilitar NDMP en el clúster, configurar un usuario de backup, configurar LIF y configurar la aplicación de backup.



Preparar configuraciones NDMP de ONTAP

Antes de configurar el acceso al backup a cinta mediante el protocolo de gestión de datos de red (NDMP), debe comprobar que la configuración planificada es compatible y comprobar que las unidades de cinta aparecen como unidades adecuadas en cada nodo, verificar que todos los nodos tienen LIF de interconexión de clústeres. E identifique si la aplicación de backup es compatible con la extensión Cluster Aware Backup (CAB).

Pasos

1. Consulte la matriz de compatibilidad del proveedor de aplicaciones de backup para obtener información sobre la compatibilidad con ONTAP (NetApp no reúne los requisitos de aplicaciones de backup de terceros con ONTAP o NDMP).

   Debe verificar que los siguientes componentes de NetApp sean compatibles:

   - La versión de ONTAP 9 que se ejecuta en el clúster.
   - El proveedor de aplicaciones de backup y la versión: Por ejemplo, Veritas NetBackup 8.2 o

CommVault.

- Los detalles de los dispositivos de cinta, como el fabricante, el modelo y la interfaz de las unidades de cinta: Por ejemplo, IBM Ultrium 8 o HPE StoreEver Ultrium 30750 LTO-8.
- Las plataformas de los nodos del clúster: Por ejemplo, FAS8700 o A400.

> Puede encontrar matrices de compatibilidad de ONTAP heredadas para aplicaciones de copia de seguridad en "Herramienta de matriz de interoperabilidad de NetApp" .

2. Compruebe que las unidades de cinta aparecen como unidades cualificadas en el archivo de configuración de cinta incorporado de cada nodo:

   a. En la interfaz de línea de comandos, vea el archivo de configuración de cinta incorporado con el `storage tape show-supported-status` comando.

```
cluster1::> storage tape show-supported-status

Node: cluster1-1
                                 Is
Tape Drives                      Supported  Support Status
-------------------------------  ---------
-------------------------------
Certance Ultrium 2               true       Dynamically Qualified
Certance Ultrium 3               true       Dynamically Qualified
Digital DLT2000                  true       Qualified
```

   b. Compare las unidades de cinta con la lista de unidades cualificadas de la salida.

> Los nombres de los dispositivos de cinta de la salida pueden variar ligeramente con respecto a los nombres de la etiqueta del dispositivo o de la matriz de interoperabilidad. Por ejemplo, Digital DLT2000 también se conoce como DLT2k. Puede ignorar estas pequeñas diferencias de nomenclatura.

   c. Si un dispositivo no aparece como cualificado en el resultado a pesar de que el dispositivo está cualificado según la matriz de interoperabilidad, descargue e instale un archivo de configuración actualizado para el dispositivo con las instrucciones en el sitio de soporte de NetApp.

      "Descargas de NetApp: Archivos de configuración de dispositivo de cinta"

   Es posible que un dispositivo cualificado no aparezca en el archivo de configuración de cinta integrado si el dispositivo de cinta fue cualificado después de enviar el nodo.

3. Compruebe que todos los nodos del clúster tienen una LIF de interconexión de clústeres:

   a. Vea las LIF de interconexión de clústeres en los nodos mediante `network interface show -role intercluster` el comando.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

b. Si no hay una LIF de interconexión de clústeres en ningún nodo, cree una LIF de interconexión de clústeres mediante `network interface create` el comando.

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

Obtenga más información sobre `network interface create` en el "Referencia de comandos del ONTAP".

"Gestión de redes"

4. Identifique si la aplicación de backup es compatible con Cluster Aware Backup (CAB) mediante la documentación proporcionada con la aplicación de backup.

   El soporte CAB es un factor clave a la hora de determinar el tipo de backup que se puede realizar.

Información relacionada

- "espectáculo de cintas de almacenamiento"
- "cinta de almacenamiento mostrar-estado-compatible"

Verificar las conexiones del dispositivo de cinta NDMP de ONTAP

Debe asegurarse de que todas las unidades e intercambiadores de medios sean visibles en ONTAP como dispositivos.

Pasos

1. Permite ver información sobre todas las unidades y los cambiadores de medios mediante `storage tape show` el comando.

```
cluster1::> storage tape show

Node: cluster1-01
Device ID               Device Type     Description
Status
----------------------  --------------  ------------------------------
--------
sw4:10.11               tape drive      HP LTO-3
normal
0b.125L1                media changer   HP MSL G3 Series
normal
0d.4                    tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                  media changer   IBM 3573-TL
normal
...
```

2. Si no se muestra una unidad de cinta, solucione el problema.
3. Si no se muestra un cambiador de medios, consulte la información sobre los cambiadores de medios mediante el `storage tape show-media-changer` comando y, a continuación, solucione el problema.

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

Información relacionada

- "Cambiador de medios de exhibición de cintas de almacenamiento"

Habilitar reservas de cinta para operaciones de respaldo NDMP de ONTAP

Debe asegurarse de que las unidades de cinta estén reservadas para que las aplicaciones de backup las operaciones de backup de NDMP.

Acerca de esta tarea

La configuración de las reservas varía en diferentes aplicaciones de backup, y esta configuración debe coincidir con la aplicación de backup y los nodos o servidores que utilizan las mismas unidades. Consulte la documentación del proveedor de la aplicación de backup para obtener los ajustes de reserva correctos.

Pasos

1. Active las reservas con el `options -option-name tape.reservations -option-value persistent` comando.

   El siguiente comando habilita reservas con `persistent` el valor:

```
cluster1::> options -option-name tape.reservations -option-value
persistent
2 entries were modified.
```

2. Verifique que las reservas estén habilitadas en todos los nodos mediante `options tape.reservations` el comando y, a continuación, revise la salida.

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                persistent

cluster1-2
    tape.reservations                persistent
2 entries were displayed.
```

Configure NDMP con ámbito SVM

Habilitar NDMP con ámbito SVM en el clúster ONTAP

Si el DMA admite la extensión Cluster Aware Backup (CAB), puede realizar un backup de todos los volúmenes alojados en diferentes nodos de un clúster mediante la habilitación de NDMP de ámbito SVM, la habilitación del servicio NDMP en el clúster (SVM de administrador) y la configuración de LIF para la conexión de datos y control.

Antes de empezar

La extensión DE LA CABINA debe ser compatible con el DMA.

Acerca de esta tarea

Al desactivar el modo de NDMP con ámbito del nodo, es posible habilitar el modo NDMP con ámbito SVM en el clúster.

Pasos

1. Habilitar modo NDMP en ámbito de SVM:

   ```
   cluster1::> system services ndmp node-scope-mode off
   ```

   El modo NDMP en el ámbito de SVM está habilitado.

2. Habilite el servicio NDMP en la SVM de administrador:

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   El tipo de autenticación se establece en `challenge` de forma predeterminada y la autenticación de texto sin formato está desactivada.

   > Para una comunicación segura, debe mantener la autenticación de texto sin formato deshabilitada.

3. Compruebe que el servicio NDMP está activado:

```
cluster1::> vserver services ndmp show
```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

Habilitar usuarios de respaldo para la autenticación NDMP de ONTAP

Para autenticar NDMP de ámbito SVM desde la aplicación de backup, debe haber un usuario administrativo con suficientes privilegios y una contraseña NDMP.

Acerca de esta tarea

Debe generar una contraseña de NDMP para los usuarios administradores de backup. Puede habilitar los usuarios administradores de backup en el nivel del clúster o la SVM; si fuera necesario, puede crear un usuario nuevo. De forma predeterminada, los usuarios con los siguientes roles pueden autenticar para el backup NDMP:

- En todo el clúster `admin`: O. `backup`
- SVM individuales: `vsadmin` O. `vsadmin-backup`

Si utiliza un usuario NIS o LDAP, el usuario debe existir en el servidor correspondiente. No puede utilizar un usuario de Active Directory.

Pasos

1. Mostrar los usuarios y permisos de administrador actuales:

   `security login show`

   Obtenga más información sobre `security login show` en el "Referencia de comandos del ONTAP".

2. Si es necesario, cree un nuevo usuario de backup de NDMP con `security login create` el comando y el rol correspondiente a una Privileges de SVM individual o para todo el clúster.

   Se puede especificar un nombre de usuario de backup local o un nombre de usuario NIS o LDAP para el `-user-or-group-name` parámetro.

   El siguiente comando crea el usuario de backup `backup_admin1` con `backup` el rol para todo el clúster:

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   El siguiente comando crea el usuario de backup `vsbackup_admin1` con `vsadmin-backup` el rol de una SVM individual:

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

Introduzca una contraseña para el nuevo usuario y confirme.

Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

3. Generar una contraseña para la SVM de administrador con `vserver services ndmp generate password` el comando.

   La contraseña generada debe utilizarse para autenticar la conexión NDMP por parte de la aplicación de copia de seguridad.

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

 Vserver: cluster1
    User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

Configurar LIF de ONTAP para NDMP con ámbito SVM

Debe identificar las LIF que se usarán para establecer una conexión de datos entre los recursos de cinta y los de datos, y para controlar la conexión entre la SVM de administrador y la aplicación de backup. Tras identificar las LIF, debe comprobar que se establecen las políticas de servicio y de recuperación tras fallos.

> 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 "Gestione el tráfico compatible".

ONTAP 9.10.1 o posterior

Pasos

1. Identifique la LIF de interconexión de clústeres alojada en los nodos mediante `network interface show` el comando con `-service-policy` el parámetro.

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

   Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

2. Identifique la LIF de gestión alojada en los nodos mediante `network interface show` el comando con `-service-policy` el parámetro.

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

3. Asegúrese de que la LIF de interconexión de clústeres incluye el `backup-ndmp-control` servicio:

   ```
   network interface service-policy show
   ```

   Obtenga más información sobre `network interface service-policy show` en el "Referencia de comandos del ONTAP".

4. Asegurarse de que la política de conmutación por error esté establecida de forma adecuada para todos los LIF:

   a. Compruebe que la política de recuperación tras fallos para la LIF de administración de clúster está establecida en `broadcast-domain-wide` y que la política de las LIF de interconexión de clústeres y gestión de nodos está establecida en `local-only` mediante el `network interface show -failover` comando.

      El siguiente comando muestra la política de conmutación por error para las LIF de gestión de clústeres, interconexión de clústeres y nodos:

```
cluster1::> network interface show -failover

           Logical          Home             Failover    Failover
Vserver    Interface        Node:Port        Policy      Group
-------    --------------   --------------   ----------  --------
cluster    cluster1_clus1   cluster1-1:e0a   local-only  cluster
                                                         Failover
Targets:
                                                         .......
cluster1   cluster_mgmt     cluster1-1:e0m   broadcast-  Default
                                                domain-wide
                                                         Failover
Targets:
                                                         .......
           IC1              cluster1-1:e0a   local-only  Default
                                                         Failover
Targets:
           IC2              cluster1-1:e0b   local-only  Default
                                                         Failover
Targets:
                                                         .......
cluster1-1 c1-1_mgmt1       cluster1-1:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
cluster1-2 c1-2_mgmt1       cluster1-2:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
```

a. Si las políticas de conmutación por error no se establecen correctamente, modifique la política de conmutación por error mediante el `network interface modify` comando con `-failover -policy` el parámetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Obtenga más información sobre `network interface modify` en el "Referencia de comandos del ONTAP".

5. Especifique las LIF necesarias para la conexión de datos mediante `vserver services ndmp modify` el comando con `preferred-interface-role` el parámetro.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. Compruebe que el rol de interfaz preferido está configurado para el clúster mediante `vserver services ndmp show` el comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .......
                .......
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9.9 o anterior

Pasos

1. Identifique las LIF de interconexión de clústeres, gestión de clústeres y gestión de nodos mediante `network interface show` el comando con `-role` el parámetro.

   El siguiente comando muestra las LIF de interconexión de clústeres:

```
cluster1::> network interface show -role intercluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ----------   ---------- ------------------ -------------
------- ----
cluster1    IC1          up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2          up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   El siguiente comando muestra la LIF de gestión del clúster:

```
cluster1::> network interface show -role cluster-mgmt

            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ----------    ---------- ------------------ -----------
------- ----
cluster1    cluster_mgmt  up/up      192.0.2.60/24      cluster1-2
e0M     true
```

El siguiente comando muestra las LIF de gestión de nodos:

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network          Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask     Node
Port    Home
----------- ----------        ---------- ---------------
------------  ------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24    cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24    cluster1-2
e0M     true
```

Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

2. Asegúrese de que la política de firewall esté habilitada para NDMP en las (`node-mgmt`LIF de interconexión de clústeres, cluster-management)(`cluster-mgmt` y gestión de nodos):

   a. Compruebe que la política de firewall está habilitada para NDMP mediante `system services firewall policy show` el comando.

      El siguiente comando muestra la política de firewall para la LIF de administración de clústeres:

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                         ndmp       0.0.0.0/0
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

El siguiente comando muestra la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

El siguiente comando muestra la política de firewall de la LIF de gestión de nodos:

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- ------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. Si la política de firewall no está habilitada, habilite la política de firewall mediante `system services firewall policy modify` el comando con `-service` el parámetro.

   El siguiente comando habilita la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Asegurarse de que la política de conmutación por error esté establecida de forma adecuada para todos los LIF:

   a. Compruebe que la política de recuperación tras fallos para la LIF de administración de clúster está establecida en `broadcast-domain-wide` y que la política de las LIF de interconexión de clústeres y gestión de nodos está establecida en `local-only` mediante el `network interface show -failover` comando.

      El siguiente comando muestra la política de conmutación por error para las LIF de gestión de clústeres, interconexión de clústeres y nodos:

```
cluster1::> network interface show -failover

           Logical            Home               Failover
Failover
Vserver    Interface          Node:Port          Policy
Group
---------- -----------------  ------------------ --------------------
--------
cluster    cluster1_clus1     cluster1-1:e0a     local-only
cluster
                                                     Failover
Targets:
                                                     .......

cluster1   cluster_mgmt       cluster1-1:e0m     broadcast-domain-
wide Default
                                                     Failover
Targets:
                                                     .......
           IC1                 cluster1-1:e0a     local-only
Default
                                                     Failover
Targets:
           IC2                 cluster1-1:e0b     local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1 cluster1-1_mgmt1   cluster1-1:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
cluster1-2 cluster1-2_mgmt1   cluster1-2:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
```

a. Si las políticas de conmutación por error no se establecen correctamente, modifique la política de conmutación por error mediante el `network interface modify` comando con `-failover -policy` el parámetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Obtenga más información sobre `network interface modify` en el "Referencia de comandos del ONTAP".

4. Especifique las LIF necesarias para la conexión de datos mediante `vserver services ndmp modify` el comando con `preferred-interface-role` el parámetro.

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. Compruebe que el rol de interfaz preferido está configurado para el clúster mediante `vserver services ndmp show` el comando.

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

Configure el NDMP de ámbito del nodo

Habilitar NDMP con alcance de nodo en el clúster ONTAP

Puede realizar backups de volúmenes alojados en un único nodo. Para ello, active el NDMP de ámbito del nodo, lo que habilita el servicio NDMP y configura una LIF para la conexión de datos y control. Esto puede hacerse para todos los nodos del clúster.

NDMP de ámbito del nodo está obsoleto en ONTAP 9.

Acerca de esta tarea

Cuando se utiliza NDMP en el modo de alcance del nodo, la autenticación debe configurarse por nodo. Para obtener más información, consulte "El artículo de la base de conocimientos "Cómo configurar la autenticación NDMP en el modo de alcance de nodo"".

Pasos

1. Habilitar modo NDMP de ámbito de nodo:

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP node-scope-mode está activado.

2. Habilite el servicio NDMP en todos los nodos del clúster:

   Si utiliza el comodín "'*'", se habilita el servicio NDMP en todos los nodos al mismo tiempo.

   Debe especificar una contraseña para la autenticación de la conexión NDMP mediante la aplicación de backup.

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. Deshabilite `-clear-text` la opción de comunicación segura de la contraseña NDMP:

   Usando la*" `disables the -clear-text` opción comodín '` en todos los nodos al mismo tiempo.

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. Compruebe que el servicio NDMP está activado y que la `-clear-text` opción está desactivada:

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

Configurar LIF de ONTAP para NDMP con ámbito de nodo

Debe identificar una LIF que se utilizará para establecer una conexión de datos y controlar la conexión entre el nodo y la aplicación de backup. Tras identificar la LIF, debe verificar que las políticas de firewall y recuperación tras fallos están establecidas para la LIF.

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 "Gestione el tráfico compatible".

ONTAP 9.10.1 o posterior

Pasos

1. Identifique la LIF de interconexión de clústeres alojada en los nodos mediante `network interface show` el comando con `-service-policy` el parámetro.

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

2. Asegúrese de que la LIF de interconexión de clústeres incluye el `backup-ndmp-control` servicio:

   ```
   network interface service-policy show
   ```

3. Asegúrese de que la normativa de recuperación tras fallos esté establecida de forma adecuada para las LIF de interconexión de clústeres:

   a. Compruebe que la política de conmutación por error de las LIF de interconexión de clústeres está establecida en `local-only` mediante `network interface show -failover` el comando.

   ```
   cluster1::> network interface show -failover
               Logical          Home               Failover
   Failover
   Vserver     Interface        Node:Port          Policy       Group
   --------    ---------------  -----------------  ------------
   --------
   cluster1    IC1               cluster1-1:e0a    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
               IC2               cluster1-2:e0b    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
   cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
   Default
                                                       Failover
   Targets:
                                                       .......
   ```

   b. Si la política de conmutación por error no está establecida correctamente, modifique la política de conmutación por error mediante el `network interface modify` comando con `-failover -policy` el parámetro.

   ```
   cluster1::> network interface modify -vserver cluster1 -lif IC1
   -failover-policy local-only
   ```

Obtenga más información acerca de `network interface show`, `network interface service-policy show` y `network interface modify` en el "Referencia de comandos del ONTAP".

ONTAP 9.9 o anterior

Pasos

1. Identifique la LIF de interconexión de clústeres alojada en los nodos mediante `network interface show` el comando con `-role` el parámetro.

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

2. Compruebe que la política de firewall está activada para NDMP en las LIF de interconexión de clústeres:

   a. Compruebe que la política de firewall está habilitada para NDMP mediante `system services firewall policy show` el comando.

   El siguiente comando muestra la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

b. Si la política de firewall no está habilitada, habilite la política de firewall mediante `system services firewall policy modify` el comando con `-service` el parámetro.

   El siguiente comando habilita la política de firewall para la LIF de interconexión de clústeres:

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. Asegúrese de que la normativa de recuperación tras fallos esté establecida de forma adecuada para las LIF de interconexión de clústeres:

   a. Compruebe que la política de conmutación por error de las LIF de interconexión de clústeres está establecida en `local-only` mediante `network interface show -failover` el comando.

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                    Failover
Targets:
                                                    .......
            IC2               cluster1-2:e0b    local-only
Default
                                                    Failover
Targets:
                                                    .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                    Failover
Targets:
                                                    .......
```

   b. Si la política de conmutación por error no está establecida correctamente, modifique la política de conmutación por error mediante el `network interface modify` comando con `-failover -policy` el parámetro.

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

Obtenga más información sobre `network interface show` y `network interface modify` en el "Referencia de comandos del ONTAP".

Configurar aplicaciones de respaldo para la configuración NDMP de ONTAP

Una vez que se configura el clúster para el acceso NDMP, debe recopilar información de la configuración del clúster y, a continuación, configurar el resto del proceso de backup en la aplicación de backup.

Pasos

1. Recopile la siguiente información configurada anteriormente en ONTAP:
   - El nombre de usuario y la contraseña que la aplicación de backup necesita para crear la conexión NDMP
   - Las direcciones IP de las LIF de interconexión de clústeres que necesita la aplicación de backup para conectarse al clúster
2. En ONTAP, muestre los alias que ONTAP asignó a cada dispositivo mediante `storage tape alias show` el comando.

   Los alias suelen ser útiles para configurar la aplicación de copia de seguridad.

   ```
   cluster1::> storage tape show -alias

     Device ID: 2a.0
   Device Type: tape drive
   Description: Hewlett-Packard LTO-5

   Node                         Alias     Mapping
   ---------------------------- --------- ------------------------------
   stsw-3220-4a-4b-02           st2       SN[HU19497WVR]
   ...
   ```

3. En la aplicación de copia de seguridad, configure el resto del proceso de copia de seguridad utilizando la documentación de la aplicación de copia de seguridad.

Después de terminar

Si se produce un evento de movilidad de datos, como un movimiento de volúmenes o una migración LIF, debe estar preparado para reiniciar todas las operaciones de backup interrumpidas.

Información relacionada

- "Mostrar alias de cinta de almacenamiento"

Replicación entre software de NetApp Element y información general de ONTAP

Puede garantizar la continuidad del negocio en un sistema Element mediante SnapMirror para replicar copias Snapshot de un volumen de Element en un destino de ONTAP. En caso de desastre en el sitio de Element, podrá seguir prestando servicio a los clientes desde el sistema ONTAP y, a continuación, reactivar el sistema Element cuando el servicio se restaure.

A partir de ONTAP 9,4, puede replicar copias de Snapshot de una LUN creada en un nodo ONTAP en un sistema Element. Puede haber creado una LUN durante una interrupción del servicio en el sitio de Element, o bien podría utilizar una LUN para migrar datos desde ONTAP al software Element.

"Configurar la replicación del software NetApp Element y ONTAP".

Información de copyright

Copyright © 2026 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.