Configuración, actualización y reversión de ONTAP

ONTAP 9

NetApp
April 16, 2024

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

Tabla de contenidos

Configure, actualice y revierta el software y el firmware de ONTAP 1
Configure ONTAP 1
Actualice ONTAP 18
Firmware y actualizaciones del sistema 159
Revierte ONTAP 166

Configure, actualice y revierta el software y el firmware de ONTAP

Configure ONTAP

Comience a utilizar la configuración del clúster de ONTAP

Puede usar System Manager o la interfaz de línea de comandos (CLI) de ONTAP para configurar clústeres de ONTAP nuevos. Antes de empezar, debe recopilar la información que necesitará para completar la configuración del clúster, como el puerto de la interfaz de gestión del clúster y la dirección IP.

NetApp le recomienda "Use System Manager para configurar clústeres nuevos". System Manager proporciona un flujo de trabajo sencillo y sencillo para la instalación y la configuración del clúster, incluidas la asignación de una dirección IP de gestión de nodos, la inicialización del clúster, la creación de un nivel local, la configuración de protocolos y el aprovisionamiento del almacenamiento inicial.

Solo es necesario hacerlo "Use la interfaz de línea de comandos de ONTAP para configurar el clúster" Si ejecuta ONTAP 9,7 o una versión anterior en una configuración de MetroCluster.
A partir de ONTAP 9.13.1, en las plataformas A800 y FAS8700 de AFF, también se puede usar la interfaz de línea de comandos de ONTAP para crear y configurar clústeres nuevos en entornos de red solo IPv6. Si necesita usar IPv6 en ONTAP 9.13.0 y versiones anteriores, o en otras plataformas en ONTAP 9.13.1 y versiones posteriores, puede usar System Manager para crear clústeres nuevos con IPv4 y a continuación "Convertir a IPv6".

Qué necesitará para la configuración del clúster

La configuración del clúster implica recopilar la información necesaria para configurar cada nodo, crear el clúster en el primer nodo y unir los nodos restantes al clúster.

Comience reuniendo toda la información relevante de las hojas de cálculo de la configuración del clúster.

La hoja de cálculo de configuración del clúster le permite registrar los valores que necesita durante el proceso de configuración del clúster. Si se proporciona un valor predeterminado, puede usar dicho valor, o bien puede introducir el que desee.

Valores predeterminados del sistema

Los valores predeterminados del sistema son los valores predeterminados de la red de clúster privada. Se recomienda usar los valores predeterminados. Sin embargo, si estos no cumplen con los requisitos, puede usar la tabla para registrar sus propios valores.

> Para los clústeres configurados de manera que usen switches de red, cada switch de clúster debe usar el tamaño de MTU de 9000.

Tipos de información	Sus valores
Puertos de red de clúster privada	
La máscara de red de clúster	

Tipos de información	Sus valores
Direcciones IP de interfaz de clúster (para cada puerto de red de clúster de cada nodo) Las direcciones IP para cada nodo deben estar en la misma subred.	

Información del clúster

Tipos de información	Sus valores
Nombre del clúster El nombre debe comenzar por una letra y debe tener menos de 44 caracteres. El nombre puede incluir los siguientes caracteres especiales: . - _	

Claves de licencia de funciones

Puede encontrar las claves de licencia para los pedidos de software iniciales o adicionales en el sitio de soporte de NetApp en **My Support** > **licencias de software**.

Tipos de información	Sus valores
Claves de licencia de funciones	

Máquina virtual de almacenamiento (SVM) de administrador

Tipos de información	Sus valores
Contraseña de administrador del clúster La contraseña de la cuenta de administrador que el clúster necesita para brindar acceso de administrador de clúster a la consola o a través de un protocolo seguro. Por motivos de seguridad, no se recomienda grabar contraseñas en esta hoja de trabajo. Las reglas predeterminadas de las contraseñas son las siguientes: • La contraseña debe tener al menos 8 caracteres. • La contraseña debe contener al menos una letra y un número.	

Tipos de información	Sus valores
Puerto de la interfaz de gestión de clústeres El puerto físico que está conectado a la red de datos y que permite que el administrador de clúster gestione el clúster.	
Dirección IP de la interfaz de gestión de clústeres Una dirección IPv4 o IPv6 exclusiva para la interfaz de gestión de clústeres. El administrador de clúster utiliza esta dirección para acceder a la SVM de administrador y gestionar el clúster. Generalmente, esta dirección debe estar en la red de datos. Puede pedirle esta dirección IP al administrador responsable de la asignación de direcciones IP en la organización. Ejemplo: 192.0.2.66	
Máscara de red de la interfaz de gestión de clústeres (IPv4) La máscara de subred que define el rango de direcciones IPv4 válidas en la red de gestión de clústeres. Ejemplo: 255.255.255.0	
Longitud de la máscara de red de la interfaz de gestión de clústeres (IPv6) Si la interfaz de gestión de clústeres utiliza una dirección IPv6, este valor representa la longitud del prefijo que define el rango de direcciones IPv6 válidas en la red de gestión de clústeres. Ejemplo: 64	
Puerta de enlace predeterminada de la interfaz de gestión de clústeres La dirección IP del enrutador de la red de gestión de clústeres.	

Tipos de información	Sus valores
Nombre de dominio DNS El nombre del dominio DNS de la red. El nombre de dominio debe estar compuesto de caracteres alfanuméricos. Para introducir varios nombres de dominio DNS, separe cada uno con una coma o un espacio.	
Las direcciones IP del servidor de nombres Las direcciones IP de los servidores de nombres DNS. Separe las direcciones con una coma o un espacio.	

Información del nodo (para cada nodo del clúster)

Tipos de información	Sus valores
Ubicación física de la controladora (opcional) Una descripción de la ubicación física de la controladora. Use una descripción que identifique la ubicación del nodo en el clúster (por ejemplo, «"Lab 5, fila 7, rack B»).	
Puerto de la interfaz de gestión de nodos El puerto físico que está conectado a la red de gestión de nodos y que permite que el administrador de clústeres gestione el nodo.	
Dirección IP de la interfaz de gestión de nodos Una dirección IPv4 o IPv6 exclusiva para la interfaz de gestión de nodos en la red de gestión. Si ha definido el puerto de la interfaz de gestión de nodos de manera que sea un puerto de datos, esta dirección IP debe ser una dirección IP exclusiva en la red de datos. Puede pedirle esta dirección IP al administrador responsable de la asignación de direcciones IP en la organización. Ejemplo: 192.0.2.66	

Tipos de información	Sus valores
Máscara de red de la interfaz de gestión de nodos (IPv4) La máscara de subred que define el rango de direcciones IP válidas en la red de gestión de nodos. Si ha definido el puerto de la interfaz de gestión de nodos de manera que sea un puerto de datos, esta máscara de red debe ser la máscara de subred de la red de datos. Ejemplo: 255.255.255.0	
Longitud de la máscara de red de la interfaz de gestión de nodos (IPv6) Si la interfaz de gestión de nodos utiliza una dirección IPv6, este valor representa la longitud del prefijo que define el rango de direcciones IPv6 válidas en la red de gestión de nodos. Ejemplo: 64	
Puerta de enlace predeterminada de la interfaz de gestión de nodos La dirección IP del enrutador de la red de gestión de nodos.	

Información del servidor NTP

Tipos de información	Sus valores
Direcciones del servidor NTP Las direcciones IP de los servidores de Protocolo de hora de red (NTP) del sitio. Estos servidores se utilizan para sincronizar la hora en todo el clúster.	

Configure ONTAP en un nuevo clúster con System Manager

System Manager proporciona un flujo de trabajo sencillo y sencillo para configurar un clúster nuevo y el almacenamiento.

En algunos casos, como determinadas puestas en marcha de MetroCluster o los clústeres que requieren direccionamiento de red IPv6, puede que tenga que usar la CLI de ONTAP para configurar un clúster nuevo. Haga clic en "aquí" Para obtener más detalles sobre estos requisitos, así como los pasos para la configuración del clúster con la CLI de ONTAP.

Antes de empezar

- Debe haber instalado, cableado y encendido el nuevo sistema de almacenamiento de acuerdo con las instrucciones de instalación y configuración de su modelo de plataforma.
  Consulte "Documentación de AFF y FAS".
- Las interfaces de red de clúster se deben configurar en cada nodo del clúster para la comunicación dentro del clúster.
- Debe tener en cuenta los siguientes requisitos de soporte de System Manager:
  - Cuando se configura manualmente la gestión de nodos mediante la CLI, System Manager solo admite IPv4 y no admite IPv6. Sin embargo, si inicia System Manager después de completar la configuración del hardware mediante DHCP con una dirección IP asignada automáticamente y con la detección de Windows, System Manager puede configurar una dirección de gestión IPv6.

    En ONTAP 9.6 y versiones anteriores, System Manager no admite puestas en marcha que requieran redes IPv6.

  - La compatibilidad con la configuración de MetroCluster está destinada a las configuraciones IP de MetroCluster, con dos nodos en cada sitio.

    En ONTAP 9.7 y versiones anteriores, System Manager no admite una nueva configuración de clúster para las configuraciones de MetroCluster.

Asigne una dirección IP de gestión de nodos

Sistema Windows

Debe conectar el equipo con Windows a la misma subred que las controladoras. De este modo se asignará automáticamente una dirección IP de gestión de nodos al sistema.

Paso

1. Desde el sistema Windows, abra la unidad **Network** para descubrir los nodos.
2. Haga doble clic en el nodo para iniciar el asistente de configuración de clúster.

Otros sistemas

Debe configurar la dirección IP de gestión de nodos para uno de los nodos del clúster. Puede usar esta dirección IP de gestión de nodos para iniciar el asistente de configuración del clúster.

Consulte "Creación del clúster en el primer nodo" Para obtener información sobre la asignación de una dirección IP de gestión de nodos.

Inicialice el clúster

Para inicializar el clúster, debe establecer una contraseña de administrador para el clúster y configurar las redes de gestión de clústeres y nodos. También puede configurar servicios como un servidor DNS para resolver nombres de host y un servidor NTP para sincronizar la hora.

Pasos

1. En un navegador web, introduzca la dirección IP de gestión de nodos que haya configurado: "https://node-management-IP"

   System Manager detecta automáticamente los nodos restantes del clúster.

2. Inicialice el sistema de almacenamiento configurando la red de gestión de clústeres y las direcciones IP de gestión de nodos para todos los nodos.

Cree su nivel local

Crear niveles locales a partir de los discos o SSD disponibles en los nodos. System Manager calcula automáticamente la configuración de mejor nivel según su hardware.

Pasos

1. Haga clic en **Panel** y, a continuación, en **preparar almacenamiento**.

   Acepte la recomendación de almacenamiento para su nivel local.

Configure los protocolos

Según las licencias habilitadas en el clúster, puede habilitar los protocolos deseados en su clúster. A continuación, debe crear interfaces de red con las que puede acceder al almacenamiento.

Pasos

1. Haga clic en **Panel** y, a continuación, en **Configurar protocolos**.
   - Habilite iSCSI o FC para el acceso SAN.
   - Habilite NFS o SMB para el acceso NAS.
   - Habilite NVMe para el acceso a FC-NVMe.

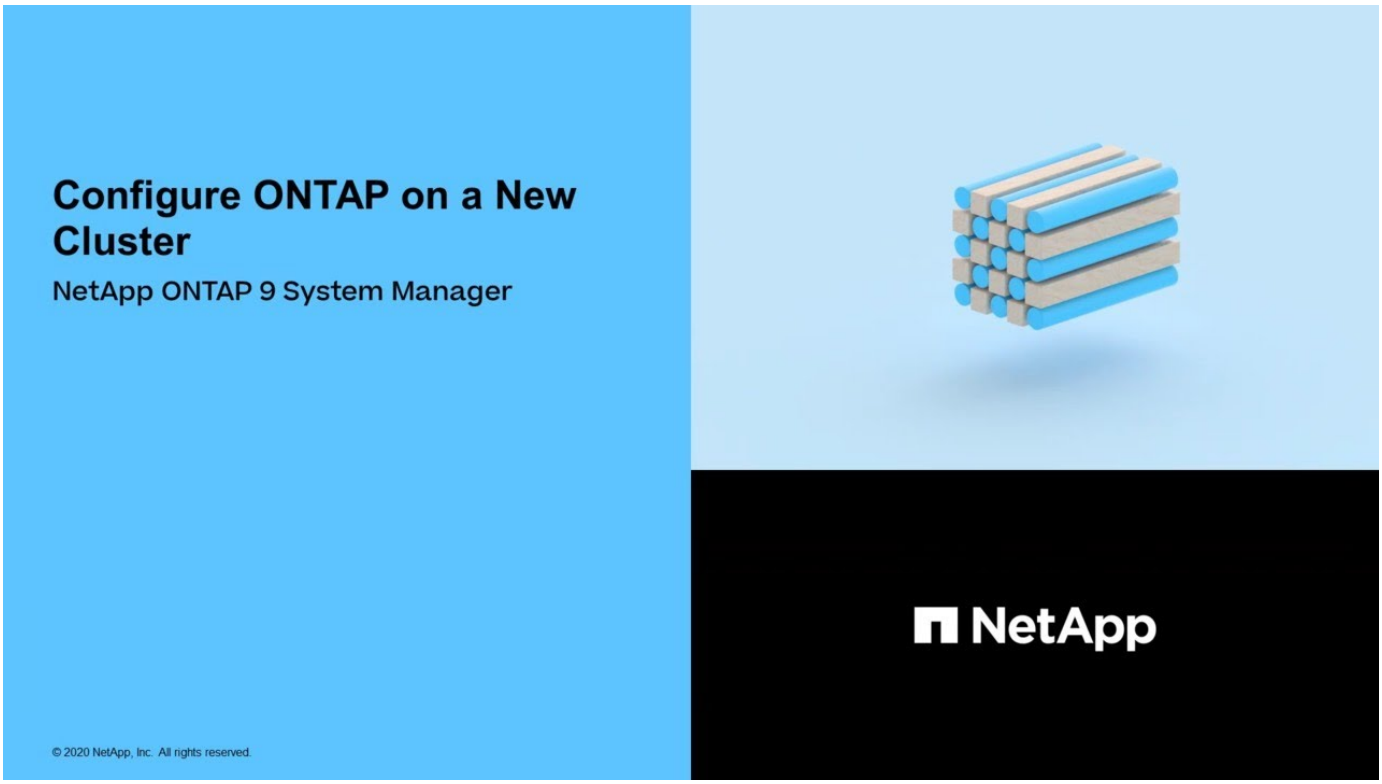
Aprovisionar almacenamiento

Después de configurar los protocolos, puede aprovisionar almacenamiento. Las opciones que vea dependen de las licencias que se instalen.

Pasos

1. Haga clic en **Panel** y, a continuación, en **aprovisionar almacenamiento**.
   - Para "Aprovisione el acceso SAN", Haga clic en **Agregar LUN**.
   - Para "Aprovisione el acceso NAS", Haga clic en **Agregar volúmenes**.
   - Para "Aprovisione el almacenamiento NVMe", Haga clic en **Agregar espacios de nombres**.

Configure ONTAP en un vídeo de clúster nuevo



Configure un clúster con la CLI

Cree el clúster en el primer nodo

Utilice el Asistente de configuración de clúster para crear el clúster en el primer nodo. El asistente le permite configurar la red del clústeres que conecta los nodos, crear la máquina virtual de almacenamiento (SVM) de administrador de clústeres, añadir las claves de licencia de funciones y crear la interfaz de gestión de nodos para el primer nodo.

Antes de empezar

- Debe haber instalado, cableado y encendido el nuevo sistema de almacenamiento de acuerdo con las instrucciones de instalación y configuración de su modelo de plataforma.
  Consulte "Documentación de AFF y FAS".
- Las interfaces de red de clúster se deben configurar en cada nodo del clúster para la comunicación dentro del clúster.
- Si va a configurar IPv6 en su clúster, IPv6 debe configurarse en la controladora de gestión base (BMC) para poder acceder al sistema mediante SSH.

Pasos

1. Encienda todos los nodos que va a añadir al clúster. Esto es necesario para habilitar la detección para la configuración del clúster.
2. Conéctese a la consola del primer nodo.

   El nodo arranca y, a continuación, se inicia el Asistente de configuración de clúster en la consola.

```
Welcome to the cluster setup wizard....
```

3. Reconozca la declaración de AutoSupport.

```
Type yes to confirm and continue {yes}: yes
```

> AutoSupport está habilitado de forma predeterminada.

4. Siga las instrucciones que aparecen en pantalla para asignar una dirección IP al nodo.

   A partir de ONTAP 9.13.1, puede asignar direcciones IPv6 para las LIF de gestión en las plataformas A800 y FAS8700. Para versiones de ONTAP anteriores a 9.13.1, o para 9.13.1 o versiones posteriores en otras plataformas, debe asignar direcciones IPv4 para las LIF de gestión y, después, convertirlas a IPv6 tras completar la configuración del clúster.

5. Pulse **Intro** para continuar.

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

6. Cree un nuevo clúster: `create`
7. Acepte los valores predeterminados del sistema o introduzca sus propios valores.
8. Una vez completada la configuración, inicie sesión en el clúster y compruebe que el clúster esté activo y que el primer nodo esté en buen estado. Para ello, introduzca el comando de la CLI de ONTAP: `cluster show`

   El siguiente ejemplo muestra un clúster en el que el primer nodo (cluster1-01) está en buen estado y puede participar:

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
```

   Puede acceder al Asistente de configuración de clúster para cambiar cualquiera de los valores introducidos para la SVM de administrador o la SVM de nodo mediante el `cluster setup` comando.

Después de terminar

Si es necesario, "Convertir de IPv4 a IPv6".

Una los nodos restantes al clúster

Después de crear un nuevo clúster, debe usar el Asistente de configuración de clúster para unir los nodos restantes al clúster de uno en uno. El asistente le permite configurar

la interfaz de gestión de nodos de cada nodo.

Cuando se unen dos nodos en un clúster, se crea un par de alta disponibilidad (ha). Si se une a 4 nodos, se crean dos pares de alta disponibilidad. Para obtener más información sobre alta disponibilidad, consulte "Obtenga más información sobre ha".

Solo puede unir un nodo a la vez al clúster. Tras comenzar a unir un nodo al clúster, debe completar la operación de unión de ese nodo y el nodo debe formar parte del clúster antes de poder unir el siguiente nodo.

Mejor práctica: Si tiene un sistema FAS2720 con 24 o menos unidades NL-SAS, debe verificar que el valor predeterminado de la configuración de almacenamiento es activo/pasivo para optimizar el rendimiento. Para obtener más información, consulte "Configuración de una configuración activo-pasivo en nodos mediante la partición de datos raíz"

1. Inicie sesión en el nodo que planea unir en el clúster.

   El asistente de configuración de clúster se inicia en la consola.

   ```
   Welcome to the cluster setup wizard....
   ```

2. Reconozca la declaración de AutoSupport.

   AutoSupport está habilitado de forma predeterminada.

   ```
   Type yes to confirm and continue {yes}: yes
   ```

3. Siga las instrucciones que aparecen en pantalla para asignar una dirección IP al nodo.

   A partir de ONTAP 9.13.1, puede asignar direcciones IPv6 para las LIF de gestión en las plataformas A800 y FAS8700. Para versiones de ONTAP anteriores a 9.13.1, o para 9.13.1 o versiones posteriores en otras plataformas, debe asignar direcciones IPv4 para las LIF de gestión y, después, convertirlas a IPv6 tras completar la configuración del clúster.

4. Pulse **Intro** para continuar.

   ```
   Do you want to create a new cluster or join an existing cluster?
   {create, join}:
   ```

5. Una el nodo al clúster: `join`
6. Siga las instrucciones que aparecen en pantalla para configurar el nodo y unirlo al clúster.
7. Tras completar la configuración, compruebe que el nodo esté en buen estado y que pueda participar en el clúster: `cluster show`

   En el siguiente ejemplo se muestra un clúster después de unirle el segundo nodo (cluster1-02):

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
cluster1-02           true    true
```

Puede acceder al Asistente de configuración de clúster para cambiar cualquiera de los valores introducidos para la SVM de administrador o la SVM de nodo mediante el comando cluster setup.

8. Repita esta acción para cada uno de los nodos restantes.

Después de terminar

Si es necesario, "Convertir de IPv4 a IPv6".

Convierta las LIF de gestión de IPv4 a IPv6

A partir de ONTAP 9.13.1, se pueden asignar direcciones IPv6 a las LIF de administración en plataformas A800 y FAS8700 durante la configuración inicial del clúster. Para versiones de ONTAP anteriores a 9.13.1, o para 9.13.1 o versiones posteriores en otras plataformas, primero debe asignar direcciones IPv4 a las LIF de gestión y, a continuación, convertir en direcciones IPv6 una vez completada la configuración del clúster.

Pasos

1. Habilite IPv6 para el clúster:

```
network options ipv6 modify -enable true
```

2. Establecer privilegio en avanzado:

```
set priv advanced
```

3. Vea la lista de prefijos de RA aprendidos en varias interfaces:

```
network ndp prefix show
```

4. Cree una LIF de gestión IPv6:

   Utilice el formato `prefix::id` En el parámetro address para construir la dirección IPv6 manualmente.

```
network interface create -vserver <svm_name> -lif <LIF> -home-node
<home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask
-length <netmask_length> -failover-policy <policy> -service-policy
<service_policy> -auto-revert true
```

5. Compruebe que la LIF se ha creado:

```
network interface show
```

6. Compruebe que se pueda acceder a la dirección IP configurada:

```
network ping6
```

7. Marcar el LIF IPv4 como inactivo de forma administrativa:

```
network interface modify -vserver <svm_name> -lif <lif_name> -status
-admin down
```

8. Elimine la LIF de gestión de IPv4:

```
network interface delete -vserver <svm_name> -lif <lif_name>
```

9. Confirmar que se ha eliminado el LIF de gestión de IPv4:

```
network interface show
```

Compruebe su clúster con Active IQ Config Advisor

Después de haber Unido todos los nodos al nuevo clúster, debe ejecutar Active IQ Config Advisor para validar su configuración y comprobar si hay errores de configuración comunes.

Config Advisor es una aplicación basada en web que instala en su portátil, máquina virtual o servidor, y funciona en plataformas Windows, Linux y Mac.

Config Advisor ejecuta una serie de comandos para validar la instalación y comprobar el estado general de la configuración, incluido el clúster y los switches de almacenamiento.

1. Descargue e instale Active IQ Config Advisor.

   "Active IQ Config Advisor"

2. Inicie Active IQ y configure una frase de contraseña cuando se le solicite.
3. Revise su configuración y haga clic en **Guardar**.
4. En la página **objetivos**, haga clic en **validación posterior a la implementación de ONTAP**.
5. Seleccione el modo guiado o experto.

   Si elige el modo guiado, los conmutadores conectados se detectan automáticamente.

6. Introduzca las credenciales del clúster.
7. (Opcional) haga clic en **validación de formulario**.
8. Para comenzar a recopilar datos, haga clic en **Guardar y evaluar**.
9. Después de completar la recopilación de datos, en **Monitor de trabajo > acciones**, vea los datos recopilados haciendo clic en el icono **Vista de datos** y vea los resultados haciendo clic en el icono **resultados**.
10. Resuelva los problemas identificados por Config Advisor.

Sincronice la hora del sistema en todo el clúster

La sincronización de la hora asegura que todos los nodos del clúster tengan la misma hora y evita errores de CIFS y Kerberos.

Debe configurarse un servidor de Protocolo de hora de red (NTP) en el sitio. A partir de ONTAP 9.5, puede configurar el servidor NTP con autenticación simétrica.
Para obtener más información, consulte "Gestionar la hora del clúster (solo administradores de clúster)".

Para sincronizar la hora en todo el clúster, debe asociarlo con uno o varios servidores NTP.

1. Compruebe que la hora y la zona horaria del sistema estén configuradas correctamente para cada nodo.

   Todos los nodos del clúster deben tener la misma zona horaria.

   a. Use el comando cluster date show para mostrar la fecha, la hora y la zona horaria actuales de cada nodo.

   ```
   cluster1::> cluster date show
   Node         Date                Time zone
   ------------ ------------------- -----------------
   cluster1-01  01/06/2015 09:35:15 America/New_York
   cluster1-02  01/06/2015 09:35:15 America/New_York
   cluster1-03  01/06/2015 09:35:15 America/New_York
   cluster1-04  01/06/2015 09:35:15 America/New_York
   4 entries were displayed.
   ```

   b. Use el comando cluster date modify para cambiar la fecha o la zona horaria de todos los nodos.

   En este ejemplo se cambia la zona horaria del clúster para que sea GMT:

```
cluster1::> cluster date modify -timezone GMT
```

2. Use el comando cluster time-service ntp Server create para asociar el clúster con el servidor NTP.

   - Para configurar el servidor NTP sin autenticación simétrica, introduzca el siguiente comando: `cluster time-service ntp server create -server server_name`
   - Para configurar el servidor NTP con autenticación simétrica, introduzca el siguiente comando: `cluster time-service ntp server create -server server_ip_address -key-id key_id`

     > La autenticación simétrica está disponible a partir de ONTAP 9.5. No está disponible en ONTAP 9.4 ni en versiones anteriores.

     En este ejemplo se supone que se ha configurado DNS para el clúster. Si no ha configurado DNS, debe especificar la dirección IP del servidor NTP:

```
cluster1::> cluster time-service ntp server create -server
ntp1.example.com
```

3. Compruebe que el clúster esté asociado con un servidor NTP: `cluster time-service ntp server show`

```
cluster1::> cluster time-service ntp server show
Server                Version
--------------------- -----------
ntp1.example.com      auto
```

Información relacionada

"Administración del sistema"

Comandos para gestionar la autenticación simétrica en servidores NTP

A partir de ONTAP 9.5, se admite la versión 3 del protocolo de tiempo de redes (NTP). NTPv3 incluye autenticación simétrica mediante claves SHA-1 que aumenta la seguridad de la red.

Para hacer esto…	Se usa este comando…
Configure un servidor NTP sin autenticación simétrica	`cluster time-service ntp server create -server server_name`
Configure un servidor NTP con autenticación simétrica	`cluster time-service ntp server create -server server_ip_address -key-id key_id`

Para hacer esto…	Se usa este comando…
Habilite la autenticación simétrica para un servidor NTP existente Un servidor NTP existente se puede modificar para habilitar la autenticación mediante la adición del identificador de clave requerido	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configure una clave NTP compartida	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` **Nota:** una ID hace referencia a las claves compartidas. El ID, su tipo y el valor deben ser idénticos tanto en el nodo como en el servidor NTP
Configure un servidor NTP con un ID de clave desconocido	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure un servidor con un ID de clave no configurado en el servidor NTP.	`cluster time-service ntp server create -server server_name -key-id key_id` **Nota:** el ID de clave, el tipo y el valor deben ser idénticos al ID de clave, el tipo y el valor configurados en el servidor NTP.
Deshabilitar la autenticación simétrica	`cluster time-service ntp server modify -server server_name -authentication disabled`

Tareas de configuración del sistema adicionales que se deben realizar

Después de configurar un clúster, puede usar System Manager o la interfaz de línea de comandos (CLI) de ONTAP para continuar configurando el clúster.

Tarea de configuración del sistema	Recurso
Configurar redes: • Cree dominios de retransmisión • Crear subredes • Cree espacios IP	"Configuración de la red"
Configure Service Processor	"Administración del sistema"
Distribuir los agregados	"Gestión de discos y agregados"

Tarea de configuración del sistema	Recurso
Crear y configurar las máquinas virtuales de almacenamiento de datos (SVM)	"Configuración de NFS" "Configuración de SMB" "Administración de SAN"
Configure las notificaciones de eventos	"Configuración de EMS"

Configure el software de cabina SAN All-Flash

Información general de la configuración del software de la cabina SAN all-flash

Las cabinas SAN all-flash (ASAS) de NetApp están disponibles a partir de ONTAP 9,7. ASAS son soluciones all-flash solo SAN creadas sobre las plataformas probadas de AFF de NetApp.

Las plataformas ASA utilizan activo-activo simétrico para la multivía. Todas las rutas son activas/optimizadas de modo que, en caso de conmutación al nodo de respaldo del almacenamiento, el host no necesita esperar a que se produzca la transición ALUA de las rutas de conmutación al nodo de respaldo para reanudar las operaciones de I/O. Esto reduce el tiempo de recuperación tras fallos.

Configure un ASA

Las cabinas SAN All-Flash (ASAS) siguen el mismo procedimiento de configuración que los sistemas no ASA.

System Manager le guía por los procedimientos necesarios para inicializar su clúster, crear un nivel local, configurar protocolos y aprovisionar almacenamiento para su ASA.

Comience a utilizar la configuración del clúster de ONTAP.

Configuración y utilidades del host ASA

La configuración del host para configurar cabinas All Flash SAN (ASAS) es la misma que la de todos los demás hosts SAN.

Puede descargar la "Software Host Utilities de NetApp" para los hosts específicos del sitio de soporte.

Formas de identificar un sistema ASA

Puede identificar un sistema ASA mediante System Manager o mediante la interfaz de línea de comandos (CLI) de ONTAP.

- **Desde el panel del Administrador del sistema**: Haz clic en **Clúster > Descripción general** y luego selecciona el nodo del sistema.

  La **PERSONALITY** se muestra como **All-Flash SAN Array**.

- **Desde la CLI**: Ingrese el `san config show` comando.

  El valor de las «cabinas SAN all-flash» es auténtico para los sistemas ASA.

Información relacionada

- "Informe técnico 4968: Integridad y disponibilidad de datos de las cabinas All-SAN de NetApp"
- "Informe técnico de NetApp 4080: Prácticas recomendadas para SAN moderno"

Límites de configuración y compatibilidad de cabinas All Flash SAN

Los límites de configuración y la compatibilidad de las cabinas All Flash SAN (ASA) varían según la versión de ONTAP.

Los detalles más actuales sobre los límites de configuración admitidos están disponibles en "Hardware Universe de NetApp".

Nodos y protocolos SAN por clúster

La compatibilidad de ASA con los protocolos SAN y los nodos por clúster es la siguiente:

Iniciando con ONTAP…	Compatibilidad con protocolos	N.o máx. De nodos por clúster
9.12.1	• NVMe (compatible con configuraciones IP de MetroCluster de 4 nodos y configuraciones IP distintas de MetroCluster) • FC • ISCSI	12
9.9.1	• NVMe (compatible con configuraciones IP que no sean de MetroCluster) • FC • ISCSI	• 12 nodos (para configuraciones IP que no sean de MetroCluser) • 8 nodos (para configuraciones IP de MetroCluster)
9,7	• FC • ISCSI	4

Compatibilidad con puertos persistentes

A partir de ONTAP 9,8, los puertos persistentes se habilitan de forma predeterminada en las cabinas all-flash SAN (ASAS) que se configuran para usar el protocolo FC. Los puertos persistentes solo están disponibles para FC y requieren pertenencia a una zona identificada por nombre de puerto WWPN.

Los puertos persistentes reducen el impacto de las tomas de control al crear un LIF en la sombra en el puerto físico correspondiente del partner de alta disponibilidad. Cuando se toma el control de un nodo, el LIF de respaldo del nodo del partner asume la identidad del LIF original, incluida la WWPNe. Antes de que el estado de la ruta al nodo tomado en defectuoso, la LIF redundante aparece como una ruta activa/optimizada para la pila MPIO del host y se cambia la I/O. De este modo, se reduce el trastorno de I/o porque el host siempre ve el mismo número de rutas al destino, incluso durante las operaciones de conmutación al nodo de respaldo del almacenamiento.

Para los puertos persistentes, las siguientes características de puerto FCP deben ser idénticas en el par de

alta disponibilidad:

- Números de puertos FCP
- Nombres de puerto FCP
- Velocidades de puerto FCP
- División en zonas basada en WWPN de LIF FCP

Si alguna de estas características no es idéntica en la pareja de alta disponibilidad, se genera el siguiente mensaje de EMS:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

Para obtener más información sobre los puertos persistentes, consulte "Informe técnico de NetApp 4080: Prácticas recomendadas para SAN moderno".

Actualice ONTAP

Información general de la actualización de ONTAP

Al actualizar el software ONTAP, puede aprovechar las nuevas y mejoradas funciones de ONTAP que le ayudarán a reducir costes, acelerar las cargas de trabajo críticas, mejorar la seguridad y ampliar el alcance de la protección de datos disponible para su organización.

Una importante actualización de ONTAP consiste en pasar de una versión con números ONTAP inferiores a superiores. Un ejemplo sería una actualización de su clúster de ONTAP 9,8 a ONTAP 9.12.1. Una actualización menor (o un parche) consiste en pasar de una versión de ONTAP inferior a una versión de ONTAP superior dentro de la misma versión numerada. Un ejemplo sería una actualización de su clúster de ONTAP 9.12.1P1 a 9.12.1P4.

Para comenzar, debe "prepare la actualización". Si tienes un contrato activo de SupportEdge para el asesor digital de Active IQ, deberías hacerlo "Planifique la actualización con el asesor de actualizaciones". El asesor de actualizaciones ofrece inteligencia que le ayuda a minimizar la incertidumbre y el riesgo al evaluar su clúster y crear un plan de actualización específico de su configuración.

Después de prepararse para la actualización, se recomienda realizar las actualizaciones con "Actualización automatizada y no disruptiva (ANDU) de System Manager". ANDU aprovecha la tecnología de conmutación al nodo de respaldo de alta disponibilidad de ONTAP para garantizar que los clústeres siguen sirviendo datos sin interrupciones durante la actualización.

> A partir de ONTAP 9.12.1, System Manager está totalmente integrado con BlueXP. Si BlueXP está configurado en tu sistema, puedes actualizarlo a través del entorno de trabajo de BlueXP.

Si necesita ayuda para actualizar su software ONTAP, los servicios profesionales de NetApp ofrecen un "Servicio de renovación gestionada". Si está interesado en usar este servicio, póngase en contacto con su representante de ventas de NetApp o con "Envíe el formulario de consulta de ventas de NetApp". El Servicio de Actualización Gestionada, así como otros tipos de soporte de actualización están disponibles para los clientes con "Servicios de SupportEdge Expert" sin coste adicional.

¿Cuándo debo actualizar ONTAP?

Debe actualizar su software ONTAP en una cadencia regular. La actualización de ONTAP le permite aprovechar las funciones y funcionalidades nuevas y mejoradas, e implementar las correcciones actuales para problemas conocidos.

Importantes renovaciones de ONTAP

Una importante actualización o versión de funciones de ONTAP suele incluir:

- Nuevas funciones de ONTAP
- Cambios clave en la infraestructura, como cambios fundamentales en el funcionamiento de NetApp WAFL o en el funcionamiento de RAID
- Compatibilidad con nuevos sistemas de hardware de ingeniería de NetApp
- Soporte para componentes de hardware de reemplazo, como tarjetas de interfaz de red más recientes o adaptadores de bus del host

Los nuevos lanzamientos de ONTAP tienen derecho a un soporte completo durante 3 años. NetApp recomienda ejecutar la versión más reciente durante 1 año tras la disponibilidad general (GA) y, a continuación, utilizar el tiempo restante dentro del plazo de soporte completo para planificar la transición a una versión de ONTAP más reciente.

Actualizaciones de revisiones de ONTAP

Las actualizaciones de parches proporcionan correcciones oportunas para errores críticos que no pueden esperar a que se publique la siguiente versión principal de la función de ONTAP. Las actualizaciones de parches no críticas se deben aplicar cada 3-6 meses. Las actualizaciones de parches críticos se deben aplicar lo antes posible.

Más información acerca de "niveles mínimos de parches recomendados" Para versiones ONTAP.

Fechas de lanzamiento de ONTAP

A partir del lanzamiento de ONTAP 9,8, NetApp ofrece lanzamientos de ONTAP dos veces al año. Si bien los planes pueden modificarse, el objetivo es ofrecer nuevos lanzamientos de ONTAP en el segundo y cuarto trimestre de cada año. Utilice esta información para planificar el período de tiempo de su actualización para aprovechar la última versión de ONTAP.

Versión	Fecha de lanzamiento
9.14.1	A enero de 2024
9.13.1	Junio de 2023
9.12.1	Febrero de 2023
9.11.1	Julio de 2022
9.10.1	A enero de 2022

Versión	Fecha de lanzamiento
9.9.1	Junio de 2021

Niveles de soporte de ONTAP

El nivel de soporte disponible para una versión específica de ONTAP varía en función de cuándo se lanzó el software.

Nivel de soporte	Soporte completo			Soporte limitado		Soporte de autoservicio		
Año	1	2	3	4	5	6	7	8
Acceso a la documentación en línea	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Soporte técnico	Sí	Sí	Sí	Sí	Sí			
Análisis de las causas subyacentes	Sí	Sí	Sí	Sí	Sí			
Descargas de software de	Sí	Sí	Sí	Sí	Sí			
Actualizaciones de servicio (versiones de parches [P-releases])	Sí	Sí	Sí					
Alertas sobre vulnerabilidades	Sí	Sí	Sí					

Información relacionada

- Aprenda "Novedades de las versiones de ONTAP compatibles actualmente".
- Más información acerca de "Versiones mínimas recomendadas de ONTAP".
- Más información acerca de "Compatibilidad con la versión del software ONTAP".
- Obtenga más información sobre la "Modelo de versión de ONTAP".

Ejecute comprobaciones automatizadas previas a la actualización de ONTAP antes de una actualización planificada

No tiene que estar en proceso de actualizar su software ONTAP para ejecutar las comprobaciones previas a la actualización automatizada de ONTAP. La ejecución de las comprobaciones previas a la actualización independientemente del proceso de actualización automatizada de ONTAP le permite ver qué comprobaciones se realizan en su clúster y le ofrece una lista de los errores o advertencias que se deben corregir antes

de empezar la actualización. Por ejemplo, supongamos que espera actualizar el software ONTAP durante un plazo de mantenimiento programado en dos semanas. Mientras espera la fecha programada, puede ejecutar las comprobaciones previas automatizadas de la actualización y realizar las acciones correctivas que sean necesarias antes de su ventana de mantenimiento. Esto reducirá los riesgos de errores de configuración inesperados después de iniciar la actualización.

Si está listo para comenzar la actualización del software ONTAP, no es necesario realizar este procedimiento. Debe seguir el "proceso de actualización automatizado", que incluye la ejecución de las comprobaciones previas de actualización automatizadas.

> Para las configuraciones de MetroCluster, primero debe ejecutar estos pasos en el clúster A y, a continuación, ejecutar los mismos pasos en el clúster B.

Antes de empezar

Usted debe "Descargue la imagen del software ONTAP de destino".

Para ejecutar las comprobaciones previas de actualización automatizadas de un "actualización directa de varios saltos", Solo necesita descargar el paquete de software para su versión de destino ONTAP. No será necesario cargar la versión intermedia de ONTAP hasta que comience la actualización. Por ejemplo, si ejecuta comprobaciones automáticas previas a la actualización para una actualización de 9,8 a 9.13.1, deberá descargar el paquete de software de ONTAP 9.13.1. No es necesario descargar el paquete de software para ONTAP 9.12.1.

Ejemplo 1. Pasos

System Manager

1. Valide la imagen de destino de ONTAP:

> Si está actualizando una configuración de MetroCluster, debe validar el clúster A y, a continuación, repetir el proceso de validación en el clúster B.

a. Según la versión de ONTAP que esté ejecutando, realice uno de los pasos siguientes:

Si está ejecutando…	Realice lo siguiente…
ONTAP 9,8 o posterior	Haga clic en **Cluster > Overview**.
ONTAP 9.5, 9.6 y 9.7	Haga clic en **Configuración** > **clúster** > **Actualizar**.
ONTAP 9.4 o anterior	Haga clic en **Configuración** > **actualización de clúster**.

b. En la esquina derecha del panel **Overview**, haga clic en ⋮.

c. Haga clic en **actualización de ONTAP**.

d. En la pestaña **Cluster Update**, agregue una nueva imagen o seleccione una imagen disponible.

Si desea…	Realice lo siguiente…
Agregue una nueva imagen de software desde una carpeta local Ya deberías tener "se ha descargado la imagen" al cliente local.	i. En **Imágenes de software disponibles**, haga clic en **Agregar desde local**. ii. Busque la ubicación en la que guardó la imagen de software, seleccione la imagen y, a continuación, haga clic en **Abrir**.
Añada una nueva imagen de software desde un servidor HTTP o FTP	i. Haga clic en **Agregar desde el servidor**. ii. En el cuadro de diálogo **Agregar una nueva imagen de software**, introduzca la URL del servidor HTTP o FTP en el que descargó la imagen del software ONTAP del sitio de soporte de NetApp. Para el FTP anónimo, debe especificar la dirección URL en el ftp://anonymous@ftpserver formato. iii. Haga clic en **Agregar**.
Seleccione una imagen disponible	Elija una de las imágenes mostradas.

e. Haga clic en **Validar** para ejecutar las comprobaciones de validación previas a la actualización.

Si se encuentran errores o advertencias durante la validación, se muestran junto con una lista de acciones correctivas. Debe resolver todos los errores antes de continuar con la actualización. Se recomienda también resolver las advertencias.

CLI

1. Cargue la imagen de software ONTAP de destino en el repositorio de paquetes del cluster:

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.13.1/image.tgz

Package download completed.
Package processing completed.
```

2. Compruebe que el paquete de software esté disponible en el repositorio del paquete de clúster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.13.1              MM/DD/YYYY 10:32:15
```

3. Ejecute las comprobaciones automatizadas previas a la actualización:

```
cluster image validate -version package_version_number -show
-validation-details true
```

> Si está realizando una "actualización directa de varios saltos",Utilice el paquete target ONTAP para la verificación. No es necesario validar la imagen de actualización intermedia por separado. Por ejemplo, si va a actualizar de 9,8 a 9.13.1, debe usar el paquete 9.13.1 para la verificación. No es necesario validar el paquete 9.12.1 por separado.

```
cluster1::> cluster image validate -version 9.14.1 -show-validation
-details true

It can take several minutes to complete validation...
Validation checks started successfully.  Run the "cluster image
show-update-progress" command to check validation status.
```

4. Compruebe el estado de validación:

```
cluster image show-update-progress
```

> Si el **Status** está en curso, espere y ejecute el comando de nuevo hasta que se complete.

```
cluster1::*> cluster image show-update-progress

Update Phase         Status                   Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                00:10:00
00:01:03

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
...
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
Overall Status       Warning           Warning
75 entries were displayed.
```

Se muestra una lista de comprobaciones previas completas y automatizadas a la actualización, junto con cualquier error o advertencia que deba solucionarse antes de comenzar el proceso de actualización.

Resultado de ejemplo

Resultado de ejemplo completo de comprobaciones previas de actualización

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed successfully.
Refer to the Upgrade Advisor Plan or the "What should I verify before I
upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP"
documentation for the remaining manual validation checks that need to
be performed before update.
Upgrade ONTAP documentation available at: https://docs.netapp.com/us-
en/ontap/upgrade/index.html
The list of checks are available at: https://docs.netapp.com/us-
en/ontap/upgrade/task_what_to_check_before_upgrade.html
Failing to do so can result in an update failure or an I/O disruption.
Please use Interoperability Matrix Tool (IMT
http://mysupport.netapp.com/matrix) to verify host system
supportability configuration information.

Validation checks started successfully.  Run the "cluster image show-
update-progress" command to check validation status.


fas2820-2n-wic-1::*> cluster image show-update-progress

                                                Estimated         Elapsed
Update Phase         Status                      Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    in-progress                00:10:00        00:00:42

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------

fas2820-2n-wic-1::*> cluster image show-update-progress

                                                Estimated         Elapsed
Update Phase         Status                      Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    completed                  00:10:00        00:01:03
```

```
Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
Configuration Status
Boot Menu Status     Warning           Warning: bootarg.init.bootmenu
is
                                       enabled on nodes: fas2820-wic-
1a,
                                       fas2820-wic-1b. The boot process
of
                                       the nodes will be delayed.
                                       Action: Set the
bootarg.init.bootmenu
                                       bootarg to false before
proceeding
                                       with the upgrade.
Broadcast Domain     OK                N/A
availability and
uniqueness for HA
pair status
CIFS compatibility   OK                N/A
status check
CLAM quorum online   OK                N/A
status check
CPU Utilization      OK                N/A
Status
Capacity licenses    OK                N/A
install status check
Check For SP/BMC     OK                N/A
Connectivity To
Nodes
```

```
Check LDAP fastbind  OK                N/A
users using
unsecure connection.
Check for unsecure   OK                N/A
kex algorithm
configurations.
Check for unsecure   OK                N/A
mac configurations.
Cloud keymanager     OK                N/A
connectivity check
Cluster health and   OK                N/A
eligibility status
Cluster quorum       OK                N/A
status check
Cluster/management   OK                N/A
switch check
Compatible New       OK                N/A
Image Check
Current system       OK                N/A
version check if it
is susceptible to
possible outage
during NDU
Data ONTAP Version   OK                N/A
and Previous
Upgrade Status
Data aggregates HA   OK                N/A
policy check
Disk status check    OK                N/A
for failed, broken
or non-compatibility
Duplicate Initiator  OK                N/A
Check
Encryption key       OK                N/A
migration status
check
External             OK                N/A
key-manager with
legacy KMIP client
check
External keymanager  OK                N/A
key server status
check
Fabricpool Object    OK                N/A
Store Availability
High Availability    OK                N/A
```

```
configuration
status check
Infinite Volume      OK                N/A
availibility check
LIF failover         OK                N/A
capability status
check
LIF health check     OK                N/A
LIF load balancing   OK                N/A
status check
LIFs is on home      OK                N/A
node status
Logically over       OK                N/A
allocated DP
volumes check
MetroCluster         OK                N/A
configuration
status check for
compatibility
Minimum number of    OK                N/A
aggregate disks
check
NAE Aggregate and    OK                N/A
NVE Volume
Encryption Check
NDMP sessions check  OK                N/A
NFS mounts status    Warning           Warning: This cluster is serving
NFS
check                                  clients. If NFS soft mounts are
used,
                                       there is a possibility of
frequent
                                       NFS timeouts and race conditions
that
                                       can lead to data corruption
during
                                       the upgrade.
                                       Action: Use NFS hard mounts, if
                                       possible. To list Vservers
running
                                       NFS, run the following command:
                                       vserver nfs show
Name Service         OK                N/A
Configuration DNS
Check
Name Service         OK                N/A
```

```
Configuration LDAP
Check
Node to SP/BMC       OK                N/A
connectivity check
OKM/KMIP enabled     OK                N/A
systems - Missing
keys check
ONTAP API to REST    Warning           Warning: NetApp ONTAP API has
been
transition warning                     used on this cluster for ONTAP
data
                                       storage management within the
last 30
                                       days. NetApp ONTAP API is
approaching
                                       end of availability.
                                       Action: Transition your
automation
                                       tools from ONTAP API to ONTAP
REST
                                       API. For more details, refer to
                                       CPC-00410 - End of availability:
                                       ONTAPI

https://mysupport.netapp.com/info/
                                       communications/ECMLP2880232.html
ONTAP Image          OK                N/A
Capability Status
OpenSSL 3.0.x        OK                N/A
upgrade validation
check
Openssh 7.2 upgrade  OK                N/A
validation check
Platform Health      OK                N/A
Monitor check
Pre-Update           OK                N/A
Configuration
Verification
RDB Replica Health   OK                N/A
Check
Replicated database  OK                N/A
schema consistency
check
Running Jobs Status  OK                N/A
SAN LIF association  OK                N/A
status check
```

```
SAN compatibility    OK                N/A
for manual
configurability
check
SAN kernel agent     OK                N/A
status check
Secure Purge         OK                N/A
operation Check
Shelves and Sensors  OK                N/A
check
SnapLock Version     OK                N/A
Check
SnapMirror           OK                N/A
Synchronous
relationship status
check
SnapMirror           OK                N/A
compatibility
status check
Supported platform   OK                N/A
check
Target ONTAP         OK                N/A
release support for
FiberBridge 6500N
check
Upgrade Version      OK                N/A
Compatibility Status
Verify all bgp       OK                N/A
peer-groups are in
the up state
Verify if a cluster  OK                N/A
management LIF
exists
Verify that e0M is   OK                N/A
home to no LIFs
with high speed
services.
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
```

```
Overall Status       Warning           Warning
75 entries were displayed.
```

Prepárese para una actualización de ONTAP

Prepárese para una actualización del software ONTAP

Prepararse correctamente para una actualización de software de ONTAP le ayuda a identificar y reducir los posibles riesgos o bloqueadores de actualización antes de iniciar el proceso de actualización. Durante la preparación de la actualización, también puede identificar cualquier consideración especial que deba tener en cuenta antes de la actualización. Por ejemplo, si se habilita el modo FIPS SSL en su clúster y las cuentas de administrador utilizan claves públicas SSH para la autenticación, debe verificar que el algoritmo de clave de host sea compatible con la versión de ONTAP de destino.

Debe hacer lo siguiente para prepararse para una actualización:

1. "Cree un plan de actualización".

   Si tiene un contrato activo de SupportEdge para "Asesor digital de Active IQ", Planifique su actualización con Upgrade Advisor. Si no tiene acceso al asesor digital de Active IQ, cree su propio plan de actualización.

2. "Elija la versión de ONTAP objetivo".
3. Revise la "Notas de la versión de ONTAP" para la versión de destino.

   La sección “Advertencias de actualización” describe los problemas potenciales que debe tener en cuenta antes de actualizar a la nueva versión. Las secciones “Novedades” y “Problemas y limitaciones conocidos” describen el nuevo comportamiento del sistema después de actualizar a la nueva versión.

4. "Confirme la compatibilidad de ONTAP para la configuración de hardware".

   La plataforma de hardware, los switches de administración de clústeres y los switches IP de MetroCluster deben admitir la versión de destino. Si el clúster está configurado para SAN, la configuración de SAN debe ser totalmente compatible.

5. "Utilice Active IQ Config Advisor para verificar que no haya errores de configuración comunes."
6. Revise el ONTAP compatible "rutas de actualización" para determinar si puede realizar una actualización directa o si necesita completar la actualización por etapas.
7. "Compruebe la configuración de recuperación tras fallos de LIF".

   Antes de realizar una actualización, tiene que verificar que las políticas de conmutación por error del clúster y los grupos de conmutación por error están configurados correctamente.

8. "Compruebe la configuración de enrutamiento de la SVM".
9. "Verificar consideraciones especiales" para el clúster.

   Si existen ciertas configuraciones en el clúster, debe realizar ciertas acciones específicas antes de iniciar una actualización de software de ONTAP.

10. "Reinicie el SP o BMC".

Cree un plan de actualización de ONTAP

Se recomienda crear un plan de actualización. Si tiene una activa "Servicios de SupportEdge" contrato para "Asesor digital de Active IQ", Puede utilizar el Asesor de actualizaciones para generar un plan de actualización. De lo contrario, debes crear tu propio plan.

Planifique su actualización con Upgrade Advisor

El servicio Asesor de actualizaciones del Asesor digital de Active IQ proporciona inteligencia que le ayuda a planificar su actualización y minimiza la incertidumbre y el riesgo.

Active IQ identifica problemas en su entorno que se pueden resolver actualizando a una versión más reciente de ONTAP. El servicio de asesor de actualización le ayuda a planificar una actualización correcta y proporciona un informe de problemas que puede que tenga que conocer en la versión de ONTAP a la que está actualizando.

Pasos

1. "Inicie Active IQ"
2. En Active IQ "vea cualquier riesgo asociado con su clúster y tome manualmente acciones correctivas".

   Los riesgos incluidos en las categorías **SW Config Change**, **HW Config Change** y **HW Replacement** deben resolverse antes de realizar una actualización de ONTAP.

3. Revise la ruta de actualización recomendada y. "genere su plan de actualización".

¿Cuánto tiempo tardará en realizarse una actualización de ONTAP?

Debería planificar al menos 30 minutos para completar los pasos preparatorios para una actualización de ONTAP, 60 minutos para actualizar cada par de alta disponibilidad y al menos 30 minutos para completar los pasos posteriores a la actualización.

> Si utiliza el cifrado de NetApp con un servidor de gestión de claves externo y el protocolo de interoperabilidad de gestión de claves (KMIP), debería esperar que la actualización de cada pareja de alta disponibilidad tenga más de una hora.

Estas directrices de duración de la actualización se basan en configuraciones y cargas de trabajo típicas. Puede usar estas directrices para estimar el tiempo que se necesita para realizar una actualización no disruptiva en su entorno. La duración real del proceso de actualización dependerá del entorno individual y del número de nodos.

Elija la versión de ONTAP objetivo para una actualización

Cuando utiliza el asesor de actualizaciones para generar un plan de actualización para su clúster, el plan incluye una versión de ONTAP de destino recomendada para la actualización. La recomendación proporcionada por el asesor de actualización se basa en la configuración actual y en la versión de ONTAP actual.

Si no utiliza el Asesor de actualizaciones para planificar la actualización, debe elegir la versión de ONTAP de destino para la actualización en función de las recomendaciones de NetApp o si tiene que estar en la versión

mínima para satisfacer las necesidades de rendimiento.

- Actualizar a la última versión disponible (recomendado)

  NetApp recomienda actualizar el software ONTAP a la versión de revisión más reciente de la última versión numerada de ONTAP. Si no es posible porque los sistemas de almacenamiento del clúster no admiten la última versión numerada, debe actualizar a la última versión numerada que se admite.

- Versión mínima recomendada

  Si desea restringir la actualización a la versión mínima recomendada para el clúster, consulte "Versiones mínimas recomendadas de ONTAP" Para determinar la versión de ONTAP a la que debe actualizar.

Confirme la compatibilidad de ONTAP para la configuración de hardware

Antes de actualizar ONTAP, debe confirmar que la configuración de hardware es compatible con la versión de ONTAP de destino.

Todas las configuraciones

Uso "Hardware Universe de NetApp" Para confirmar que la plataforma de hardware, el clúster y los switches de administración son compatibles con la versión de ONTAP de destino. El clúster y los switches de administración incluyen los switches de red de clúster (NX-OS), los switches de red de gestión (IOS) y el archivo de configuración de referencia (RCF). Si el clúster y los switches de gestión son compatibles, pero no ejecutan las versiones mínimas de software necesarias para la versión ONTAP de destino, actualice los switches a versiones de software compatibles.

- "Descargas de NetApp: Switches de clúster de Broadcom"
- "Descargas de NetApp: Switches Ethernet de Cisco"
- "Descargas de NetApp: Switches de clúster de NetApp"

> Si necesita actualizar los switches, NetApp recomienda primero completar la actualización del software de ONTAP y, a continuación, realizar la actualización del software de los switches.

Configuraciones de MetroCluster

Antes de actualizar ONTAP, si tiene una configuración de MetroCluster, utilice el "Herramienta de matriz de interoperabilidad de NetApp" Para confirmar que los switches IP de MetroCluster son compatibles con la versión de ONTAP de destino.

Configuraciones SAN

Antes de actualizar ONTAP, si el clúster está configurado para SAN, utilice "Herramienta de matriz de interoperabilidad de NetApp" Para confirmar que la configuración de SAN es totalmente compatible.

Deben ser compatibles todos los componentes DE SAN, como la versión de software de la ONTAP de destino, el sistema operativo host y las revisiones, el software de utilidades del host requerido, el software multivía y los controladores y el firmware de adaptadores.

Identifique errores de configuración con Active IQ Config Advisor

Antes de actualizar ONTAP, puede utilizar la herramienta Active IQ Config Advisor para

comprobar si hay errores comunes de configuración.

Active IQ Config Advisor es una herramienta de validación de configuración para sistemas NetApp. Puede ponerse en marcha tanto en sitios seguros como en sitios no seguros para la recopilación de datos y el análisis del sistema.

> La compatibilidad con Active IQ Config Advisor está limitada y solo está disponible en línea.

Pasos

1. Inicie sesión en la "Sitio de soporte de NetApp", Y, a continuación, haga clic en **Herramientas** > **Herramientas**.
2. En **Active IQ Config Advisor**, haga clic en "Descargue la aplicación".
3. Descargue, instale y ejecute Active IQ Config Advisor.
4. Después de ejecutar Active IQ Config Advisor, revise el resultado de la herramienta y siga las recomendaciones que se proporcionan para resolver cualquier problema detectado por la herramienta.

Rutas de actualización de ONTAP admitidas

La versión de ONTAP que puede actualizar a depende de la plataforma de hardware y de la versión de ONTAP que se ejecuta actualmente en los nodos del clúster.

Para verificar que la plataforma de hardware es compatible con la versión de actualización de destino, consulte "Hardware Universe de NetApp". Utilice la "Herramienta de matriz de interoperabilidad de NetApp" para "confirme la compatibilidad con la configuración".

Para determinar su versión actual de ONTAP:

- En System Manager, haga clic en **clúster > Descripción general**.
- Desde la interfaz de línea de comandos (CLI), utilice `cluster image show` comando.
  También puede utilizar el `system node image show` comando en el nivel de privilegio avanzado para mostrar los detalles.

Tipos de rutas de actualización

Siempre que sea posible, se recomiendan las actualizaciones automatizadas no disruptivas (ANDU). Dependiendo de sus versiones actuales y de destino, su ruta de actualización será **direct**, **direct multi-hop**, o **multi-stage**.

- **Directo**
  Siempre puede actualizar directamente a la familia de versiones adyacentes de ONTAP mediante una sola imagen de software. En la mayoría de las versiones, también se puede instalar una imagen de software que permite actualizar directamente a versiones que sean dos versiones superiores a la versión en ejecución.

  Por ejemplo, puede utilizar la ruta de actualización directa de 9.8 a 9.9.1, o de 9.8 a 9.10.1.

  Nota: A partir de ONTAP 9.11.1, las imágenes de software admiten la actualización directa a versiones que son tres o más versiones superiores a la versión en ejecución. Por ejemplo, puede utilizar la ruta de actualización directa de 9,8 a 9.12.1.

  Se admiten todas las rutas de actualización *DIRECT* para "clústeres de versión mixta".

- **Multihop directo**
  Para algunas actualizaciones automáticas no disruptivas (ANDU) a versiones no adyacentes, debe instalar la imagen de software en una versión intermedia y en la versión de destino. El proceso de actualización automatizado utiliza la imagen intermedia en segundo plano para completar la actualización a la versión de destino.

  Por ejemplo, si el clúster ejecuta 9.3 y desea actualizar a 9.7, deberá cargar los paquetes de instalación de ONTAP para 9.5 y 9.7, a continuación, iniciar ANDU en 9.7. ONTAP actualiza automáticamente el clúster en primer lugar a 9,5 y, posteriormente, a 9,7. Debe esperar varias operaciones de toma de control/devolución y reinicios relacionados durante el proceso.

- **Multi-etapa**
  Si no hay disponible una ruta de varios saltos directa o directa para su versión de destino no adyacente, primero debe actualizar a una versión intermedia compatible y, a continuación, actualizar a la versión de destino.

  Por ejemplo, si está ejecutando 9.6 y desea actualizar a 9.11.1, debe completar una actualización en varias etapas: Primero de 9.6 a 9.8 y después de 9.8 a 9.11.1. Las actualizaciones desde versiones anteriores pueden requerir tres o más etapas, con varias actualizaciones intermedias.

  Nota: antes de comenzar las actualizaciones multietapa, asegúrese de que su versión de destino es compatible con su plataforma de hardware.

Antes de iniciar una actualización importante, se recomienda actualizar primero a la versión de revisión más reciente de la versión de ONTAP que se está ejecutando en el clúster. Esto garantiza que se resuelvan los problemas en la versión actual de ONTAP antes de la actualización.

Por ejemplo, si el sistema está ejecutando ONTAP 9.3P9 y está planeando actualizar a 9.11.1, primero debe actualizar a la versión de revisión 9.3 más reciente, luego siga la ruta de actualización de 9.3 a 9.11.1.

Descubra "Versiones de ONTAP mínimas recomendadas en el sitio de soporte de NetApp".

Rutas de actualización admitidas

Las siguientes rutas de actualización se admiten para actualizaciones automatizadas y manuales de su software ONTAP. Estas rutas de actualización se aplican a ONTAP y ONTAP Select en las instalaciones. Hay diferentes "Rutas de actualización admitidas para Cloud Volumes ONTAP".

> **Para clusters ONTAP de versiones mixtas**: Todas las rutas de actualización *direct* y *direct multi-hop* incluyen versiones ONTAP compatibles con clusters de versiones mixtas. Las versiones de ONTAP incluidas en las actualizaciones *multi-stage* no son compatibles con los clústeres de versiones mixtas. Por ejemplo, una actualización de 9,8 a 9.12.1 es una actualización *DIRECT*. Un clúster con nodos que ejecutan 9,8 y 9.12.1 es un clúster de versión mixta que se admite. Una actualización de 9,8 a 9.13.1 es una actualización *multi-stage*. No se admite un clúster con nodos que ejecuten 9,8 y 9.13.1 en una versión mixta de clúster.

Desde ONTAP 9.10.1 y posterior

Las actualizaciones manuales y automatizadas desde ONTAP 9.10.1 y versiones posteriores siguen las mismas rutas de actualización.

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automática o manual es…
9.13.1	9.14.1	directo
9.12.1	9.14.1	directo
	9.13.1	directo
9.11.1	9.14.1	directo
	9.13.1	directo
	9.12.1	directo
9.10.1	9.14.1	directo
	9.13.1	directo
	9.12.1	directo
	9.11.1	directo

Desde ONTAP 9.9.1

Las actualizaciones manuales y automatizadas de ONTAP 9.9.1 siguen las mismas rutas de actualización.

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automática o manual es…
9.9.1	9.14.1	multietapa -9,9.1→9.13.1 -9.13.1→9.14.1
	9.13.1	directo
	9.12.1	directo
	9.11.1	directo
	9.10.1	directo

Desde ONTAP 9,8

Las actualizaciones manuales y automatizadas de ONTAP 9,8 siguen las mismas rutas de actualización.

Si actualiza una configuración de IP de MetroCluster de 9,8 a 9.10.1 o posterior en cualquiera de las plataformas siguientes, debe actualizar a 9.9.1 antes de actualizar a la versión 9.10.1 o una versión posterior.

- FAS2750
- FAS500f
- AFF A220
- AFF A250

Los clústeres de las configuraciones IP de MetroCluster en estas plataformas no se pueden actualizar directamente de la versión 9,8 a la versión 9.10.1 o una versión posterior. Las rutas de actualización directa enumeradas se pueden utilizar para el resto de plataformas.

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada o manual es…
9,8	9.14.1	multietapa -9,8 → 9.12.1 -9.12.1 → 9.14.1
9.13.1	multietapa -9,8 → 9.12.1 -9.12.1 → 9.13.1	9.12.1
directo	9.11.1	directo
9.10.1	directo	9.9.1

Desde ONTAP 9,7

Las rutas de actualización de ONTAP 9,7 pueden variar en función de si se realiza una actualización automatizada o manual.

Rutas automatizadas

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada es…
9,7	9.14.1	multietapa -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multietapa -9,7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multietapa -9,7 → 9,8 -9,8 → 9.12.1
	9.11.1	salto múltiple directo (requiere imágenes para 9,8 y 9.11.1)
	9.10.1	Salto múltiple directo (se necesitan imágenes para la versión 9,8 y 9.10.1P1 o posterior P)
	9.9.1	directo
	9,8	directo

Rutas manuales

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta de actualización manual es…
9,7	9.14.1	multietapa -9,7 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multietapa -9,7 → 9.9.1 -9.9.1 → 9.13.1
	9.12.1	multietapa - 9,7 → 9,8 - 9,8 → 9.12.1
	9.11.1	multietapa - 9,7 → 9,8 - 9,8 → 9.11.1
	9.10.1	multietapa - 9,7 → 9,8 - 9,8 → 9.10.1
	9.9.1	directo
	9,8	directo

Desde ONTAP 9,6

Las rutas de actualización de ONTAP 9,6 pueden variar en función de si se realiza una actualización automatizada o manual.

Rutas automatizadas

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada es…
9,6	9.14.1	multietapa -9,6 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.14.1
	9.13.1	multietapa -9,6 → 9,8 -9,8 → 9.12.1 -9.12.1 → 9.13.1
	9.12.1	multietapa - 9,6 → 9,8 -9,8 → 9.12.1
	9.11.1	multietapa - 9,6 → 9,8 - 9,8 → 9.11.1
	9.10.1	Salto múltiple directo (se necesitan imágenes para la versión 9,8 y 9.10.1P1 o posterior P)
	9.9.1	multietapa - 9,6 → 9,8 - 9,8 → 9.9.1
	9,8	directo
	9,7	directo

Rutas manuales

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta de actualización manual es…
9,6	9.14.1	multietapa - 9,6 → 9,8 - 9,8 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multietapa - 9,6 → 9,8 - 9,8 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multietapa - 9,6 → 9,8 - 9,8 → 9.12.1
	9.11.1	multietapa - 9,6 → 9,8 - 9,8 → 9.11.1
	9.10.1	multietapa - 9,6 → 9,8 - 9,8 → 9.10.1
	9.9.1	multietapa - 9,6 → 9,8 - 9,8 → 9.9.1
	9,8	directo
	9,7	directo

Desde ONTAP 9,5

Las rutas de actualización de ONTAP 9,5 pueden variar en función de si se realiza una actualización automatizada o manual.

Rutas automatizadas

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada es…
9,5	9.14.1	multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.13.1
	9.12.1	multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.12.1
	9.11.1	multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.11.1
	9.10.1	multietapa - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.10.1
	9.9.1	salto múltiple directo (requiere imágenes para 9,7 y 9,9.1)
	9,8	multietapa - 9,5 → 9,7 - 9,7 → 9,8
	9,7	directo
	9,6	directo

Rutas de actualización manuales

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta de actualización manual es…
9,5	9.14.1	multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multietapa - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multietapa - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multietapa - 9,5 → 9,7 - 9,7 → 9,8
	9,7	directo
	9,6	directo

Desde ONTAP 9,4-9,0

Las rutas de actualización de ONTAP 9,4, 9,3, 9,2, 9,1 y 9,0 pueden variar en función de si se realiza una actualización automatizada o manual.

Actualización automatizada

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada es…
9,4	9.14.1	multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.13.1
	9.12.1	multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.12.1
	9.11.1	multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.11.1
	9.10.1	multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1) - 9.9.1 → 9.10.1
	9.9.1	multietapa - 9,4 → 9,5 - 9,5 → 9.9.1 (multi-hop directo, requiere imágenes para 9,7 y 9,9.1)
	9,8	multietapa - 9,4 → 9,5 - 9,5 → 9,8 (multi-hop directo, requiere imágenes para 9,7 y 9,8)
	9,7	multietapa - 9,4 → 9,5 - 9,5 → 9,7
	9,6	multietapa - 9,4 → 9,5 - 9,5 → 9,6
	9,5	directo

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada es…
9,3	9.14.1	multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1 - 9.13.1 → 9.14.1
	9.13.1	multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.13.1
	9.12.1	multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.10.1 (multi-hop directo, requiere imágenes para 9,8 y 9.10.1)
	9.9.1	multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1
	9,8	multietapa - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9,8
	9,7	salto múltiple directo (requiere imágenes para 9,5 y 9,7)
	9,6	multietapa - 9,3 → 9,5 - 9,5 → 9,6
	9,5	directo
	9,4	no disponible

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada es…
9,2		

		- 9,7 → 9,3
	9,7	multietapa - 9,2 → 9,3 - 9,3 → 9,7 (multietapa con automatización de imágenes para 9,5 y 9,7)
Si su versión actual de ONTAP es…	**Y su versión ONTAP de destino es…**	**Su ruta de actualización automatizada es…**
	9,6	multietapa - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multietapa - 9,3 → 9,5 - 9,5 → 9,6
	9,4	no disponible
	9,3	directo

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada es…
9,1		

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada es…
	9,7	multietapa - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7)
	9,6	multietapa - 9,1 → 9,3 - 9,3 → 9,6 (multi-hop directo, requiere imágenes para 9,5 y 9,6)
	9,5	multietapa - 9,1 → 9,3 - 9,3 → 9,5
	9,4	no disponible
	9,3	directo
	9,2	no disponible

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Su ruta de actualización automatizada es…
9,0		

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	Ruta de actualización automatizada es…
		- 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9.9.1
	9,8	multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7) - 9,7 → 9,8
	9,7	multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,7 (multi-hop directo, requiere imágenes para 9,5 y 9,7)
	9,6	multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5
	9,4	no disponible
	9,3	multietapa - 9,0 → 9,1 - 9,1 → 9,3
	9,2	no disponible
	9,1	directo

Rutas de actualización manuales

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta DE actualización DE ANDU es…
9,4	9.14.1	multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multietapa - 9,4 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8
	9,7	multietapa - 9,4 → 9,5 - 9,5 → 9,7
	9,6	multietapa - 9,4 → 9,5 - 9,5 → 9,6
	9,5	directo

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta DE actualización DE ANDU es…
9,3	9.14.1	multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.14.1
	9.13.1	multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1 - 9.12.1 → 9.13.1
	9.12.1	multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.12.1
	9.11.1	multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.11.1
	9.10.1	multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1 - 9.9.1 → 9.10.1
	9.9.1	multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multietapa - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8
	9,7	multietapa - 9,3 → 9,5 - 9,5 → 9,7
	9,6	multietapa - 9,3 → 9,5 - 9,5 → 9,6
	9,5	directo
	9,4	no disponible

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta DE actualización DE ANDU es…
9,2		

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta DE actualización DE ANDU es…
	9,7	multietapa - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7
	9,6	multietapa - 9,2 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multietapa - 9,2 → 9,3 - 9,3 → 9,5
	9,4	no disponible
	9,3	directo

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta DE actualización DE ANDU es…
9,1		

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta DE actualización DE ANDU es…
	9,7	multietapa - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7
	9,6	multietapa - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multietapa - 9,1 → 9,3 - 9,3 → 9,5
	9,4	no disponible
	9,3	directo
	9,2	no disponible

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta DE actualización DE ANDU es…
9,0		

Si su versión actual de ONTAP es…	Y su versión ONTAP de destino es…	La ruta DE actualización DE ANDU es…
		- 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9.9.1
	9,8	multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7 - 9,7 → 9,8
	9,7	multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,7
	9,6	multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5 - 9,5 → 9,6
	9,5	multietapa - 9,0 → 9,1 - 9,1 → 9,3 - 9,3 → 9,5
	9,4	no disponible
	9,3	multietapa - 9,0 → 9,1 - 9,1 → 9,3
	9,2	no disponible
	9,1	directo

Data ONTAP 8

Asegúrese de verificar que su plataforma puede ejecutar la versión de ONTAP de destino mediante el "Hardware Universe de NetApp".

Nota: la Guía de actualización de Data ONTAP 8.3 indica erróneamente que en un clúster de cuatro nodos, debe planificar la actualización del nodo que tenga el valor épsilon en último lugar. Esto ya no es un requisito para las actualizaciones a partir de Data ONTAP 8.2.3. Para obtener más información, consulte "ID de error de NetApp Bugs Online: 805277".

Desde Data ONTAP 8.3.x

Puede actualizar directamente a ONTAP 9.1 y, posteriormente, actualizar a versiones posteriores.

De versiones de Data ONTAP anteriores a 8.3.x, incluidas 8.2.x.

Primero es necesario actualizar a Data ONTAP 8.3.x y, después, actualizar a ONTAP 9.1 y, posteriormente, actualizar a versiones posteriores.

Compruebe la configuración de recuperación tras fallos de LIF

Antes de actualizar ONTAP, debe comprobar que las políticas de conmutación por error y los grupos de conmutación por error del clúster están configurados correctamente.

Durante el proceso de actualización, las LIF se migran en función del método de actualización. En función del método de actualización, es posible que se utilice la política de conmutación por error del LIF.

Si tiene 8 nodos o más en el clúster, la actualización automatizada se realiza mediante el método de lote. El método de actualización por lotes implica dividir el clúster en varios lotes de actualización, actualizar el conjunto de nodos del primer lote, actualizar sus partners de alta disponibilidad (ha) y, a continuación, repetir el proceso para los lotes restantes. En ONTAP 9.7 y versiones anteriores, si se utiliza el método por lotes, los LIF se migran al partner de alta disponibilidad del nodo que se actualiza. En ONTAP 9.8 y versiones posteriores, si se utiliza el método por lotes, los LIF se migran al otro grupo por lotes.

Si tiene menos de 8 nodos en el clúster, la actualización automatizada se realiza mediante el método de reversión. El método de actualización gradual implica iniciar una operación de conmutación al respaldo en cada nodo de un par de alta disponibilidad, actualizar el nodo que ha conmutado al nodo de respaldo, iniciar el retorno al nodo primario y, a continuación, repetir el proceso de cada par de alta disponibilidad del clúster. Si se usa el método de reversión, las LIF se migran al nodo de destino de conmutación por error tal como se define en la política de conmutación por error de LIF.

Pasos

1. Mostrar la política de recuperación tras fallos para cada LIF de datos:

Si la versión de ONTAP es…	Utilice este comando
9,6 o posterior	`network interface show -service-policy *data* -failover`
9,5 o anterior	`network interface show -role data -failover`

   Este ejemplo muestra la configuración predeterminada de la conmutación por error de un clúster de dos nodos con dos LIF de datos:

```
cluster1::> network interface show -role data -failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- ---------------
---------------
vs0
         lif0            node0:e0b             nextavail       system-
defined
                         Failover Targets: node0:e0b, node0:e0c,
                                           node0:e0d, node0:e0e,
                                           node0:e0f, node1:e0b,
                                           node1:e0c, node1:e0d,
                                           node1:e0e, node1:e0f
vs1
         lif1            node1:e0b             nextavail       system-
defined
                         Failover Targets: node1:e0b, node1:e0c,
                                           node1:e0d, node1:e0e,
                                           node1:e0f, node0:e0b,
                                           node0:e0c, node0:e0d,
                                           node0:e0e, node0:e0f
```

El campo **objetivos de conmutación por error** muestra una lista priorizada de destinos de conmutación por error para cada LIF. Por ejemplo, si 'lif0' conmuta por error desde su puerto raíz (e0b en node0), primero intenta conmutar por error al puerto e0c en node0. Si lif0 no puede conmutar al nodo de respaldo a e0c, intenta conmutar al puerto e0d en node0, etc.

2. Si la política de conmutación por error se establece en **disabled** para cualquier LIF, que no sea LIF de SAN, utilice el `network interface modify` comando para habilitar la conmutación al nodo de respaldo.
3. Para cada LIF, compruebe que el campo **objetivos de conmutación por error** incluye puertos de datos de un nodo diferente que permanecerán activos mientras se esté actualizando el nodo de inicio de la LIF.

   Puede utilizar el `network interface failover-groups modify` comando para agregar un destino de conmutación por error al grupo de conmutación por error.

   Ejemplo

   ```
   network interface failover-groups modify -vserver vs0 -failover-group
   fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
   ```

Información relacionada

"Gestión de redes y LIF"

Comprobar la configuración de enrutamiento de SVM

Para evitar interrupciones, antes de actualizar el software ONTAP, debe asegurarse de que la ruta predeterminada de la SVM pueda alcanzar cualquier dirección de red que no sea accesible por una ruta más específica. Se recomienda configurar una ruta predeterminada para una SVM. Para obtener más información, consulte "SU134: El acceso a la red puede verse interrumpido por una configuración de enrutamiento incorrecta en ONTAP".

La tabla de enrutamiento de una SVM determina la ruta de red que la SVM utiliza para comunicarse con un destino. Es importante comprender cómo funcionan las tablas de enrutamiento para evitar problemas de red antes de que ocurran.

Las reglas de enrutamiento son las siguientes:

- ONTAP enruta el tráfico por la ruta disponible más específica.
- ONTAP enruta el tráfico por una ruta de puerta de enlace predeterminada (con 0 bits de máscara de red) como último recurso, cuando no hay más rutas específicas disponibles.

En el caso de rutas con el mismo destino, máscara de red y métrica, no hay garantía de que el sistema utilice la misma ruta después de un reinicio o después de una actualización. Esto puede ser especialmente un problema si ha configurado varias rutas predeterminadas.

Consideraciones especiales

Consideraciones especiales antes de una actualización de ONTAP

Ciertas configuraciones de clúster requieren que realice acciones específicas antes de iniciar una actualización del software de ONTAP. Por ejemplo, si tiene una configuración de SAN, debe verificar que cada host esté configurado con el número correcto de rutas directas e indirectas antes de comenzar la actualización.

Revise la siguiente tabla para determinar qué pasos adicionales debe tomar.

Antes de actualizar ONTAP, pregúntese…	Si su respuesta es sí, entonces haga esto…
¿Mi clúster está actualmente en estado de versión mixta?	Compruebe los requisitos de versión mixta
¿Tengo una configuración de MetroCluster?	Consulte los requisitos específicos de actualización de las configuraciones de MetroCluster
¿Tengo una configuración SAN?	Compruebe la configuración del host SAN
¿Hay definidas relaciones de SnapMirror en mi clúster?	"Comprobar la compatibilidad de las versiones de ONTAP para las relaciones de SnapMirror"
¿He definido relaciones de SnapMirror para tipo DP? ¿Estoy actualizando a ONTAP 9.12.1 o una versión posterior?	"Convierta las relaciones de tipo DP existentes a XDP"
¿Uso el cifrado de almacenamiento de NetApp con servidores de gestión de claves externos?	Elimine todas las conexiones existentes del servidor de gestión de claves

Antes de actualizar ONTAP, pregúntese…	Si su respuesta es sí, entonces haga esto…
¿He cargado grupos de red en SVM?	Vefiry que el archivo netgroup está presente en cada nodo
¿Tengo clientes LDAP que utilizan SSLv3?	Configure los clientes LDAP para que usen TLS
¿Estoy utilizando protocolos orientados a sesiones?	Examinar las consideraciones relativas a los protocolos orientados a las sesiones
¿Está habilitado el modo FIPS de SSL en un clúster donde las cuentas de administrador se autentican con una clave pública SSH?	Verifique el soporte del algoritmo de clave de host SSH

Clústeres de ONTAP de versión mixta

Un clúster de ONTAP de versión mixta consta de nodos que ejecutan dos versiones principales de ONTAP diferentes durante un tiempo limitado. Por ejemplo, si un clúster actualmente consta de nodos que ejecutan ONTAP 9,8 y 9.12.1, el clúster es un clúster de una versión mixta. De igual forma, un clúster en el que nodos ejecuten ONTAP 9.9.1 y 9.13.1 sería un clúster de versiones mixtas. NetApp admite clústeres ONTAP de versión mixta durante períodos limitados y en situaciones específicas.

A continuación se muestran los casos más comunes en los que un clúster de ONTAP tendrá una versión mixta:

- Actualizaciones del software ONTAP en grandes clústeres
- Es necesario actualizar el software ONTAP cuando piensa añadir nodos nuevos a un clúster

La información se aplica a las versiones de ONTAP que admiten sistemas de plataformas NetApp, como los sistemas A-Series y C-Series de AFF, ASA, FAS y C-Series. La información no se aplica a las versiones de cloud de ONTAP (9.x.0) como 9.12.0.

Requisitos para clústeres de ONTAP de versión mixta

Si su clúster tiene que introducir una versión mixta de ONTAP, debe conocer los requisitos y las restricciones importantes.

- No puede haber más de dos versiones principales de ONTAP diferentes en un clúster en un momento dado. Por ejemplo, se admite ONTAP 9.9.1 y 9.13.1, pero ONTAP 9,9.1, 9.12.1 y 9.13.1 no lo es. Los clústeres que tienen nodos en ejecución con niveles de revisión P o D diferentes de la misma versión de ONTAP, como ONTAP 9,9.1P1 y 9,9.1P5, no se consideran clústeres de ONTAP de versiones mixtas.
- Mientras el clúster tiene una versión mixta, no debe introducir ningún comando que modifique la operación o la configuración del clúster, excepto los necesarios para la actualización o el proceso de migración de datos. Por ejemplo, no deben realizarse actividades como la migración LIF, las operaciones planificadas de conmutación por error de almacenamiento o la creación o eliminación de objetos a gran escala hasta que hayan finalizado la actualización y la migración de datos.
- Para un funcionamiento óptimo del clúster, la cantidad de tiempo que el clúster tenga el estado de versión mixta debe ser lo más breve posible. La cantidad máxima de tiempo que puede permanecer un clúster en una versión mixta depende de la versión de ONTAP más baja del clúster.

Si la versión más baja de ONTAP que se ejecuta en el clúster de versiones mixtas es:	A continuación, puede permanecer en un estado de versión mixta durante un máximo de
ONTAP 9,8 o superior	90 días
ONTAP 9,7 o inferior	7 días

- A partir de ONTAP 9,8, la diferencia de versión entre los nodos originales y los nuevos no puede ser superior a cuatro. Por ejemplo, un clúster ONTAP de versión mixta podría tener nodos que ejecuten ONTAP 9,8 y 9.12.1, o bien podría tener nodos que ejecuten ONTAP 9.9.1 y 9.13.1. Sin embargo, no se admitiría una versión mixta de un clúster de ONTAP con nodos que ejecuten ONTAP 9,8 y 9.13.1.

  Si desea ver una lista completa de los clústeres de versiones mixtas compatibles, consulte "rutas de actualización admitidas". Todas las rutas de actualización *DIRECT* se admiten para clústeres de versiones mixtas.

Actualización de la versión de ONTAP de un clúster de gran tamaño

Una situación en la que se puede introducir un estado en un clúster de versiones mixtas implica actualizar la versión ONTAP de un clúster con varios nodos para aprovechar las funciones disponibles en versiones posteriores de ONTAP 9. Cuando necesite actualizar la versión de ONTAP de un clúster más grande, deberá introducir un estado de clúster de versiones mixtas durante un período de tiempo a medida que actualice cada nodo del clúster.

Añadir nuevos nodos a un clúster de ONTAP

Otra situación para introducir un estado de cluster de versiones mixtas implica la adición de nuevos nodos al clúster. Es posible añadir nodos nuevos al clúster para expandir su capacidad, o es posible añadir nodos nuevos como parte del proceso de reemplazar por completo las controladoras. En cualquier caso, debe habilitar la migración de sus datos desde controladoras existentes a los nodos nuevos en el sistema nuevo.

Si piensa agregar nodos nuevos al clúster y esos nodos requieren una versión mínima de ONTAP que sea posterior a la versión que se está ejecutando actualmente en el clúster, debe realizar las actualizaciones de software compatibles de los nodos existentes del clúster antes de agregar los nodos nuevos.

Lo ideal sería que actualizara todos los nodos existentes a la versión mínima de ONTAP que requieran los nodos que planea agregar al clúster. Sin embargo, si esto no es posible porque algunos de sus nodos existentes no admiten la versión posterior de ONTAP, deberá introducir un estado de versión mixta durante una cantidad limitada de tiempo como parte del proceso de actualización. Si tiene nodos que no admiten la versión mínima de ONTAP requerida por las controladoras nuevas, debe hacer lo siguiente:

1. "Renovar" Los nodos que no admiten la versión mínima de ONTAP requerida por las nuevas controladoras hasta la versión máxima de ONTAP que admiten.

   Por ejemplo, si tiene un sistema FAS8080 con ONTAP 9,5 y va a añadir una nueva plataforma C-Series con ONTAP 9.12.1, debería actualizar su sistema FAS8080 a ONTAP 9,8 (que es la versión máxima de ONTAP que admite).

2. "Añada los nodos nuevos al clúster".
3. "Migrar los datos" de los nodos que se están quitando del clúster a los nodos recién añadidos.
4. "Quite los nodos no compatibles del clúster".
5. "Renovar" los nodos restantes del clúster a la misma versión de los nuevos nodos.

De manera opcional, actualice el clúster completo (incluidos los nodos nuevos) al "última versión de parche recomendada" De la versión de ONTAP que se ejecuta en los nodos nuevos.

Para obtener más información sobre la migración de datos, consulte:

- "Cree un agregado y mueva volúmenes a los nuevos nodos"
- "Configuración de nuevas conexiones iSCSI para movimientos de volúmenes SAN"
- "Movimiento de volúmenes con cifrado"

Requisitos de actualización de ONTAP para configuraciones de MetroCluster

Antes de actualizar el software ONTAP en una configuración MetroCluster, los clústeres deben cumplir ciertos requisitos.

- Ambos clústeres deben ejecutar la misma versión de ONTAP.

  Puede comprobar la versión de ONTAP con el comando version.

- Si está realizando una actualización importante de ONTAP, la configuración de MetroCluster debe estar en modo normal.
- Si está realizando una actualización de ONTAP de parche, la configuración de MetroCluster puede estar en modo normal o de conmutación.
- Para todas las configuraciones, excepto clústeres de dos nodos, puede actualizar de forma no disruptiva ambos clústeres al mismo tiempo.

  Para la actualización no disruptiva de clústeres de dos nodos, es necesario actualizar los clústeres de un nodo a uno.

- Los agregados de ambos clústeres no deben volver a asignar el estado de RAID.

  Durante la reparación de MetroCluster, los agregados reflejados se resincronizan. Puede verificar si la configuración de MetroCluster está en este estado mediante la `storage aggregate plex show -in -progress true` comando. Si se sincroniza algún agregado, no se debe realizar una actualización hasta que se complete la resincronización.

- Se producirá un error en las operaciones de conmutación al nodo de respaldo negociadas mientras la actualización está en curso.

  Para evitar problemas con las operaciones de actualización o reversión, no intente realizar una conmutación de sitios no planificada durante una operación de actualización o reversión a menos que todos los nodos de ambos clústeres estén ejecutando la misma versión de ONTAP.

Requisitos de configuración para el funcionamiento normal de MetroCluster

- Los LIF de SVM de origen deben estar activos y ubicados en sus nodos principales.

  No es necesario que los LIF de datos de las SVM de destino estén en funcionamiento o que estén en sus nodos de inicio.

- Todos los agregados del sitio local deben estar en línea.
- Todos los volúmenes raíz y de datos que pertenecen a las SVM del clúster local deben estar en línea.

Requisitos de configuración para la conmutación de sitios de MetroCluster

- Todos los LIF deben estar activos y ubicados en sus nodos principales.
- Todos los agregados deben estar en línea, excepto los agregados raíz en el sitio de recuperación ante desastres.

  Los agregados raíz del sitio de recuperación tras desastres están sin conexión durante determinadas fases de la conmutación.

- Todos los volúmenes deben estar en línea.

Información relacionada

"Verificación del estado de red y almacenamiento de las configuraciones de MetroCluster"

Compruebe la configuración del host SAN antes de actualizar ONTAP

La actualización de ONTAP en un entorno SAN cambia qué rutas son directas. Antes de actualizar un clúster SAN, debe comprobar que cada host esté configurado con el número correcto de rutas directas e indirectas y que cada host esté conectado a las LIF correctas.

Pasos

1. En cada host, compruebe que se haya configurado un número suficiente de rutas directas e indirectas y que cada ruta esté activa.

   Cada host debe tener una ruta a cada nodo del clúster.

2. Compruebe que cada host está conectado a una LIF en cada nodo.

   Debe registrar la lista de iniciadores para la comparación después de la actualización.

Durante…	Introduzca…
ISCSI	`iscsi initiator show -fields igroup,initiator-name,tpgroup`
FC	`fcp initiator show -fields igroup,wwpn,lif`

SnapMirror

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

> La interoperabilidad es bidireccional.

Interoperabilidad para ONTAP versión 9,3 y posterior

Versión ONTAP…	Interactúa con estas versiones anteriores de ONTAP…																	
	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	9,4	9,3
9.14.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No	No
9.14.0*	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	No	No	No	No
9.13.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No	No
9.13.0*	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	No	No	No	No
9.12.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No	No
9.12.0*	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	No	No	No	No
9.11.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No	No
9.11.0*	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	No	No
9.10.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9.10.0*	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	No	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9.9.1	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No

9.9.0*	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	No
9,8	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	**Sí**
9,7	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	**Sí**
9,6	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	No	**Sí**
9,5	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**
9,4	No	No	No	No	No	No	No	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**
9,3	No	No	No	No	No	No	No	No	No	No	No	No	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**	**Sí**

Relaciones de SnapMirror Synchronous

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

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

Relaciones de recuperación ante desastres de SVM de SnapMirror

- 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 locales principales más nuevas o dos versiones de cloud principales más recientes, 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).

Origen	Destino																	
	9,3	9,4	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
9,3	Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración													
9,4		Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración												
9,5			Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración											

9,6				Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración										
9,7					Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración									
9,8						Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración								
9.9.0*							Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración							

9.9.1								Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración						
9.10.0*									Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración					
9.10.1										Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración				
9.11.0*											Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración			

9.11.1												Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración		
9.12.0*													Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración	
9.12.1														Recuperación antedesastres/Migración	Migración	Migración	Migración	Migración
9.13.0*															Recuperación antedesastres/Migración	Migración	Migración	Migración

9.13.1																Recuperación antedesastres/Migración	Migración	Migración
9.14.0*																	Recuperación antedesastres/Migración	Migración
9.14.1																		Recuperación antedesastres/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	9,2	9,1	9
9.11.1	Sí	No	No	No	No	No	No	No	No	No	No	No

9.10.1	Sí	Sí	No	No	No	No	No	No	No	No	No	No
9.9.1	Sí	Sí	Sí	No	No	No	No	No	No	No	No	No
9,8	No	Sí	Sí	Sí	No	No	No	No	No	No	No	No
9,7	No	No	Sí	Sí	Sí	No	No	No	No	No	No	No
9,6	No	No	No	Sí	Sí	Sí	No	No	No	No	No	No
9,5	No	No	No	No	Sí	Sí	Sí	No	No	No	No	No
9,4	No	No	No	No	No	Sí	Sí	Sí	No	No	No	No
9,3	No	No	No	No	No	No	Sí	Sí	Sí	No	No	No
9,2	No	No	No	No	No	No	No	Sí	Sí	Sí	No	No
9,1	No	No	No	No	No	No	No	No	Sí	Sí	Sí	No
9	No	No	No	No	No	No	No	No	No	Sí	Sí	Sí

La interoperabilidad no es bidireccional.

Convierta una relación de tipo DP 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.

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. Para obtener información previa, consulte "XDP sustituye a DP como la opción predeterminada de SnapMirror".
- 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 siguiente ejemplo, se muestra el resultado de `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 que le resulte útil conservar una copia del `snapmirror show` salida de comando para realizar un seguimiento de la configuración de relaciones existente.

2. En los volúmenes de origen y destino, asegúrese de que ambos volúmenes tengan una copia Snapshot común:

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

En el siguiente ejemplo se muestra el `volume snapshot show` salida 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>
```

Para obtener una sintaxis completa del comando, consulte "página de manual".

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

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

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

4. Rompa la relación de tipo de DP existente:

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

Para obtener una sintaxis completa del comando, consulte "página de manual".

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

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

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

5. Si la eliminación automática de las copias Snapshot está habilitada en el volumen de destino, desactívelo:

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

En el ejemplo siguiente se deshabilita la eliminación automática de copias 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>
```

Para obtener una sintaxis completa del comando, consulte "página de manual".

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

En el siguiente ejemplo, se elimina la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `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
```

8. Puede utilizar la salida que ha retenido de `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. Para obtener una sintaxis de comando completa, consulte la página man.

> 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 de desastres de SnapMirror entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup` con el valor predeterminado `MirrorAllSnapshots` política:

```
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` opcional, pero debe tener en cuenta que se pueden perder ahorros en eficiencia del almacenamiento. Para obtener una sintaxis completa del comando, consulte la página man: "Comando SnapMirror resync".

> 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, vuelva a establecer la relación entre el volumen de origen `volA` encendido `svm1` y el volumen de destino `volA_dst` encendido `svm_backup`:

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

10. Si ha deshabilitado la eliminación automática de copias Snapshot, vuelva a habilitarla:

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

Después de terminar

1. Utilice la `snapmirror show` Comando para verificar que la relación de SnapMirror se ha creado.
2. Una vez que el volumen de destino de SnapMirror XDP comienza a actualizar las copias snapshot tal como se define en la política de SnapMirror, utilice el resultado de `snapmirror list-destinations` Comando del clúster de origen para mostrar la nueva relación de XDP de SnapMirror.

Elimine las conexiones del servidor de gestión de claves externo existentes antes de actualizar ONTAP

Antes de actualizar ONTAP, si ejecuta ONTAP 9,2 o una versión anterior con el cifrado de almacenamiento de NetApp (NSE) y se actualiza a ONTAP 9,3 o posterior, debe utilizar la interfaz de línea de comandos (CLI) para eliminar cualquier conexión existente del servidor de gestión de claves externa (KMIP).

Pasos

1. Compruebe que las unidades NSE estén desbloqueadas, abiertas y configuradas con el ID seguro de fabricación predeterminado 0x0:

```
storage encryption disk show -disk *
```

2. Entre en el modo de privilegio avanzado:

```
set -privilege advanced
```

3. Utilice el ID seguro de fabricación predeterminado 0x0 para asignar la clave FIPS a los discos de cifrado automático (SED):

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

4. Compruebe que se haya completado la asignación de la clave FIPS a todos los discos:

```
storage encryption disk show-status
```

5. Verifique que el **mode** para todos los discos esté configurado en data

```
storage encryption disk show
```

6. Vea los servidores KMIP configurados:

```
security key-manager show
```

7. Elimine los servidores KMIP configurados:

```
security key-manager delete -address kmip_ip_address
```

8. Elimine la configuración del gestor de claves externo:

```
security key-manager delete-kmip-config
```

> Este paso no quita los certificados de NSE.

El futuro

Una vez completada la actualización, debe hacerlo Vuelva a configurar las conexiones del servidor KMIP.

Compruebe que el archivo netgroup está presente en todos los nodos antes de actualizar ONTAP

Antes de actualizar ONTAP, si ha cargado netgroups en máquinas virtuales de almacenamiento (SVM), debe verificar que el archivo netgroup esté presente en cada nodo. Si falta un archivo de grupo de red en un nodo, puede provocar un error en la actualización.

Pasos

1. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

2. Muestre el estado del grupo de red para cada SVM:

```
vserver services netgroup status
```

3. Compruebe que, en cada SVM, cada nodo muestra el mismo valor hash de archivo netgroup:

```
vserver services name-service netgroup status
```

De ser así, puede omitir el siguiente paso y continuar con la actualización o la reversión. De lo contrario, continúe con el siguiente paso.

4. En cualquier nodo del clúster, cargue manualmente el archivo netgroup:

```
vserver services netgroup load -vserver vserver_name -source uri
```

Este comando descarga el archivo netgroup en todos los nodos. Si ya existe un archivo de netgroup en un nodo, se sobrescribe.

Información relacionada

"Trabajar con netgroups"

Configure los clientes LDAP para que utilicen TLS para obtener la mayor seguridad

Antes de actualizar ONTAP, debe configurar clientes LDAP mediante SSLv3 para establecer comunicaciones seguras con servidores LDAP con el fin de utilizar TLS. SSL no estará disponible después de la actualización.

De forma predeterminada, las comunicaciones LDAP entre las aplicaciones cliente y servidor no están cifradas. Debe desactivar el uso de SSL e imponer el uso de TLS.

Pasos

1. Compruebe que los servidores LDAP del entorno son compatibles con TLS.

Si no lo hacen, no continúe. Debe actualizar los servidores LDAP a una versión compatible con TLS.

2. Compruebe qué configuraciones del cliente LDAP de ONTAP tienen LDAP sobre SSL/TLS habilitado:

```
vserver services name-service ldap client show
```

Si no hay ninguno, puede omitir los pasos restantes. Sin embargo, debe considerar utilizar LDAP sobre TLS para mejorar la seguridad.

3. Para cada configuración de cliente LDAP, desactivar SSL para que aplique el uso de TLS:

```
vserver services name-service ldap client modify -vserver vserver_name
-client-config ldap_client_config_name -allow-ssl false
```

4. Compruebe que ya no se permite el uso de SSL en ningún cliente LDAP:

```
vserver services name-service ldap client show
```

Información relacionada

"Gestión de NFS"

Consideraciones sobre los protocolos orientados a las sesiones

Los clústeres y los protocolos orientados a la sesión pueden causar efectos adversos en clientes y aplicaciones en ciertas áreas, como el servicio de I/O durante las actualizaciones.

Si utiliza protocolos orientados a la sesión, tenga en cuenta lo siguiente:

- SMB

  Si usted sirve recursos compartidos de disponibilidad continua (CA) con SMBv3, puede utilizar el sistema automatizado
  Método de actualización no disruptivo (con System Manager o CLI) y no se producen interrupciones experimentado por el cliente.

  Si presta servicio a recursos compartidos con SMBv1 o SMBv2, o recursos compartidos que no son de CA con SMBv3, las sesiones del cliente se interrumpen durante las operaciones de toma de control y reinicio de la actualización. Debe dirigir a los usuarios para que terminen sus sesiones antes de actualizarlas.

  Hyper-V y SQL Server sobre SMB admiten operaciones no disruptivas (NDO). Si configuró una solución Hyper-V o SQL Server mediante SMB, los servidores de aplicaciones y las máquinas virtuales o bases de datos contenidas permanecen en línea y proporcionan disponibilidad continua durante la actualización de ONTAP.

- NFSv4. X

  Los clientes de NFSv4.x podrán recuperarse automáticamente de las pérdidas de conexión sufridas durante la actualización con procedimientos de recuperación de NFSv4.x. Las aplicaciones pueden experimentar un retraso de I/o temporal durante este proceso.

- NDMP

  Se pierde el estado y el usuario cliente debe volver a intentar la operación.

- Backups y restauraciones

  Se pierde el estado y el usuario cliente debe volver a intentar la operación.

  > No inicie una copia de seguridad ni restaure durante o inmediatamente antes de una actualización. Si lo hace, se puede producir la pérdida de datos.

- Aplicaciones (por ejemplo, Oracle o Exchange)

  Los efectos dependen de las aplicaciones. Para las aplicaciones basadas en tiempo de espera, es posible que pueda cambiar la configuración de tiempo de espera a más largo que el tiempo de reinicio de ONTAP

para minimizar los efectos adversos.

Verifique la compatibilidad con el algoritmo de clave de host SSH antes de actualizar ONTAP

Antes de actualizar ONTAP, si se habilita el modo FIPS SSL en un clúster donde las cuentas de administrador se autentican con una clave pública SSH, debe asegurarse de que el algoritmo de clave de host sea compatible con la versión de ONTAP de destino.

La siguiente tabla indica los algoritmos de tipo de clave de host que se admiten para las conexiones SSH de ONTAP. Estos tipos de claves no se aplican a la configuración de la autenticación pública SSH.

Versión de ONTAP	Tipos de clave compatibles con el modo FIPS	Tipos de clave compatibles con el modo no FIPS
9.11.1 y posterior	ecdsa-sha2-nistp256	ecdsa-sha2-nistp256 rsa-sha2-512 rsa-sha2-256 ssh-ed25519 ssh-dss ssh-rsa
9.10.1 y anteriores	ecdsa-sha2-nistp256 ssh-ed25519	ecdsa-sha2-nistp256 ssh-ed25519 ssh-dss ssh-rsa

La compatibilidad con el algoritmo de clave de host ssh-ed25519 se elimina a partir de ONTAP 9.11.1.

Para obtener más información, consulte "Configurar la seguridad de red con FIPS".

Las cuentas de clave pública SSH existentes sin algoritmos de clave soportados deben volver a configurarse con un tipo de clave soportada antes de actualizar o se producirá un error en la autenticación del administrador.

"Obtenga más información sobre cómo habilitar cuentas de claves públicas de SSH."

Reinicie el SP o BMC para preparar la actualización del firmware durante una actualización de ONTAP

No es necesario actualizar manualmente el firmware antes de proceder con una actualización de ONTAP. El firmware del clúster se incluye con el paquete de actualización de ONTAP y se copia en el dispositivo de arranque de cada nodo. El nuevo firmware se instala como parte del proceso de actualización.

El firmware de los siguientes componentes se actualiza automáticamente si la versión del clúster es más antigua que el firmware que se incluye con el paquete de actualización de ONTAP:

- BIOS/CARGADOR
- Service Processor (SP) o controlador de gestión de placa base (BMC)
- Bandeja de almacenamiento

- Disco
- Flash Cache

Para prepararse para una actualización fluida, debe reiniciar el SP o BMC antes de que comience la actualización.

Paso

1. Reinicie el SP o BMC antes de realizar la actualización:

   ```
   system service-processor reboot-sp -node node_name
   ```

   Solo reinicie un SP o BMC a la vez. Espere a que el SP o BMC reiniciado recicle por completo antes de reiniciar el siguiente.

También puede hacerlo "actualice el firmware manualmente" Entre actualizaciones de ONTAP. Si tiene Active IQ, puede "Consulte la lista de versiones de firmware incluidas actualmente en la imagen ONTAP".

Las versiones actualizadas del firmware están disponibles de la siguiente manera:

- "Firmware del sistema (BIOS, BMC, SP)"
- "Firmware de la bandeja"
- "Firmware de disco y Flash Cache"

Descargue la imagen del software ONTAP

Antes de actualizar ONTAP, primero debe descargar la imagen del software de ONTAP de destino desde el sitio de soporte de NetApp. Según la versión de ONTAP, puede descargar el software ONTAP en un servidor HTTPS, HTTP o FTP de la red o en una carpeta local.

Si está ejecutando…	Puede descargar la imagen en esta ubicación…
ONTAP 9.6 y posteriores	• Un servidor HTTPS El certificado de CA del servidor debe instalarse en el sistema local. • Una carpeta local • Un servidor HTTP o FTP
ONTAP 9,4 y versiones posteriores	• Una carpeta local • Un servidor HTTP o FTP
ONTAP 9,0 y versiones posteriores	Un servidor HTTP o FTP

Acerca de esta tarea

- Si realiza una actualización automatizada no disruptiva (ANDU) mediante un "ruta de actualización directa de varios saltos", usted necesita "descargue" El paquete de software para la versión de ONTAP intermedia y la versión de ONTAP de destino necesaria para la actualización. Por ejemplo, si va a actualizar de

ONTAP 9,8 a ONTAP 9.13.1, debe descargar los paquetes de software tanto para ONTAP 9.12.1 como para ONTAP 9.13.1. Consulte "rutas de actualización admitidas" para determinar si la ruta de actualización requiere la descarga de un paquete de software intermedio.

- Si actualiza un sistema con el cifrado de volúmenes de NetApp a ONTAP 9.5 o una versión posterior, debe descargar la imagen del software ONTAP para países no restringidos, que incluye el cifrado de volúmenes de NetApp.

  Si utiliza la imagen del software de ONTAP para países restringidos a fin de actualizar un sistema con el cifrado de volúmenes de NetApp, el sistema produce una alarma y perderá el acceso a los volúmenes.

- No es necesario descargar un paquete de software independiente para su firmware. La actualización del firmware del clúster se incluye con el paquete de actualización de software ONTAP y se copia en el dispositivo de arranque de cada nodo. El nuevo firmware se instala como parte del proceso de actualización.

Pasos

1. Busque el software ONTAP de destino en la "Descargas de software" Del sitio de soporte de NetApp.

   Para una actualización de ONTAP Select, seleccione **actualización de nodo de ONTAP Select**.

2. Copie la imagen del software (por ejemplo, 97_q_image.tgz) en la ubicación adecuada.

   Según la versión de ONTAP, la ubicación será un directorio desde el que se servirá la imagen al sistema local o a una carpeta local del sistema de almacenamiento.

Métodos de actualización de ONTAP

Métodos de actualización del software ONTAP

Puede realizar una actualización automatizada del software ONTAP con System Manage. Como alternativa, puede realizar una actualización automatizada o manual con la interfaz de línea de comandos (CLI) de ONTAP. El método que utiliza para actualizar ONTAP depende de la configuración, la versión actual de ONTAP y el número de nodos del clúster. NetApp recomienda usar System Manager para realizar actualizaciones automatizadas a menos que la configuración requiera un enfoque diferente. Por ejemplo, si tiene una configuración de MetroCluster con 4 nodos que ejecuten ONTAP 9,3 o posterior, debería utilizar System Manager para llevar a cabo una actualización automatizada (a veces denominada actualización no disruptiva automatizada o ANDU). Si tiene una configuración de MetroCluster con nodos 8 que ejecutan ONTAP 9,2 o una versión anterior, debe usar la CLI para realizar una actualización manual.

Una actualización puede ejecutarse mediante el proceso de actualización gradual o el proceso de actualización en lote. Ambos elementos no disruptivos.

Para las actualizaciones automatizadas, ONTAP instala automáticamente la imagen ONTAP de destino en cada nodo, valida los componentes del clúster para garantizar que el clúster se pueda actualizar sin interrupciones y, a continuación, ejecuta una actualización en lote o en segundo plano en función del número de nodos. En el caso de las actualizaciones manuales, el administrador confirma manualmente que cada nodo del clúster está listo para la actualización y, a continuación, realiza los pasos necesarios para ejecutar una actualización gradual.

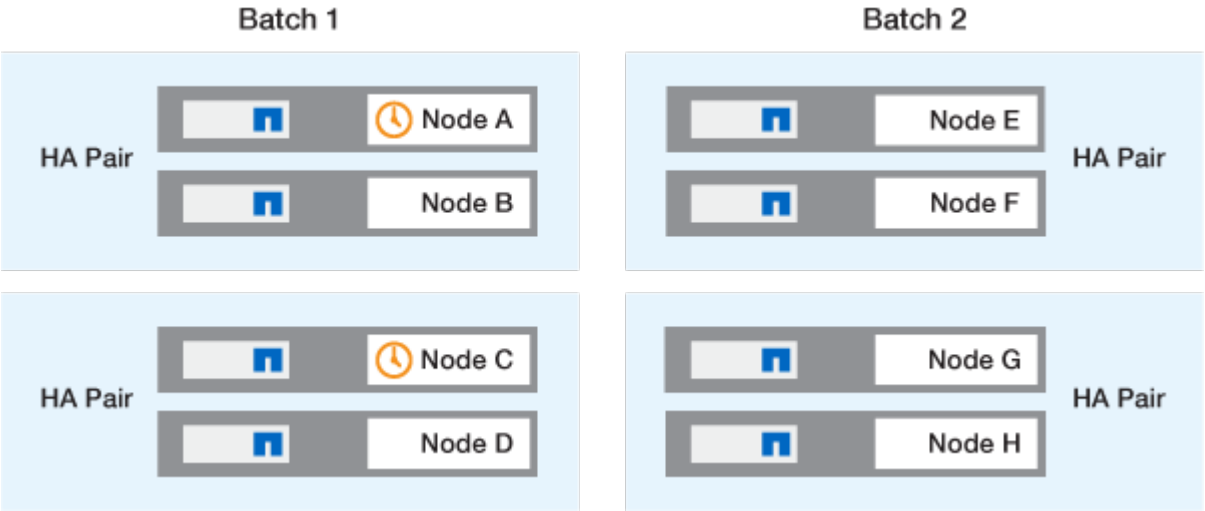
Actualizaciones graduales de ONTAP

El proceso de actualización gradual es la opción predeterminada para los clústeres con menos de 8 nodos. En el proceso de actualización gradual, un nodo se desconecta y se actualiza mientras su compañero toma el control de su almacenamiento. Cuando se completa la actualización del nodo, el nodo asociado le devuelve el control al nodo propietario original y el proceso se repite en el nodo asociado. Cada par de alta disponibilidad adicional se actualiza en secuencia hasta que todos los pares de alta disponibilidad ejecutan la versión de destino.

Actualizaciones en lotes de ONTAP

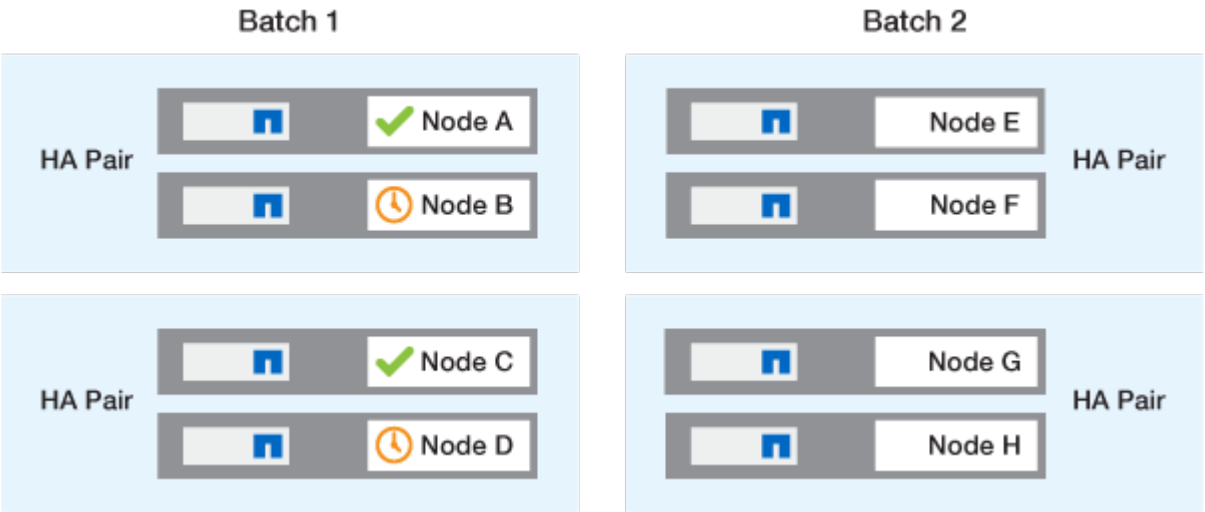
El proceso de actualización por lotes es el predeterminado para clústeres de 8 nodos o más. En el proceso de actualización por lotes, el clúster se divide en dos lotes. Cada lote contiene varios pares de alta disponibilidad. En el primer lote, el primer nodo de cada par de alta disponibilidad se actualiza simultáneamente con el primer nodo de los demás pares de alta disponibilidad del lote.

En el siguiente ejemplo, hay dos pares de alta disponibilidad en cada lote. Cuando comienza la actualización por lotes, los nodos A y C se actualizan simultáneamente.



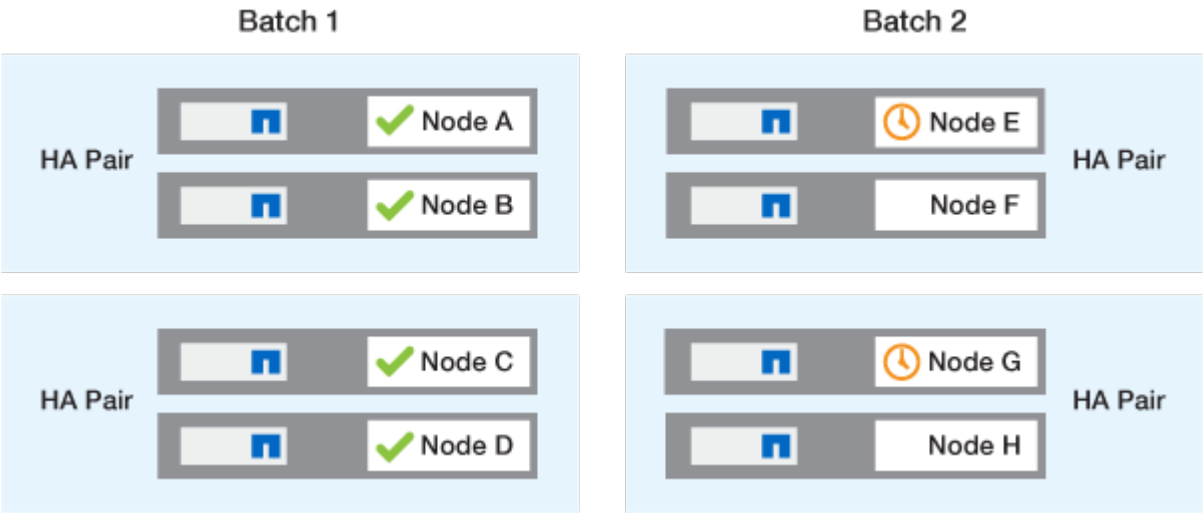
Una vez completada la actualización de los primeros nodos de cada par de alta disponibilidad, los nodos asociados del lote 1 se actualizan simultáneamente.

En el siguiente ejemplo, después de actualizar los nodos A y C, los nodos B y D se actualizan simultáneamente.



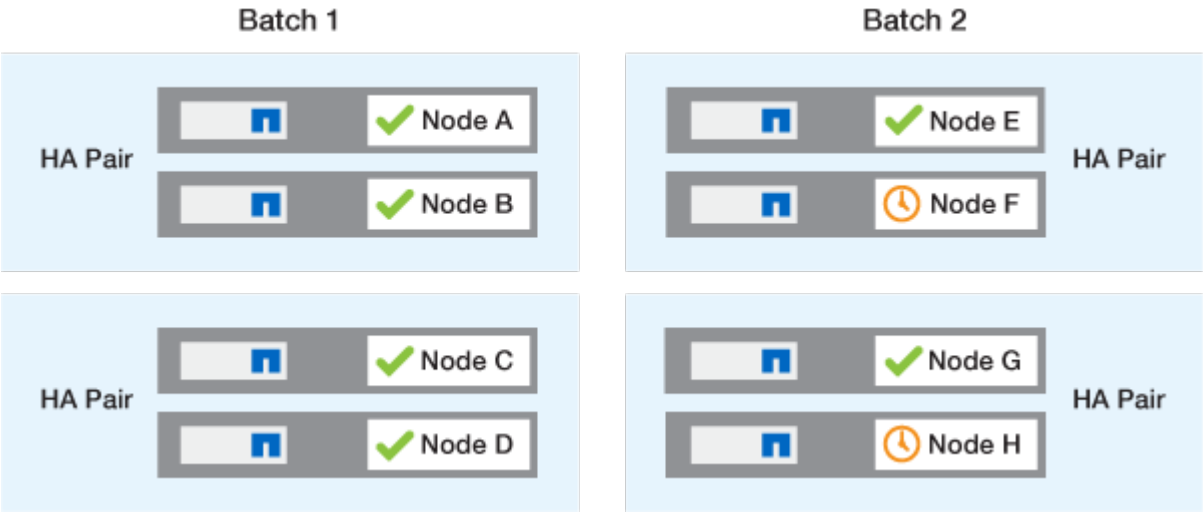
A continuación, el proceso se repite para los nodos en el lote 2. El primer nodo de cada par de alta disponibilidad se actualiza de forma simultánea con el primer nodo de los demás pares de alta disponibilidad del lote.

En el siguiente ejemplo, el nodo E y el nodo G se actualizan simultáneamente.



Una vez completada la actualización de los primeros nodos de cada par de alta disponibilidad, los nodos asociados del lote 2 se actualizan simultáneamente.

En el siguiente ejemplo, el nodo F y el nodo H se actualizan simultáneamente para completar el proceso de actualización por lotes.



Métodos de actualización de ONTAP recomendados según la configuración

Los métodos de actualización admitidos por la configuración se enumeran por orden de uso recomendado.

Configuración	Versión de ONTAP	Número de nodos	Método de actualización recomendado
Estándar	9,0 o posterior	2 o más	• Automatización no disruptiva gracias a System Manager • Automatización no disruptiva gracias a la interfaz de línea de comandos
Estándar	9,0 o posterior	Único	"Interrupción automatizada"
MetroCluster	9,3 o posterior	8	• Automatización no disruptiva gracias a la interfaz de línea de comandos • Manual no disruptivo para MetroCluster de 4 o 8 nodos con la CLI
MetroCluster	9,3 o posterior	2,4	• Automatización no disruptiva gracias a System Manager • Automatización no disruptiva gracias a la interfaz de línea de comandos
MetroCluster	9.2 o anterior	4, 8	Manual no disruptivo para MetroCluster de 4 o 8 nodos con la CLI
MetroCluster	9.2 o anterior	2	Manual no disruptivo para MetroCluster de 2 nodos utilizando la línea de comandos

ANDU El uso de System Manager es el método de actualización recomendado para todas las actualizaciones de revisiones, independientemente de la configuración.

> A. actualización manual disruptiva se puede realizar en cualquier configuración. Sin embargo, no se debe realizar una actualización disruptiva a menos que se pueda desconectar el clúster durante la actualización. Si trabaja en un entorno SAN, debe estar preparado para apagar o suspender todos los clientes SAN antes de realizar una actualización disruptiva. Las actualizaciones disruptivas se realizan mediante la interfaz de línea de comandos de ONTAP.

Actualización automatizada y no disruptiva de ONTAP

Cuando realiza una actualización automatizada, ONTAP instala automáticamente la imagen de ONTAP de destino en cada nodo, valida que el clúster pueda actualizarse correctamente y, a continuación, ejecuta cualquiera de ellos actualización por lotes o sucesivas en el segundo plano según el número de nodos del clúster.

Si es compatible con su configuración, debe usar System Manager para realizar una actualización automatizada. Si la configuración no admite la actualización automatizada mediante System Manager, puede utilizar la interfaz de línea de comandos (CLI) de ONTAP para realizar una actualización automatizada.

> Modificar el ajuste de `storage failover modify-auto-giveback` La opción de comando antes del inicio de una actualización automática no disruptiva (ANDU) no afecta al proceso de actualización. EL proceso ANDU ignora cualquier valor predefinido para esta opción durante la toma de control/devolución necesaria para la actualización. Por ejemplo, establecer `-autogiveback` A False antes de comenzar ANDU no interrumpe la actualización automática antes de la devolución.

Antes de empezar

- Usted debe "prepare la actualización".
- Usted debe "Descargue la imagen del software ONTAP" Para la versión de ONTAP objetivo.

  Si está realizando una "actualización directa de varios saltos", Necesita descargar las dos imágenes ONTAP necesarias para su específico "ruta de actualización".

- Para cada pareja de alta disponibilidad, cada nodo debe tener uno o varios puertos en el mismo dominio de retransmisión.

  Si tiene 8 nodos o más, se utiliza el método de actualización por lotes en la actualización automática no disruptiva. En ONTAP 9.7 y versiones anteriores, si se utiliza el método por lotes, los LIF se migran al partner de alta disponibilidad del nodo que se actualiza. Si los partners no tienen ningún puerto en el mismo dominio de retransmisión, la migración LIF falla.

  En ONTAP 9.8 y versiones posteriores, si se utiliza el método por lotes, los LIF se migran al otro grupo por lotes.

- Si actualiza ONTAP en una configuración de MetroCluster FC, el clúster debe habilitarse para una conmutación de sitios no planificada automática.
- Si no tiene previsto supervisar el progreso del proceso de actualización, debería hacerlo "Solicite notificaciones EMS de errores que puedan requerir intervención manual".
- Si tiene un clúster de un solo nodo, siga el "actualización automatizada y disruptiva" proceso.

  Las actualizaciones de los clústeres de un solo nodo causan interrupciones.

Ejemplo 2. Pasos

System Manager

1. Valide la imagen de destino de ONTAP:

> Si está actualizando una configuración de MetroCluster, debe validar el clúster A y, a continuación, repetir el proceso de validación en el clúster B.

a. Según la versión de ONTAP que esté ejecutando, realice uno de los pasos siguientes:

Si está ejecutando…	Realice lo siguiente…
ONTAP 9,8 o posterior	Haga clic en **Cluster > Overview**.
ONTAP 9.5, 9.6 y 9.7	Haga clic en **Configuración** > **clúster** > **Actualizar**.
ONTAP 9.4 o anterior	Haga clic en **Configuración** > **actualización de clúster**.

b. En la esquina derecha del panel **Overview**, haga clic en ⋮.

c. Haga clic en **actualización de ONTAP**.

d. En la pestaña **Cluster Update**, agregue una nueva imagen o seleccione una imagen disponible.

Si desea…	Realice lo siguiente…
Agregue una nueva imagen de software desde una carpeta local Ya deberías tener "se ha descargado la imagen" al cliente local.	i. En **Imágenes de software disponibles**, haga clic en **Agregar desde local**. ii. Busque la ubicación en la que guardó la imagen de software, seleccione la imagen y, a continuación, haga clic en **Abrir**.
Añada una nueva imagen de software desde un servidor HTTP o FTP	i. Haga clic en **Agregar desde el servidor**. ii. En el cuadro de diálogo **Agregar una nueva imagen de software**, introduzca la URL del servidor HTTP o FTP en el que descargó la imagen del software ONTAP del sitio de soporte de NetApp. Para el FTP anónimo, debe especificar la dirección URL en el ftp://anonymous@ftpserver formato. iii. Haga clic en **Agregar**.
Seleccione una imagen disponible	Elija una de las imágenes mostradas.

e. Haga clic en **Validar** para ejecutar las comprobaciones de validación previas a la actualización.

Si se encuentran errores o advertencias durante la validación, se muestran junto con una lista de acciones correctivas. Debe resolver todos los errores antes de continuar con la actualización. Se recomienda también resolver las advertencias.

2. Haga clic en **Siguiente**.
3. Haga clic en **Actualizar**.

   La validación se realizará de nuevo. Los errores o advertencias restantes se muestran junto con una lista de acciones correctivas. Es necesario corregir los errores antes de continuar con la actualización. Si la validación se completa con advertencias, corrija las advertencias o seleccione **Actualizar con advertencias**.

   > De manera predeterminada, ONTAP utiliza el "proceso de actualización por lotes" para actualizar clústeres con ocho o más nodos. A partir de ONTAP 9.10.1, si lo prefiere, puede seleccionar **Actualizar un par de alta disponibilidad a la vez** para anular el valor predeterminado y hacer que su clúster actualice un par de alta disponibilidad a la vez mediante el proceso de actualización gradual.

   En el caso de las configuraciones de MetroCluster con más de 2 nodos, el proceso de actualización de ONTAP se inicia simultáneamente en los pares de alta disponibilidad en ambos sitios. Para una configuración de MetroCluster de 2 nodos, la actualización se inicia primero en el sitio donde no se inicia la actualización. La actualización en el sitio restante comienza después de que la primera actualización se haya completado por completo.

4. Si la actualización se detiene debido a un error, haga clic en el mensaje de error para ver los detalles y, a continuación, corrija el error y. "reanude la actualización".

Después de terminar

Cuando la actualización se haya completado correctamente, el nodo se reiniciará y se le redirigirá a la página de inicio de sesión de System Manager. Si el nodo tarda mucho tiempo en reiniciarse, debe actualizar el navegador.

CLI

1. Validar la imagen del software de destino ONTAP

   > Si va a actualizar una configuración de MetroCluster, primero debe ejecutar los siguientes pasos en el clúster A y, a continuación, ejecutar los mismos pasos en el clúster B.

   a. Elimine el paquete de software de ONTAP anterior:

   ```
   cluster image package delete -version previous_ONTAP_Version
   ```

   b. Cargue la imagen de software ONTAP de destino en el repositorio de paquetes del cluster:

   ```
   cluster image package get -url location
   ```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.13.1/image.tgz

Package download completed.
Package processing completed.
```

Si está realizando una "actualización directa de varios saltos", También es necesario cargar el paquete de software para la versión intermedia de ONTAP necesaria para su actualización. Por ejemplo, si está actualizando de 9,8 a 9.13.1, debe cargar el paquete de software para ONTAP 9.12.1 y a continuación utilizar el mismo comando para cargar el paquete de software de 9.13.1.

c. Compruebe que el paquete de software esté disponible en el repositorio del paquete de clúster:

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.13.1              MM/DD/YYYY 10:32:15
```

d. Ejecute las comprobaciones automatizadas previas a la actualización:

```
cluster image validate -version package_version_number
```

Si está realizando una "actualización directa de varios saltos", Solo necesita utilizar el paquete ONTAP de destino para la verificación. No es necesario validar la imagen de actualización intermedia por separado. Por ejemplo, si va a actualizar de 9,8 a 9.13.1, use el paquete 9.13.1 para verificación. No es necesario validar el paquete 9.12.1 por separado.

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed...
```

a. Supervise el progreso de la validación:

```
cluster image show-update-progress
```

b. Complete todas las acciones necesarias identificadas por la validación.

c. Si va a actualizar una configuración de MetroCluster, repita los pasos anteriores en el clúster B.

2. Genere un cálculo de actualización de software:

```
cluster image update -version package_version_number -estimate-only
```

> Si va a actualizar una configuración de MetroCluster, puede ejecutar este comando en el clúster A o en el clúster B. No es necesario ejecutarlo en ambos clústeres.

La estimación de actualización de software muestra detalles sobre cada componente que se va a actualizar, así como la duración estimada de la actualización.

3. Realice la actualización de software:

```
cluster image update -version package_version_number
```

- Si está realizando una "actualización directa de varios saltos", Utilice la versión ONTAP de destino para el paquete_VERSION_NUMBER. Por ejemplo, si va a actualizar de ONTAP 9,8 a 9.13.1, utilice 9.13.1 como package_version_number.
- De manera predeterminada, ONTAP utiliza el "proceso de actualización por lotes" para actualizar clústeres con ocho o más nodos. Si lo prefiere, puede usar el `-force-rolling` parámetro para anular el proceso predeterminado y que el clúster actualice un nodo a la vez mediante el proceso de actualización gradual.
- Tras completar cada toma de control y devolución, la actualización espera durante 8 minutos para permitir que las aplicaciones cliente se recuperen desde la pausa en las operaciones de I/o que se producen durante la toma de control y el retorno al nodo primario. Si el entorno requiere más o menos tiempo para la estabilización de clientes, puede usar el `-stabilize-minutes` parámetro para especificar otra cantidad de tiempo de estabilización.
- Para las configuraciones MetroCluster con más de 4 nodos, la actualización automatizada comienza simultáneamente en los pares de alta disponibilidad en ambos sitios. Para una configuración MetroCluster de 2 nodos, la actualización se inicia en el sitio donde no se inicia la actualización. La actualización en el sitio restante comienza después de que la primera actualización se haya completado por completo.

```
cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status     Error-Action
--------------------- ----------
---------------------------------------------
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>
```

4. Muestre el progreso de la actualización del clúster:

```
cluster image show-update-progress
```

Si va a actualizar una configuración de MetroCluster de 4 o 8 nodos, el `cluster image show-update-progress` el comando solo muestra el progreso del nodo en el que ejecuta el comando. Debe ejecutar el comando en cada nodo para ver el progreso de cada nodo.

5. Compruebe que la actualización se ha completado correctamente en cada nodo.

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress

                                                Estimated
Elapsed
Update Phase         Status                      Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                   00:10:00
00:02:07
Data ONTAP updates   completed                   01:31:00
01:39:00
Post-update checks   completed                   00:10:00
00:02:00
3 entries were displayed.

Updated nodes: node0, node1.
```

6. Active una notificación de AutoSupport:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Si el clúster no está configurado para enviar mensajes de AutoSupport, se guardará una copia de la notificación de forma local.

7. Si va a actualizar una configuración de MetroCluster FC de 2 nodos, compruebe que el clúster esté habilitado para la conmutación automática de sitios no planificada.

> Si va a actualizar una configuración estándar, una configuración de IP de MetroCluster o una configuración de FC de MetroCluster superior a 2 nodos, no necesita realizar este paso.

a. Compruebe si la conmutación automática no planificada está habilitada:

```
metrocluster show
```

Si la conmutación automática no planificada está habilitada, aparecerá la siguiente instrucción en el resultado del comando:

```
AUSO Failure Domain    auso-on-cluster-disaster
```

a. Si la sentencia no aparece en la salida, habilite la conmutación automática no planificada:

```
metrocluster modify -auto-switchover-failure-domain auso-on-
cluster-disaster
```

b. Compruebe que se ha activado la conmutación automática no planificada:

```
metrocluster show
```

Reanude la actualización del software ONTAP tras un error en el proceso de actualización automatizada

Si una actualización automática del software ONTAP se detiene debido a un error, debe resolver el error y, a continuación, continuar con la actualización. Una vez resuelto el error, puede optar por continuar con el proceso de actualización automatizada o completar manualmente el proceso de actualización. Si decide continuar con la actualización automatizada, no realice ninguno de los pasos de actualización de forma manual.

Ejemplo 3. Pasos

System Manager

1. Según la versión de ONTAP que esté ejecutando, realice uno de los pasos siguientes:

Si está ejecutando…	Realice lo siguiente…
ONTAP 9,8 o posterior	Haga clic en **Cluster** > **Overview**
ONTAP 9,7, 9,6 o 9,5	Haga clic en **Configuración** > **clúster** > **Actualizar**.
ONTAP 9.4 o anterior	• Haga clic en **Configuración** > **actualización de clúster**. • En la esquina derecha del panel **Descripción general**, haz clic en los tres puntos verticales azules y selecciona **Actualización de ONTAP**.

2. Continúe la actualización automatizada o cancele la actualización y continúe manualmente.

Si desea…	Realice lo siguiente…
Reanude la actualización automatizada	Haga clic en **Reanudar**.
Cancele la actualización automatizada y continúe manualmente	Haga clic en **Cancelar**.

CLI

1. Vea el error de actualización:

```
cluster image show-update-progress
```

2. Resuelva el error.
3. Reanude la actualización:

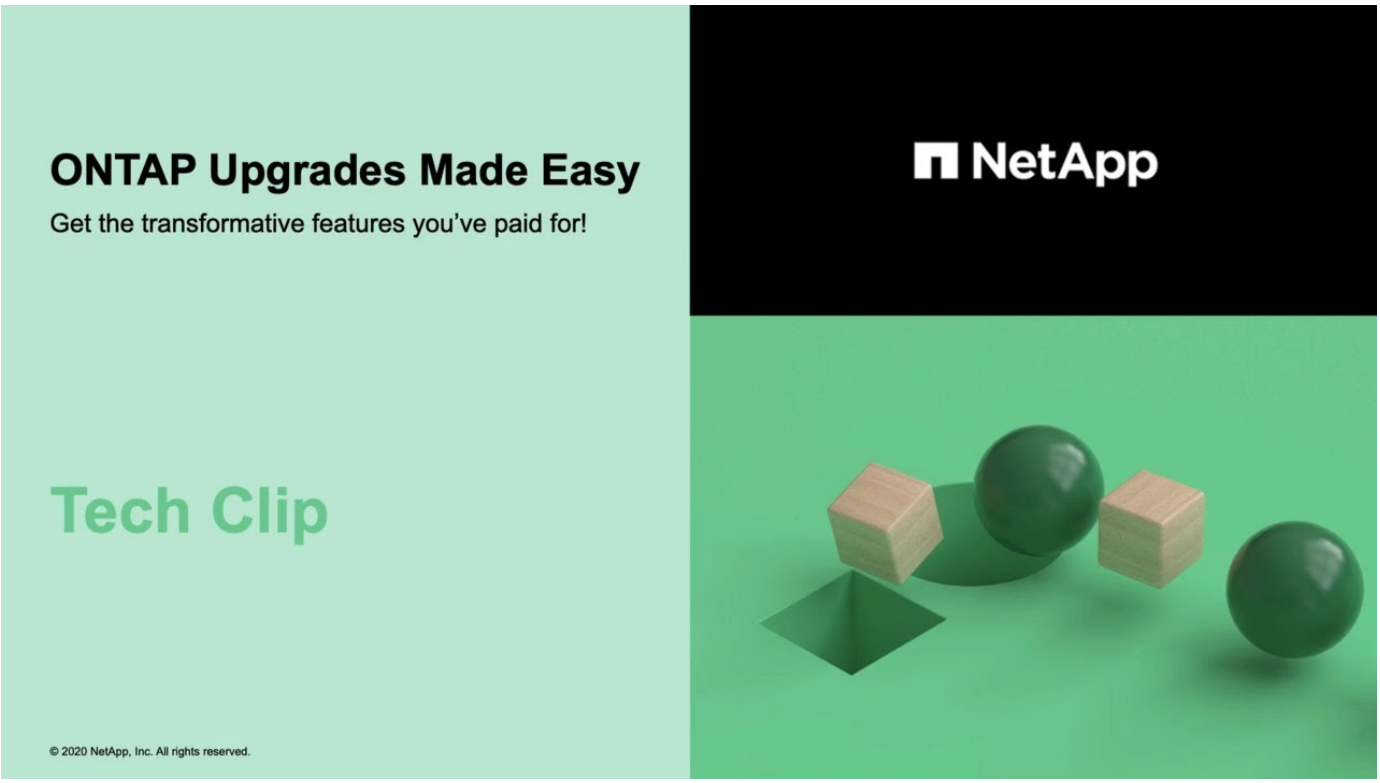
Si desea…	Introduzca el siguiente comando…
Reanude la actualización automatizada	`cluster image resume-update`
Cancele la actualización automatizada y continúe manualmente	`cluster image cancel-update`

Después de terminar

"Realice las comprobaciones posteriores a la actualización".

Vídeo: Las actualizaciones se han realizado con facilidad

Eche un vistazo a las funcionalidades de actualización simplificadas de ONTAP de System Manager en ONTAP 9.8.



Información relacionada

- "Inicie Active IQ"
- "Documentación de Active IQ"

Actualizaciones manuales

Instale el paquete de software ONTAP para las actualizaciones manuales

Después de descargar el paquete de software de ONTAP para una actualización manual, debe instalarlo localmente antes de comenzar la actualización.

Pasos

1. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar: `set -privilege advanced`

   El aviso avanzado (`*>`) aparece.

2. Instale la imagen.

Si tiene la siguiente configuración…	Se usa este comando…
• MetroCluster sin MetroCluster • MetroCluster de 2 nodos	`system node image update -node * -package _location_ -replace -package true -setdefault true -background true` *Location* puede ser un servidor Web o una carpeta local, según la versión de ONTAP. Consulte `system node image update` manual para más detalles. Este comando instala la imagen de software en todos los nodos simultáneamente. Para instalar la imagen en cada nodo de uno en uno, no especifique el `-background` parámetro.
• MetroCluster de 4 nodos • Configuración de MetroCluster de 8 nodos	`system node image update -node * -package location -replace -package true -background true -setdefault false` Debe emitir este comando en ambos clústeres. Este comando utiliza una consulta ampliada para cambiar la imagen de software de destino, que se instala como la imagen alternativa en cada nodo.

3. Introduzca `y` para continuar cuando se le solicite.
4. Compruebe que la imagen de software está instalada en cada nodo.

```
system node image show-update-progress -node *
```

Este comando muestra el estado actual de la instalación de la imagen de software. Debe continuar ejecutando este comando hasta que todos los nodos informen un **Estado de ejecución** de **salido**, y un **Estado de salida** de **éxito**.

El comando de actualización de imagen del nodo del sistema puede fallar y mostrar mensajes de error o advertencia. Después de resolver errores o advertencias, puede volver a ejecutar el comando.

Este ejemplo muestra un clúster de dos nodos en el que la imagen de software se instala correctamente en ambos nodos:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Actualización manual no disruptiva de ONTAP mediante la CLI (configuraciones estándar)

La actualización automatizada mediante System Manager es el método de actualización preferido. Si System Manager no admite la configuración, puede utilizar la interfaz de línea de comandos (CLI) de ONTAP para realizar una actualización manual no disruptiva. Para actualizar un clúster de dos o más nodos mediante el método manual no disruptivo, debe iniciar una operación de conmutación por error en cada nodo de un par de alta disponibilidad, actualizar el nodo «'error'», iniciar la devolución y, a continuación, repetir el proceso para cada pareja de alta disponibilidad del clúster.

Antes de empezar

Debe haber realizado una actualización satisfecha "preparación" requisitos.

Actualizar el primer nodo de una pareja de alta disponibilidad

Puede actualizar el primer nodo de un par de alta disponibilidad iniciando la toma de control por parte del partner de nodo. El partner presta servicio a los datos del nodo mientras se actualiza el primer nodo.

Si realiza una actualización principal, el primer nodo que se va a actualizar debe ser el mismo nodo en el que haya configurado las LIF de datos para conectividad externa e instalado la primera imagen de ONTAP.

Después de actualizar el primer nodo, debe actualizar el nodo del compañero con la mayor rapidez posible. No permita que los dos nodos permanezcan en un "versión mixta" estado más largo de lo necesario.

Pasos

1. Actualice el primer nodo del clúster invocando un mensaje de AutoSupport:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Esta notificación de AutoSupport incluye un registro del estado del sistema justo antes de la actualización. Guarda información útil sobre la solución de problemas en caso de que haya un problema con el proceso de actualización.

Si el clúster no está configurado para enviar mensajes de AutoSupport, se guardará una copia de la notificación de forma local.

2. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (`*>`) aparece.

3. Establezca la nueva imagen del software ONTAP como la imagen predeterminada:

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

El comando system image modify utiliza una consulta ampliada para cambiar la nueva imagen de software ONTAP (que se instala como imagen alternativa) a la imagen predeterminada del nodo.

4. Supervise el progreso de la actualización:

```
system node upgrade-revert show
```

5. Compruebe que la nueva imagen del software ONTAP está configurada como la imagen predeterminada:

```
system image show
```

En el siguiente ejemplo, image2 es la nueva versión de ONTAP y se establece como la imagen predeterminada del nodo 0:

```
cluster1::*> system image show
                 Is      Is                Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------- -------------------
node0
         image1  false   true    X.X.X     MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1  true    true    X.X.X     MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

6. Deshabilite la devolución automática del nodo del partner si está habilitada:

```
storage failover modify -node nodenameB -auto-giveback false
```

Si el clúster es un clúster de dos nodos, se muestra un mensaje que le advierte que al deshabilitar la devolución automática se impide que los servicios del clúster de gestión se conecten en el evento de un fallo alternativo. Introduzca `y` para continuar.

7. Compruebe que la devolución automática está deshabilitada para el partner de nodo:

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node     auto-giveback
-------- -------------
node1    false
1 entry was displayed.
```

8. Ejecute el siguiente comando dos veces para determinar si el nodo que se va a actualizar está sirviendo a cualquier cliente

```
system node run -node nodenameA -command uptime
```

El comando uptime muestra el número total de operaciones que el nodo ha realizado para clientes NFS, SMB, FC e iSCSI desde que se inició por última vez el nodo. Para cada protocolo, debe ejecutar el comando dos veces para determinar si el número de operaciones está aumentando. Si aumentan, el nodo actualmente sirve clientes para ese protocolo. Si no aumentan, el nodo no ofrece actualmente clientes para ese protocolo.

> Debe tomar una nota de cada protocolo que ha aumentado las operaciones de cliente de manera que, después de actualizar el nodo, pueda verificar que el tráfico del cliente se haya reanudado.

En el ejemplo siguiente se muestra un nodo con operaciones NFS, SMB, FC e iSCSI. Sin embargo, actualmente el nodo sólo ofrece clientes NFS e iSCSI.

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. Migre todos los LIF de datos del nodo:

```
network interface migrate-all -node nodenameA
```

10. Compruebe las LIF que ha migrado:

```
network interface show
```

Para obtener más información acerca de los parámetros que puede utilizar para comprobar el estado de LIF, consulte la página show man de la interfaz de red.

El ejemplo siguiente muestra que las LIF de datos de nodo 0 se migraron correctamente. Para cada LIF, los campos incluidos en este ejemplo le permiten comprobar el nodo y el puerto de inicio de la LIF, el nodo y el puerto actuales al que se ha migrado la LIF y el estado operativo y administrativo de la LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node0     e0a       node1     e0a       up          up
vs0     data002 node0     e0b       node1     e0b       up          up
vs0     data003 node0     e0b       node1     e0b       up          up
vs0     data004 node0     e0a       node1     e0a       up          up
4 entries were displayed.
```

11. Inicie una toma de control:

```
storage failover takeover -ofnode nodenameA
```

No especifique el parámetro -option Immediate porque se requiere una toma de control normal para el nodo que se va a realizar la operación para arrancar en la nueva imagen de software. Si no ha migrado manualmente las LIF desde el nodo, migran automáticamente al partner de alta disponibilidad del nodo para garantizar que no hay interrupciones del servicio.

El primer nodo arranca hasta la espera del estado de devolución.

> Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que el nodo está fuera del quórum del clúster. Puede ignorar esta notificación y continuar con la actualización.

12. Compruebe que la toma de control se ha realizado correctamente:

```
storage failover show
```

Es posible que aparezcan mensajes de error que indiquen problemas de versiones no coincidentes y de formato del buzón. Se trata del comportamiento esperado y representa un estado temporal en una actualización no disruptiva importante y no es perjudicial.

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo 0 tiene el estado esperando devolución y su partner está en el estado de toma de control.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
------------------------------------
node0          node1          -        Waiting for giveback (HA
mailboxes)
node1          node0          false    In takeover
2 entries were displayed.
```

13. Espere al menos ocho minutos para que surtan efecto las siguientes condiciones:
    - La multivía del cliente (si está implementada) se estabiliza.
    - Los clientes se recuperan de la pausa en una operación de I/o que se produce durante la toma de control.

      El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos, en función de las características de las aplicaciones cliente.

14. Devuelva los agregados al primer nodo:

```
storage failover giveback -ofnode nodenameA
```

La devolución devuelve primero el agregado raíz al nodo del partner y, después de que ese nodo haya terminado de arrancarse, devuelve los agregados que no son raíz y los LIF que se hayan establecido en revertir automáticamente. El nodo que se acaba de arrancar empieza a suministrar datos a los clientes desde cada agregado en cuanto se devuelva dicho agregado.

15. Compruebe que se han devuelto todos los agregados:

```
storage failover show-giveback
```

Si el campo Estado de devolución indica que no hay agregados que devolver, se devolverán todos los agregados. Si se vetó la devolución, el comando muestra el progreso de devolución y qué subsistema vetó la devolución.

16. Si no se ha devuelto ningún agregado, realice los siguientes pasos:

a. Revise la solución de veto para determinar si desea abordar la condición "vertical" o anular el veto.
b. Si es necesario, tratar la condición "verto" descrita en el mensaje de error, asegurándose de que las operaciones identificadas se cancelen con gracia.
c. Vuelva a ejecutar el comando de recuperación tras fallos del almacenamiento.

   Si ha decidido anular la condición "VETE", establezca el parámetro -override-vetoes en TRUE.

17. Espere al menos ocho minutos para que surtan efecto las siguientes condiciones:
    - La multivía del cliente (si está implementada) se estabiliza.
    - Los clientes se recuperan de la pausa en una operación de I/o que se produce durante la devolución.

    El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos, en función de las características de las aplicaciones cliente.

18. Compruebe que la actualización se ha realizado correctamente para el nodo:

    a. Vaya al nivel de privilegio avanzado :

    ```
    set -privilege advanced
    ```

    b. Compruebe que el estado de la actualización se haya completado para el nodo:

    ```
    system node upgrade-revert show -node nodenameA
    ```

    El estado debe aparecer como completo.

    Si el estado no se completa, póngase en contacto con el soporte técnico.

    a. Vuelva al nivel de privilegio de administrador:

    ```
    set -privilege admin
    ```

19. Compruebe que los puertos del nodo estén activos:

    ```
    network port show -node nodenameA
    ```

    Debe ejecutar este comando en un nodo que se haya actualizado a la versión superior de ONTAP 9.

    En el ejemplo siguiente se muestra que todos los puertos del nodo están en funcionamiento:

```
cluster1::> network port show -node node0
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node0
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

20. Revierte los LIF al nodo:

```
network interface revert *
```

Este comando muestra las LIF que se han migrado del nodo.

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. Compruebe que los LIF de datos del nodo se hayan revertido correctamente al nodo y que estén en funcionamiento:

```
network interface show
```

En el ejemplo siguiente se muestra que todos los LIF de datos alojados en el nodo se han revertido correctamente al nodo y que su estado operativo está en funcionamiento:

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0         e0a
true
            data002      up/up    192.0.2.121/24     node0         e0b
true
            data003      up/up    192.0.2.122/24     node0         e0b
true
            data004      up/up    192.0.2.123/24     node0         e0a
true
4 entries were displayed.
```

22. Si anteriormente ha determinado que este nodo sirve a clientes, compruebe que el nodo está proporcionando servicio para cada protocolo que estaba sirviendo anteriormente:

```
system node run -node nodenameA -command uptime
```

La operación se restablece a cero durante la actualización.

En el ejemplo siguiente se muestra que el nodo actualizado ha reanudado el servicio a sus clientes NFS e iSCSI:

```
cluster1::> system node run -node node0 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. Vuelva a habilitar la devolución automática en el nodo del partner si estaba previamente deshabilitada:

```
storage failover modify -node nodenameB -auto-giveback true
```

Debe continuar para actualizar el partner de alta disponibilidad del nodo lo más rápido posible. Si debe suspender el proceso de actualización por cualquier motivo, ambos nodos de la pareja de alta disponibilidad deben ejecutar la misma versión de ONTAP.

Actualizar el nodo del partner en una pareja de alta disponibilidad

Después de actualizar el primer nodo de un par de alta disponibilidad, actualiza su compañero iniciando la toma de control sobre él. El primer nodo sirve los datos del partner mientras se actualiza el nodo del partner.

1. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar:

```
set -privilege advanced
```

   El aviso avanzado (`*>`) aparece.

2. Establezca la nueva imagen del software ONTAP como la imagen predeterminada:

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

   El comando system image modify utiliza una consulta ampliada para cambiar la nueva imagen de software ONTAP (que se instala como imagen alternativa) que es la imagen predeterminada del nodo.

3. Supervise el progreso de la actualización:

```
system node upgrade-revert show
```

4. Compruebe que la nueva imagen del software ONTAP está configurada como la imagen predeterminada:

```
system image show
```

   En el siguiente ejemplo: `image2` Es la nueva versión de ONTAP y se establece como imagen predeterminada en el nodo:

```
cluster1::*> system image show
                 Is      Is                Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------- -------------------
node0
         image1  false   false   X.X.X     MM/DD/YYYY TIME
         image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1  false   true    X.X.X     MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

5. Deshabilite la devolución automática del nodo del partner si está habilitada:

```
storage failover modify -node nodenameA -auto-giveback false
```

   Si el clúster es un clúster de dos nodos, se muestra un mensaje que le advierte que al deshabilitar la devolución automática se impide que los servicios del clúster de gestión se conecten en el evento de un

fallo alternativo. Introduzca `y` para continuar.

6. Compruebe que la devolución automática está deshabilitada para el nodo asociado:

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node     auto-giveback
-------- -------------
node0    false
1 entry was displayed.
```

7. Ejecute el siguiente comando dos veces para determinar si el nodo que se va a actualizar está sirviendo a cualquier cliente:

```
system node run -node nodenameB -command uptime
```

El comando uptime muestra el número total de operaciones que el nodo ha realizado para clientes NFS, SMB, FC e iSCSI desde que se inició por última vez el nodo. Para cada protocolo, debe ejecutar el comando dos veces para determinar si el número de operaciones está aumentando. Si aumentan, el nodo actualmente sirve clientes para ese protocolo. Si no aumentan, el nodo no ofrece actualmente clientes para ese protocolo.

NOTA: Debe tomar nota de cada protocolo que tiene cada vez más operaciones de cliente para que después de actualizar el nodo, pueda verificar que el tráfico de cliente se ha reanudado.

En el ejemplo siguiente se muestra un nodo con operaciones NFS, SMB, FC e iSCSI. Sin embargo, actualmente el nodo sólo ofrece clientes NFS e iSCSI.

```
cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. Migre todos los LIF de datos del nodo:

```
network interface migrate-all -node nodenameB
```

9. Compruebe el estado de cualquier LIF que haya migrado:

```
network interface show
```

Para obtener más información acerca de los parámetros que puede utilizar para comprobar el estado de LIF, consulte la página show man de la interfaz de red.

El ejemplo siguiente muestra que las LIF de datos del nodo 1 se migraron correctamente. Para cada LIF, los campos incluidos en este ejemplo le permiten comprobar el nodo y el puerto de inicio de la LIF, el nodo y el puerto actuales al que se ha migrado la LIF y el estado operativo y administrativo de la LIF.

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node1     e0a       node0     e0a       up          up
vs0     data002 node1     e0b       node0     e0b       up          up
vs0     data003 node1     e0b       node0     e0b       up          up
vs0     data004 node1     e0a       node0     e0a       up          up
4 entries were displayed.
```

10. Inicie una toma de control:

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

No especifique el parámetro -option Immediate porque se requiere una toma de control normal para el nodo que se va a realizar la operación para arrancar en la nueva imagen de software. Si no ha migrado manualmente las LIF desde el nodo, migran automáticamente al partner de alta disponibilidad del nodo para que no haya interrupciones del servicio.

Aparece una advertencia. Debe entrar `y` para continuar.

El nodo que se ha tomado arranca hasta esperando el estado de devolución.

> Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que el nodo está fuera del quórum del clúster. Puede ignorar esta notificación y continuar con la actualización.

11. Compruebe que la toma de control se ha realizado correctamente:

```
storage failover show
```

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo 1 está en

estado esperando devolución del nodo y su compañero está en estado de toma de control.

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        In takeover
node1          node0          false    Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

12. Espere al menos ocho minutos para que surtan efecto las siguientes condiciones:

    +
    La multivía del cliente (si está implementada) se estabiliza.
    Los clientes se recuperan de la pausa en la I/o que se produce durante la toma de control.

    +
    El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos, según las características de las aplicaciones cliente.

13. Devolver los agregados al nodo partner:

    ```
    storage failover giveback -ofnode nodenameB
    ```

    La operación de devolución devuelve en primer lugar el agregado raíz al nodo del partner y, después de que ese nodo haya finalizado el arranque, devuelve los agregados que no son raíz y los LIF que se hayan configurado para que se revierten automáticamente. El nodo que se acaba de arrancar empieza a suministrar datos a los clientes desde cada agregado en cuanto se devuelva dicho agregado.

14. Compruebe que se devuelven todos los agregados:

    ```
    storage failover show-giveback
    ```

    Si el campo Giveback Status indica que no hay agregados que devolver, se devuelven todos los agregados. Si se vetó la devolución, el comando muestra el progreso de devolución y qué subsistema vetó la operación de devolución.

15. Si no se devuelve ningún agregado, realice los siguientes pasos:
    a. Revise la solución de veto para determinar si desea abordar la condición "vertical" o anular el veto.
    b. Si es necesario, tratar la condición "verto" descrita en el mensaje de error, asegurándose de que las operaciones identificadas se cancelen con gracia.
    c. Vuelva a ejecutar el comando de recuperación tras fallos del almacenamiento.

       Si ha decidido anular la condición "VETE", establezca el parámetro -override-vetoes en TRUE.

16. Espere al menos ocho minutos para que surtan efecto las siguientes condiciones:
    - La multivía del cliente (si está implementada) se estabiliza.
    - Los clientes se recuperan de la pausa en una operación de I/o que se produce durante la devolución.

      El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos, en función de las características de las aplicaciones cliente.

17. Compruebe que la actualización se ha realizado correctamente para el nodo:

    a. Vaya al nivel de privilegio avanzado :

    ```
    set -privilege advanced
    ```

    b. Compruebe que el estado de la actualización se haya completado para el nodo:

    ```
    system node upgrade-revert show -node nodenameB
    ```

    El estado debe aparecer como completo.

    Si el estado no es completo, desde el nodo, ejecute el comando system node upgrade-revert upgrade. Si el comando no completa la actualización, póngase en contacto con el soporte técnico.

    a. Vuelva al nivel de privilegio de administrador:

    ```
    set -privilege admin
    ```

18. Compruebe que los puertos del nodo estén activos:

    ```
    network port show -node nodenameB
    ```

    Este comando debe ejecutarse en un nodo que se ha actualizado a ONTAP 9.4.

    En el ejemplo siguiente se muestra que todos los puertos de datos del nodo están en funcionamiento:

```
cluster1::> network port show -node node1
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

19. Revierte los LIF al nodo:

```
network interface revert *
```

Este comando muestra las LIF que se han migrado del nodo.

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. Compruebe que los LIF de datos del nodo se hayan revertido correctamente al nodo y que estén en funcionamiento:

```
network interface show
```

En el ejemplo siguiente se muestra que todos los LIF de datos alojados en el nodo se vuelven a restaurar correctamente al nodo y que su estado operativo es up:

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node1         e0a
true
            data002      up/up    192.0.2.121/24     node1         e0b
true
            data003      up/up    192.0.2.122/24     node1         e0b
true
            data004      up/up    192.0.2.123/24     node1         e0a
true
4 entries were displayed.
```

21. Si anteriormente ha determinado que este nodo sirve a clientes, compruebe que el nodo está proporcionando servicio para cada protocolo que estaba sirviendo anteriormente:

```
system node run -node nodenameB -command uptime
```

La operación se restablece a cero durante la actualización.

En el ejemplo siguiente se muestra que el nodo actualizado ha reanudado el servicio a sus clientes NFS e iSCSI:

```
cluster1::> system node run -node node1 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. Si este fue el último nodo del clúster que se actualizó, active una notificación de AutoSupport:

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

Esta notificación de AutoSupport incluye un registro del estado del sistema justo antes de la actualización. Guarda información útil sobre la solución de problemas en caso de que haya un problema con el proceso de actualización.

Si el clúster no está configurado para enviar mensajes de AutoSupport, se guardará una copia de la notificación de forma local.

23. Confirme que el nuevo software ONTAP se está ejecutando en ambos nodos de la pareja de alta

disponibilidad:

```
set -privilege advanced
```

```
system node image show
```

En el siguiente ejemplo, image2 es la versión actualizada de ONTAP y es la versión predeterminada en ambos nodos:

```
cluster1::*> system node image show
                 Is      Is                Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------- -------------------
node0
         image1  false   false   X.X.X     MM/DD/YYYY TIME
         image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1  false   false   X.X.X     MM/DD/YYYY TIME
         image2  true    true    Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

24. Vuelva a habilitar la devolución automática en el nodo del partner si estaba previamente deshabilitada:

```
storage failover modify -node nodenameA -auto-giveback true
```

25. Compruebe que el cluster está en quórum y que los servicios se están ejecutando mediante `cluster show` y.. `cluster ring show` comandos (nivel de privilegio avanzado).

    Debe realizar este paso antes de actualizar cualquier par de alta disponibilidad adicional.

26. Vuelva al nivel de privilegio de administrador:

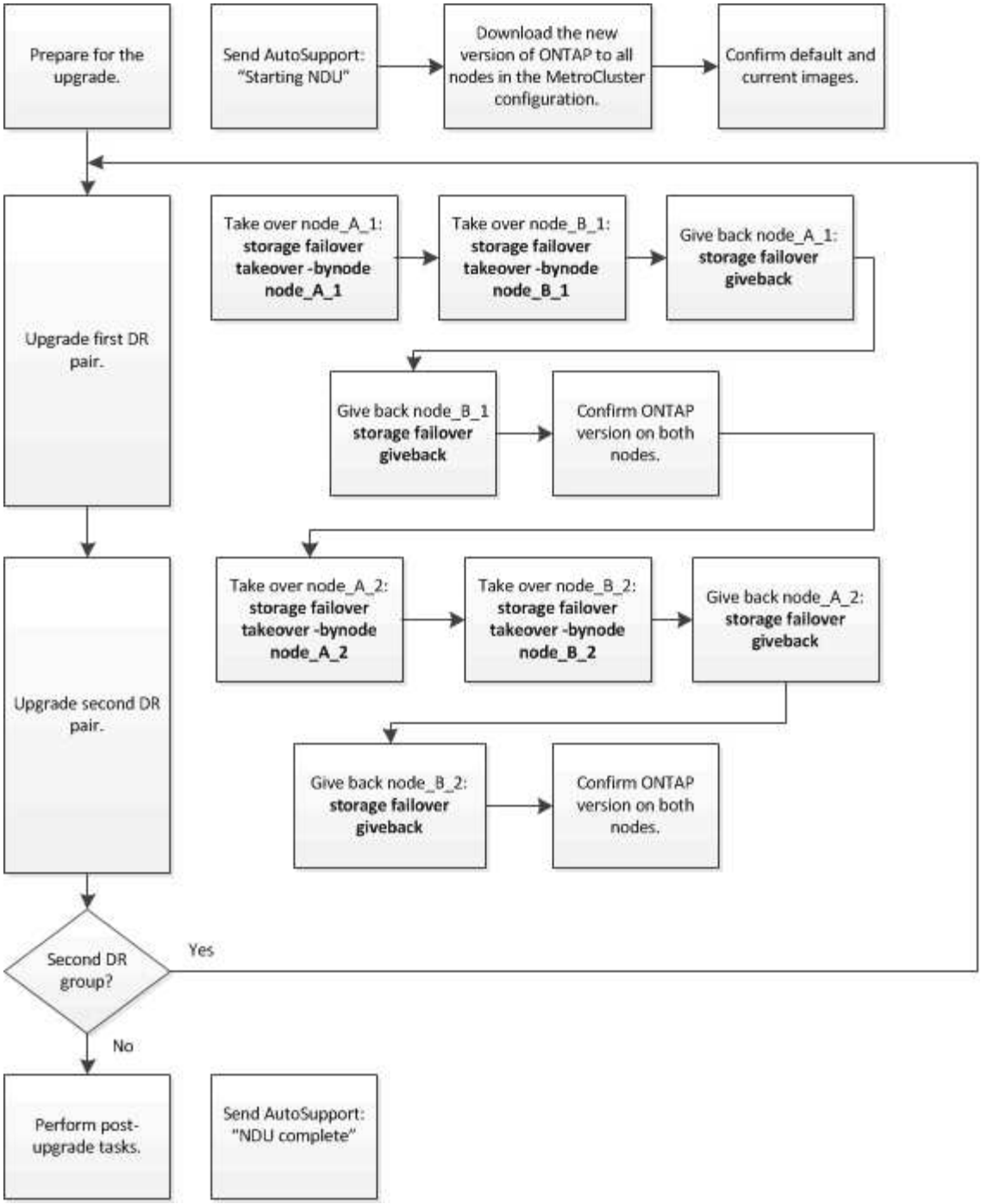
```
set -privilege admin
```

27. Actualice cualquier par de alta disponibilidad adicional.

Actualización manual de ONTAP no disruptiva de una configuración de MetroCluster de cuatro u ocho nodos mediante la CLI

Una actualización manual de una configuración de MetroCluster de cuatro u ocho nodos implica la preparación de la actualización, la actualización de los pares de recuperación ante desastres en cada uno o dos grupos de recuperación ante desastres simultáneamente y la realización de las tareas posteriores a la actualización.

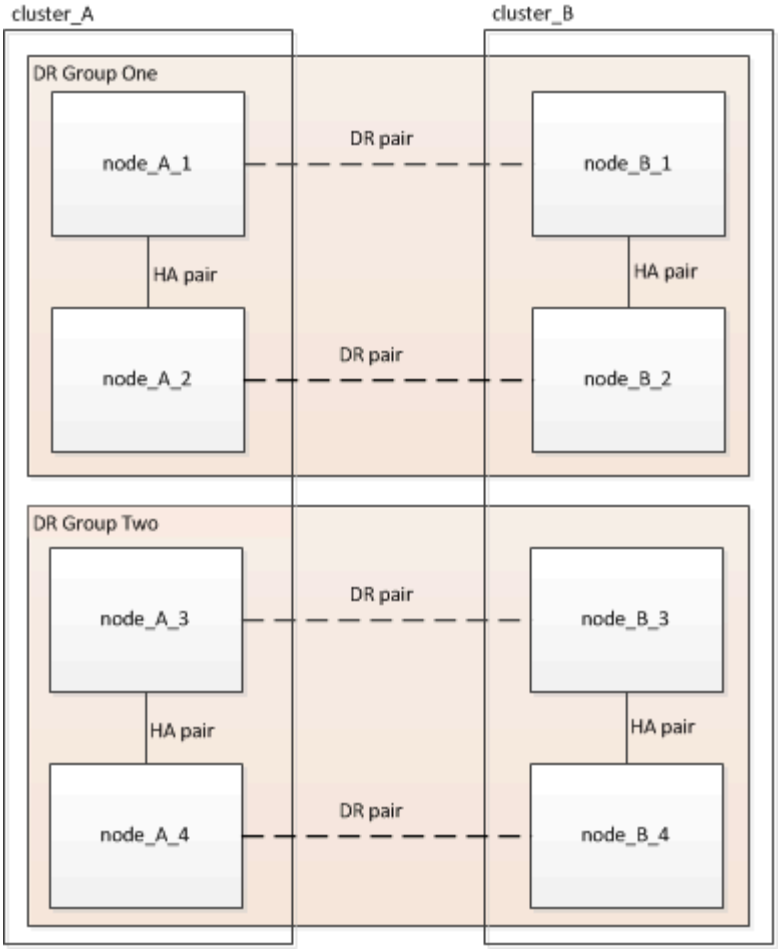
- Esta tarea se aplica a las siguientes configuraciones:
  - Configuraciones IP o FC de MetroCluster de cuatro nodos que ejecuten ONTAP 9.2 o una versión anterior
  - Configuraciones de MetroCluster FC de ocho nodos, independientemente de la versión de ONTAP
- Si tiene una configuración MetroCluster de dos nodos, no utilice este procedimiento.
- Las siguientes tareas hacen referencia a las versiones anterior y nueva de ONTAP.
  - Al actualizar, la versión antigua es una versión anterior de ONTAP, con un número de versión inferior al de la nueva versión de ONTAP.
  - Al realizar la degradación, la versión anterior es una versión posterior de ONTAP, con un número de versión superior al de la nueva versión de ONTAP.
- En esta tarea se utiliza el siguiente flujo de trabajo de alto nivel:



Diferencias cuando se actualiza el software ONTAP en una configuración de MetroCluster de ocho o cuatro nodos

El proceso de actualización de software MetroCluster varía en función de si haya ocho o cuatro nodos en la configuración de MetroCluster.

Una configuración MetroCluster está compuesta por uno o dos grupos de recuperación ante desastres. Cada grupo de recuperación ante desastres consta de dos parejas de alta disponibilidad, un par de alta disponibilidad en cada clúster MetroCluster. Un MetroCluster de ocho nodos incluye dos grupos de recuperación ante desastres:



Actualiza un grupo de recuperación ante desastres cada vez.

Para configuraciones MetroCluster de cuatro nodos:

1. Actualizar grupo de DR uno:
   a. Actualice NODE_A_1 y NODE_B_1.
   b. Actualice NODE_A_2 y NODE_B_2.

Para configuraciones MetroCluster de ocho nodos, el procedimiento de actualización del grupo de recuperación ante desastres se realiza dos veces:

1. Actualizar grupo de DR uno:
   a. Actualice NODE_A_1 y NODE_B_1.
   b. Actualice NODE_A_2 y NODE_B_2.
2. Actualizar grupo DR dos:
   a. Actualice NODE_A_3 y NODE_B_3.
   b. Actualice NODE_A_4 y NODE_B_4.

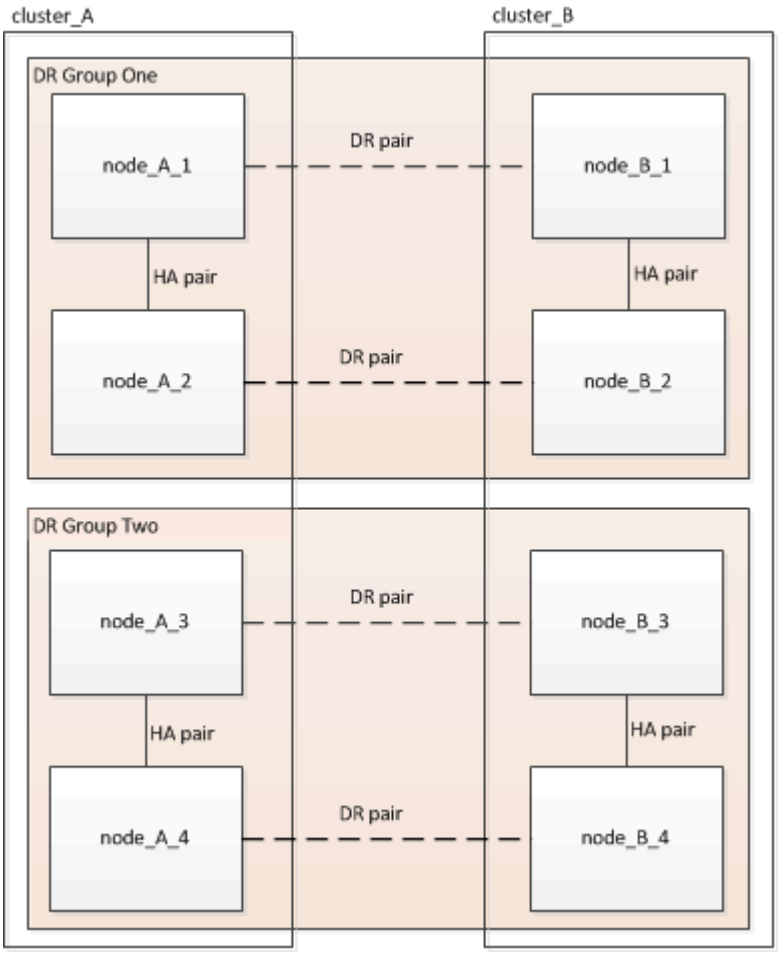
Preparar la actualización de un grupo de recuperación ante desastres de MetroCluster

Antes de actualizar el software ONTAP en los nodos, debe identificar las relaciones de recuperación ante desastres entre los nodos, enviar un mensaje de AutoSupport para iniciar una actualización y confirmar la versión de ONTAP que se está ejecutando en cada nodo.

Debe tener "descargado" y.. "instalado" las imágenes de software.

Esta tarea debe repetirse en cada grupo de recuperación ante desastres. Si la configuración del MetroCluster consta de ocho nodos, hay dos grupos de recuperación ante desastres. Por lo tanto, esta tarea debe repetirse en cada grupo de recuperación ante desastres.

Los ejemplos que se proporcionan en esta tarea utilizan los nombres que se muestran en la siguiente ilustración para identificar los clústeres y los nodos:



1. Identifique las parejas de recuperación ante desastres en la configuración:

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
  (metrocluster node show)
dr-group-id cluster     node       dr-partner
----------- -------     --------   ----------
1           cluster_A   node_A_1   node_B_1
1           cluster_A   node_A_2   node_B_2
1           cluster_B   node_B_1   node_A_1
1           cluster_B   node_B_2   node_A_2
4 entries were displayed.

cluster_A::>
```

2. Establezca el nivel de privilegio de admin en Advanced, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (`*>`) aparece.

3. Confirme la versión de ONTAP en cluster_A:

```
system image show
```

```
cluster_A::*> system image show
                 Is      Is                Install
Node     Image   Default Current Version   Date
-------- ------- ------- ------- -------   -------------------
node_A_1
         image1  true    true    X.X.X     MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y     MM/DD/YYYY TIME
node_A_2
         image1  true    true    X.X.X     MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. Confirme la versión en cluster_B:

```
system image show
```

```
cluster_B::*> system image show
                 Is      Is                  Install
Node     Image   Default Current Version     Date
-------- ------- ------- ------- -------     -------------------
node_B_1
         image1  true    true    X.X.X       MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y       MM/DD/YYYY TIME
node_B_2
         image1  true    true    X.X.X       MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.

cluster_B::>
```

5. Active una notificación de AutoSupport:

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

Esta notificación de AutoSupport incluye un registro del estado del sistema antes de la actualización. Guarda información útil sobre la solución de problemas si hay un problema con el proceso de actualización.

Si su clúster no está configurado para enviar mensajes de AutoSupport, se guardará una copia de la notificación de forma local.

6. Para cada nodo del primer conjunto, establezca la imagen del software ONTAP de destino como la imagen predeterminada:

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

Este comando utiliza una consulta ampliada para cambiar la imagen de software de destino, que se instala como imagen alternativa, para que sea la imagen predeterminada del nodo.

7. Compruebe que la imagen del software ONTAP de destino esté establecida como la imagen predeterminada en cluster_A:

```
system image show
```

En el siguiente ejemplo, image2 es la nueva versión de ONTAP y se define como la imagen predeterminada en cada uno de los nodos del primer conjunto:

```
cluster_A::*> system image show
                 Is      Is              Install
Node     Image   Default Current Version Date
-------- ------- ------- ------- ------- -------------------
node_A_1
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y   MM/DD/YYYY TIME
node_A_2
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true   false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

a. Compruebe que la imagen del software ONTAP de destino esté establecida como la imagen predeterminada en CLÚSTER_B:

```
system image show
```

En el siguiente ejemplo se muestra que la versión de destino está establecida como imagen predeterminada en cada uno de los nodos del primer conjunto:

```
cluster_B::*> system image show
                 Is      Is              Install
Node     Image   Default Current Version Date
-------- ------- ------- ------- ------- -------------------
node_A_1
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y   MM/YY/YYYY TIME
node_A_2
         image1  false   true    X.X.X   MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y   MM/DD/YYYY TIME

2 entries were displayed.
```

8. Determine si los nodos que se van a actualizar actualmente sirven a clientes dos veces para cada nodo:

```
system node run -node target-node -command uptime
```

El comando UpTime muestra el número total de operaciones que el nodo ha realizado para clientes NFS, CIFS, FC e iSCSI desde que se inició por última vez el nodo. Para cada protocolo, debe ejecutar el comando dos veces para determinar si el número de operaciones está aumentando. Si aumentan, el nodo actualmente sirve clientes para ese protocolo. Si no aumentan, el nodo no ofrece actualmente clientes para ese protocolo.

Debe tomar una nota de cada protocolo que ha aumentado las operaciones de cliente de manera que, una vez actualizado el nodo, pueda verificar que el tráfico del cliente se haya reanudado.

Este ejemplo muestra un nodo con operaciones NFS, CIFS, FC e iSCSI. Sin embargo, actualmente el nodo sólo ofrece clientes NFS e iSCSI.

```
 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

Actualizar la primera pareja de recuperación ante desastres en un grupo de recuperación ante desastres de MetroCluster

Debe realizar una toma de control y una devolución de los nodos en el orden correcto para que la nueva versión de ONTAP sea la versión actual del nodo.

Todos los nodos deben ejecutar la versión anterior de ONTAP.

En esta tarea, se actualizan NODE_A_1 y NODE_B_1.

Si ha actualizado el software ONTAP en el primer grupo de recuperación ante desastres y ahora está actualizando el segundo grupo de recuperación ante desastres en una configuración MetroCluster de ocho nodos, en esta tarea debería actualizar NODE_A_3 y NODE_B_3.

1. Si el software MetroCluster Tiebreaker está habilitado, esta opción está deshabilitada.
2. Para cada nodo del par de alta disponibilidad, deshabilite el retorno automático:

   ```
   storage failover modify -node target-node -auto-giveback false
   ```

   Este comando se debe repetir para cada nodo de la pareja de ha.

3. Compruebe que la devolución automática está desactivada:

   ```
   storage failover show -fields auto-giveback
   ```

   Este ejemplo muestra que se ha deshabilitado la devolución automática de control en ambos nodos:

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 false
node_x_2 false
2 entries were displayed.
```

4. Asegúrese de que las I/O no superen el ~50 % en cada controladora y que el uso de CPU no supere el ~50 % por controladora.
5. Inicie la toma de control del nodo de destino en cluster_A:

   No especifique el parámetro -option Immediate porque se requiere una toma de control normal para los nodos que se van a realizar la operación para arrancar en la nueva imagen de software.

   a. Asumir el control del partner de recuperación ante desastres en cluster_A (nodo_A_1):

   ```
   storage failover takeover -ofnode node_A_1
   ```

   El nodo arranca con el estado "esperando la devolución".

   > Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que los nodos no tienen quórum de clúster. Puede ignorar esta notificación y continuar con la actualización.

   b. Compruebe que la toma de control se ha realizado correctamente:

   ```
   storage failover show
   ```

   El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo_A_1 está en el estado "esperando devolución" y el nodo_A_2 está en el estado "durante toma de control".

```
 cluster1::> storage failover show
                                Takeover
 Node           Partner         Possible State Description
 -------------- -------------- --------
-------------------------------------
 node_A_1       node_A_2       -        Waiting for giveback (HA
mailboxes)
 node_A_2       node_A_1       false    In takeover
 2 entries were displayed.
```

6. Asumir el control del partner de recuperación ante desastres en cluster_B (nodo_B_1):

   No especifique el parámetro -option Immediate porque se requiere una toma de control normal para los

nodos que se van a realizar la operación para arrancar en la nueva imagen de software.

a. Asuma el control node_B_1:

```
storage failover takeover -ofnode node_B_1
```

El nodo arranca con el estado "esperando la devolución".

> Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que los nodos no tienen quórum de clúster. Puede ignorar esta notificación y continuar con la actualización.

b. Compruebe que la toma de control se ha realizado correctamente:

```
storage failover show
```

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo B_1 está en el estado "esperando devolución" y el nodo B_2 está en el estado "durante toma de control".

```
 cluster1::> storage failover show
                                Takeover
 Node           Partner         Possible State Description
 -------------- -------------- --------
-------------------------------------
 node_B_1       node_B_2       -        Waiting for giveback (HA
mailboxes)
 node_B_2       node_B_1       false    In takeover
 2 entries were displayed.
```

7. Espere al menos ocho minutos para asegurarse de las siguientes condiciones:
   - La multivía del cliente (si está implementada) se estabiliza.
   - Los clientes se recuperan de la pausa en la I/o que se produce durante la toma de control.

     El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos en función de las características de las aplicaciones cliente.

8. Devuelva los agregados a los nodos de destino:

Después de actualizar la configuración IP de MetroCluster a ONTAP 9.5 o una versión posterior, los agregados estarán en estado degradado durante un breve periodo de tiempo antes de volver a sincronizar y volver a un estado de reflejo.

a. Proporcione los agregados al partner de recuperación ante desastres en cluster_A:

```
storage failover giveback -ofnode node_A_1
```

b. Proporcione los agregados al partner de recuperación ante desastres en cluster_B:

```
storage failover giveback -ofnode node_B_1
```

La operación de devolución devuelve primero el agregado raíz al nodo y, después de que el nodo haya terminado de arrancarse, devuelve los agregados que no son raíz.

9. Compruebe que todos los agregados se han devuelto emitiendo el siguiente comando en ambos clústeres:

```
storage failover show-giveback
```

Si el campo Estado de devolución indica que no hay agregados que devolver, se devolverán todos los agregados. Si se vetó la devolución, el comando muestra el progreso de devolución y qué subsistema vetó la devolución.

10. Si no se ha devuelto ningún agregado, realice lo siguiente:
    a. Revise la solución de veto para determinar si desea abordar la condición "vertical" o anular el veto.
    b. Si es necesario, tratar la condición "verto" descrita en el mensaje de error, asegurándose de que las operaciones identificadas se cancelen con gracia.
    c. Vuelva a introducir el comando de devolución del nodo de respaldo del almacenamiento.

    Si ha decidido anular la condición "VETE", establezca el parámetro -override-vetoes en TRUE.

11. Espere al menos ocho minutos para asegurarse de las siguientes condiciones:
    - La multivía del cliente (si está implementada) se estabiliza.
    - Los clientes se recuperan de la pausa en la I/o que se produce durante la devolución.

    El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos en función de las características de las aplicaciones cliente.

12. Establezca el nivel de privilegio de admin en Advanced, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (`*>`) aparece.

13. Confirme la versión en cluster_A:

```
system image show
```

En el siguiente ejemplo se muestra que la impresora image2 del sistema debe ser la versión predeterminada y actual en node_A_1:

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image   Default Current Version  Date
-------- ------- ------- ------- -------- -------------------
node_A_1
         image1  false   false    X.X.X   MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y   MM/DD/YYYY TIME
node_A_2
         image1  false   true     X.X.X   MM/DD/YYYY TIME
         image2  true    false    Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

14. Confirme la versión en cluster_B:

```
system image show
```

En el siguiente ejemplo se muestra que la imagen 2 del sistema (ONTAP 9.0.0) es la versión predeterminada y actual en node_A_1:

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image   Default Current Version  Date
-------- ------- ------- ------- -------- -------------------
node_B_1
         image1  false   false    X.X.X   MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y   MM/DD/YYYY TIME
node_B_2
         image1  false   true     X.X.X   MM/DD/YYYY TIME
         image2  true    false    Y.Y.Y   MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

Actualizar la segunda pareja de recuperación ante desastres en un grupo de recuperación ante desastres de MetroCluster

Debe realizar una toma de control y una devolución del nodo en el orden correcto para que la nueva versión de ONTAP sea la versión actual del nodo.

Debe haber actualizado el primer par DR (node_A_1 y node_B_1).

En esta tarea, se actualizan NODE_A_2 y NODE_B_2.

Si ha actualizado el software ONTAP en el primer grupo de recuperación ante desastres y ahora está actualizando el segundo grupo de recuperación ante desastres en una configuración MetroCluster de ocho nodos, en esta tarea está actualizando NODE_A_4 y NODE_B_4.

1. Migre todos los LIF de datos del nodo:

```
network interface migrate-all -node nodenameA
```

2. Inicie la toma de control del nodo de destino en cluster_A:

   No especifique el parámetro -option Immediate porque se requiere una toma de control normal para los nodos que se van a realizar la operación para arrancar en la nueva imagen de software.

   a. Asuma el control del partner de recuperación ante desastres en cluster_A:

   ```
   storage failover takeover -ofnode node_A_2 -option allow-version-
   mismatch
   ```

   > La `allow-version-mismatch` Esta opción no es necesaria para las actualizaciones de ONTAP 9.0 a ONTAP 9.1 o para cualquier actualización de parches.

   El nodo arranca con el estado "esperando la devolución".

   Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que los nodos no tienen quórum de clúster. Puede ignorar esta notificación y continuar con la actualización.

   b. Compruebe que la toma de control se ha realizado correctamente:

   ```
   storage failover show
   ```

   El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo_A_2 está en el estado "esperando devolución" y el nodo_A_1 está en el estado "durante toma de control".

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
------------------------------------
node_A_1       node_A_2       false    In takeover
node_A_2       node_A_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

3. Inicie la toma de control del nodo de destino en cluster_B:

   No especifique el parámetro -option Immediate porque se requiere una toma de control normal para los

nodos que se van a realizar la operación para arrancar en la nueva imagen de software.

a. Asumir el control del partner de recuperación ante desastres en cluster_B (nodo_B_2):

Si va a actualizar desde…	Introduzca este comando…
ONTAP 9.2 o ONTAP 9.1	`storage failover takeover -ofnode node_B_2`
ONTAP 9.0 o Data ONTAP 8.3.x	`storage failover takeover -ofnode node_B_2 -option allow-version-mismatch` La `allow-version-mismatch` Esta opción no es necesaria para las actualizaciones de ONTAP 9.0 a ONTAP 9.1 o para cualquier actualización de parches.

El nodo arranca con el estado "esperando la devolución".

> Si AutoSupport está habilitado, se envía un mensaje de AutoSupport que indica que los nodos están fuera del quórum del clúster. Puede ignorar con toda tranquilidad esta notificación y continuar con la actualización.

b. Compruebe que la toma de control se ha realizado correctamente:

```
storage failover show
```

El siguiente ejemplo muestra que la toma de control se ha realizado correctamente. El nodo B_2 está en el estado "esperando devolución" y el nodo B_1 está en el estado "durante toma de control".

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
------------------------------------
node_B_1       node_B_2       false    In takeover
node_B_2       node_B_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

4. Espere al menos ocho minutos para asegurarse de las siguientes condiciones:

- La multivía del cliente (si está implementada) se estabiliza.
- Los clientes se recuperan de la pausa en la I/o que se produce durante la toma de control.

  El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos en función de las características de las aplicaciones cliente.

5. Devuelva los agregados a los nodos de destino:

   Después de actualizar la configuración IP de MetroCluster a ONTAP 9.5, los agregados estarán en estado degradado durante un breve periodo de tiempo antes de volver a sincronizar y a un estado reflejado.

   a. Proporcione los agregados al partner de recuperación ante desastres en cluster_A:

   ```
   storage failover giveback –ofnode node_A_2
   ```

   b. Proporcione los agregados al partner de recuperación ante desastres en cluster_B:

   ```
   storage failover giveback –ofnode node_B_2
   ```

   La operación de devolución devuelve primero el agregado raíz al nodo y, después de que el nodo haya terminado de arrancarse, devuelve los agregados que no son raíz.

6. Compruebe que todos los agregados se han devuelto emitiendo el siguiente comando en ambos clústeres:

   ```
   storage failover show-giveback
   ```

   Si el campo Estado de devolución indica que no hay agregados que devolver, se devolverán todos los agregados. Si se vetó la devolución, el comando muestra el progreso de devolución y qué subsistema vetó la devolución.

7. Si no se ha devuelto ningún agregado, realice lo siguiente:
   a. Revise la solución de veto para determinar si desea abordar la condición "vertical" o anular el veto.
   b. Si es necesario, tratar la condición "verto" descrita en el mensaje de error, asegurándose de que las operaciones identificadas se cancelen con gracia.
   c. Vuelva a introducir el comando de devolución del nodo de respaldo del almacenamiento.

      Si ha decidido anular la condición "VETE", establezca el parámetro -override-vetoes en TRUE.

8. Espere al menos ocho minutos para asegurarse de las siguientes condiciones:
   - La multivía del cliente (si está implementada) se estabiliza.
   - Los clientes se recuperan de la pausa en la I/o que se produce durante la devolución.

     El tiempo de recuperación es específico del cliente y puede tardar más de ocho minutos en función de las características de las aplicaciones cliente.

9. Establezca el nivel de privilegio de admin en Advanced, introduciendo **y** cuando se le solicite continuar:

```
set -privilege advanced
```

El aviso avanzado (`*>`) aparece.

10. Confirme la versión en cluster_A:

```
system image show
```

El siguiente ejemplo muestra que la imagen 2 del sistema (imagen ONTAP de destino) es la versión predeterminada y actual en node_A_2:

```
cluster_B::*> system image show
                 Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- ---------- -------------------
node_A_1
         image1  false   false    X.X.X     MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y     MM/DD/YYYY TIME
node_A_2
         image1  false   false    X.X.X     MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

11. Confirme la versión en cluster_B:

```
system image show
```

El siguiente ejemplo muestra que System image2 (imagen ONTAP de destino) es la versión predeterminada y actual en NODE_B_2:

```
cluster_B::*> system image show
                 Is      Is                  Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- ---------- -------------------
node_B_1
         image1  false   false    X.X.X     MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y     MM/DD/YYYY TIME
node_B_2
         image1  false   false    X.X.X     MM/DD/YYYY TIME
         image2  true    true     Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

12. Para cada nodo del par de alta disponibilidad, habilite la devolución automática:

```
storage failover modify -node target-node -auto-giveback true
```

Este comando se debe repetir para cada nodo de la pareja de ha.

13. Compruebe que la devolución automática está activada:

```
storage failover show -fields auto-giveback
```

Este ejemplo muestra que se ha habilitado la devolución automática de control en ambos nodos:

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 true
node_x_2 true
2 entries were displayed.
```

Actualización no disruptiva de una configuración de MetroCluster de dos nodos en ONTAP 9,2 o versiones anteriores

La forma en que se actualiza una configuración de MetroCluster de dos nodos varía en función de su versión de ONTAP. Si ejecuta ONTAP 9,2 o una versión anterior, debe usar este procedimiento para realizar una actualización manual no disruptiva que incluya iniciar una conmutación de sitios negociada, actualizar el clúster en el sitio ««fallido»», iniciar una conmutación de retorno y, a continuación, repetir el proceso en el clúster en el otro sitio.

Si tiene una configuración MetroCluster de dos nodos que ejecute ONTAP 9,3 o una versión posterior, ejecute

un Actualización automatizada mediante System Manager.

Pasos

1. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar:

```
set -privilege advanced
```

   El aviso avanzado (`*>`) aparece.

2. En el clúster que se va a actualizar, instale la nueva imagen de software ONTAP como predeterminada:

```
system node image update -package package_location -setdefault true
-replace-package true
```

```
cluster_B::*> system node image update -package
http://www.example.com/NewImage.tgz -setdefault true -replace-package
true
```

3. Compruebe que la imagen del software de destino está definida como la imagen predeterminada:

```
system node image show
```

   El siguiente ejemplo muestra eso `NewImage` se establece como la imagen predeterminada:

```
cluster_B::*> system node image show
                    Is      Is                           Install
Node     Image      Default Current Version              Date
-------- -------    ------- ------- --------------------
-------------------
node_B_1
         OldImage  false   true    X.X.X                MM/DD/YYYY TIME
         NewImage  true    false   Y.Y.Y                MM/DD/YYYY TIME
2 entries were displayed.
```

4. Si la imagen del software de destino no está definida como la imagen predeterminada, cámbiela:

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. Compruebe que todas las SVM del clúster tengan un estado de estado:

```
metrocluster vserver show
```

6. En el clúster que no se está actualizando, inicie una conmutación de sitios negociada:

```
metrocluster switchover
```

La operación puede llevar varios minutos. Puede usar el comando MetroCluster operation show para verificar que la conmutación se ha completado.

En el siguiente ejemplo, se realiza una conmutación negociada en el clúster remoto ("cluster_A'"). Esto hace que el clúster local ("'cluster_B") se detenga para que pueda actualizarlo.

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
         Vservers on cluster "cluster_B" and
         automatically re-start them on cluster
         "cluster_A". It will finally gracefully shutdown
         cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. Compruebe que todas las SVM del clúster tengan un estado de estado:

```
metrocluster vserver show
```

8. Resincronizar los agregados de datos en el clúster de «eurviving»:

```
metrocluster heal -phase aggregates
```

Después de actualizar la configuración IP de MetroCluster a ONTAP 9.5 o una versión posterior, los agregados estarán en estado degradado durante un breve periodo de tiempo antes de volver a sincronizar y volver a un estado de reflejo.

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. Compruebe que la operación de reparación se ha realizado correctamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. Resincronice los agregados raíz en el clúster «esencial»:

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. Compruebe que la operación de reparación se ha realizado correctamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. En el clúster detenido, arranque el nodo desde el símbolo del sistema del CARGADOR:

```
boot_ontap
```

13. Espere a que termine el proceso de arranque y, a continuación, compruebe que todas las SVM del clúster estén en estado:

```
metrocluster vserver show
```

14. Haga una regreso desde el cluster «de la revolución»:

```
metrocluster switchback
```

15. Compruebe que la conmutación de estado se ha completado correctamente:

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. Compruebe que todas las SVM del clúster tengan un estado de estado:

```
metrocluster vserver show
```

17. Repita todos los pasos anteriores en el otro clúster.
18. Compruebe que la configuración de MetroCluster sea correcta:
    a. Compruebe la configuración:

    ```
    metrocluster check run
    ```

    ```
    cluster_A::> metrocluster check run
    Last Checked On: MM/DD/YYYY TIME
    Component           Result
    ------------------- ---------
    nodes               ok
    lifs                ok
    config-replication  ok
    aggregates          ok
    4 entries were displayed.

    Command completed. Use the "metrocluster check show -instance"
    command or sub-commands in "metrocluster check" directory for
    detailed results.
    To check if the nodes are ready to do a switchover or switchback
    operation, run "metrocluster switchover -simulate" or "metrocluster
    switchback -simulate", respectively.
    ```

    b. Si desea ver resultados más detallados, utilice el comando MetroCluster check run:

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

c. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

d. Simule la operación switchover:

```
metrocluster switchover -simulate
```

e. Revise los resultados de la simulación de switchover:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
    Operation: switchover
        State: successful
   Start time: MM/DD/YYYY TIME
     End time: MM/DD/YYYY TIME
       Errors: -
```

f. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

g. Repita estos mismos pasos en el otro clúster.

Después de terminar

Realice cualquier "tareas posteriores a la actualización".

Información relacionada

"Recuperación ante desastres de MetroCluster"

Actualización manual disruptiva de ONTAP mediante la interfaz de línea de comandos

Si puede desconectar el clúster para actualizar a una nueva versión de ONTAP, puede utilizar el método de actualización disruptiva. Este método tiene varios pasos: Deshabilitar la conmutación por error de almacenamiento para cada pareja de alta disponibilidad, reiniciar cada nodo del clúster y, a continuación, volver a habilitar la conmutación por error del almacenamiento.

- Debe "descargue" y.. "instale" la imagen de software.
- Si opera en un entorno SAN, todos los clientes SAN deben cerrarse o suspenderse hasta que se complete la actualización.

  Si los clientes SAN no se apagan o suspenden antes de una actualización disruptiva , los sistemas de archivos cliente y las aplicaciones sufren errores que pueden requerir recuperación manual una vez completada la actualización.

En una actualización disruptiva, se requiere un tiempo de inactividad porque la conmutación por error de almacenamiento está deshabilitada para cada par de alta disponibilidad y se actualiza cada nodo. Cuando se deshabilita la conmutación al respaldo de almacenamiento, cada nodo se comporta como un clúster de un solo nodo; es decir, los servicios del sistema asociados con el nodo se interrumpen mientras se tarda en reiniciar el sistema.

Pasos

1. Establezca el nivel de privilegio de admin en Advanced, introduciendo **y** cuando se le solicite continuar:

   ```
   set -privilege advanced
   ```

   El aviso avanzado (`*>`) aparece.

2. Establezca la nueva imagen del software ONTAP como la imagen predeterminada:

   ```
   system image modify {-node * -iscurrent false} -isdefault true
   ```

   Este comando utiliza una consulta ampliada para cambiar la imagen de software de ONTAP de destino (que se instala como imagen alternativa) y que sea la imagen predeterminada de cada nodo.

3. Compruebe que la nueva imagen del software ONTAP está configurada como la imagen predeterminada:

   ```
   system image show
   ```

   En el ejemplo siguiente, la imagen 2 es la nueva versión de ONTAP y se establece como la imagen predeterminada en ambos nodos:

```
cluster1::*> system image show
                  Is      Is                 Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------- -------------------
node0
         image1  false   true    X.X.X     MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1  false   true    X.X.X     MM/DD/YYYY TIME
         image2  true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

4. Realice uno de los siguientes pasos:

Si el clúster consta de…	Realice lo siguiente…
Un nodo	Continúe con el próximo paso.

Dos nodos	a. Deshabilite alta disponibilidad del clúster:
	`cluster ha modify -configured false`
	Introduzca `y` para continuar cuando se le solicite.
	b. Desactive la conmutación por error del almacenamiento para el par de alta disponibilidad:
	`storage failover modify -node * -enabled false`

Más de dos nodos	Deshabilite la recuperación tras fallos del almacenamiento para cada pareja de alta disponibilidad del clúster: `storage failover modify -node * -enabled false`

5. Reiniciar un nodo en el clúster:

```
system node reboot -node nodename -ignore-quorum-warnings
```

No reinicie más de un nodo a la vez.

El nodo arranca la nueva imagen de ONTAP. Aparece la solicitud de inicio de sesión de ONTAP, que indica que el proceso de reinicio ha finalizado.

6. Después de que el nodo o el conjunto de nodos se haya reiniciado con la nueva imagen ONTAP, establezca el nivel de privilegio en AVANZADO:

```
set -privilege advanced
```

Introduzca **y** cuando se le solicite continuar

7. Confirme que el nuevo software se está ejecutando:

```
system node image show
```

En el siguiente ejemplo, image1 es la nueva versión de ONTAP y se establece como la versión actual del nodo 0:

```
cluster1::*> system node image show
                 Is      Is                  Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------   -------------------
node0
         image1  true    true    X.X.X       MM/DD/YYYY TIME
         image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
node1
         image1  true    false   X.X.X      MM/DD/YYYY TIME
         image2  false   true    Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.
```

8. Compruebe que la actualización se haya realizado correctamente:

   a. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

   b. Compruebe que el estado de la actualización se haya completado para cada nodo:

   ```
   system node upgrade-revert show -node nodename
   ```

El estado debe aparecer como completo.

Si el estado es no completo, "Comuníquese con el soporte de NetApp" inmediatamente.

a. Vuelva al nivel de privilegio de administrador:

```
set -privilege admin
```

9. Repita los pasos 2 a 8 en cada nodo adicional.
10. Si el clúster consta de dos o más nodos, habilite la conmutación por error del almacenamiento para cada pareja de alta disponibilidad del clúster:

```
storage failover modify -node * -enabled true
```

11. Si el clúster consta de solo dos nodos, habilite la alta disponibilidad de los clústeres:

```
cluster ha modify -configured true
```

Qué hacer después de una actualización de ONTAP

Qué hacer después de una actualización de ONTAP

Después de actualizar ONTAP, hay varias tareas que debe realizar para verificar la disponibilidad del clúster.

1. "Compruebe el clúster".

   Después de actualizar ONTAP, debe comprobar la versión del clúster, el estado del clúster y el estado del almacenamiento. Si utiliza una configuración de MetroCluster FC, también debe verificar que el clúster esté habilitado para la conmutación automática no planificada.

2. "Compruebe que todas las LIF se encuentran en los puertos domésticos".

   Durante un reinicio, es posible que algunas LIF se hayan migrado a sus puertos de conmutación al respaldo asignados. Tras actualizar un clúster, debe habilitar y revertir cualquier LIF que no esté en sus puertos de inicio.

3. Verificación "consideraciones especiales" específicas de su clúster.

   Si existen ciertas configuraciones en el clúster, es posible que deba realizar pasos adicionales después de actualizar.

4. "Actualización del paquete de cualificación de disco (DQP)".

   El DQP no se actualiza como parte de una actualización de ONTAP.

Compruebe el clúster después de actualizar ONTAP

Después de actualizar ONTAP, compruebe la versión del clúster, el estado del clúster y el estado del almacenamiento. Para configuraciones de FC de MetroCluster, compruebe también que el clúster esté habilitado para la conmutación de sitios automática no planificada.

Comprobar la versión del clúster

Una vez que se hayan actualizado todos los pares de HA, debe usar el comando version para verificar que todos los nodos estén ejecutando la versión de destino.

La versión del clúster es la versión más baja de ONTAP que se ejecuta en cualquier nodo del clúster. Si la versión del clúster no es la versión de ONTAP de destino, puede actualizar el clúster.

1. Compruebe que la versión del clúster es la versión de ONTAP de destino:

```
version
```

2. Si la versión del clúster no es la versión de ONTAP de destino, debe comprobar el estado de actualización de todos los nodos:

```
system node upgrade-revert show
```

Compruebe el estado del clúster

Después de actualizar un clúster, debe comprobar que los nodos estén en buen estado y que sean elegibles para participar en el clúster, y que el clúster esté en quórum.

1. Compruebe que los nodos del clúster estén en línea y que puedan participar en el clúster:

```
cluster show
```

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

   Si alguno de los nodos no es saludable o no apto, compruebe los registros de EMS en busca de errores y realice acciones correctivas.

2. Configure el nivel de privilegio en Advanced:

```
set -privilege advanced
```

3. Verifique los detalles de configuración de cada proceso RDB.
   - Las épocas de la base de datos relacional y la base de datos deben coincidir para cada nodo.
   - El maestro de quórum por anillo debe ser el mismo para todos los nodos.

     Tenga en cuenta que cada anillo puede tener un maestro de quórum diferente.

Para mostrar este proceso RDB:	Introduzca este comando…
Aplicación de gestión	`cluster ring show -unitname mgmt`
Base de datos de ubicación del volumen	`cluster ring show -unitname vldb`
Administrador de interfaz virtual	`cluster ring show -unitname vifmgr`
Daemon de gestión de SAN	`cluster ring show -unitname bcomd`

     Este ejemplo muestra el proceso de la base de datos de ubicación del volumen:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Si va a trabajar en un entorno SAN, compruebe que cada nodo se encuentra en quórum DE SAN:

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master            Cluster           Quorum        Availability
Operational
Node              Node              Status        Status        Status
----------------- ----------------- ------------- -------------
-------------
cluster1-01       cluster1-01       in-quorum     true
operational
                  cluster1-02       in-quorum     true
operational
2 entries were displayed.
```

Información relacionada

"Administración del sistema"

Verifique que la conmutación de sitios automática no planificada está habilitada (solo configuraciones de MetroCluster FC).

Si el clúster está en una configuración de MetroCluster FC, debe verificar que la conmutación automática no planificada esté habilitada después de actualizar ONTAP.

Si está utilizando una configuración IP de MetroCluster, omita este procedimiento.

Pasos

1. Compruebe si la conmutación automática no planificada está habilitada:

   ```
   metrocluster show
   ```

   Si la conmutación automática no planificada está habilitada, aparecerá la siguiente instrucción en el resultado del comando:

   ```
   AUSO Failure Domain  auso-on-cluster-disaster
   ```

2. Si la sentencia no aparece, active una conmutación automática no planificada:

   ```
   metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
   disaster
   ```

3. Compruebe que se ha activado un switchover no planificado automático:

   ```
   metrocluster show
   ```

Información relacionada

"Gestión de discos y agregados"

Verifique que todos los LIFS están en los puertos de inicio después de la actualización de ONTAP

Durante el reinicio que se produce como parte del proceso de actualización de ONTAP, es posible que algunas LIF se migren de sus puertos principales a los puertos de conmutación al nodo de respaldo asignados. Después de una actualización, debe activar y revertir los LIF que no estén en sus puertos principales.

Pasos

1. Mostrar el estado de todas las LIF:

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

   Si **Status Admin** está “caído” o **is home** es “falso” para cualquier LIF, continúe con el siguiente paso.

2. Habilite las LIF de datos:

   ```
   network interface modify {-role data} -status-admin up
   ```

3. Revertir los LIF a sus puertos raíz:

   ```
   network interface revert *
   ```

4. Compruebe que todas las LIF se encuentran en sus puertos de inicio:

   ```
   network interface show
   ```

   Este ejemplo muestra que todas las LIF para SVM vs0 están en sus puertos iniciales.

```
cluster1::> network interface show -vserver vs0
         Logical    Status     Network          Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask     Node     Port    Home
-------- ---------- ---------- --------------- -------- ------- ----
vs0
         data001    up/up      192.0.2.120/24  node0    e0e     true
         data002    up/up      192.0.2.121/24  node0    e0f     true
         data003    up/up      192.0.2.122/24  node0    e2a     true
         data004    up/up      192.0.2.123/24  node0    e2b     true
         data005    up/up      192.0.2.124/24  node1    e0e     true
         data006    up/up      192.0.2.125/24  node1    e0f     true
         data007    up/up      192.0.2.126/24  node1    e2a     true
         data008    up/up      192.0.2.127/24  node1    e2b     true
8 entries were displayed.
```

Configuraciones especiales

Consideraciones especiales tras una actualización de ONTAP

Si se configura el clúster con alguna de las siguientes funciones, es posible que deba realizar pasos adicionales después de actualizar el software ONTAP.

Pregúntese…	Si su respuesta es sí, entonces haga esto…
¿He actualizado desde ONTAP 9,7 o anterior a ONTAP 9,8 o posterior?	Compruebe la configuración de red Quite el servicio LIF EMS de las políticas de servicio de red que no proporcionan accesibilidad al destino EMS
¿Mi clúster está en una configuración MetroCluster?	Compruebe el estado de las redes y el almacenamiento
¿Tengo una configuración SAN?	Compruebe su configuración SAN
¿Actualizo desde ONTAP 9,3 o anterior? ¿Utilizo el cifrado del almacenamiento de NetApp?	Volver a configurar las conexiones del servidor KMIP
¿Tengo reflejos de uso compartido de carga?	Reubicar los volúmenes de origen de reflejos de uso compartido de carga movidos
¿Tengo cuentas de usuario para el acceso al procesador de servicio (SP) que se hayan creado antes de ONTAP 9,9.1?	Compruebe el cambio en las cuentas que pueden acceder a Service Processor

Verifique la configuración de red después de una actualización de ONTAP desde ONTAP 9,7x o una versión anterior

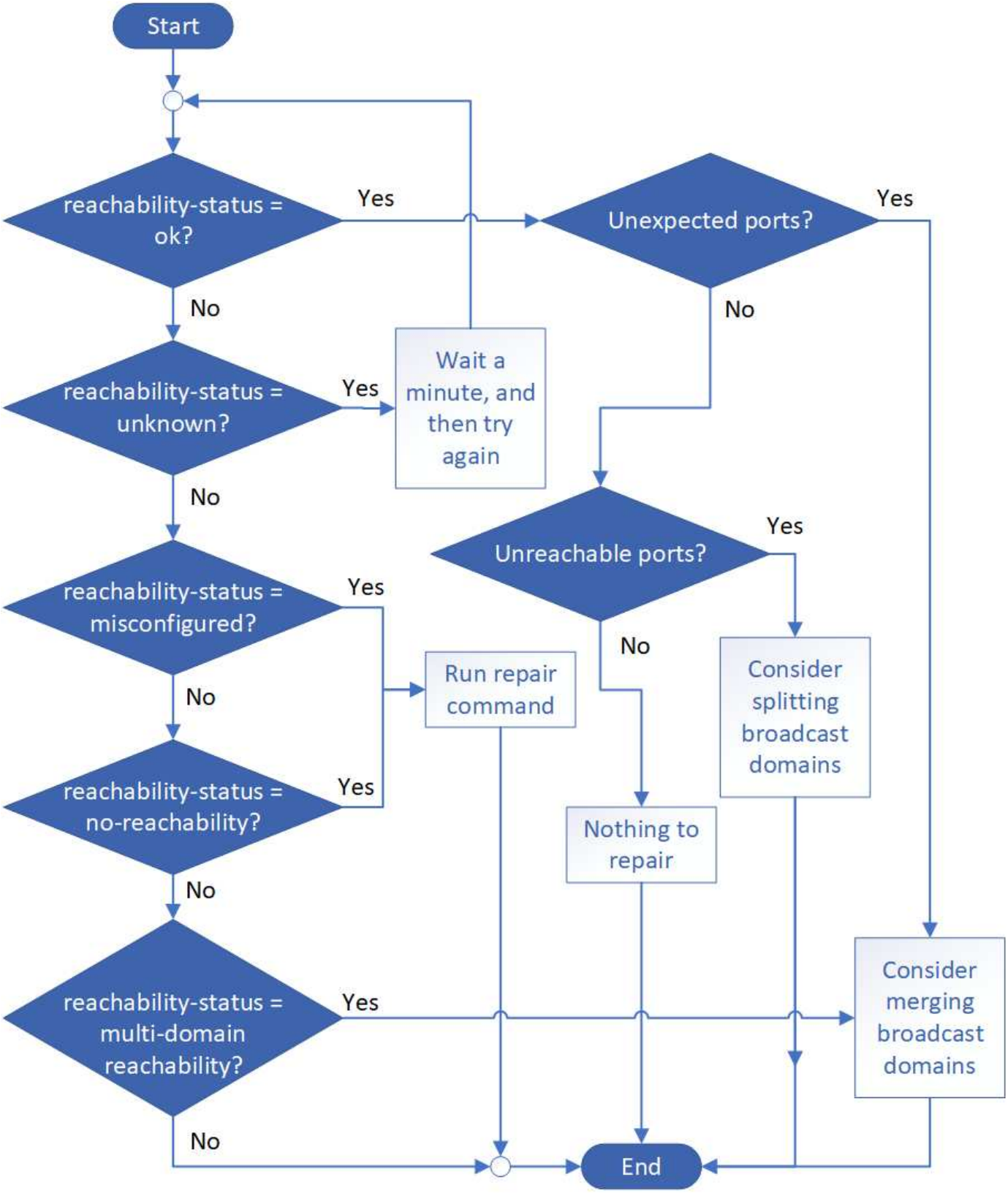
Después de realizar una actualización desde ONTAP 9,7x o anterior a ONTAP 9,8 o posterior, debe verificar la configuración de red. Después de la actualización, ONTAP supervisa automáticamente la accesibilidad de la capa 2.

Paso

1. Compruebe que cada puerto tiene accesibilidad al dominio de retransmisión esperado:

```
network port reachability show -detail
```

El resultado del comando contiene resultados de accesibilidad. Use el árbol de decisión y la tabla siguientes para comprender los resultados de la accesibilidad (estado de la accesibilidad) y determinar qué hacer, si es que hay algo, a continuación.



accesibilidad-estado	Descripción

de acuerdo	El puerto tiene capacidad de acceso de capa 2 a su dominio de difusión asignado. Si el reachability-status es "ok", pero hay "puertos inesperados", considere combinar uno o más dominios de difusión. Para obtener más información, consulte "Fusionar dominios de retransmisión". Si el reachability-status es "ok", pero hay "puertos inaccesibles", considere dividir uno o más dominios de difusión. Para obtener más información, consulte "Divida los dominios de retransmisión". Si el estado de accesibilidad es "correcto" y no hay puertos inesperados o no accesibles, la configuración es correcta.
función mal configurada	El puerto no tiene posibilidad de recurrir a la capa 2 a su dominio de difusión asignado; sin embargo, el puerto tiene capacidad de acceso de capa 2 a un dominio de difusión diferente. Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto al dominio de retransmisión al que se le habrá accesibilidad: `network port reachability repair -node -port` Para obtener más información, consulte "Reparar la accesibilidad del puerto".
ausencia de accesibilidad	El puerto no tiene posibilidad de recurrir a ningún dominio de difusión existente de capa 2. Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto a un dominio de retransmisión creado automáticamente en el espacio IP predeterminado: `network port reachability repair -node -port` Para obtener más información, consulte "Reparar la accesibilidad del puerto".
accesibilidad multi-dominio	El puerto tiene la habilidad de la capa 2 para su dominio de broadcast asignado; sin embargo, también tiene la habilidad de la capa 2 para al menos otro dominio de broadcast. Examine la configuración física del conmutador y la conectividad para determinar si es incorrecta o si el dominio de difusión asignado al puerto necesita combinarse con uno o más dominios de difusión. Para obtener más información, consulte "Fusionar dominios de retransmisión" o. "Reparar la accesibilidad del puerto".
desconocido	Si el estado de accesibilidad es "desconocido", espere unos minutos y vuelva a intentar el comando.

Después de reparar un puerto, necesita comprobar y resolver las LIF y VLAN desplazadas. Si el puerto era parte de un grupo de interfaces, también necesita comprender lo que ha sucedido con ese grupo de

interfaces. Para obtener más información, consulte "Reparar la accesibilidad del puerto".

Quite el servicio LIF de EMS de las políticas de servicio de red

Si tiene mensajes del sistema de gestión de eventos (EMS) configurados antes de actualizar de ONTAP 9.7 o anterior a ONTAP 9.8 o posterior , después de la actualización, es posible que los mensajes de EMS no se envíen.

Durante la actualización, Management-ems, que es el servicio LIF de EMS, se agrega a todas las políticas de servicio existentes. Esto permite enviar mensajes de EMS desde cualquiera de las LIF asociadas con cualquiera de las políticas de servicio. Si la LIF seleccionada no tiene accesibilidad al destino de notificaciones de eventos, el mensaje no se entrega.

Para evitar esto, después de la actualización, debe eliminar el servicio LIF de EMS de las políticas de servicio de red que no proporcionan accesibilidad al destino.

Pasos

1. Identificar las LIF y las políticas de servicio de red asociadas mediante las cuales se pueden enviar mensajes de EMS:

```
network interface show -fields service-policy -services management-ems
```

```
vserver        lif            service-policy
-------------- ------------ ------------------
cluster-1      cluster_mgmt
                                     default-management
cluster-1      node1-mgmt
                                     default-management
cluster-1      node2-mgmt
                                     default-management
cluster-1      inter_cluster
                                     default-intercluster
4 entries were displayed.
```

2. Compruebe cada LIF para obtener conectividad con el destino EMS:

```
network ping -lif lif_name -vserver svm_name -destination
destination_address
```

Realice esto en cada nodo.

Ejemplos

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. Introduzca el nivel de privilegio avanzado:

```
set advanced
```

4. Para los LIF que no tienen habilidad, quite el servicio LIF Management-ems de las políticas de servicio correspondientes:

```
network interface service-policy remove-service -vserver svm_name
-policy service_policy_name -service management-ems
```

5. Compruebe que el LIF de ems de gestión solo esté asociado a las LIF que proporcionan accesibilidad al destino de EMS:

```
network interface show -fields service-policy -services management-ems
```

Enlaces relacionados

"LIF y políticas de servicio en ONTAP 9.6 y posteriores"

Comprobar el estado de redes y almacenamiento de las configuraciones de MetroCluster tras una actualización de ONTAP

Después de actualizar un clúster de ONTAP en una configuración de MetroCluster, debe comprobar el estado de las LIF, los agregados y los volúmenes de cada clúster.

1. Compruebe el estado de la LIF:

```
network interface show
```

En un funcionamiento normal, los LIF de las SVM de origen deben tener el estado de administrador de en activo y estar ubicados en sus nodos raíz. Los LIF para las SVM de destino no necesitan estar en marcha o ubicados en sus nodos iniciales. Sin embargo, todos los LIF tienen el estado de administrador activo, pero no es necesario que estén ubicados en sus nodos iniciales.

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
                         up/up    192.0.2.1/24       cluster1-01
                                                                   e2a
true
            cluster1-a1_clus2
                         up/up    192.0.2.2/24       cluster1-01
                                                                   e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                   e3a
true
            cluster1-a1_inet4_intercluster1
                         up/up    198.51.100.2/24    cluster1-01
                                                                   e3c
true
            ...

27 entries were displayed.
```

2. Compruebe el estado de los agregados:

```
storage aggregate show -state !online
```

Este comando muestra todos los agregados que *not* están en línea. En el funcionamiento normal, todos los agregados ubicados en el sitio local deben estar en línea. Sin embargo, si la configuración de MetroCluster está de conmutación, los agregados raíz del sitio de recuperación ante desastres pueden estar sin conexión.

Este ejemplo muestra un clúster en funcionamiento normal:

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

Este ejemplo muestra un clúster con conmutación de sitios, en el que los agregados raíz del sitio de recuperación ante desastres están sin conexión:

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
                0B        0B    0% offline      0 cluster2-01
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

3. Compruebe el estado de los volúmenes:

```
volume show -state !online
```

Este comando muestra los volúmenes que *not* están en línea.

Si la configuración de MetroCluster tiene un funcionamiento normal (no está en estado de conmutación por sitios), el resultado debe mostrar todos los volúmenes que pertenecen a las SVM secundarias del clúster (los que tienen el nombre de SVM anexado con "-mc").

Esos volúmenes solo entran en línea en caso de que se produzca un cambio.

Este ejemplo muestra un clúster con un funcionamiento normal, en el cual los volúmenes del sitio de recuperación ante desastres no están en línea.

```
cluster1::> volume show -state !online
  (volume show)
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2-mc    vol1         aggr1_b1     -          RW            -
-     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -
-     -
vs2-mc    vol2         aggr1_b1     -          RW            -
-     -
vs2-mc    vol3         aggr1_b1     -          RW            -
-     -
vs2-mc    vol4         aggr1_b1     -          RW            -
-     -
5 entries were displayed.
```

4. Compruebe que no haya volúmenes incoherentes:

```
volume show -is-inconsistent true
```

Consulte el artículo de la base de conocimientos "Volumen que muestra una incoherencia de WAFL" sobre la forma de abordar los volúmenes incoherentes.

Comprobar la configuración DE SAN tras una actualización

Tras una actualización de ONTAP, en un entorno SAN, debe verificar que cada iniciador que esté conectado a una LIF antes de que la actualización se haya reconectado correctamente a la LIF.

1. Compruebe que cada iniciador está conectado a la LIF correcta.

   Debe comparar la lista de iniciadores con la lista que ha realizado durante la preparación de la actualización.

Durante…	Introduzca…
ISCSI	`iscsi initiator show -fields igroup,initiator-name,tpgroup`

Durante…	Introduzca…
FC	`fcp initiator show -fields igroup,wwpn,lif`

Vuelva a configurar las conexiones del servidor KMIP después de una actualización de ONTAP 9,2 o una versión anterior

Después de realizar la actualización desde ONTAP 9,2 o una versión anterior a ONTAP 9,3 o una versión posterior, debe volver a configurar todas las conexiones del servidor de gestión de claves externa (KMIP).

Pasos

1. Configure la conectividad del gestor de claves:

```
security key-manager setup
```

2. Añada sus servidores KMIP:

```
security key-manager add -address key_management_server_ip_address
```

3. Compruebe que los servidores KMIP están conectados:

```
security key-manager show -status
```

4. Consulte los servidores de claves:

```
security key-manager query
```

5. Cree una nueva clave de autenticación y contraseña:

```
security key-manager create-key -prompt-for-key true
```

   La frase de contraseña debe tener un mínimo de 32 caracteres.

6. Consulte la nueva clave de autenticación:

```
security key-manager query
```

7. Asigne la nueva clave de autenticación a sus discos de cifrado automático (SED):

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

Asegúrese de que está utilizando la nueva clave de autenticación de su consulta.

8. Si es necesario, asigne una clave FIPS al SED:

```
storage encryption disk modify -disk disk_id -fips-key-id
fips_authentication_key_id
```

Si la configuración de seguridad requiere el uso de claves diferentes para la autenticación de datos y la autenticación FIPS 140-2-2, debe crear una clave independiente para cada una. Si no es así, puede usar la misma clave de autenticación para el cumplimiento de FIPS que se usa para acceder a los datos.

Reubicar volúmenes de origen de reflejos de uso compartido de carga movidos después de una actualización de ONTAP

Después de actualizar ONTAP, tiene que mover los volúmenes de origen de reflejos de uso compartido de carga nuevamente a sus ubicaciones previas a la actualización.

Pasos

1. Identifique la ubicación a la que se va a mover el volumen de origen de reflejos de uso compartido de carga mediante el registro creado antes de mover el volumen de origen de reflejos de uso compartido de carga.
2. Mueva el volumen de origen de reflejos de uso compartido de carga de vuelta a su ubicación original:

```
volume move start
```

Cambio en las cuentas de usuario que pueden acceder a Service Processor

Si ha creado cuentas de usuario en ONTAP 9,8 o una versión anterior que pueden acceder al procesador de servicio (SP) con un rol no de administrador y actualiza a ONTAP 9.9.1 o una versión posterior, cualquier valor que no sea administrador en la `-role` el parámetro se modifica a. `admin`.

Para obtener más información, consulte "Cuentas que pueden acceder al SP".

Actualice el paquete de cualificación de disco

Después de actualizar el software de ONTAP, debe descargar e instalar el paquete de cualificación de disco de ONTAP (DQP). El DQP no se actualiza como parte de una actualización de ONTAP.

El DQP contiene los parámetros adecuados para la interacción ONTAP con todas las unidades recién cualificadas. Si su versión del DQP no contiene información para una unidad recién cualificada, ONTAP no tendrá la información necesaria para configurar correctamente la unidad.

Se recomienda actualizar el DQP cada trimestre. También debe actualizar el DQP por los siguientes motivos:

- Siempre que se añada un nuevo tipo o tamaño de unidad a un nodo del clúster

  Por ejemplo, si ya tiene unidades de 1 TB y añade unidades de 2 TB, debe comprobar la actualización más reciente del DQP.

- Cada vez que se actualiza el firmware de disco
- Siempre que estén disponibles los archivos DQP o firmware de disco más nuevos

Información relacionada

- "Descargas de NetApp: Paquete de cualificación de disco"
- "Descargas de NetApp: Firmware de la unidad de disco"

Firmware y actualizaciones del sistema

Descripción general de las actualizaciones del sistema y el firmware

En función de la versión de ONTAP, puede habilitar el firmware automático y las actualizaciones del sistema.

Versión de ONTAP	Lo que se incluye en las actualizaciones automáticas
9.13.1 y posterior	• Base de datos de zona horaria de ONTAP • Firmware de almacenamiento para dispositivos de almacenamiento, discos y bandejas de discos • Firmware del SP/BMC para los procesadores de servicio y los módulos BMC
9.10.1 y posterior	• Firmware de almacenamiento para dispositivos de almacenamiento, discos y bandejas de discos • Firmware del SP/BMC para los procesadores de servicio y los módulos BMC
9.9.1 y anteriores	No admitido

Si ejecuta ONTAP 9.9.1 o una versión anterior, o si no tiene "actualizaciones automáticas del sistema" habilitado, puede "realice las actualizaciones de firmware manualmente".

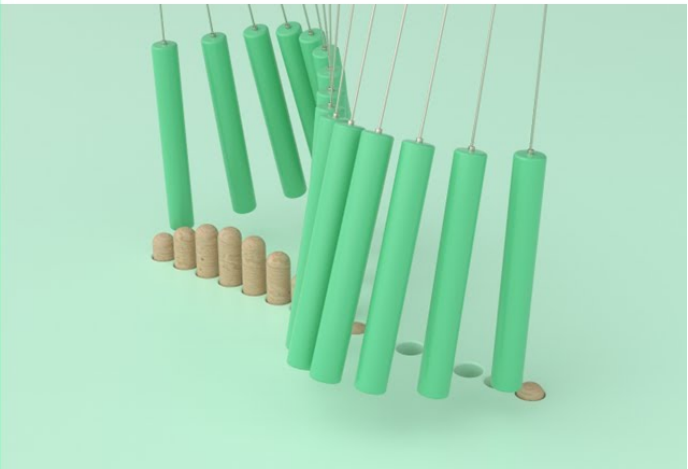
Si ejecuta ONTAP 9.12.1 o una versión anterior, o si no tiene "actualizaciones automáticas del sistema" Activado, puede actualizar la base de datos de zona horaria manualmente. Consulte el artículo de la base de conocimientos, "Cómo actualizar la información de zona horaria en ONTAP 9", para más detalles.

Vídeo: Función de actualización automática del firmware

Echa un vistazo a la función de actualización automática de firmware disponible a partir de ONTAP 9.10.1.

Automatic Firmware Update feature is available starting in ONTAP 9.10.1

By Jim Svesnik,
Quality Assurance Engineer



Cómo se programan las actualizaciones automáticas para la instalación

Todos los nodos elegibles del mismo clúster se agrupan para realizar actualizaciones automáticas. El plazo en el que se programan los nodos elegibles para la actualización automática varía en función del nivel de prioridad de la actualización y el porcentaje de sistemas del entorno que requieren la actualización.

Por ejemplo, si el 10% o menos de su total de sistemas son elegibles para una actualización sin prioridad, la actualización está programada para todos los sistemas elegibles dentro de 1 semana. Sin embargo, si el 76 % o más de sus sistemas totales pueden optar a una actualización sin prioridad, la actualización se escalonará en los sistemas aptos durante 8 semanas. Esta instalación escalonada ayuda a mitigar los riesgos de su entorno general si se produce un problema con una actualización que debe solucionarse.

El porcentaje del total de sistemas programados para actualizaciones automáticas por semana es el siguiente:

Para actualizaciones críticas

% de sistemas que requieren actualización	% de actualizaciones que se producen en la semana 1	% de actualizaciones que se producen en la semana 2
50 % o menos	100 %	
Del 50 al 100 %	30 %	70 %

Para actualizaciones de alta prioridad

% de sistemas que requieren actualización	% de actualizaciones que se producen por semana			
	semana 1	**semana 2**	**semana 3**	**semana 4**
25% o menos	100 %			
26-50%	30 %	70 %		
50-100%	10 %	20 %	30 %	40 %

Para actualizaciones de prioridad normales

% de sistemas que requieren actualización	% de actualizaciones que se producen por semana							
	semana 1	**semana 2**	**semana 3**	**semana 4**	**semana 5**	**semana 6**	**semana 7**	**semana 8**
10% o menos	100 %							
11-20%	30 %	70 %						
21-50%	10 %	20 %	30 %	40 %				
51-75%	5 %	10 %	15 %	20 %	20 %	30 %		
76-100%	5 %	5 %	10 %	10 %	15 %	15 %	20 %	20 %

Active las actualizaciones automáticas

A partir de ONTAP 9.10.1, puede habilitar las actualizaciones automáticas para permitir que ONTAP descargue e instale actualizaciones de firmware sin la intervención del usuario.

A partir de ONTAP 9.13.1, estas actualizaciones automáticas también incluyen actualizaciones automáticas de la base de datos de zona horaria.

Antes de empezar

Debe tener un derecho de soporte vigente. Esto se puede validar en el "Sitio de soporte de NetApp" En la página **Detalles del sistema**.

Acerca de esta tarea

Para habilitar las actualizaciones automáticas, primero debe habilitar AutoSupport con HTTPS. Si AutoSupport no está habilitado en el clúster, o si AutoSupport está habilitado en el clúster con otro protocolo de transporte, tendrá la opción de habilitarla con HTTPS durante este procedimiento.

Pasos

1. En System Manager, haga clic en **Eventos**.
2. En la sección **Overview**, junto a **Enable automatic update**, haz clic en **Actions>Enable**.

3. Si no dispone de AutoSupport con HTTPS habilitado, seleccione para habilitarlo.
4. Acepte los términos y condiciones y seleccione **Guardar**.

Información relacionada

"Solucione problemas de entrega de mensajes de AutoSupport a través de HTTP o HTTPS"

Modificar actualizaciones automáticas

Cuando se habilitan las actualizaciones automáticas, de forma predeterminada, ONTAP detecta, descarga e instala automáticamente todas las actualizaciones de firmware recomendadas y, a partir de ONTAP 9.13.1, las actualizaciones de la base de datos de zona horaria de ONTAP. Si desea ver las actualizaciones recomendadas antes de instalarlas o si desea que las recomendaciones se descarten automáticamente, puede modificar el comportamiento predeterminado según sus preferencias.

Pasos

1. En System Manager, haga clic en **clúster > Configuración**.
2. En la sección **actualización automática**, haga clic en ⋮ para ver una lista de acciones.
3. Haga clic en **Editar configuración de actualización automática**.
4. Especifique las acciones por defecto que se van a realizar para cada tipo de evento.

   Puede elegir actualizar automáticamente, mostrar notificaciones o descartar automáticamente las actualizaciones para cada tipo de evento.

   ⓘ La base de datos de zona horaria de ONTAP está controlada por el tipo de evento de ARCHIVOS DEL SISTEMA.

Administrar las actualizaciones automáticas recomendadas

El registro de actualización automática muestra una lista de recomendaciones de actualización y detalles sobre cada una, incluyendo una descripción, categoría, hora programada para la instalación, estado y cualquier error. Puede ver el log y, a continuación, decidir qué acción desea realizar para cada recomendación.

Pasos

1. Vea la lista de recomendaciones:

Vista desde Configuración del clúster	Vista en la pestaña Actualización de firmware
a. Haga clic en **clúster > Configuración**. b. En la sección **actualización automática**, haga clic en ⋮, A continuación, haga clic en **Ver todas las actualizaciones automáticas**.	a. Haga clic en **Cluster > Overview**. b. En la sección **Descripción general**, haga clic en **más** ⋮, A continuación, haga clic en **actualización de ONTAP**. c. Seleccione la ficha **actualización del firmware**. d. En la ficha **actualización del firmware**, haga clic en **más** ⋮, A continuación, haga clic en **Ver todas las actualizaciones automáticas**.

2. Haga clic en ⋮ junto a la descripción para ver una lista de acciones que puede realizar con la recomendación.

   Se puede realizar una de las siguientes acciones, según el estado de la recomendación:

Si la actualización está en este estado…	Le permite…
No se ha programado	**Actualizar**: Inicia el proceso de actualización. **Programación**: Permite establecer una fecha para iniciar el proceso de actualización. **Descartar**: Elimina la recomendación de la lista.
Se ha programado	**Actualizar**: Inicia el proceso de actualización. **Editar programación**: Le permite modificar la fecha programada para iniciar el proceso de actualización. **Cancelar programa**: Cancela la fecha programada.
Ha sido despedido	**Undismiss**: Devuelve la recomendación a la lista.
Se está aplicando o se está descargando	**Cancelar**: Cancela la actualización.

Actualice el firmware manualmente

A partir de ONTAP 9,9.1, si está registrado con "Active IQ Unified Manager", Puede recibir alertas en System Manager que le informen cuando las actualizaciones de firmware de los dispositivos compatibles, como el disco, las bandejas de discos, el procesador de servicio (SP) o la controladora de gestión de placa base (BMC) están pendientes en el clúster.

Si está ejecutando ONTAP 9,8 o no está registrado en Active IQ Unified Manager, puede ir al sitio de soporte de NetApp para descargar las actualizaciones de firmware.

Antes de empezar

Para prepararse para una actualización de firmware fluida, debe reiniciar el SP o BMC antes de que comience la actualización. Puede utilizar el `system service-processor reboot-sp -node node_name` comando para reiniciar.

Pasos

Siga el procedimiento adecuado basado en su versión de ONTAP y si está registrado en Active IQ Unified Manager.

ONTAP 9.9.1 y versiones posteriores con Active IQ

1. En System Manager, vaya a **Dashboard**.

   En la sección **Estado**, aparece un mensaje si hay alguna actualización de firmware recomendada para el clúster.

2. Haga clic en el mensaje de alerta.

   La ficha **actualización del firmware** se muestra en la página **Actualizar**.

3. Haga clic en **Descarga desde el sitio de soporte de NetApp** para obtener la actualización de firmware que desee realizar.

   Se mostrará el sitio de soporte de NetApp.

4. Inicie sesión en el sitio de soporte de NetApp y descargue el paquete de imagen de firmware necesario para la actualización.
5. Copie los archivos en un servidor HTTP o FTP de la red o en una carpeta local.
6. En System Manager, haga clic en **clúster > Descripción general**.
7. En la esquina derecha del panel **Descripción general**, haga clic en **más** ⋮ Y seleccione **actualización de ONTAP**.
8. Haga clic en **actualización del firmware**.
9. Según la versión de ONTAP, haga lo siguiente:

ONTAP 9.9.1 y 9.10.0	ONTAP 9.10.1 y posteriores
a. Seleccione **desde servidor** o **Cliente local** b. Proporcione la URL del servidor o la ubicación del archivo.	a. En la lista de actualizaciones recomendadas, selecciona **Acciones**. b. Haga clic en **Actualizar** para instalar la actualización inmediatamente o en **Programar** para programarla para más tarde. Si la actualización ya está programada, puedes **Editar** o **Cancelar**. c. Seleccione el botón **Actualizar firmware**.

ONTAP 9,8 y posteriores sin Active IQ

1. Desplácese hasta la "Sitio de soporte de NetApp" e inicie sesión.
2. Seleccione el paquete de firmware que desea utilizar para actualizar el firmware del clúster.
3. Copie los archivos en un servidor HTTP o FTP de la red o en una carpeta local.
4. En System Manager, haga clic en **clúster > Descripción general**.
5. En la esquina derecha del panel **Descripción general**, haga clic en **más** ⋮ Y seleccione **actualización de ONTAP**.
6. Haga clic en **actualización del firmware**.

7. Según la versión de ONTAP, haga lo siguiente:

ONTAP 9,8, 9.9.1 y 9.10.0	ONTAP 9.10.1 y posteriores
1. Seleccione **desde servidor** o **Cliente local** 2. Proporcione la URL del servidor o la ubicación del archivo.	1. En la lista de actualizaciones recomendadas, selecciona **Acciones**. 2. Haga clic en **Actualizar** para instalar la actualización inmediatamente o en **Programar** para programarla para más tarde. Si la actualización ya está programada, puedes **Editar** o **Cancelar**. 3. Seleccione el botón **Actualizar firmware**.

Después de terminar

Puede supervisar o verificar las actualizaciones en **Resumen de actualización del firmware**. Para ver las actualizaciones que se han descartado o no se han podido instalar, haga clic en **Clúster > Configuración > Actualización automática > Ver todas las actualizaciones automáticas**.

Revierte ONTAP

Información general sobre revert ONTAP

Para realizar la transición de un clúster a una versión de ONTAP anterior, debe ejecutar una nueva versión.

La información de esta sección le guiará por los pasos que debe seguir antes y después de la reversión, incluidos los recursos que debe leer y las comprobaciones necesarias antes y después de la reversión que debe realizar.

> Si necesita realizar la transición de un clúster de ONTAP 9.1 a ONTAP 9.0, debe utilizar el procedimiento de degradación documentado "aquí".

¿Necesito soporte técnico para revertir?

Es posible revertir sin ayuda en clústeres nuevos o de prueba. Debe llamar al soporte técnico para revertir los clústeres de producción. También debe llamar al soporte técnico si experimenta alguna de las siguientes situaciones:

- Está en un entorno de producción y la reversión falla o se encuentra con cualquier problema antes o después de la reversión, como:
  - El proceso de reversión falla y no puede finalizar.
  - El proceso de reversión finaliza, pero el clúster no se puede utilizar en un entorno de producción.
  - El proceso de reversión se finaliza y el clúster se pone en producción, pero no está satisfecho con su comportamiento.
- Creó volúmenes en ONTAP 9.5 o una versión posterior y debe revertir a una versión anterior. Los volúmenes que utilizan compresión adaptativa deben descomprimidos antes de revertir.

Rutas de reversión

La versión de ONTAP a la que se puede revertir varía según la versión de ONTAP que se esté ejecutando actualmente en los nodos. Puede utilizar el `system image show` Comando para determinar la versión de ONTAP que se ejecuta en cada nodo.

Estas directrices solo se refieren a versiones ONTAP en las instalaciones. Para obtener información acerca de cómo revertir la ONTAP en el cloud, consulte "Revertir o degradar Cloud Volumes ONTAP".

Puede revertir de…	Para…
ONTAP 9.14.1	ONTAP 9.13.1
ONTAP 9.13.1	ONTAP 9.12.1
ONTAP 9.12.1	ONTAP 9.11.1
ONTAP 9.11.1	ONTAP 9.10.1
ONTAP 9.10.1	ONTAP 9.9.1
ONTAP 9.9.1	ONTAP 9,8
ONTAP 9,8	ONTAP 9,7
ONTAP 9,7	ONTAP 9,6
ONTAP 9,6	ONTAP 9,5
ONTAP 9,5	ONTAP 9,4
ONTAP 9,4	ONTAP 9,3
ONTAP 9,3	ONTAP 9,2
ONTAP 9,2	ONTAP 9,1
ONTAP 9,1 o ONTAP 9	Data ONTAP 8,3.x

Si necesita cambiar de ONTAP 9.1 a 9.0, debe seguir el "proceso de degradación" aquí documentado.

¿Qué debería leer antes de revertir?

Recursos que debe revisar antes de revertir

Antes de revertir ONTAP, debe confirmar el soporte de hardware y revisar los recursos para saber cuáles son los problemas que se pueden encontrar o que son necesarios resolver.

1. Revise la "Notas de la versión de ONTAP 9" para la versión de destino.

   En la sección "'Precauciones importantes'" se describen los posibles problemas que debe tener en cuenta antes de la degradación o la reversión.

2. Confirme que su plataforma de hardware es compatible con la versión de destino.

   "Hardware Universe de NetApp"

3. Confirme que su clúster y los switches de gestión son compatibles en la versión de destino.

   Debe verificar que las versiones del software NX-OS (switches de red de clúster), IOS (switches de red de gestión) y archivo de configuración de referencia (RCF) sean compatibles con la versión de ONTAP a la que desea revertir.

   "Descargas de NetApp: Switch Ethernet de Cisco"

4. Si su clúster está configurado para SAN, confirme que la configuración SAN es totalmente compatible.

   Deben ser compatibles todos los componentes DE SAN, como la versión de software de la ONTAP de destino, el sistema operativo y parches del host, el software de utilidades del host necesario y los controladores y firmware del adaptador.

   "Herramienta de matriz de interoperabilidad de NetApp"

Consideraciones sobre la reversión

Debe tener en cuenta los problemas y limitaciones de la reversión antes de iniciar una nueva versión de ONTAP.

- La reversión es disruptiva.

  Durante la reversión no se puede acceder a ningún cliente. Si va a revertir un clúster de producción, asegúrese de incluir esta interrupción en su planificación.

- La reversión afecta a todos los nodos del clúster.

  La reversión afecta a todos los nodos del clúster; sin embargo, la reversión debe realizarse y completarse en cada par de alta disponibilidad antes de que se reviertan otros pares de alta disponibilidad.

- La reversión se completa cuando todos los nodos ejecutan la nueva versión de destino.

  Cuando el clúster tiene un estado de versión mixta, no debe introducir ningún comando que altere la operación o configuración del clúster, excepto si es necesario para cumplir con los requisitos de reversión; se permiten las operaciones de supervisión.

> Si ha revertido algunos nodos, pero no todos, no intente actualizar el clúster de nuevo a la versión de origen.

- Al revertir un nodo, borra los datos almacenados en caché en un módulo Flash Cache.

  Como no hay datos en caché en el módulo Flash Cache, el nodo admite solicitudes de lectura iniciales del disco, lo que provoca una disminución del rendimiento de lectura durante este período. El nodo vuelve a llenar la caché conforme sirve solicitudes de lectura.

- Una LUN de la que se realiza el backup a cinta que se ejecuta en ONTAP 9.x solo se puede restaurar a las versiones 9.x y posteriores, y no a una versión anterior.
- Si la versión actual de ONTAP admite la funcionalidad ACP (IBACP) en banda y se revierte a una versión de ONTAP que no admite IBACP, se deshabilita la ruta alternativa hacia la bandeja de discos.
- Si alguna de las máquinas virtuales de almacenamiento (SVM) utiliza LDAP, debe deshabilitarse la referencia de LDAP antes de volver a verla.
- En sistemas MetroCluster IP que usan switches compatibles con MetroCluster pero no validados con MetroCluster, la versión de ONTAP 9.7 a 9.6 resulta disruptiva, ya que no es compatible con sistemas que utilicen ONTAP 9.6 y versiones anteriores.

Cosas que verificar antes de revertir

Antes de revertir, debe comprobar el estado del clúster, el estado del almacenamiento y la hora del sistema. También debe eliminar todos los trabajos de clúster que se estén ejecutando y terminar correctamente las sesiones de SMB que no estén disponibles continuamente.

Compruebe el estado del clúster

Antes de revertir el clúster, debe comprobar que los nodos están en buen estado y que pueden participar en el clúster, así como que el clúster tiene quórum.

1. Compruebe que los nodos del clúster estén en línea y que puedan participar en el clúster: `cluster show`

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ```

   Si alguno de los nodos no es saludable o no apto, compruebe los registros de EMS en busca de errores y realice acciones correctivas.

2. Establezca el nivel de privilegio en Advanced:
   `set -privilege advanced`

   Introduzca `y` para continuar.

3. Verifique los detalles de configuración de cada proceso RDB.

- Las épocas de la base de datos relacional y la base de datos deben coincidir para cada nodo.
- El maestro de quórum por anillo debe ser el mismo para todos los nodos.

  Tenga en cuenta que cada anillo puede tener un maestro de quórum diferente.

Para mostrar este proceso RDB:	Introduzca este comando…
Aplicación de gestión	`cluster ring show -unitname mgmt`
Base de datos de ubicación del volumen	`cluster ring show -unitname vldb`
Administrador de interfaz virtual	`cluster ring show -unitname vifmgr`
Daemon de gestión de SAN	`cluster ring show -unitname bcomd`

  Este ejemplo muestra el proceso de la base de datos de ubicación del volumen:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Vuelva al nivel de privilegio de administrador:
   `set -privilege admin`
5. Si va a trabajar en un entorno SAN, compruebe que cada nodo se encuentra en quórum DE SAN: `event log show -severity informational -message-name scsiblade.*`

   El mensaje de evento scsiblade más reciente para cada nodo debe indicar que el scsi-blade está en quórum.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time             Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Información relacionada

"Administración del sistema"

Comprobación del estado del almacenamiento

Antes de revertir un clúster, debe comprobar el estado de los discos, los agregados y los volúmenes.

1. Compruebe el estado del disco:

Para comprobar…	Realice lo siguiente…
Discos rotos	a. Mostrar cualquier disco roto: `storage disk show -state broken` b. Retire o sustituya los discos rotos.
Discos sometidos a mantenimiento o reconstrucción	a. Muestre cualquier disco en estado de mantenimiento, pendiente o reconstrucción: `storage disk show -state maintenance
pending	reconstructing` .. Espere a que la operación de mantenimiento o reconstrucción finalice antes de continuar.

2. Compruebe que todos los agregados están en línea mostrando el estado del almacenamiento físico y lógico, incluidos los agregados de almacenamiento: `storage aggregate show -state !online`

   Este comando muestra los agregados que *not* están en línea. Todos los agregados deben estar en línea antes y después de realizar una actualización o versión posterior principales.

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. Verifique que todos los volúmenes estén en línea mostrando los volúmenes que *not* en línea: `volume show -state !online`

   Todos los volúmenes deben estar en línea antes y después de realizar una actualización o versión posterior principales.

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. Compruebe que no haya volúmenes incoherentes: `volume show -is-inconsistent true`

   Consulte el artículo de la base de conocimientos "Volumen que muestra una incoherencia de WAFL" sobre la forma de abordar los volúmenes incoherentes.

Información relacionada

"Gestión de discos y agregados"

Verificación de la hora del sistema

Antes de revertir, debe verificar que NTP está configurado y que la hora está sincronizada en todo el clúster.

1. Compruebe que el clúster esté asociado con un servidor NTP: `cluster time-service ntp server show`
2. Compruebe que cada nodo tiene la misma fecha y hora: `cluster date show`

```
cluster1::> cluster date show
Node      Date                Timezone
--------- ------------------- -------------------------
node0     4/6/2013 20:54:38   GMT
node1     4/6/2013 20:54:38   GMT
node2     4/6/2013 20:54:38   GMT
node3     4/6/2013 20:54:38   GMT
4 entries were displayed.
```

Compruebe que no hay trabajos en ejecución

Antes de revertir el software ONTAP, debe comprobar el estado de los trabajos del clúster. Si cualquier trabajo de agregado, volumen, NDMP (volcado o restauración) o Snapshot (como crear, eliminar, mover, modificar, replicar, y los trabajos de montaje) están en ejecución o en cola, debe permitir que los trabajos finalicen correctamente o detener las entradas en cola.

1. Revise la lista de trabajos en ejecución o en cola de agregados, volúmenes o copias Snapshot: `job show`

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
8629   Vol Reaper           cluster1   -              Queued
       Description: Vol Reaper Job
8630   Certificate Expiry Check
                            cluster1   -              Queued
       Description: Certificate Expiry Check
.
.
.
```

2. Elimine cualquier trabajo que esté en ejecución o en cola de agregados, volúmenes o copias Snapshot: `job delete -id job_id`

```
cluster1::> job delete -id 8629
```

3. Compruebe que no haya trabajos de agregado, volumen ni Snapshot en ejecución ni en la cola: `job show`

   En este ejemplo, se han eliminado todos los trabajos en ejecución y en cola:

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
9944   SnapMirrorDaemon_7_2147484678
                            cluster1   node1          Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                            cluster1   node0          Dormant
       Description: SnapMirror Service Job
2 entries were displayed
```

Sesiones SMB que deben finalizar

Antes de revertir, debe identificar y terminar con dignidad cualquier sesión SMB que no esté disponible de forma continua.

No es necesario terminar los recursos compartidos SMB disponibles de forma continua, a los que acceden los clientes de Hyper-V o Microsoft SQL Server con el protocolo SMB 3.0 antes de la actualización o la degradación.

1. Identifique cualquier sesión SMB establecida que no esté disponible continuamente: `vserver cifs session show -continuously-available No -instance`

   Este comando muestra información detallada sobre cualquier sesión SMB que no tiene disponibilidad continua. Debe terminarlas antes de continuar con la degradación de ONTAP.

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
      Workstation IP address: 203.0.113.20
    Authentication Mechanism: NTLMv2
                 Windows User: CIFSLAB\user1
                    UNIX User: nobody
                  Open Shares: 1
                   Open Files: 2
                   Open Other: 0
               Connected Time: 8m 39s
                    Idle Time: 7m 45s
            Protocol Version: SMB2_1
      Continuously Available: No
1 entry was displayed.
```

2. Si es necesario, identifique los archivos que están abiertos para cada sesión SMB que ha identificado: `vserver cifs session file show -session-id session_ID`

```
cluster1::> vserver cifs session file show -session-id 1

Node:       node1
Vserver:    vs1
Connection: 4160072788
Session:    1
File    File      Open Hosting
Continuously
ID      Type      Mode Volume          Share                 Available
------- --------- ---- --------------- ---------------------
------------
1       Regular   rw   vol10           homedirshare          No
Path: \TestDocument.docx
2       Regular   rw   vol10           homedirshare          No
Path: \file1.txt
2 entries were displayed.
```

Autenticación NVMe en banda

Si va a revertir desde ONTAP 9.12.1 o posterior a ONTAP 9.12.0 o anterior, debe "desactive la autenticación

en banda" antes de revertir. Si la autenticación en banda con DH-HMAC-CHAP no está desactivada, se producirá un error en la reversión.

¿Qué más debería comprobar antes de revertir?

Comprobaciones previas a la reversión

En función de su entorno, debe tener en cuenta ciertos factores antes de revertir. Empiece por revisar la siguiente tabla para ver qué consideraciones especiales debe tener en cuenta.

Pregúntese…	Si su respuesta es sí, entonces haga esto…
¿Mi clúster ejecuta SnapMirror?	• Revisar las consideraciones de revertir sistemas con relaciones de SnapMirror síncrono • Consulte los requisitos de la modificación de versiones para relaciones de SnapMirror y SnapVault
¿Mi clúster ejecuta SnapLock?	Establezca los períodos de compromiso automático
¿Hay volúmenes FlexClone divididos?	Intercambio físico de bloques inverso
¿Tengo volúmenes FlexGroup?	Deshabilite la funcionalidad Qtree
¿Tengo servidores CIFS en modo grupo de trabajo?	Mover o eliminar servidores CIFS en modo Workgroup
¿Tengo volúmenes deduplicados?	Comprobar que el volumen contiene suficiente espacio libre
¿Tengo copias Snapshot?	Preparar copias de Snapshop
¿Estoy volviendo a ONTAP 8.3.x?	Identifique las cuentas de usuario que utilizan la función hash SHA-2
¿La protección contra ransomware se configuró para ONTAP 9.11.1 o posterior?	Compruebe las licencias antiransomware
¿Está configurado el acceso multiprotocolo de S3 para ONTAP 9.12.1 o posterior?	Quitar la configuración de bloque NAS de S3
¿Está configurada la conexión troncal de sesiones de NFSv4,1 para ONTAP 9.14.1 o posterior?	Elimine la configuración de troncalización de sesión NFSv4,1

Comprobaciones previas a la reversión de MetroCluster

Según la configuración de MetroCluster, debe tener en cuenta ciertos factores antes de revertir. Empiece por revisar la siguiente tabla para ver qué consideraciones especiales debe tener en cuenta.

Pregúntese…	Si su respuesta es sí, entonces haga esto…
¿Tengo una configuración MetroCluster de dos o cuatro nodos?	Deshabilitar la conmutación automática sin planificar

Pregúntese…	Si su respuesta es sí, entonces haga esto…
¿Tengo una configuración MetroCluster IP o estructural de cuatro u ocho nodos que ejecute ONTAP 9.12.1 o posterior?	Deshabilite IPsec

SnapMirror

Consideraciones que tener en cuenta para revertir sistemas con relaciones de SnapMirror síncrono

Debe estar al tanto de las consideraciones para las relaciones de SnapMirror síncrono antes de revertir de ONTAP 9.6 a ONTAP 9.5.

Antes de revertir, debe realizar los siguientes pasos si tiene relaciones de SnapMirror síncrono:

- Debe eliminar cualquier relación de SnapMirror Synchronous en la que el volumen de origen esté sirviendo datos mediante NFSv4 o SMB.

  ONTAP 9.5 no admite NFSv4 y SMB.

- Debe eliminar todas las relaciones de SnapMirror síncrono en una puesta en marcha en cascada de reflejos.

  No se admite una puesta en marcha en cascada de reflejos mediante relaciones de SnapMirror síncrono en ONTAP 9.5.

- Si las copias Snapshot comunes en ONTAP 9.5 no están disponibles durante la reversión, debe inicializar la relación de SnapMirror síncrono después de revertir.

  Tras dos horas de actualización a ONTAP 9.6, las copias Snapshot comunes de ONTAP 9.5 se reemplazan automáticamente por las copias Snapshot comunes de ONTAP 9.6. Por lo tanto, no puede volver a sincronizar la relación de SnapMirror síncrono tras revertir si las copias Snapshot comunes de ONTAP 9.5 no están disponibles.

Requisitos de nueva versión para relaciones de SnapMirror y SnapVault

El comando de reversión del nodo del sistema le notifica cualquier relación de SnapMirror y SnapVault que sea necesario eliminar o reconfigurar para que se complete el proceso de nueva versión. Sin embargo, debe tener en cuenta estos requisitos antes de iniciar la reversión.

- Todas las relaciones de reflejo de protección de datos y SnapVault deben ponerse en modo inactivo y después romperse.

  Una vez completada la reversión, puede volver a sincronizar y reanudar estas relaciones si existe una copia Snapshot común.

- Las relaciones de SnapVault no deben contener los siguientes tipos de políticas de SnapMirror:
  - reflejo asíncrono

    Debe eliminar cualquier relación que utilice este tipo de política.

  - Reflejo de AndVault

Si alguna de estas relaciones existe, debe cambiar la política de SnapMirror a mirror-vault.

- Se deben eliminar todas las relaciones de reflejo con uso compartido de carga y los volúmenes de destino.
- Deben eliminarse las relaciones de SnapMirror con volúmenes de destino de FlexClone.
- Debe deshabilitarse la compresión de red para cada política de SnapMirror.
- La regla all_source_snapshot debe eliminarse de cualquier política de SnapMirror de tipo reflejo asíncrono.

> Las operaciones de restauración de snapshot de archivo único (SFSR) y de restauración de snapshot de archivo parcial (PFSR) se obsoletos en el volumen raíz.

- Todas las operaciones de restauración de archivo único y de snapshot que se estén ejecutando actualmente deben completarse antes de que pueda continuar la reversión.

  Puede esperar a que finalice la operación de restauración o anularla.

- Todas las operaciones incompletas de restauración de archivos individuales y Snapshot deben eliminarse mediante el comando snapmirror restore.

Configure periodos de confirmación automática para volúmenes SnapLock antes de revertir

Para revertir a ONTAP 9, el valor del período de compromiso automático para los volúmenes de SnapLock se debe establecer en horas, no días. Antes de intentar la reversión, debe comprobar el valor de compromiso automático de los volúmenes SnapLock y modificarlo de días a horas, de ser necesario.

1. Compruebe que haya volúmenes SnapLock en el clúster que tengan periodos de compromiso automático no compatibles:`volume snaplock show -autocommit-period *days`
2. Modifique los periodos de compromiso automático no compatibles a horas: `volume snaplock modify -vserver vserver_name -volume volume_name -autocommit-period value hours`

Revierta el uso compartido de bloques físicos en volúmenes FlexClone separados

Si dividió un volumen FlexClone de su volumen principal, se deberá deshacer el uso compartido de cualquier bloque físico entre el clon y su volumen principal antes de revertir desde ONTAP 9.4 o una versión posterior de ONTAP.

Esta tarea solo es aplicable a sistemas AFF cuando se ha ejecutado la división en alguno de los volúmenes FlexClone.

1. Inicie sesión en el nivel de privilegio avanzado: `set -privilege advanced`
2. Identifique los volúmenes FlexClone divididos con bloques físicos compartidos: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
Node            Vserver   Volume        Aggregate
--------------- --------- ------------- -------------
node1           vs1       vol_clone1    aggr1
node2           vs2       vol_clone2    aggr2
2 entries were displayed.
```

3. Deshace el uso compartido de bloques físicos en todos los volúmenes FlexClone divididos por el clúster: `volume clone sharing-by-split undo start-all`
4. Compruebe que no hay volúmenes FlexClone divididos con bloques físicos compartidos: `volume clone sharing-by-split show`

```
cluster1::> volume clone sharing-by-split show
This table is currently empty.
```

Deshabilite la funcionalidad Qtree en volúmenes FlexGroup antes de revertir

Los qtrees de volúmenes de FlexGroup no son compatibles antes de ONTAP 9.3. Debe deshabilitar la funcionalidad para qtrees en volúmenes de FlexGroup antes de revertir de ONTAP 9.3 a una versión anterior de ONTAP.

La funcionalidad Qtree se habilita al crear un qtree o si se modifican los atributos de estilo de seguridad y modo oplock del qtree predeterminado.

1. Identifique y elimine todos los qtrees no predeterminados en cada volumen de FlexGroup que estén habilitados con la funcionalidad Qtree:

   a. Inicie sesión en el nivel de privilegio avanzado: `set -privilege advanced`

   b. Compruebe si hay algún volumen de FlexGroup habilitado con la funcionalidad Qtree.

      Para ONTAP 9.6 o posterior, utilice: `volume show -is-qtree-caching-enabled true`

      Para ONTAP 9.5 o anterior, utilice: `volume show -is-flexgroup-qtree-enabled true`

```
cluster1::*> volume show -is-flexgroup-qtree-enabled true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs0       fg           -            online     RW        320MB
220.4MB   31%
```

   c. Elimine todos los qtrees no predeterminados de cada volumen de FlexGroup que estén habilitados con la funcionalidad de qtree: `volume qtree delete -vserver svm_name -volume volume_name`

`-qtree qtree_name`

Si la funcionalidad Qtree se encuentra habilitada porque se modificaron los atributos del qtree predeterminado y, si no tiene ningún qtree, puede omitir este paso.

```
cluster1::*> volume qtree delete -vserver vs0 -volume fg -qtree qtree4
WARNING: Are you sure you want to delete qtree qtree4 in volume fg
vserver vs0?  {y|n}: y
[Job 38] Job is queued: Delete qtree qtree4 in volume fg vserver vs0.
```

2. Deshabilite la funcionalidad Qtree en cada volumen FlexGroup: `volume flexgroup qtree-disable -vserver svm_name -volume volume_name`

```
cluster1::*> volume flexgroup qtree-disable -vserver vs0 -volume fg
```

3. Identificar y eliminar cualquier copia de Snapshot que esté habilitada con la funcionalidad de qtree.

   a. Compruebe si hay alguna copia Snapshot habilitada con la funcionalidad para qtrees: `volume snapshot show -vserver vserver_name -volume volume_name -fields is-flexgroup-qtree-enabled`

```
cluster1::*> volume snapshot show -vserver vs0 -volume fg -fields is-
flexgroup-qtree-enabled
vserver volume snapshot is-flexgroup-qtree-enabled
------- ------ -------- --------------------------
vs0     fg     fg_snap1 true
vs0     fg     daily.2017-09-27_0010 true
vs0     fg     daily.2017-09-28_0010 true
vs0     fg     snapmirror.0241f354-a865-11e7-a1c0-
00a098a71764_2147867740.2017-10-04_124524 true
```

   b. Elimine todas las copias Snapshot que están habilitadas con la funcionalidad para qtrees: `volume snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot_name -force true -ignore-owners true`

   Las copias Snapshot que deben eliminarse incluyen copias Snapshot regulares y las copias Snapshot realizadas para relaciones de SnapMirror. Si ha creado alguna relación de SnapMirror para los volúmenes de FlexGroup con un clúster de destino que ejecute ONTAP 9.2 o una versión anterior, debe eliminar todas las copias de Snapshot que se realizaron cuando se habilitó el volumen de FlexGroup de origen para la funcionalidad de qtree.

```
cluster1::> volume snapshot delete -vserver vs0 -volume fg -snapshot
daily.2017-09-27_0010 -force true -ignore-owners true
```

Información relacionada

"Gestión de volúmenes de FlexGroup"

Identificar y mover servidores SMB en modo de grupo de trabajo

Antes de realizar una reversión, debe eliminar cualquier servidor SMB en modo de grupo de trabajo o moverlos a un dominio. El modo de grupo de trabajo no es compatible con las versiones de ONTAP anteriores a ONTAP 9.

1. Identificar cualquier servidor SMB con un estilo de autenticación de grupo de trabajo: `vserver cifs show`
2. Mueva o elimine los servidores identificados:

Si va a…	A continuación, utilice este comando….
Mover el servidor SMB del grupo de trabajo a un dominio de Active Directory:	`vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*
Elimine el servidor SMB	`vserver cifs delete -vserver vserver_name`

3. Si eliminó el servidor SMB, introduzca el nombre de usuario del dominio y la contraseña de usuario.

Información relacionada

"Gestión de SMB"

Verifique que los volúmenes deduplicados tengan suficiente espacio libre antes de revertir

Antes de revertir desde cualquier versión de ONTAP 9, debe asegurarse de que los volúmenes contengan espacio libre suficiente para la operación de reversión.

El volumen debe tener suficiente espacio para acomodar el ahorro que se obtuvo mediante la detección en línea de bloques de ceros. Consulte el artículo de la base de conocimientos "Cómo observar ahorros de espacio gracias a la deduplicación, la compresión y la compactación en ONTAP 9".

Si se habilitó tanto la deduplicación como la compresión de datos en un volumen que se desea revertir, se debe revertir la compresión de datos antes de revertir la deduplicación.

1. Use el comando volume Efficiency show con la opción -fields para ver el progreso de las operaciones de eficiencia que se están ejecutando en los volúmenes.

   El siguiente comando muestra el progreso de las operaciones de eficiencia: `volume efficiency show -fields vserver,volume,progress`

2. Use el comando volume Efficiency stop con la opción -all para detener todas las operaciones de deduplicación activas y en cola.

   El siguiente comando detiene todas las operaciones de deduplicación activas y en cola en el volumen Vola: `volume efficiency stop -vserver vs1 -volume VolA -all`

3. Utilice el comando set -Privilege Advanced para iniciar sesión en el nivel de privilegio avanzado.

4. La eficiencia de volumen se debe usar con la opción -version para degradar los metadatos de eficiencia de un volumen a una versión específica de ONTAP.

   El siguiente comando revierte los metadatos de eficiencia del volumen Vola a ONTAP 9.x: `volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x`

   > El comando de reversión de la eficiencia del volumen revierte los volúmenes presentes en el nodo en el que se ejecuta este comando. Este comando no revierte volúmenes entre nodos.

5. El comando volume Efficiency show se utiliza con la opción -op-status para supervisar el progreso de la degradación.

   El siguiente comando supervisa y muestra el estado de la degradación: `volume efficiency show -vserver vs1 -op-status Downgrading`

6. Si la reversión no se realiza correctamente, use el comando volume Efficiency show con la opción -instance para ver por qué ha fallado la reversión.

   El siguiente comando muestra información detallada sobre todos los campos: `volume efficiency show -vserver vs1 -volume vol1 - instance`

7. Una vez finalizada la operación de reversión, vuelva al nivel de privilegio de administrador: `set -privilege admin`

   "Gestión de almacenamiento lógico"

Prepare las copias Snapshot antes de revertir

Antes de revertir a una versión de ONTAP anterior, debe deshabilitar todas las políticas de copia de Snapshot y eliminar las copias de Snapshot que se crearon después de actualizar a la versión actual.

Si va a revertir en un entorno de SnapMirror, primero debe eliminar las siguientes relaciones de reflejo:

- Todas las relaciones de mirroring de uso compartido de carga
- Todas las relaciones de mirroring de protección de datos que se crearon en ONTAP 8.3.x.
- Todas las relaciones de mirroring de protección de datos si el clúster se volvió a crear en ONTAP 8.3.x.

  a. Deshabilite las políticas de copia Snapshot para todas las SVM de datos: `volume snapshot policy modify -vserver * -enabled false`

  b. Deshabilite las políticas de copia Snapshot para los agregados de cada nodo:

     i. Identifique los agregados del nodo mediante el comando run-nodenodenameaggr status.

     ii. Deshabilite la política de copia Snapshot de cada agregado: `run -node nodename aggr options aggr_name nosnap on`

     iii. Repita este paso con cada uno de los nodos restantes.

  c. Deshabilite las políticas de copia Snapshot para el volumen raíz de cada nodo:

     i. Identifique el volumen raíz del nodo mediante el comando run-nodenodesmalevol status.

El volumen raíz se identifica por la palabra root en la columna Options del resultado del comando vol status.

```
vs1::> run -node node1 vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

i. Deshabilite la política de copia Snapshot en el volumen raíz: `run -node nodename vol options root_volume_name nosnap on`

ii. Repita este paso con cada uno de los nodos restantes.

d. Elimine todas las copias Snapshot que se crearon después de actualizar a la versión actual:

i. Configure el nivel de privilegio en Advanced: `set -privilege advanced`

ii. Desactive las instantáneas:`snapshot policy modify -vserver * -enabled false`

iii. Elimine las copias Snapshot de la versión más reciente del nodo: `volume snapshot prepare-for-revert -node nodename`

Este comando elimina las copias Snapshot de una versión más reciente en cada volumen de datos, agregado raíz y volumen raíz.

Si alguna copia de Snapshot no se puede eliminar, el comando falla y notifica las acciones necesarias que debe realizar para poder eliminar las copias de Snapshot. Debe completar las acciones necesarias y volver a ejecutar el comando prepare-for-revert de la snapshot del volumen antes de continuar con el siguiente paso.

```
cluster1::*> volume snapshot prepare-for-revert -node node1

Warning: This command will delete all Snapshot copies that have the
format used by the current version of ONTAP. It will fail if any
Snapshot copy polices are enabled, or
         if any Snapshot copies have an owner. Continue? {y|n}: y
```

i. Compruebe que las copias Snapshot se han eliminado: `volume snapshot show -node nodename`

Si queda alguna copia Snapshot de la versión más reciente, obligue a eliminar: `volume snapshot delete {-fs-version 9.0 -node nodename -is-constituent true} -ignore-owners -force`

ii. Repita este paso c para cada uno de los nodos restantes.

iii. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Estos pasos deben ejecutarse en los dos clústeres de la configuración de MetroCluster.

Identifique las cuentas de usuario que utilizan la función hash SHA-2

Si va a revertir de ONTAP 9.1 o ONTAP 9.0 a ONTAP 8.3.x, los usuarios de cuentas SHA-2 ya no podrán autenticarse con sus contraseñas. Antes de revertir, debe identificar las cuentas de usuario que utilizan la función hash SHA-2, de modo que, después de revertir, pueda hacer que restablezcan sus contraseñas para utilizar el tipo de cifrado (MD5) admitido por la versión a la que se revierte.

1. Cambie a la configuración de privilegio a avanzado: `set -privilege advanced`
2. Identifique las cuentas de usuario que utilizan SHA-2 tiene función: `security login show -vserver * -username * -application * -authentication-method password -hash-function !md5`
3. Conserve el resultado del comando para utilizarlo después de la reversión.

> Durante la reversión, se le pedirá que ejecute el comando Advanced `security login password-prepare-to-downgrade` Para restablecer su propia contraseña para utilizar la función hash MD5. Si su contraseña no está cifrada con MD5, el comando le solicita una nueva contraseña y la cifra con MD5, lo que permite autenticar su credencial después de la reversión.

Compruebe las licencias de protección contra ransomware autónomas antes de volver de ONTAP 9.11.1 o posterior

Si configuró la protección de ransomware autónoma (ARP) y revierte de ONTAP 9.11.1 o una versión posterior a ONTAP 9.10.1 o una versión anterior, puede experimentar mensajes de advertencia y funcionalidad ARP limitada.

En ONTAP 9.11.1, la licencia Anti-ransomware reemplazó la licencia de gestión de claves multi-tenant (MTKM). Si el sistema tiene la licencia Anti_ransomware pero no tiene licencia MT_EK_MGMT, verá una advertencia durante la reversión de que ARP no puede habilitarse en volúmenes nuevos al revertir.

Los volúmenes con protección existente seguirán funcionando normalmente después de la reversión y el estado ARP puede mostrarse con la interfaz de línea de comandos ONTAP. System Manager no puede mostrar el estado de ARP sin la licencia de MTKM.

Por lo tanto, si desea que ARP continúe después de revertir a ONTAP 9.10.1, asegúrese de que la licencia MTKM está instalada antes de revertir. "Más información sobre las licencias de ARP."

Quite la configuración de bloque NAS de S3 antes de revertir de ONTAP 9.12.1 o posterior

Si ha configurado el acceso de cliente S3 para datos de NAS, antes de revertir desde ONTAP 9.12.1 o posterior a ONTAP 9.11.1 o versiones anteriores, debe usar la interfaz de línea de comandos (CLI) de ONTAP para quitar la configuración de bucket NAS y para eliminar cualquier asignación de nombre (S3 usuarios para usuarios Windows o Unix).

Acerca de esta tarea

Las siguientes tareas se completan en segundo plano durante el proceso de reversión.

- Quite todas las creaciones de objetos singleton completadas parcialmente (es decir, todas las entradas de directorios ocultos).

- Quite todos los directorios ocultos; puede haber uno en cada volumen al que se pueda acceder desde la raíz de la exportación asignada desde el bloque NAS de S3.
- Retire la tabla de carga.
- Elimine los valores de usuario predeterminados de unix-user y Windows-default para todos los servidores S3 configurados.

Pasos

1. Eliminar la configuración del bucket NAS de S3:

```
vserver object-store-server bucket delete -vserver _svm_name_ -bucket
_s3_nas_bucket_name_
```

2. Eliminar asignaciones de nombres para UNIX:

```
vserver name-mapping delete -vserver _svm_name_ -direction s3-unix
```

3. Eliminar asignaciones de nombres para Windows:

```
vserver name-mapping delete -vserver _svm_name_ -direction s3-win
```

4. Quite los protocolos S3 de la SVM:

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

Elimine la configuración de trunking de sesión NFSv4,1 antes de revertir desde ONTAP 9.14.1 o una versión posterior

Si ha activado la conexión troncal para las conexiones de cliente y vuelve a una versión anterior a ONTAP 9.14.1, debe deshabilitar la conexión troncal en cualquier servidor NFSv4,1 antes de revertir.

Cuando introduzca la `revert-to` comando, verá un mensaje de advertencia para informarle de que deshabilite la conexión troncal antes de continuar.

Después de volver a una versión anterior de ONTAP, los clientes que utilizan conexiones troncalizadas vuelven a utilizar una única conexión. El rendimiento de sus datos se verá afectado, pero no habrá interrupción. El comportamiento de reversión es el mismo que modificar la opción de Trunking NFSv4,1 para la SVM de enabled a disabled.

Pasos

1. Desactive la troncalización en el servidor NFSv4,1:
   `vserver nfs modify -vserver svm_name -v4.1-trunking disabled`
2. Compruebe que NFS está configurado como desee:
   `vserver nfs show -vserver svm_name`

Deshabilite la conmutación de sitios no planificada automática antes de revertir las configuraciones de MetroCluster de dos y cuatro nodos

Antes de revertir una configuración de MetroCluster de dos o cuatro nodos, se debe deshabilitar la conmutación automática sin planificar (AUSO).

1. En los dos clústeres de MetroCluster, deshabilite la conmutación automática no planificada:
   `metrocluster modify -auto-switchover-failure-domain auso-disabled`

Información relacionada

"Gestión y recuperación ante desastres de MetroCluster"

Deshabilite IPsec antes de revertir las configuraciones de MetroCluster

Antes de revertir una configuración de MetroCluster, debe deshabilitar IPsec.

No puede revertir ONTAP en una configuración de MetroCluster que ejecute ONTAP 9.12.1 con IPsec habilitada. Antes de revertir, se realiza una comprobación para asegurarse de que no hay configuraciones IPsec en la configuración de MetroCluster. Debe eliminar cualquier configuración IPsec presente y deshabilitar IPsec antes de continuar con el proceso de reversión. Revertir ONTAP se bloquea si IPsec está habilitada, incluso cuando no se ha configurado ninguna directiva de usuario.

Descargue e instale la imagen del software de ONTAP

Primero, tiene que descargar el software ONTAP del sitio de soporte de NetApp; entonces puede instalarlo.

Descargue la imagen del software

Para degradar o revertir de ONTAP 9.4 y versiones posteriores, puede copiar la imagen del software ONTAP del sitio de soporte de NetApp a una carpeta local. Para una degradación o para revertir a ONTAP 9.3 o una versión anterior, debe copiar la imagen del software ONTAP en un servidor HTTP o FTP de la red.

Debe tener en cuenta la siguiente información importante:

- Las imágenes de software son específicas para los modelos de la plataforma.

  Debe obtener la imagen correcta para su clúster. Las imágenes de software, la información de versión de firmware y el firmware más reciente para el modelo de su plataforma están disponibles en el sitio de soporte de NetApp.

- Las imágenes de software incluyen la versión más reciente del firmware del sistema disponible cuando se publicó una versión concreta de ONTAP.
- Si va a cambiar a un sistema con el cifrado de volúmenes de NetApp desde ONTAP 9.5 o posterior, debe descargar la imagen del software ONTAP para países no restringidos, que incluye el cifrado de volúmenes de NetApp.

  Si utiliza la imagen de software de ONTAP para países restringidos a fin de degradar o revertir un sistema con el cifrado de volúmenes de NetApp, el sistema tendrá una alarma y perderá el acceso a los volúmenes.

  a. Busque el software ONTAP de destino en la "Descargas de software" Del sitio de soporte de NetApp.

b. Copie la imagen del software.

   - Para ONTAP 9.3 o una versión anterior, copie la imagen de software (por ejemplo, 93_q_image.tgz) del sitio de soporte de NetApp en el directorio del servidor HTTP o FTP a partir del que se servirá la imagen.
   - Para ONTAP 9.4 o posterior, copie la imagen de software (por ejemplo, 97_q_image.tgz) del sitio de soporte de NetApp en el directorio del servidor HTTP o FTP a partir del que se servirá la imagen o en una carpeta local.

Instale la imagen del software

Debe instalar la imagen de software de destino en los nodos del clúster.

- Si va a degradar o revertir un sistema con cifrado de volumen de NetApp desde ONTAP 9.5 o posterior, debe haber descargado la imagen del software ONTAP para países no restringidos, que incluye el cifrado de volúmenes de NetApp.

  Si utiliza la imagen de software de ONTAP para países restringidos a fin de degradar o revertir un sistema con el cifrado de volúmenes de NetApp, el sistema tendrá una alarma y perderá el acceso a los volúmenes.

  a. Establezca el nivel de privilegio en avanzado, introduzca **y** cuando se le solicite continuar: `set -privilege advanced`

     El aviso avanzado (`*>`) aparece.

  b. Instale la imagen de software en los nodos.

     Este comando descarga e instala la imagen de software en todos los nodos al mismo tiempo. Para descargar e instalar la imagen en cada nodo de uno en uno, no especifique el parámetro -background.

     - Si va a degradar o revertir una configuración que no sea de MetroCluster o una configuración de MetroCluster de dos nodos:`system node image update -node * -package location -replace-package true -setdefault true -background true`

       Este comando utiliza una consulta ampliada para cambiar la imagen de software de destino, que se instala como imagen alternativa, para que sea la imagen predeterminada del nodo.

     - Si va a revertir una configuración MetroCluster de cuatro u ocho nodos, debe emitir el siguiente comando en ambos clústeres: `system node image update -node * -package location -replace-package true true -background true -setdefault false`

       Este comando utiliza una consulta ampliada para cambiar la imagen de software de destino, que se instala como la imagen alternativa en cada nodo.

  c. Introduzca `y` para continuar cuando se le solicite.

  d. Compruebe que la imagen de software se haya descargado e instalado en cada nodo: `system node image show-update-progress -node *`

     Este comando muestra el estado actual de la descarga e instalación de la imagen de software. Debe continuar ejecutando este comando hasta que todos los nodos informen sobre un estado de ejecución de salida y un estado de salida correcto.

     El comando de actualización de imagen del nodo del sistema puede fallar y mostrar mensajes de error

o advertencia. Después de resolver errores o advertencias, puede volver a ejecutar el comando.

Este ejemplo muestra un clúster de dos nodos en el cual la imagen de software se descarga y se instala correctamente en ambos nodos:

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

Revertir un clúster de ONTAP

Para desconectar el clúster y volver a una versión ONTAP anterior, debe deshabilitar la conmutación por error del almacenamiento y los LIF de datos, abordar las condiciones previas para la reversión, revertir la configuración del clúster y del sistema de archivos en un nodo y, a continuación, repetir el proceso para cada nodo adicional del clúster.

Debe haber completado la reversión "verificaciones" y.. "comprobaciones previas".

Al revertir un clúster se necesita que el clúster se desconecte durante la duración de la versión re.

1. Configure el nivel de privilegio en Advanced: `set -privilege advanced`

   Introduzca **y** cuando se le solicite continuar.

2. Compruebe que el software ONTAP de destino está instalado: `system image show`

   El siguiente ejemplo muestra que la versión 9.1 está instalada como imagen alternativa en ambos nodos:

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------   -------------------
node0
         image1  true    true    9.2        MM/DD/YYYY TIME
         image2  false   false   9.1        MM/DD/YYYY TIME
node1
         image1  true    true    9.2        MM/DD/YYYY TIME
         image2  false   false   9.1        MM/DD/YYYY TIME
4 entries were displayed.
```

3. Deshabilite todas las LIF de datos del clúster: `network interface modify {-role data} -status-admin down`
4. Determinar si tiene relaciones de FlexCache entre clústeres: `flexcache origin show-caches -relationship-type inter-cluster`
5. Si hay destellos entre clústeres, deshabilite los datos del clúster de caché: `network interface modify -vserver vserver_name -lif lif_name -status-admin down`
6. Si el clúster consta de solo dos nodos, deshabilite el clúster de alta disponibilidad: `cluster ha modify -configured false`
7. deshabilite la recuperación tras fallos del almacenamiento para los nodos del par de alta disponibilidad de cualquiera de los nodos: `storage failover modify -node nodename -enabled false`

   Solo tiene que deshabilitar la conmutación por error del almacenamiento una vez para el par de alta disponibilidad. Cuando deshabilita la conmutación al respaldo de almacenamiento para un nodo, la conmutación al respaldo de almacenamiento también se deshabilita en el compañero de nodo.

8. Inicie sesión en el nodo que desea revertir.

   Para revertir un nodo, debe haber iniciado sesión en el clúster a través de la LIF de gestión del nodo del nodo.

9. Establezca la imagen de software ONTAP de destino del nodo en ser la imagen predeterminada: `system image modify -node nodename -image target_image -isdefault true`
10. Verifique que la imagen del software de ONTAP de destino se esté establecida como la imagen predeterminada del nodo que está revirtiendo: `system image show`

    En el siguiente ejemplo, se muestra que la versión 9.1 se establece como la imagen predeterminada en el nodo 0:

```
cluster1::*> system image show
                 Is      Is                  Install
Node     Image   Default Current Version    Date
-------- ------- ------- ------- --------   -------------------
node0
         image1  false   true    9.2        MM/DD/YYYY TIME
         image2  true    false   9.1        MM/DD/YYYY TIME
node1
         image1  true    true    9.2        MM/DD/YYYY TIME
         image2  false   false   9.1        MM/DD/YYYY TIME
4 entries were displayed.
```

11. Si el clúster solo consta de dos nodos, compruebe que el nodo no esté configurado con épsilon:

    a. Compruebe si el nodo está actualmente configurado con épsilon: `cluster show -node nodename`

    En el siguiente ejemplo se muestra que el nodo está configurado con épsilon:

```
cluster1::*> cluster show -node node1

          Node: node1
          UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
       Epsilon: true
   Eligibility: true
        Health: true
```

    a. Si el nodo no está configurado con épsilon, márquelo como falso en el nodo para que se pueda transferir el valor épsilon al partner del nodo: `cluster modify -node nodenameA -epsilon false`

    b. Transfiera el valor épsilon al partner del nodo marcando épsilon true en el nodo del partner: `cluster modify -node nodenameB -epsilon true`

12. Compruebe que el nodo esté listo para la nueva versión: `system node revert-to -node nodename -check-only true -version 9.x`

    El parámetro check-only identifica las condiciones previas que se deben abordar antes de revertir, como los siguientes ejemplos:

    - Deshabilitar la recuperación tras fallos del almacenamiento
    - Deshabilitar la política de Snapshot
    - Eliminar copias de Snapshot que se crearon después de actualizar a la versión posterior de ONTAP

13. Compruebe que se han tratado todas las condiciones previas: `system node revert-to -node nodename -check-only true -version 9.x`

14. Revierte la configuración del clúster del nodo: `system node revert-to -node nodename -version 9.x`

La opción -version hace referencia a la versión de destino. Por ejemplo, si el software que ha instalado y verificado es ONTAP 9.1, el valor correcto de la opción -version es 9.1.

La configuración del clúster se revierte y luego se cierra la sesión en el clustershell.

15. Vuelva a iniciar sesión en el clustershell y, a continuación, cambie al nodeshell: `run -node nodename`

    Después de iniciar sesión de nuevo en el clustershell, puede tardar unos minutos antes de que esté listo para aceptar el comando nodeshell. Por lo tanto, si el comando falla, espere unos minutos y vuelva a intentarlo.

16. Revierte la configuración del sistema de archivos del nodo: `revert_to 9.x`

    Este comando verifica que la configuración del sistema de archivos del nodo está lista para revertirse y después lo revierte. Si se identifican las condiciones previas, debe abordarlas y a continuación, vuelva a ejecutar el comando revert_to.

    > El uso de una consola del sistema para supervisar el proceso de reversión muestra más detalles que los que se ven en el infierno.

    Si se cumple LA FUNCIÓN AUTOBOOT, cuando el comando finaliza, el nodo se reiniciará en ONTAP.

    Si el INICIO AUTOMÁTICO es falso, cuando el comando finaliza el símbolo del sistema del CARGADOR se muestra. Introduzca `yes` para revertir y después usarlo `boot_ontap` para reiniciar manualmente el nodo.

17. Cuando el nodo se haya reiniciado, confirme que el nuevo software está en ejecución: `system node image show`

    En el siguiente ejemplo, image1 es la nueva versión de ONTAP y se establece como la versión actual del nodo 0:

    ```
    cluster1::*> system node image show
                     Is      Is                  Install
    Node     Image   Default Current Version    Date
    -------- ------- ------- ------- --------   -------------------
    node0
             image1  true    true    X.X.X       MM/DD/YYYY TIME
             image2  false   false   Y.Y.Y      MM/DD/YYYY TIME
    node1
             image1  true    false   X.X.X      MM/DD/YYYY TIME
             image2  false   true    Y.Y.Y      MM/DD/YYYY TIME
    4 entries were displayed.
    ```

18. Compruebe que el estado de reversión se ha completado para cada nodo: `system node upgrade-revert show -node nodename`

    El estado debe aparecer como Finalizado, No Necesario o No hay ninguna entrada de tabla devuelta.

19. Repetición [step-6] por [step-16] En el otro nodo del par de alta disponibilidad.

20. Si el clúster consta de solo dos nodos, vuelva a habilitar el clúster de alta disponibilidad: `cluster ha modify -configured true`
21. vuelva a activar la recuperación tras fallos de almacenamiento en ambos nodos si se deshabilitó anteriormente: `storage failover modify -node nodename -enabled true`
22. Repetición [step-5] por [step-19] Para cada par de alta disponibilidad adicional y ambos clústeres en Configuración de MetroCluster.

¿Qué debo hacer luego de revertir mi clúster?

Verifique el estado del clúster y del almacenamiento después de la degradación o la reversión

Después de degradar o revertir un clúster, debe comprobar que los nodos estén en buen estado y que puedan participar en el clúster, así como que el clúster esté de quórum. También debe verificar el estado de los discos, los agregados y los volúmenes.

Compruebe el estado del clúster

1. Compruebe que los nodos del clúster estén en línea y que puedan participar en el clúster: `cluster show`

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

   Si alguno de los nodos no es saludable o no apto, compruebe los registros de EMS en busca de errores y realice acciones correctivas.

2. Establezca el nivel de privilegio en Advanced:
   `set -privilege advanced`

   Introduzca `y` para continuar.

3. Verifique los detalles de configuración de cada proceso RDB.
   - Las épocas de la base de datos relacional y la base de datos deben coincidir para cada nodo.
   - El maestro de quórum por anillo debe ser el mismo para todos los nodos.

     Tenga en cuenta que cada anillo puede tener un maestro de quórum diferente.

Para mostrar este proceso RDB:	Introduzca este comando…
Aplicación de gestión	`cluster ring show -unitname mgmt`
Base de datos de ubicación del volumen	`cluster ring show -unitname vldb`
Administrador de interfaz virtual	`cluster ring show -unitname vifmgr`

Para mostrar este proceso RDB:	Introduzca este comando…
Daemon de gestión de SAN	`cluster ring show -unitname bcomd`

Este ejemplo muestra el proceso de la base de datos de ubicación del volumen:

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`
5. Si va a trabajar en un entorno SAN, compruebe que cada nodo se encuentra en quórum DE SAN: `event log show -severity informational -message-name scsiblade.*`

   El mensaje de evento scsiblade más reciente para cada nodo debe indicar que el scsi-blade está en quórum.

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time             Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

Información relacionada

"Administración del sistema"

Comprobación del estado del almacenamiento

Después de revertir o degradar un clúster, debe verificar el estado de los discos, agregados y volúmenes.

1. Compruebe el estado del disco:

Para comprobar…	Realice lo siguiente…
Discos rotos	a. Mostrar cualquier disco roto: `storage disk show -state broken` b. Retire o sustituya los discos rotos.
Discos sometidos a mantenimiento o reconstrucción	a. Muestre cualquier disco en estado de mantenimiento, pendiente o reconstrucción: `storage disk show -state maintenance
pending	reconstructing` .. Espere a que la operación de mantenimiento o reconstrucción finalice antes de continuar.

2. Compruebe que todos los agregados están en línea mostrando el estado del almacenamiento físico y lógico, incluidos los agregados de almacenamiento: `storage aggregate show -state !online`

   Este comando muestra los agregados que *not* están en línea. Todos los agregados deben estar en línea antes y después de realizar una actualización o versión posterior principales.

   ```
   cluster1::> storage aggregate show -state !online
   There are no entries matching your query.
   ```

3. Verifique que todos los volúmenes estén en línea mostrando los volúmenes que *not* en línea: `volume show -state !online`

   Todos los volúmenes deben estar en línea antes y después de realizar una actualización o versión posterior principales.

   ```
   cluster1::> volume show -state !online
   There are no entries matching your query.
   ```

4. Compruebe que no haya volúmenes incoherentes: `volume show -is-inconsistent true`

   Consulte el artículo de la base de conocimientos "Volumen que muestra una incoherencia de WAFL" sobre la forma de abordar los volúmenes incoherentes.

Información relacionada

"Gestión de discos y agregados"

Permite el cambio automático para configuraciones de MetroCluster

En este tema, se proporciona información sobre las tareas adicionales que debe realizar tras la nueva versión de las configuraciones de MetroCluster.

1. Habilitar la conmutación de sitios automática no planificada: `metrocluster modify -auto -switchover-failure-domain auso-on-cluster-disaster`

2. Validar la configuración de MetroCluster: `metrocluster check run`

Habilite y revierte las LIF a los puertos de inicio después de una reversión

Durante un reinicio, es posible que algunas LIF se hayan migrado a sus puertos de conmutación al respaldo asignados. Después de revertir un clúster, debe habilitar y revertir cualquier LIF que no esté en sus puertos iniciales.

El comando network interface revert revierte una LIF que no está actualmente de su puerto de inicio a su puerto de inicio, siempre y cuando el puerto de inicio esté operativo. Cuando se crea la LIF, se especifica el puerto inicial de una LIF; puede determinar el puerto inicial de una LIF mediante el comando network interface show.

1. Mostrar el estado de todas las LIF: `network interface show`

   Este ejemplo muestra el estado de todas las LIF de una máquina virtual de almacenamiento (SVM).

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001    down/down  192.0.2.120/24     node0         e0e
true
            data002    down/down  192.0.2.121/24     node0         e0f
true
            data003    down/down  192.0.2.122/24     node0         e2a
true
            data004    down/down  192.0.2.123/24     node0         e2b
true
            data005    down/down  192.0.2.124/24     node0         e0e
false
            data006    down/down  192.0.2.125/24     node0         e0f
false
            data007    down/down  192.0.2.126/24     node0         e2a
false
            data008    down/down  192.0.2.127/24     node0         e2b
false
8 entries were displayed.
```

   Si alguna LIF aparece con el estado Status Admin de down o with an is home status de false, continúe con el siguiente paso.

2. Habilite las LIF de datos: `network interface modify {-role data} -status-admin up`

```
cluster1::> network interface modify {-role data} -status-admin up
8 entries were modified.
```

3. Revertir los LIF a sus puertos raíz: `network interface revert *`

   Este comando revierte todas las LIF a sus puertos principales.

```
cluster1::> network interface revert *
8 entries were acted on.
```

4. Compruebe que todas las LIF se encuentran en sus puertos de inicio: `network interface show`

   Este ejemplo muestra que todas las LIF para SVM vs0 están en sus puertos iniciales.

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0         e0e
true
            data002      up/up    192.0.2.121/24     node0         e0f
true
            data003      up/up    192.0.2.122/24     node0         e2a
true
            data004      up/up    192.0.2.123/24     node0         e2b
true
            data005      up/up    192.0.2.124/24     node1         e0e
true
            data006      up/up    192.0.2.125/24     node1         e0f
true
            data007      up/up    192.0.2.126/24     node1         e2a
true
            data008      up/up    192.0.2.127/24     node1         e2b
true
8 entries were displayed.
```

Habilite las políticas de copia Snapshot después de revertir

Después de revertir a una versión anterior de ONTAP, debe habilitar las políticas de

copia de Snapshot para comenzar de nuevo a crear copias de Snapshot.

Es posible volver a habilitar las programaciones de Snapshot que se deshabilitaron antes de revertir a una versión anterior de ONTAP.

1. Habilite políticas de copia Snapshot para todas las SVM de datos:

   ```
   volume snapshot policy modify -vserver * -enabled true

   snapshot policy modify pg-rpo-hourly -enable true
   ```

2. Para cada nodo, habilite la normativa de copia Snapshot del volumen raíz mediante el comando run-nodenodenodenamevol optionsroot_vol_namenosnap off.

   ```
   cluster1::> run -node node1 vol options vol0 nosnap off
   ```

Verificar el acceso del cliente (SMB y NFS)

Para los protocolos configurados, probar el acceso desde los clientes SMB y NFS para verificar que se pueda acceder al clúster.

Verifique las entradas del firewall IPv6

Una nueva versión de cualquier versión de ONTAP 9 podría resultar en que falten entradas predeterminadas del firewall IPv6 para algunos servicios en las políticas del firewall. Debe comprobar que las entradas de firewall necesarias se han restaurado en el sistema.

1. Compruebe que todas las directivas de firewall son correctas comparándolas con las directivas predeterminadas: `system services firewall policy show`

   En el siguiente ejemplo, se muestran las políticas predeterminadas:

```
cluster1::*> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
                 rsh        allow  0.0.0.0/0
                 snmp       allow  0.0.0.0/0
                 ssh        allow  0.0.0.0/0
                 telnet     allow  0.0.0.0/0
data
                 dns        allow  0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       allow  0.0.0.0/0, ::/0
                 ntp        deny   0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
.
.
.
```

2. Agregue manualmente todas las entradas predeterminadas del firewall IPv6 que falten creando una nueva política de firewall: `system services firewall policy create`

```
cluster1::*> system services firewall policy create -policy newIPv6
-service ssh -action allow -ip-list ::/0
```

3. Aplique la nueva política a la LIF para permitir el acceso a un servicio de red: `network interface modify`

```
cluster1::*> network interface modify -vserver VS1 -lif LIF1
-firewall-policy newIPv6
```

Revertir la función hash de contraseña al tipo de cifrado admitido

Si vuelve de ONTAP 9.1 o ONTAP 9.0 a ONTAP 8.3.x, los usuarios de cuentas SHA-2 ya no pueden autenticarse con sus contraseñas. Las contraseñas deben restablecerse para utilizar el tipo de cifrado MDS.

1. Establezca una contraseña temporal para cada cuenta de usuario SHA-2 que usted tenga identificado

antes de la reversión: `security login password -username user_name -vserver vserver_name`

2. Comunique la contraseña temporal a los usuarios afectados y haga que inicien sesión a través de una consola o sesión SSH para cambiar sus contraseñas según lo indique el sistema.

Consideraciones que tener en cuenta si actualizar manualmente el firmware del SP

Si la funcionalidad de actualización automática del SP está habilitada (por defecto), la degradación o la reversión a ONTAP 8.3.x no requiere una actualización manual del firmware del SP. El firmware del SP se actualiza automáticamente a la versión compatible más reciente compatible, compatible con la versión de ONTAP a la que se revierte o degradó.

Si la funcionalidad de actualización automática del SP está deshabilitada (no se recomienda), una vez que se complete el proceso de reversión o degradación de ONTAP, debe actualizar manualmente el firmware del SP a una versión compatible con la versión de ONTAP a la que se revierte o se degrada.

"Matriz de compatibilidad de BIOS/ONTAP de NetApp"

"Descargas de NetApp: Diagnóstico y firmware del sistema"

Cambio en las cuentas de usuario que pueden acceder a Service Processor

Si creó cuentas de usuario en ONTAP 9.8 o una versión anterior, actualice a ONTAP 9.9.1 o una versión posterior (cuando la `-role` parámetro se cambia a. `admin`), y luego volvió a ONTAP 9.8 o anterior, el `-role` el parámetro se restaura a su valor original. No obstante, debe verificar que los valores modificados sean aceptables.

Durante la reversión, si se ha eliminado el rol de un usuario del SP, se registrará el mensaje "rbac.spuser.role.notfound" EMS".

Para obtener más información, consulte "Cuentas que pueden acceder al SP".

Información de copyright

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

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

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

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

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

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

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

Información de la marca comercial

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