



Utilice comandos para sustituir la controladora del sistema para actualizar el hardware de la controladora introducido en ONTAP 9.15.1

Upgrade controllers

NetApp
July 05, 2024

Tabla de contenidos

Utilice comandos para sustituir la controladora del sistema para actualizar el hardware de la controladora introducido en ONTAP 9.15.1 1

- Descripción general 1
- Automatice el proceso de actualización de la controladora 2
- Decida si desea utilizar el procedimiento de reubicación de agregados 2
- Herramientas y documentación necesarias 3
- Directrices para actualizar controladoras con ARL 3
- Descripción general de la actualización de ARL 4
- Etapa 1. Prepare la actualización 7
- Fase 2. Reubicar y retirar el nodo 1 12
- Etapa 3. Instale y arranque el nodo 3 16
- Etapa 4. Reubicar y retirar el 2 35
- Etapa 5. Instale y arranque el nodo 4 38
- Etapa 6. Complete la actualización 58
- Solucionar problemas 66
- Referencias 72

Utilice comandos para sustituir la controladora del sistema para actualizar el hardware de la controladora introducido en ONTAP 9.15.1

Descripción general

Este procedimiento describe cómo actualizar el hardware de la controladora mediante la reubicación de agregados (ARL) para las siguientes configuraciones del sistema:

Método	Versión de ONTAP	Sistemas compatibles
Uso <code>system controller replace</code> comandos	9.15.1 o posterior	"Enlace a la matriz de sistemas admitidos"



No puede utilizar este procedimiento para actualizar una configuración de IP o FC de MetroCluster. Para actualizar una configuración de MetroCluster, consulte ["Referencias"](#) para vincular a la documentación *Actualización y ampliación de MetroCluster*.

Durante el procedimiento, debe actualizar el hardware de la controladora original con el hardware de la controladora de reemplazo y, de este modo, reubicar la propiedad de agregados que no son raíz. Puede migrar agregados varias veces de nodo a nodo para confirmar que al menos un nodo está sirviendo datos desde los agregados a través del procedimiento de actualización. También puede migrar las interfaces lógicas de datos (LIF) y asignar los puertos de red de la nueva controladora a los grupos de interfaces a medida que continúa.

Terminología utilizada en esta información

En esta información, los nodos originales reciben el nombre de "nodo 1" y "nodo 2", mientras que los nuevos se denominan "nodo 3" y "nodo 4". Durante el procedimiento descrito, el nodo 1 se reemplaza por nodo 3, y el nodo 2 se reemplaza por nodo 4.

Los términos "1", "2", "nodo 3" y "nodo 4" solo se usan para distinguir entre los nodos originales y los nuevos. Cuando siga el procedimiento, deberá sustituir los nombres reales de los nodos originales y los nuevos. Sin embargo, en realidad los nombres de los nodos no cambian: El nodo 3 tiene el nombre 1-nodo y el nodo 4 tiene el nombre 2 después de actualizar el hardware de la controladora.

Información importante:

- Este procedimiento es complejo y asume que tiene habilidades avanzadas de administración de ONTAP. Usted también debe leer y entender el ["Directrices para actualizar controladoras con ARL"](#) y la ["Descripción general de la actualización de ARL"](#) secciones antes de comenzar la actualización.
- En este procedimiento se asume que el hardware de la controladora de reemplazo es nuevo y no se ha usado. En este procedimiento no se incluyen los pasos necesarios para preparar las controladoras usadas con `wipeconfig` el comando. Debe ponerse en contacto con el soporte técnico si se utilizó previamente el hardware de la controladora de reemplazo.
- Puede usar este procedimiento para actualizar el hardware de la controladora en clústeres con más de dos nodos; sin embargo, debe realizar el procedimiento por separado para cada pareja de alta disponibilidad (ha) del clúster.
- Cuando actualiza a un sistema AFF A70, AFF A90 o AFF A1K introducido en ONTAP 9.15.1, ONTAP convierte la eficiencia del almacenamiento de todos los volúmenes existentes con thin provisioning,

incluidos los que no utilizan la eficiencia del almacenamiento, y aplica las nuevas funciones de eficiencia del almacenamiento que utilizan la funcionalidad de descarga del hardware. Se trata de un proceso automático en segundo plano, sin impacto visible en el rendimiento del sistema. "[Leer más](#)"

Automatice el proceso de actualización de la controladora

Durante la actualización de una controladora, se reemplaza la controladora por otra controladora que ejecuta una plataforma más nueva o más potente. Este contenido proporciona los pasos para el procedimiento parcialmente automatizado, que utiliza comprobaciones automáticas de accesibilidad de puertos de red para simplificar aún más la experiencia de actualización de la controladora.

Decida si desea utilizar el procedimiento de reubicación de agregados

En este procedimiento se describe cómo actualizar las controladoras de almacenamiento en una pareja de alta disponibilidad con nuevas controladoras a la vez que se conservan los datos y los discos existentes. Se trata de un procedimiento complejo que sólo deben ser utilizados por administradores con experiencia.

Puede utilizar este procedimiento en las siguientes circunstancias:

- Utiliza ONTAP 9.15.1 o una versión posterior.
- No quiere añadir las nuevas controladoras como una nueva pareja de alta disponibilidad al clúster y migrar los datos mediante el procedimiento de movimiento de volúmenes.
- Tiene experiencia en la administración de ONTAP y se siente cómodo con los riesgos de trabajar en el modo de privilegios de diagnóstico.



Puede usar el cifrado de almacenamiento de NetApp (NSE), el cifrado de volúmenes de NetApp (NVE) y el cifrado de agregados de NetApp (NAE) con este procedimiento.

No puede utilizar este procedimiento en las siguientes circunstancias:

- Va a actualizar un AFF A800 a un AFF A70 o AFF A90. Para realizar esta actualización de AFF A800, consulte "[Referencias](#)" el enlace a comandos *use «system controller replace» para actualizar los modelos de controladoras en el mismo chasis.*
- Va a actualizar un sistema V-Series o un sistema de almacenamiento de virtualización de FlexArray a través de una cabina externa para almacenamiento back-end. Póngase en contacto con el soporte técnico para obtener opciones para actualizar un sistema V-Series o FlexArray.
- Va a actualizar una configuración IP o FC MetroCluster. Para actualizar una configuración de MetroCluster, consulte "[Referencias](#)" para vincular a la documentación *Actualización y ampliación de MetroCluster.*

La siguiente tabla muestra la matriz de modelo admitida para la actualización del controlador.

Controladora existente	Controladora de reemplazo
AFF A300	AFF A70, AFF A90 y AFF A1K
AFF A400	AFF A70, AFF A90 y AFF A1K

Controladora existente	Controladora de reemplazo
AFF A700	AFF A70, AFF A90 y AFF A1K
AFF A900	AFF A90 y AFF A1K



AFF A70 y AFF A90 son sistemas integrados con discos internos. Las dos controladoras y los discos están en un único chasis. No es posible actualizar un sistema existente si las nuevas controladoras tienen unidades internas.

Si la combinación del modelo de actualización de la controladora no se encuentra en la tabla anterior, póngase en contacto con el soporte técnico.

Si prefiere un método diferente de actualización del hardware de la controladora y desea realizar movimientos de volúmenes, consulte ["Referencias"](#) Para enlazar con *Upgrade moviendo volúmenes o Storage*.

Consulte ["Referencias"](#) Para establecer un enlace al centro de documentación de *ONTAP 9*, donde puede acceder a la documentación de producto de *ONTAP 9*.

Herramientas y documentación necesarias

Debe disponer de herramientas específicas para instalar el nuevo hardware y debe consultar otros documentos durante el proceso de actualización.

Se necesitan las siguientes herramientas para realizar la actualización:

- Correa de conexión a tierra
- Destornillador Phillips número 2

Vaya a la ["Referencias"](#) para acceder a la lista de documentos de referencia y sitios de referencia necesarios para esta actualización

Directrices para actualizar controladoras con ARL

Para comprender si puede utilizar ARL para actualizar un par de controladoras que ejecuten *ONTAP 9.15.1* o posterior depende de la plataforma y de la configuración de las controladoras originales y de sustitución.

Actualizaciones compatibles de ARL

Antes de actualizar un par de nodos mediante este procedimiento ARL, revise los siguientes requisitos para asegurarse de que la configuración es compatible:

- Compruebe que ARL se puede realizar en los controladores originales y de sustitución.
- Compruebe el tamaño de todos los agregados definidos y el número de discos que admite el sistema original. A continuación, puede comparar los tamaños de agregado y el número de discos que admiten el tamaño del agregado y el número de discos que admite el nuevo sistema. Consulte ["Referencias"](#) el enlace a *Hardware Universe* donde está disponible esta información. El tamaño de agregado y el número de discos que admite el nuevo sistema deben ser iguales o mayores que el tamaño del agregado y el número de discos que admite el sistema original.

- Valide en las reglas de combinación de clústeres si los nodos nuevos pueden formar parte del clúster con los nodos existentes cuando se sustituye la controladora original. Para obtener más información sobre las reglas de mezcla de clústeres, consulte ["Referencias"](#) el enlace a *Hardware Universe*.
- Migre y vuelva a alojar los LIF de clúster a dos puertos de clúster por nodo si tiene un sistema, como un AFF 700, con la siguiente configuración:
- Más de dos puertos de clúster por nodo
- Una tarjeta de interconexión de clúster en slot4 en modo de partición para crear los puertos E4A, e4b, e4c y e4d, y los puertos E4E, e4f, e4g y e4h



Si se realiza una actualización de la controladora con más de dos puertos de clúster por nodo, es posible que falten LIF de clúster en la nueva controladora después de la actualización.

Para obtener más información, consulte el artículo de la base de conocimientos ["Cómo eliminar LIF de clúster no deseadas o innecesarias"](#).

La actualización de la controladora mediante ARL es compatible en sistemas configurados con volúmenes de SnapLock Enterprise y SnapLock Compliance.

Clústeres de dos nodos sin switches

Si va a actualizar nodos en un clúster sin switches de dos nodos, puede dejar los nodos en el clúster sin switches mientras realiza la actualización. No es necesario convertirlos en un clúster con switches.

ARL no admite actualizaciones

No es posible actualizar controladoras de reemplazo que no admiten las bandejas de discos conectadas a las controladoras originales.

Consulte ["Referencias"](#) Para establecer un vínculo con el *Hardware Universe* para obtener información sobre soporte de disco.

Si desea actualizar controladoras de nivel básico con unidades internas, consulte link to ["Referencias"](#) *Upgrade moviendo volúmenes o almacenamiento* y vaya al procedimiento *Actualizar un par de nodos que ejecutan Clustered Data ONTAP moviendo volúmenes*.

Solucionar problemas

Si se produce algún problema durante la actualización de las controladoras, consulte ["Solucionar problemas"](#) para obtener más información y posibles soluciones.

Si no encuentra ninguna solución al problema que encontró, póngase en contacto con el soporte técnico.

Descripción general de la actualización de ARL

Antes de actualizar los nodos mediante ARL, debe comprender cómo funciona el procedimiento. En este contenido, el procedimiento se divide en varias etapas.

Actualice el par de nodos

Para actualizar la pareja de nodos, debe preparar los nodos originales y realizar una serie de pasos en los nodos original y en los nuevos. A continuación, puede retirar los nodos originales.

Información general sobre la secuencia de actualizaciones de ARL

Durante el procedimiento, debe actualizar el hardware de la controladora original con el hardware de la controladora de reemplazo, una controladora cada vez, aprovechando la configuración de par de alta disponibilidad para reubicar la propiedad de agregados que no son raíz. Todos los agregados que no son raíz deben pasar por dos reubicaciones para llegar a su destino final, que es el nodo actualizado correcto.

Cada agregado tiene un propietario particular y un propietario actual. El propietario del hogar es el propietario real del agregado, y el propietario actual es el propietario temporal.

La siguiente tabla describe las tareas de alto nivel que realiza durante cada etapa y el estado de propiedad del agregado al final de la etapa. Los pasos detallados se proporcionan más adelante en el procedimiento:

Etapa	Descripción
"Etapa 1. Prepare la actualización"	<p>Durante la fase 1, realizará comprobaciones previas y, si fuera necesario, corrija la propiedad del agregado. Debe registrar determinada información si gestiona el cifrado del almacenamiento mediante OKM y puede optar por desactivar las relaciones de SnapMirror.</p> <p>Propiedad del agregado al final de la fase 1:</p> <ul style="list-style-type: none">• El nodo 1 es el propietario raíz y el propietario actual de los agregados del nodo 1.• El nodo 2 es el propietario particular y el propietario actual de los agregados del nodo 2.
"Fase 2. Reubicar y retirar el nodo 1"	<p>Durante la fase 2, debe reubicar agregados no raíz y LIF de datos NAS al nodo 1 en el nodo 2. Este proceso está en gran medida automatizado; la operación se pausa para permitir comprobar su estado. Debe reanudar manualmente la operación. Si es necesario, reubique los agregados que han fallado o que han vetado. Antes de retirar el nodo 1, registre la información del nodo 1 para su uso más adelante. También es posible preparar el modo de reiniciar el sistema de los nodos 3 y los nodos 4 más adelante en el procedimiento.</p> <p>Propiedad del agregado al final de la fase 2:</p> <ul style="list-style-type: none">• El nodo 2 es el propietario actual de los agregados del nodo 1.• El nodo 2 es el propietario particular y el propietario actual de agregados del nodo 2.

Etapa	Descripción
<p>"Etapa 3. Instale y arranque el nodo 3"</p>	<p>Durante la fase 3, debe instalar y arrancar el nodo 3, compruebe que los puertos de gestión del nodo y del clúster del nodo 1 estén en línea en el nodo 3 y verifique la instalación del nodo 3. Si utiliza el cifrado de volúmenes de NetApp (NVE), debe restaurar la configuración del gestor de claves. También se deben reubicar los LIF de datos NAS del nodo 1 y los agregados no raíz del nodo 2 al nodo 3, y verificar que las LIF SAN existan en el nodo 3.</p> <p>Propiedad agregada al final de la etapa 3:</p> <ul style="list-style-type: none"> • Node3 es el propietario raíz y el propietario actual de los agregados del nodo 1. • El nodo 2 es el propietario particular y el propietario actual de agregados del nodo 2.
<p>"Etapa 4. Reubicar y retirar el 2"</p>	<p>Durante la fase 4, se reubicarán los agregados no raíz y los LIF de datos NAS del nodo 2 al nodo 3. También puede grabar la información del nodo 2 para utilizarla más adelante en el procedimiento antes de retirar el nodo 2.</p> <p>Propiedad agregada al final de la etapa 4:</p> <ul style="list-style-type: none"> • Node3 es el propietario raíz y el propietario actual de los agregados que originalmente pertenecían al nodo 1. • El nodo 2 es el propietario en casa de los agregados 2. • El nodo 3 es el propietario actual de agregados de 2 nodos.
<p>"Etapa 5. Instale y arranque el nodo 4"</p>	<p>Durante la fase 5, debe instalar y arrancar el nodo 4, compruebe que los puertos de gestión del clúster y de los nodos del nodo 2 estén en línea en el nodo 4 y verifique la instalación del nodo 4. Si utiliza NVE, debe restaurar la configuración del gestor de claves. También se deben reubicar los LIF de datos NAS 2 y los agregados no raíz de nodo 3 a nodo 4, y verificar que las LIF SAN existan en el nodo 4.</p> <p>Propiedad agregada al final de la etapa 5:</p> <ul style="list-style-type: none"> • Nodo 3 es el propietario raíz y el propietario actual de los agregados que originalmente pertenecían al nodo 1. • Node4 es el propietario nacional y el propietario actual de agregados que pertenecía originalmente al nodo 2.
<p>"Etapa 6. Complete la actualización"</p>	<p>Durante la fase 6, confirme que los nodos nuevos están configurados correctamente y, si los nodos nuevos tienen la función de cifrado habilitada, debe configurar y configurar el cifrado de almacenamiento o NVE. También debe retirar los nodos antiguos y reanudar las operaciones de SnapMirror.</p>

Etapa 1. Prepare la actualización

Descripción general de la etapa 1

Durante la fase 1, realizará comprobaciones previas y, si fuera necesario, corrija la propiedad del agregado. También registra cierta información si gestiona el cifrado del almacenamiento mediante el administrador de claves incorporado y puede optar por desactivar las relaciones de SnapMirror.

Pasos

1. ["Prepare los nodos para la actualización"](#)
2. ["Gestione el cifrado del almacenamiento con el gestor de claves incorporado"](#)

Prepare los nodos para la actualización

El proceso de reemplazo de la controladora comienza con una serie de comprobaciones previas. También se recopila información sobre los nodos originales para usar más adelante del procedimiento y, si es necesario, determinar el tipo de unidades de cifrado automático que se están usando.

Pasos

1. Inicie el proceso de sustitución de la controladora con el siguiente comando en la línea de comandos de ONTAP:

```
system controller replace start -nodes <node_names>
```



Solo puede ejecutar el comando `system controller replace start` en el nivel de privilegio avanzado: `set -privilege advanced`

Verá un resultado similar al siguiente ejemplo. La salida muestra la versión de ONTAP que se ejecuta en el clúster:

Warning: 1. Current ONTAP version is 9.15.1

2. Verify that NVMEM or NVRAM batteries of the new nodes are charged, and charge them if they are not. You need to physically check the new nodes to see if the NVMEM or NVRAM batteries are charged. You can check the battery status either by connecting to a serial console or using SSH, logging into the Service Processor (SP) or Baseboard Management Controller (BMC) for your system, and use the system sensors to see if the battery has a sufficient charge.

Attention: Do not try to clear the NVRAM contents. If there is a need to clear the contents of NVRAM, contact NetApp technical support.

3. If a controller was previously part of a different cluster, run wipeconfig before using it as the replacement controller.

4. Note: This is not a MetroCluster configuration. Controller replacement supports only ARL based procedure.

Do you want to continue? {y|n}: y

2. Pulse `y`, verá la siguiente salida:

```
Controller replacement operation: Prechecks in progress.  
Controller replacement operation has been paused for user intervention.
```

El sistema ejecuta las siguientes comprobaciones previas; registre la salida de cada comprobación previa para utilizarla más adelante en el procedimiento:

Comprobación previa	Descripción
Comprobación del estado del clúster	Comprueba todos los nodos del clúster para confirmar que están en buen estado.
Comprobación del estado de reubicación de agregados	Comprueba si ya hay una reubicación de agregados en curso. Si hay otra reubicación de agregado en curso, la comprobación falla.
Comprobación del nombre del modelo	Comprueba si los modelos de controlador son compatibles con este procedimiento. Si los modelos no son compatibles, la tarea falla.
Comprobación de quórum de clúster	Comprueba que los nodos que se van a sustituir tengan quórum. Si los nodos no están en quórum, la tarea falla.

Comprobación previa	Descripción
Comprobación de la versión de la imagen	Comprueba que los nodos que se reemplazan ejecuten la misma versión de ONTAP. Si las versiones de la imagen ONTAP son diferentes, la tarea fallará. Los nodos nuevos deben tener la misma versión de ONTAP 9.x instalada en ellos que se haya instalado en los nodos originales. Si los nodos nuevos tienen instalada una versión diferente de ONTAP, debe reiniciar el sistema las controladoras nuevas después de instalarlas. Para obtener instrucciones sobre cómo actualizar ONTAP, consulte "Referencias" Para enlazar a <i>Upgrade ONTAP</i> .
Comprobación de estado de HA	Comprueba si los dos nodos que se van a reemplazar se encuentran en una configuración de parejas de alta disponibilidad. Si no está habilitada la conmutación por error del almacenamiento para las controladoras, la tarea falla.
Comprobación del estado del agregado	Si los nodos que se van a sustituir tienen agregados propios para los que no son el propietario principal, la tarea fallará. Los nodos no deben tener ningún agregado que no sea local.
Comprobación del estado del disco	Si alguno de los nodos que se van a reemplazar tiene discos ausentes o con errores, la tarea falla. Si falta algún disco, consulte "Referencias" Para establecer un vínculo a la gestión de discos y agregados con la CLI, <i>administración de almacenamiento lógico con la CLI y Administración de alta disponibilidad</i> para configurar el almacenamiento para el par de alta disponibilidad.
Comprobación del estado de LIF de datos	Comprueba si alguno de los nodos que se van a reemplazar tiene LIF de datos no locales. Los nodos no deben contener ninguna LIF de datos para la cual no sean el propietario principal. Si uno de los nodos contiene LIF de datos no locales, la tarea falla.
Estado de LIF del clúster	Comprueba si los LIF del clúster están activos para ambos nodos. Si las LIF del clúster están inadas, la tarea falla.
Comprobación del estado de ASUP	Si no se configuran las notificaciones de ASUP, la tarea falla. Debe habilitar ASUP antes de iniciar el procedimiento de reemplazo de controladora.
Comprobación del uso de CPU	Comprueba si el uso de CPU es superior al 50 % en el caso de cualquiera de los nodos que se van a sustituir. Si el uso de CPU es superior al 50 % durante un período de tiempo considerable, la tarea falla.
Comprobación de reconstrucción de agregados	Comprueba si la reconstrucción se está produciendo en algún agregado de datos. Si la reconstrucción del agregado está en curso, la tarea falla.
Comprobación de trabajo de afinidad de nodo	Comprueba si se están ejecutando trabajos de afinidad de nodos. Si se están ejecutando trabajos de afinidad de nodo, la comprobación falla.

- Una vez iniciada la operación de sustitución de la controladora y que se completen las comprobaciones previas, la operación se coloca en pausa para recoger información de resultado que se pueda necesitar más adelante al configurar el nodo 3.

Antes de iniciar la actualización, migra y vuelve a alojar los LIF de clúster en dos puertos de clúster por nodo si tiene un sistema, como un AFF 700, con la siguiente configuración:

- Más de dos puertos de clúster por nodo
- Una tarjeta de interconexión de clúster en slot4 en modo de partición para crear los puertos E4A, e4b, e4c y e4d, y los puertos E4E, e4f, e4g y e4h



Si se realiza una actualización de la controladora con más de dos puertos de clúster por nodo, es posible que falten LIF de clúster en la nueva controladora después de la actualización.

Para obtener más información, consulte el artículo de la base de conocimientos "[Cómo eliminar LIF de clúster no deseadas o innecesarias](#)".

4. Ejecute el siguiente conjunto de comandos según lo indicado por el procedimiento de reemplazo de la controladora en la consola del sistema.

Desde el puerto serie conectado a cada nodo, ejecute y guarde el resultado de los siguientes comandos de forma individual:

- `vserver services name-service dns show`
- `network interface show -curr-node <local> -role <cluster,intercluster,node-mgmt,cluster-mgmt,data>`
- `network port show -node <local> -type physical`
- `service-processor show -node <local> -instance`
- `network fcp adapter show -node <local>`
- `network port ifgrp show -node <local>`
- `system node show -instance -node <local>`
- `run -node <local> sysconfig`
- `storage aggregate show -r`
- `storage aggregate show -node <local>`
- `volume show -node <local>`
- `system license show -owner <local>`
- `storage encryption disk show`
- `security key-manager onboard show-backup`
- `security key-manager external show`
- `security key-manager external show-status`
- `network port reachability show -detail -node <local>`



Si se está utilizando el cifrado de volúmenes de NetApp (NVE) o el cifrado de agregado de NetApp (NAE) con el gestor de claves incorporado (OKM), mantenga la frase de acceso del administrador de claves preparada para completar el administrador de claves para resincronizar más adelante en el procedimiento.

5. Si su sistema utiliza unidades de autocifrado, consulte el artículo de la base de conocimientos "[Cómo saber si una unidad tiene la certificación FIPS](#)" Para determinar el tipo de unidades de autocifrado que se están utilizando en la pareja de alta disponibilidad que se está actualizando. El software ONTAP admite dos tipos de unidades de autocifrado:

- Unidades SAS o NVMe con cifrado en almacenamiento de NetApp (NSE) certificado FIPS
- Unidades NVMe (SED) con autocifrado no FIPS

["Obtenga más información sobre las unidades de autocifrado compatibles"](#).

Corrija la propiedad del agregado si fallan las comprobaciones previas de ARL

Si falla la comprobación del estado del agregado, debe devolver los agregados propiedad del nodo asociado al nodo propietario principal e iniciar de nuevo el proceso de comprobaciones previas.

Pasos

1. Devolver los agregados que actualmente pertenecen al nodo asociado al nodo propietario principal:

```
storage aggregate relocation start -node source_node -destination destination_node -aggregate-list *
```

2. Compruebe que ni el nodo 1 ni el nodo 2 siguen teniendo agregados cuyos propietarios son actualmente (pero no el propietario del hogar):

```
storage aggregate show -nodes node_name -is-home false -fields owner-name, home-name, state
```

En el ejemplo siguiente se muestra el resultado del comando cuando un nodo es al mismo tiempo el propietario actual y el propietario principal de los agregados:

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields owner-name,home-name,state
aggregate   home-name  owner-name  state
-----
aggr1       node1      node1       online
aggr2       node1      node1       online
aggr3       node1      node1       online
aggr4       node1      node1       online

4 entries were displayed.
```

Después de terminar

Debe reiniciar el proceso de sustitución de la controladora:

```
system controller replace start -nodes node_names
```

Licencia

Si quiere información detallada sobre las licencias de ONTAP, consulte ["Gestión de licencias"](#).



El uso de funciones sin licencia en la controladora puede provocar que no cumpla el contrato de licencia.

Gestione el cifrado del almacenamiento con el gestor de claves incorporado

Puede utilizar Onboard Key Manager (OKM) para gestionar las claves de cifrado. Si tiene configurado OKM, debe registrar la frase de acceso y el material de copia de seguridad antes de iniciar la actualización.

Pasos

1. Registre la clave de acceso para todo el clúster.

Esta es la frase de acceso que se introdujo cuando se configuró o actualizó OKM con la CLI o la API REST.

2. Ejecute el para realizar un backup de la información del gestor de claves `security key-manager onboard show-backup` comando.

Desactivar las relaciones de SnapMirror (opcional)

Antes de continuar con el procedimiento, debe confirmar que todas las relaciones de SnapMirror se ponen en modo inactivo. Cuando una relación de SnapMirror se pone en modo inactivo, sigue en modo inactivo tras reinicios y recuperaciones tras fallos.

Pasos

1. Compruebe el estado de la relación de SnapMirror en el clúster de destino:

```
snapmirror show
```



Si el estado es "transferencia", debe anular dichas transferencias:
`snapmirror abort -destination-vserver vserver_name`

La anulación falla si la relación de SnapMirror no se encuentra en el estado "transfiriendo".

2. Desactive todas las relaciones entre el clúster:

```
snapmirror quiesce -destination-vserver *
```

Fase 2. Reubicar y retirar el nodo 1

Descripción general de la etapa 2

Durante la fase 2, debe reubicar agregados no raíz y LIF de datos NAS al nodo 1 en el nodo 2. Este proceso está en gran medida automatizado; la operación se pausa para permitir comprobar su estado. Debe reanudar manualmente la operación. Si es necesario, reubique los agregados que han fallado o que han vetado. También registra la

información necesaria de node1, retira node1 y prepara netboot node3 y node4 más adelante en el procedimiento.

Pasos

1. "Reubique los agregados que no son raíz y los LIF de datos NAS que pertenecen al nodo 1 al nodo 2"
2. "Se han producido fallos en la reubicación o los agregados vetados"
3. "Retire el nodo 1"
4. "Prepárese para el arranque desde el red"

Reubique los agregados que no son raíz y los LIF de datos NAS que pertenecen al nodo 1 al nodo 2

Antes de poder sustituir el nodo 1 por el nodo 3, debe mover los agregados que no son raíz y las LIF de datos NAS del nodo 1 al nodo 2 antes de mover, en última instancia, los recursos del nodo 1 al nodo 3.

Antes de empezar

La operación ya se debe poner en pausa cuando se inicia la tarea, por lo que se debe reanudar manualmente.

Acerca de esta tarea

Una vez migrados los agregados y las LIF, la operación se coloca en pausa con fines de verificación. En este momento, debe verificar si todos los agregados que no son raíz y los LIF de datos no SAN se migran al nodo 3.



El propietario principal de los agregados y las LIF no está modificado; solo se modifica el propietario actual.

Pasos

1. Reanudar las operaciones de movimiento de LIF de datos NAS y reubicación de agregados:

```
system controller replace resume
```

Todos los agregados que no son raíz y los LIF de datos NAS están migrados del nodo 1 al nodo 2.

La operación se pone en pausa para permitir verificar si todos los agregados que no son raíz del nodo 1 y las LIF de datos que no son SAN se han migrado al nodo 2.

2. Comprobar el estado de las operaciones de reubicación de agregados y movimiento de LIF de datos de NAS:

```
system controller replace show-details
```

3. Con la operación en pausa, verifique que todos los agregados que no son raíz estén en línea para su estado en el nodo 2:

```
storage aggregate show -node node2 -state online -root false
```

En el ejemplo siguiente, los agregados no raíz en el nodo 2 están en línea:

```
cluster::> storage aggregate show -node node2 state online -root false
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID Status
aggr_1	744.9GB	744.8GB	0%	online	5	node2	raid_dp,normal
aggr_2	825.0GB	825.0GB	0%	online	1	node2	raid_dp,normal

2 entries were displayed.

Si los agregados se encuentran sin conexión o en estado no externo en el nodo 2, deben estar en línea usando el siguiente comando en el nodo 2, una vez para cada agregado:

```
storage aggregate online -aggregate aggr_name
```

4. Verifique que todos los volúmenes estén en línea en el nodo 2 mediante el siguiente comando en el nodo 2 y examinar su salida:

```
volume show -node node2 -state offline
```

Si alguno de los volúmenes está sin conexión en el nodo 2, debe volver a ponerlos en línea usando el siguiente comando en el nodo 2, una vez para cada volumen:

```
volume online -vserver vserver_name -volume volume_name
```

La *vserver_name* para utilizarlo con este comando se encuentra en el resultado del anterior `volume show` comando.

5. Si alguna LIF está inactiva, establezca el estado administrativo de las LIF en up Con el siguiente comando, una vez para cada LIF:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node nodename -status-admin up
```

Se han producido fallos en la reubicación o los agregados vetados

Si alguno de los agregados no se puede reubicar o vetar, debe reubicar los agregados manualmente o, si es necesario, anular los vetos o las comprobaciones de destino.

Acerca de esta tarea

La operación de reubicación se pondrá en pausa debido al error.

Pasos

1. Compruebe los registros del sistema de gestión de eventos (EMS) para determinar por qué no se ha podido reubicar o vetar el agregado.
2. Reubicar agregados que fallen o vetados:

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr_name -ndo-controller-upgrade true
```

3. Cuando se le solicite, introduzca *y*.
4. Puede forzar la reubicación mediante uno de los siguientes métodos:

Opción	Descripción
Anulación de las comprobaciones de veto	Utilice el siguiente comando: <pre>storage aggregate relocation start -node <i>node1</i> -destination <i>node2</i> -aggregate-list <i>aggr_list</i> -ndo -controller-upgrade true -override-vetoes true</pre>
Sobreescribir comprobaciones de destino	Utilice el siguiente comando: <pre>storage aggregate relocation start -node <i>node1</i> -destination <i>node2</i> -aggregate-list <i>aggr_list</i> -ndo -controller-upgrade true -override-vetoes true -override-destination-checks true</pre>

Retire el nodo 1

Para retirar el nodo 1, reanude el funcionamiento automatizado para deshabilitar el par de alta disponibilidad con el nodo 2 y apague correctamente el nodo 1. Más adelante en el procedimiento, quite *node1* del rack o el chasis.

Pasos

1. Reanude la operación:

```
system controller replace resume
```

2. Compruebe que el nodo 1 se ha detenido:

```
system controller replace show-details
```

Después de terminar

Puede decomisionar el nodo 1 cuando finalice la actualización. Consulte ["Retire el sistema antiguo"](#).

Prepárese para el arranque desde el red

Después de montar físicamente en rack los nodos 3 y 4 posteriormente en el procedimiento, es posible que deba volver a arrancar. El término "reiniciar el sistema" significa que se inicia desde una imagen ONTAP almacenada en un servidor remoto. Cuando se prepara para el arranque por red, se coloca una copia de la imagen de arranque de ONTAP 9 en un servidor web al que el sistema pueda acceder.

También puede utilizar la opción de arranque USB para realizar un arranque desde el sistema. Consulte el artículo de la base de conocimientos ["Cómo utilizar el comando boot_recovery LOADER para instalar ONTAP para la configuración inicial de un sistema"](#).

Antes de empezar

- Compruebe que puede acceder a un servidor HTTP con el sistema.
- Consulte "[Referencias](#)" Para crear un enlace al *sitio de soporte de NetApp* y descargar los archivos del sistema necesarios para su plataforma y la versión correcta de ONTAP.

Acerca de esta tarea

Debe reiniciar el sistema de las controladoras nuevas si no tienen la misma versión de ONTAP 9 instalada en ellas que se instala en las controladoras originales. Tras instalar cada controladora nueva, arranque el sistema desde la imagen de ONTAP 9 almacenada en el servidor web. A continuación, puede descargar los archivos correctos en el dispositivo multimedia de arranque para posteriores arranques del sistema.

Pasos

1. Acceda al sitio de soporte de NetApp para descargar los archivos utilizados para realizar el arranque desde el sistema.
2. Descargue el software ONTAP adecuado de la sección de descarga de software del sitio de soporte de NetApp y almacene el `<ontap_version>_image.tgz` archivo en un directorio accesible a través de la web.
3. Cambie al directorio accesible a la Web y compruebe que los archivos que necesita están disponibles.

La lista de directorios debe contener el siguiente archivo:

`<ontap_version>_image.tgz`



No es necesario extraer el contenido del `<ontap_version>_image.tgz` archivo.

Utilizará la información de los directorios en "[Etapa 3](#)".

Etapa 3. Instale y arranque el nodo 3

Descripción general de la etapa 3

Durante la fase 3, debe instalar y arrancar el nodo 3, compruebe que los puertos de gestión del nodo y del clúster del nodo 1 estén en línea en el nodo 3 y verifique la instalación del nodo 3. Si utiliza el cifrado de volúmenes de NetApp (NVE), debe restaurar la configuración del gestor de claves. También se deben reubicar los LIF de datos NAS del nodo 1 y los agregados no raíz del nodo 2 al nodo 3, y verificar que las LIF SAN existan en el nodo 3.

Pasos

1. "[Instale y arranque el nodo 3](#)"
2. "[Verifique la instalación del nodo 3](#)"
3. "[Restaure la configuración de gestor de claves en el nodo 3](#)"
4. "[Mueva agregados que no son raíz y LIF de datos NAS que pertenecen al nodo 1 del nodo 2 al nodo 3](#)"

Instale y arranque el nodo 3

Instale node3 en el rack, transfiera las conexiones de node1 a node3, arranque node3 e instale ONTAP. A continuación, deberá reasignar cualquiera de los discos de repuesto de

node1, los discos que pertenezcan al volumen raíz y los agregados que no sean raíz que no se hayan reubicado en la versión node2 anteriormente en el proceso, como se explica en esta sección.

Acerca de esta tarea

La operación de reubicación se detiene al principio de esta etapa. Este proceso está en gran medida automatizado; la operación se pausa para permitir comprobar su estado. Debe reanudar manualmente la operación. Además, debe verificar que los LIF SAN se hayan conectado correctamente y estén asignados a los puertos físicos FC correctos en node3.

Es necesario reiniciar el nodo 3 si no tiene la misma versión de ONTAP 9 que está instalada en el nodo 1. Después de instalar el nodo 3, arranque desde la imagen ONTAP 9 almacenada en el servidor web. A continuación, puede descargar los archivos correctos en el dispositivo multimedia de arranque para posteriores arranques del sistema, siguiendo las instrucciones en "[Prepárese para el arranque desde el red](#)".

Pasos

1. Asegúrese de que dispone de espacio en rack para el nodo 3.

Los requisitos de espacio y altura para los nodos nuevos pueden ser diferentes de los existentes. Planifique los requisitos de espacio para el escenario de actualización.

2. instale el nodo 3 en el rack siguiendo las *instrucciones de instalación y configuración* del modelo de nodo.
3. nodo de cable 3, moviendo las conexiones del nodo 1 al nodo 3.

A partir de ONTAP 9.15.1, los nuevos modelos de controladora tienen solo un puerto «llave» para la controladora de gestión de la placa base (BMC) y las conexiones de gestión. Planifique los cambios de cableado en consecuencia.

- Consola (puerto de gestión remota)
- Clúster y puertos de alta disponibilidad
- Puertos de datos
- Puertos de gestión de clústeres y nodos
- SCSI con conexión en serie (SAS) y puertos de almacenamiento Ethernet
- Configuraciones SAN: Puertos Ethernet iSCSI, FC y switch NVMe/FC

Es posible que deba cambiar los cables de interconexión entre las controladoras antigua y nueva para permitir la interoperabilidad entre los distintos modelos de controladora y de tarjeta. Consulte la "[procedimientos de instalación del sistema](#)" para obtener un mapa de cableado de las bandejas de almacenamiento Ethernet de los sistemas.



Para las controladoras incluidas en ONTAP 9.15.1 y versiones posteriores, las interconexiones de clúster y alta disponibilidad utilizan los mismos puertos. Para las configuraciones conectadas por switch, es necesario conectar puertos similares al mismo switch de clúster. Por ejemplo, al actualizar a un AFF A1K desde una controladora existente, debe conectar los puertos e1a de ambos nodos a un switch y los puertos e7a de ambos nodos en el segundo switch.

4. Active la alimentación del nodo 3 y, a continuación, interrumpa el proceso de arranque pulsando Ctrl-C en el terminal de la consola para acceder al indicador de entorno de arranque.



Cuando se arranca el nodo 3, es posible que se muestre el siguiente mensaje de advertencia:

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely because the battery is discharged but could be due to other
temporary conditions.
When the battery is ready, the boot process will complete and services
will be engaged.
To override this delay, press 'c' followed by 'Enter'
```

5. Si aparece el mensaje de advertencia en [Paso 4](#), realice las siguientes acciones:
 - a. Compruebe todos los mensajes de la consola que puedan indicar un problema distinto a una batería NVRAM baja y, si es necesario, realice las acciones correctivas necesarias.
 - b. Deje que la batería se cargue y finalice el proceso de arranque.



Atención: No anular el retardo; si no se permite que la batería se cargue, se podrían producir pérdidas de datos.



Consulte "[Prepárese para el arranque desde el red](#)".

6. Configure la conexión netboot eligiendo una de las siguientes acciones.



Se deben utilizar el puerto e IP de gestión como conexión para reiniciar el sistema. No utilice una IP de LIF de datos ni una interrupción del servicio de datos mientras se realiza la actualización.

Si el protocolo de configuración dinámica de hosts (DHCP) es...	Realice lo siguiente...
Ejecutando	Configure la conexión automáticamente mediante el siguiente comando en el símbolo del sistema del entorno de arranque: <code>ifconfig e0M -auto</code>

Si el protocolo de configuración dinámica de hosts (DHCP) es...	Realice lo siguiente...
No se está ejecutando	<p>Configure manualmente la conexión mediante el siguiente comando en el símbolo del sistema del entorno de arranque:</p> <pre>ifconfig e0M -addr=<i>filer_addr</i> -mask=<i>netmask</i> -gw=<i>gateway</i> -dns=<i>dns_addr</i> -domain=<i>dns_domain</i></pre> <p><i>filer_addr</i> Es la dirección IP del sistema de almacenamiento (obligatorio). <i>netmask</i> es la máscara de red del sistema de almacenamiento (obligatoria). <i>gateway</i> es la puerta de enlace del sistema de almacenamiento (obligatorio). <i>dns_addr</i> Es la dirección IP de un servidor de nombres en la red (opcional). <i>dns_domain</i> Es el nombre de dominio del servicio de nombres de dominio (DNS) (opcional).</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Es posible que sean necesarios otros parámetros para la interfaz. Introduzca <code>help ifconfig</code> en el símbolo del sistema del firmware para obtener detalles.</p> </div>

7. Lleve a cabo netboot en el nodo 3:

```
netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz
```

La <path_to_the_web-accessible_directory> debería conducir al lugar en el que se ha descargado el <ontap_version>_image.tgz en la sección "[Prepárese para el arranque desde el red](#)".

 No interrumpa el arranque.

8. en el menú de inicio, seleccione la opción (7) `Install new software first`.

Esta opción del menú descarga e instala la nueva imagen de ONTAP en el dispositivo de arranque.

Ignore el siguiente mensaje:

```
This procedure is not supported for Non-Disruptive Upgrade on an HA pair
```

La nota se aplica a las actualizaciones no disruptivas de ONTAP, no a las actualizaciones de controladoras.

 Utilice siempre netboot para actualizar el nodo nuevo a la imagen deseada. Si utiliza otro método para instalar la imagen en la nueva controladora, podría instalarse la imagen incorrecta. Este problema se aplica a todas las versiones de ONTAP. El procedimiento para reiniciar el sistema combinado con la opción (7) `Install new software` Limpia el soporte de arranque y coloca la misma versión ONTAP en ambas particiones de imagen.

9. Si se le solicita continuar con el procedimiento, introduzca `y`, Y cuando se le solicite el paquete, escriba la dirección URL:

```
http://<web_server_ip/path_to_web-  
accessible_directory>/<ontap_version>_image.tgz
```

10. Lleve a cabo los siguientes pasos para reiniciar el módulo del controlador:

- a. Introduzca `n` para omitir la recuperación del backup cuando aparezca la siguiente solicitud:

```
Do you want to restore the backup configuration now? {y|n}
```

- b. Introduzca `y` para reiniciar cuando vea el siguiente aviso:

```
The node must be rebooted to start using the newly installed software. Do  
you want to reboot now? {y|n}
```

El módulo del controlador se reinicia pero se detiene en el menú de inicio porque el dispositivo de arranque se ha reformateado y los datos de configuración deben restaurarse.

11. Seleccione el modo de mantenimiento `5` desde el menú de inicio y entrar `y` cuando se le pida que continúe con el arranque.
12. Compruebe que la controladora y el chasis están configurados como ha:

```
ha-config show
```

En el siguiente ejemplo, se muestra el resultado del `ha-config show` comando:

```
Chassis HA configuration: ha  
Controller HA configuration: ha
```



El sistema graba en una PROM tanto si se encuentran en un par ha como en una configuración independiente. El estado debe ser el mismo en todos los componentes del sistema independiente o del par de alta disponibilidad.

13. Si la controladora y el chasis no están configurados como HA, utilice los siguientes comandos para corregir la configuración:

```
ha-config modify controller ha
```

```
ha-config modify chassis ha
```

14. Confirme que todos los puertos Ethernet utilizados para conectarse a las bandejas Ethernet están configurados como almacenamiento:

```
storage port show
```

La salida mostrada depende de la configuración del sistema. El siguiente ejemplo de salida es para un nodo con una única tarjeta de almacenamiento en slot11. La salida del sistema puede ser diferente:

```
*> storage port show
Port Type Mode      Speed (Gb/s) State      Status  VLAN ID
-----
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

15. Modifique los puertos que no están configurados en el almacenamiento:

```
storage port modify -p <port> -m storage
```

Todos los puertos Ethernet conectados a las bandejas de almacenamiento deben estar configurados como almacenamiento para permitir el acceso a los discos y las bandejas.

16. Salga del modo de mantenimiento:

```
halt
```

Interrumpa el arranque automático pulsando `Ctrl-C` en el símbolo del sistema del entorno de arranque.

17. En el nodo 2, compruebe la fecha, la hora y la zona horaria del sistema:

```
date
```

18. En node3, compruebe la fecha mediante el siguiente comando en el símbolo del sistema del entorno de inicio:

```
show date
```

19. Si es necesario, establezca la fecha en node3:

```
set date <mm/dd/yyyy>
```

20. En node3, compruebe la hora con el siguiente comando en el símbolo del sistema del entorno de arranque:

```
show time
```

21. Si es necesario, ajuste la hora en node3:

```
set time <hh:mm:ss>
```

22. En el cargador de arranque, defina el ID del sistema asociado en node3:

```
setenv partner-sysid <node2_sysid>
```

Para nodo 3, `partner-sysid` debe ser del nodo 2.

- a. Guarde los ajustes:

```
saveenv
```

23. Compruebe el `partner-sysid` para el nodo 3:

```
printenv partner-sysid
```

24. Si tiene unidades de cifrado de almacenamiento de NetApp (NSE) instaladas, siga estos pasos.



Si aún no lo ha hecho anteriormente en el procedimiento, consulte el artículo de la base de conocimientos "[Cómo saber si una unidad tiene la certificación FIPS](#)" para determinar el tipo de unidades de autocifrado que están en uso.

a. Configurado `bootarg.storageencryption.support` para `true` o `false`:

Si están en uso las siguientes unidades...	Entonces...
Unidades NSE que cumplen con los requisitos de autocifrado de FIPS 140-2 de nivel 2	<code>setenv bootarg.storageencryption.support true</code>
SED de NetApp no con FIPS	<code>setenv bootarg.storageencryption.support false</code>

b. Vaya al menú de inicio especial y seleccione la opción (10) Set Onboard Key Manager recovery secrets.

Introduzca la frase de acceso y la información de copia de seguridad registrada anteriormente. Consulte "[Gestione el cifrado del almacenamiento con el gestor de claves incorporado](#)".

25. Nodo de arranque en el menú de arranque:

```
boot_ontap menu
```

26. En `node3`, vaya al menú de arranque y usando `22/7`, seleccione la opción oculta `boot_after_controller_replacement`. En el aviso, introduzca el nodo 1 para reasignar los discos del nodo 1 al nodo 3, según el ejemplo siguiente.

Expanda el ejemplo de salida de consola

```
LOADER-A> boot_ontap menu
.
<output truncated>
.
All rights reserved.
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
.
<output truncated>
.
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7
(22/7) Print this secret List
(25/6) Force boot with multiple filesystem disks missing.
(25/7) Boot w/ disk labels forced to clean.
(29/7) Bypass media errors.
(44/4a) Zero disks if needed and create new flexible root volume.
(44/7) Assign all disks, Initialize all disks as SPARE, write DDR
labels
.
<output truncated>
.
(wipeconfig) Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition) Boot after MCC transition
(9a) Unpartition all disks and remove
their ownership information.
(9b) Clean configuration and
initialize node with partitioned disks.
```

```
(9c) Clean configuration and initialize node with whole disks.
(9d) Reboot the node.
(9e) Return to main boot menu.
The boot device has changed. System configuration information could be lost. Use option (6) to restore the system configuration, or option (4) to initialize all disks and setup a new system. Normal Boot is prohibited.
```

Please choose one of the following:

- (1) Normal Boot.
- (2) Boot without /etc/rc.
- (3) Change password.
- (4) Clean configuration and initialize all disks.
- (5) Maintenance mode boot.
- (6) Update flash from backup config.
- (7) Install new software first.
- (8) Reboot node.
- (9) Configure Advanced Drive Partitioning.
- (10) Set Onboard Key Manager recovery secrets.
- (11) Configure node for external key management.

```
Selection (1-11)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup to disks. Are you sure you want to continue?: yes
```

```
.
<output truncated>
```

```
.
Controller Replacement: Provide name of the node you would like to replace:<nodename of the node being replaced>
```

```
Changing sysid of node nodel disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id = 536940063
Partner sysid = 4294967295, owner sysid = 536940063
```

```
.
<output truncated>
```

```
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot device
varfs_backup_restore: successfully restored env file to the boot device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
```

```

<node reboots>
System rebooting...
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
<output truncated>
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
Login:

```



En el ejemplo de resultado de la consola anterior, ONTAP le solicitará el nombre del nodo asociado si el sistema utiliza discos de partición avanzada de disco (ADP).

27. Si el sistema entra en un bucle de reinicio con el mensaje `no disks found`, indica que se ha producido un problema con la reasignación del disco. Consulte ["Solucionar problemas"](#) para resolver el problema.
28. Pulse `Ctrl-C` durante el arranque automático para detener el nodo en `LOADER>` el símbolo del sistema.
29. En el aviso del CARGADOR, introduzca el modo de mantenimiento:

```
boot_ontap maint
```

30. Verifique la conectividad de discos, la cadena del modelo de controladora, la configuración de alta disponibilidad y otros detalles relacionados con la conectividad de hardware.
31. Salga del modo de mantenimiento:

```
halt
```

32. En el símbolo del SISTEMA DEL CARGADOR, arranque:

```
boot_ontap menu
```

Ahora, en el arranque, el nodo puede detectar todos los discos que se le habían asignado previamente y puede arrancar según se esperaba.

Cuando los nodos de clúster que desea reemplazar utilizan cifrado de volumen raíz, ONTAP no puede leer la información de los volúmenes desde los discos. Restaure las claves del volumen raíz.



Esto solo se aplica cuando el volumen raíz utiliza el cifrado de volúmenes de NetApp.

- a. Vuelva al menú de inicio especial:

```
LOADER> boot_ontap menu
```

```
Please choose one of the following:  
(1) Normal Boot.  
(2) Boot without /etc/rc.  
(3) Change password.  
(4) Clean configuration and initialize all disks.  
(5) Maintenance mode boot.  
(6) Update flash from backup config.  
(7) Install new software first.  
(8) Reboot node.  
(9) Configure Advanced Drive Partitioning.  
(10) Set Onboard Key Manager recovery secrets.  
(11) Configure node for external key management.  
  
Selection (1-11)? 10
```

b. Seleccione **(10) establecer secretos de recuperación de Onboard Key Manager**

c. Introduzca `y` en el siguiente símbolo del sistema:

```
This option must be used only in disaster recovery procedures. Are you sure?  
(y or n): y
```

d. En la solicitud de, introduzca la frase de contraseña del gestor de claves.

e. Introduzca los datos de copia de seguridad cuando se le solicite.



Debe haber obtenido la clave de acceso y los datos de backup en la "[Prepare los nodos para la actualización](#)" sección de este procedimiento.

f. Después de que el sistema se inicie de nuevo en el menú de inicio especial, ejecute la opción **(1) Inicio normal**



Es posible que se encuentre un error en este momento. Si se produce un error, repita los subpasos de [Paso 32](#) hasta que el sistema arranque normalmente.

Verifique la instalación del nodo 3

Debe verificar que los puertos físicos del nodo 1 se asignan correctamente a los puertos físicos del nodo 3. Esto permitirá que el nodo 3 se comunique con otros nodos del clúster y con la red después de la actualización.

Acerca de esta tarea

Consulte "[Referencias](#)" Para enlazar con *Hardware Universe* y obtener información acerca de los puertos en los nuevos nodos. Utilizará la información más adelante en esta sección.

La distribución del puerto físico puede variar según el modelo de los nodos. Cuando se arranque el nuevo nodo, ONTAP intentará determinar qué puertos deberían alojar las LIF del clúster para que quoren

automáticamente.

Si los puertos físicos del nodo 1 no se asignan directamente a los puertos físicos del nodo 3, la sección posterior [Restaurar la configuración de red en el nodo 3](#) se debe utilizar para reparar la conectividad de red.

Después de instalar y arrancar el nodo 3, es necesario verificar que esté instalado correctamente. Es necesario esperar a que el nodo 3 se una al quórum y, luego, reanudar la operación de reubicación.

En este momento del procedimiento, la operación se pausará cuando el quórum de node3 se una a otra.

Pasos

1. Verifique que el nodo 3 se haya Unido al quórum:

```
cluster show -node node3 -fields health
```

El resultado del `health` el campo debe ser `true`.

2. Verifique que el nodo 3 forme parte del mismo clúster que el nodo 2 y que esté en buen estado:

```
cluster show
```

3. Cambiar al modo de privilegio avanzado:

```
set advanced
```

4. Compruebe el estado del funcionamiento de sustitución de la controladora y compruebe que está en pausa y en el mismo estado que tenía antes de detener el nodo 1 para realizar las tareas físicas de instalación de nuevas controladoras y mover cables:

```
system controller replace show
```

```
system controller replace show-details
```

5. Reanude la operación de sustitución de la controladora:

```
system controller replace resume
```

6. La sustitución de la controladora se detendrá por la intervención indicando el siguiente mensaje:

```
Cluster::*> system controller replace show
```

Node	Status	Error-Action

Node1(now node3)	Paused-for-intervention	Follow the instructions given in
Node2	None	Step Details

Step Details:

To complete the Network Reachability task, the ONTAP network configuration must be manually adjusted to match the new physical network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For detailed commands and instructions, refer to the "Re-creating VLANs, ifgrps, and broadcast domains" section of the upgrade controller hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-replacement network displaced-vlans restore" to restore the VLAN on the desired port.

2 entries were displayed.



En este procedimiento, se ha cambiado el nombre de la sección *Re-creating VLAN, ifgrps y dominios de broadcast Restore network Configuration on node3*.

7. Con el reemplazo de la controladora en estado de pausa, continúe a la siguiente sección de este documento para restaurar la configuración de red en el nodo.

Restaurar la configuración de red en el nodo 3

Una vez que se confirma que el nodo 3 está en quórum y que se puede comunicar con el nodo 2, compruebe que las VLAN del nodo 1, los grupos de interfaces y los dominios de retransmisión se ven en el nodo 3. Además, verifique que todos los puertos de red de nodo 3 estén configurados en los dominios de retransmisión correctos.

Acerca de esta tarea

Para obtener más información sobre la creación y recreación de VLAN, grupos de interfaces y dominios de retransmisión, consulte ["Referencias"](#) Para establecer un vínculo con *Network Management*.

Pasos

1. Enumere todos los puertos físicos que se encuentran en node1 actualizado (denominado node3):

```
network port show -node node3
```

Se muestran todos los puertos de red física, los puertos VLAN y los puertos del grupo de interfaces en el nodo. A partir de esta salida, puede ver los puertos físicos que se han movido al Cluster Dominio de difusión por ONTAP. Puede usar esta salida para decidir qué puertos se deben usar como puertos miembro de grupo de interfaces, puertos base de VLAN o puertos físicos independientes para alojar LIF.

2. Enumere los dominios de retransmisión del clúster:

```
network port broadcast-domain show
```

3. Muestre la accesibilidad de todos los puertos de red de node3:

```
network port reachability show
```

Debería ver un resultado como el siguiente ejemplo:

```
ClusterA::*> network port reachability show
Node      Port      Expected Reachability      Reachability
Status
-----
node1_node3
      e0M      Default:Mgmt      ok
      e10a     Default:Default   ok
      e10b     -                 no-reachability
      e10c     Default:Default   ok
      e10d     -                 no-reachability
      e1a      Cluster:Cluster   ok
      e1b     -                 no-reachability
      e7a      Cluster:Cluster   ok
      e7b     -                 no-reachability
node2_node4
      e0M      Default:Mgmt      ok
      e4a     Default:Default   ok
      e4b     -                 no-reachability
      e4c     Default:Default   ok
      e4d     -                 no-reachability
      e3a     Cluster:Cluster   ok
      e3b     Cluster:Cluster   ok
18 entries were displayed.
```

En el ejemplo anterior, 1_nodo 3 solo arranca tras el reemplazo de la controladora. Algunos puertos no tienen la posibilidad de acceder a sus dominios de retransmisión esperados y deben repararse.

4. repare la accesibilidad de cada uno de los puertos del nodo 3 con un estado de accesibilidad distinto de ok. Ejecute el siguiente comando, primero en cualquier puerto físico y, después, en todos los puertos VLAN, de uno en uno:

```
network port reachability repair -node <node_name> -port <port_name>
```

Debería ver un resultado como el siguiente ejemplo:

```
Cluster ::> reachability repair -node nodel_node3 -port e4a
```

```
Warning: Repairing port "nodel_node3: e4a" may cause it to move into a  
different broadcast domain, which can cause LIFs to be re-homed away  
from the port. Are you sure you want to continue? {y|n}:
```

Se espera un mensaje de advertencia, como se muestra anteriormente, para los puertos con un estado de accesibilidad que puede ser diferente del estado de accesibilidad del dominio de difusión en el que se encuentra actualmente. Revise la conectividad del puerto y la respuesta `y` o `n` según corresponda.

Verifique que todos los puertos físicos tengan la habilidad esperada:

```
network port reachability show
```

A medida que se realiza la reparación de accesibilidad, ONTAP intenta colocar los puertos en los dominios de retransmisión correctos. Sin embargo, si no se puede determinar la accesibilidad de un puerto y no pertenece a ninguno de los dominios de difusión existentes, ONTAP creará nuevos dominios de difusión para estos puertos.

5. Si la configuración del grupo de interfaces no coincide con la nueva distribución de puertos físicos de la controladora, modifíquela mediante los siguientes pasos.
 - a. Primero debe eliminar los puertos físicos que deben ser puertos miembro del grupo de interfaces de su pertenencia a dominio de retransmisión. Para ello, puede utilizar el siguiente comando:

```
network port broadcast-domain remove-ports -broadcast-domain <broadcast-  
domain_name> -ports <node_name:port_name>
```

- b. Añada un puerto miembro a un grupo de interfaces:

```
network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port  
<port_name>
```

- c. El grupo de interfaces se añade automáticamente al dominio de retransmisión aproximadamente un minuto después de añadir el primer puerto miembro.
 - d. Compruebe que el grupo de interfaces se ha agregado al dominio de retransmisión apropiado:

```
network port reachability show -node <node_name> -port <ifgrp>
```

Si el estado de accesibilidad del grupo de interfaces no es `ok`, asígnelo al dominio de difusión apropiado:

```
network port broadcast-domain add-ports -broadcast-domain  
<broadcast_domain_name> -ports <node:port>
```

6. Asigne los puertos físicos adecuados al `Cluster` dominio de retransmisión mediante los siguientes

pasos:

- a. Determine qué puertos tienen la posibilidad de recurrir al Cluster dominio de difusión :

```
network port reachability show -reachable-broadcast-domains Cluster:Cluster
```

- b. Repare cualquier puerto con la accesibilidad al Cluster dominio de retransmisión, si su estado de accesibilidad no es ok:

```
network port reachability repair -node <node_name> -port <port_name>
```

7. Mueva los puertos físicos restantes a sus dominios de retransmisión correctos mediante uno de los siguientes comandos:

```
network port reachability repair -node <node_name> -port <port_name>
```

```
network port broadcast-domain remove-port
```

```
network port broadcast-domain add-port
```

Compruebe que no hay puertos inesperados o inaccesibles presentes. Compruebe el estado de la accesibilidad de todos los puertos físicos mediante el siguiente comando y examine el resultado para confirmar que el estado es ok:

```
network port reachability show -detail
```

8. Restaure cualquier VLAN que pueda haberse desplazado siguiendo los pasos siguientes:

- a. Enumerar las VLAN desplazadas:

```
cluster controller-replacement network displaced-vlans show
```

Se debe mostrar una salida como la siguiente:

```
Cluster::*> displaced-vlans show
(cluster controller-replacement network displaced-vlans show)
      Original
Node   Base Port   VLANs
-----
Node1   a0a         822, 823
        e4a         822, 823
2 entries were displayed.
```

- b. Restaure las VLAN desplazadas de sus puertos base anteriores:

```
cluster controller-replacement network displaced-vlans restore
```

A continuación se muestra un ejemplo de restauración de VLAN que se han desplazado del grupo de interfaces "a0a" al mismo grupo de interfaces:

```
Cluster::*> displaced-vlans restore -node node1_node3 -port a0a
-destination-port a0a
```

Este es un ejemplo de restauración de VLAN desplazadas en el puerto "e9a" en el puerto e9d':

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e9a
-destination-port e9d
```

Cuando una restauración VLAN se realiza correctamente, las VLAN desplazadas se crean en el puerto de destino especificado. Se produce un error en la restauración de VLAN si el puerto de destino es miembro de un grupo de interfaces o si el puerto de destino está inactivo.

Espere aproximadamente un minuto para que las VLAN recién restauradas se coloquen en sus dominios de retransmisión correspondientes.

- a. Cree nuevos puertos VLAN según sea necesario para los puertos VLAN que no se encuentran en el `cluster controller-replacement network displaced-vlans show` salida pero se debe configurar en otros puertos físicos.
9. Elimine todos los dominios de retransmisión vacíos después de que se hayan completado todas las reparaciones de puertos:

```
network port broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

10. Compruebe la accesibilidad del puerto:

```
network port reachability show
```

Cuando todos los puertos se configuran y se añaden correctamente a los dominios de retransmisión correctos, el `network port reachability show` el comando debería informar el estado de la accesibilidad como `ok` para todos los puertos conectados y el estado como `no-reachability` para puertos sin conectividad física. Si algún puerto informa de un estado distinto a estos dos, realice la reparación de accesibilidad y añada o quite puertos de sus dominios de retransmisión como se indica en [Paso 4](#).

11. Compruebe que todos los puertos se han colocado en dominios de retransmisión:

```
network port show
```

12. Compruebe que todos los puertos de los dominios de retransmisión tengan la unidad de transmisión máxima (MTU) correcta configurada:

```
network port broadcast-domain show
```

13. Restaure los puertos iniciales de LIF, especificando los puertos de inicio de Vserver y LIF, si los hubiera, que deben restaurarse mediante los siguientes pasos:

- a. Enumere las LIF que están desplazadas:

```
displaced-interface show
```

b. Restaure los nodos de inicio de LIF y sus puertos iniciales:

```
cluster controller-replacement network displaced-interface restore-home-node  
-node <node_name> -vserver <vserver_name> -lif-name <LIF_name>
```

14. Verifique que todas las LIF tienen un puerto doméstico y que están administrativamente más arriba:

```
network interface show -fields home-port, status-admin
```

Restaure la configuración de gestor de claves en el nodo 3

Si utiliza el cifrado de volúmenes de NetApp (NVE) y el cifrado de agregados de NetApp (NAE) para cifrar volúmenes en el sistema que se está actualizando, la configuración de cifrado debe sincronizarse con los nodos nuevos. Si no se sincroniza el gestor de claves, cuando se reinstalan los agregados del nodo 1 del nodo 2 al nodo 3 mediante ARL, es posible que se produzcan fallos, ya que el nodo 3 no tiene las claves de cifrado necesarias para poner en línea volúmenes y agregados cifrados.

Acerca de esta tarea

Para sincronizar la configuración de cifrado con los nuevos nodos, realice los siguientes pasos:

Pasos

1. Ejecute el siguiente comando desde node3:

```
security key-manager onboard sync
```

2. Compruebe que la clave SVM-KEK se restaure en "TRUE" en el nodo 3 antes de reubicar los agregados de datos:

```
::> security key-manager key query -node node3 -fields restored -key  
-type SVM-KEK
```

Ejemplo

```
::> security key-manager key query -node node3 -fields restored -key  
-type SVM-KEK
```

node	vserver	key-server	key-id
restored			
-----	-----	-----	-----
node3	svm1	""	0000000000000000020000000000a008a81976
true			2190178f9350e071fbb90f00000000000000000

Mueva agregados que no son raíz y LIF de datos NAS que pertenecen al nodo 1 del nodo 2 al nodo 3

Después de verificar la configuración de red en el nodo 3 y antes de reubicar agregados del nodo 2 al nodo 3, es necesario comprobar que los LIF de datos NAS que pertenecen al nodo 1 que están actualmente en el nodo 2 se encuentren en el nodo 3. También debe verificar que las LIF SAN existan en el nodo 3.

Acerca de esta tarea

Las LIF remotas gestionan el tráfico a LUN DE SAN durante el procedimiento de actualización. No es necesario mover LIF DE SAN durante la actualización para el estado del clúster o del servicio. Los LIF SAN no se mueven a menos que tengan que asignarse a nuevos puertos. Verifique que las LIF estén en buen estado y se encuentren en puertos adecuados después de poner el nodo 3 en línea.

Pasos

1. Los LIF iSCSI encuentran de forma automática los puertos iniciales correctos mediante el análisis de accesibilidad. Los LIF SAN FC y NVMe/FC no se mueven automáticamente. Continúan mostrando el puerto raíz en el que estaban antes de actualizar.

Compruebe los LIF SAN en node3:

- a. Modifique cualquier LIF de SAN iSCSI que informe de un estado de operación inactivo a los nuevos puertos de datos:

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif>
```

- b. Modifique todos los LIF FC y NVMe/FC SAN que residan en la nueva controladora e informen de un estado operativo «inactivo» en los puertos FCP de la nueva controladora:

```
network interface modify -vserver <vserver> -lif <fc_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif>
```

2. Reanude la operación de reubicación:

```
system controller replace resume
```

El sistema ejecuta las siguientes tareas:

- Comprobación de quórum del clúster
- Comprobación del ID del sistema
- Comprobación de la versión de la imagen
- Comprobación de la plataforma de destino

- Comprobación de accesibilidad de red

La operación se detiene en esta fase de la comprobación de accesibilidad de red.

3. Reanude la operación de reubicación:

```
system controller replace resume
```

El sistema realiza las siguientes comprobaciones:

- Comprobación del estado del clúster
- Comprobación del estado de LIF de clúster

Después de realizar estas comprobaciones, el sistema reubica los agregados que no son raíz y los LIF de datos NAS que pertenecen al nodo 1 en la nueva controladora, el nodo 3. La operación de reemplazo de la controladora se coloca en pausa una vez que se completa la reubicación de recursos.

4. Comprobar el estado de las operaciones de reubicación de agregados y movimiento de LIF de datos de NAS:

```
system controller replace show-details
```

Si el procedimiento de reemplazo de la controladora está en pausa, compruebe y corrija el error, si corresponde, y luego emita `resume` para continuar la operación.

5. Si es necesario, restaure y devuelva los LIF desplazados. Enumerar las LIF desplazadas:

```
cluster controller-replacement network displaced-interface show
```

Si alguna LIF se ha desplazado, restaure el nodo de inicio al nodo 3:

```
cluster controller-replacement network displaced-interface restore-home-node
```

6. Reanude la operación para solicitar que el sistema realice las comprobaciones previas necesarias:

```
system controller replace resume
```

El sistema realiza las siguientes comprobaciones posteriores:

- Comprobación de quórum del clúster
- Comprobación del estado del clúster
- Comprobación de reconstrucción de los agregados
- Comprobación del estado del agregado
- Comprobación del estado del disco
- Comprobación del estado de LIF de clúster
- Comprobación del volumen

Etapa 4. Reubicar y retirar el 2

Descripción general de la etapa 4

Durante la fase 4, se reubicarán los agregados no raíz y los LIF de datos NAS del nodo 2 al nodo 3. También debe registrar la información necesaria de node2 para utilizarla más adelante en el procedimiento y, a continuación, retirar node2.

Pasos

1. "Reubique los agregados que no son raíz y los LIF de datos NAS del nodo 2 al nodo 3"
2. "Retire el nodo 2"

Reubique los agregados que no son raíz y los LIF de datos NAS del nodo 2 al nodo 3

Antes de sustituir node2 con node4, debe reubicar los agregados no raíz y los LIF de datos NAS que node2 posee a node3.

Antes de empezar

Una vez completadas las comprobaciones posteriores a la fase anterior, la versión de recursos para el nodo 2 se iniciará automáticamente. Los agregados que no son raíz y los LIF de datos que no son SAN se migran del nodo 2 al nodo 3.

Acerca de esta tarea

Las LIF remotas gestionan el tráfico a LUN DE SAN durante el procedimiento de actualización. No es necesario mover LIF DE SAN durante la actualización para el estado del clúster o del servicio.

Una vez migrados los agregados y las LIF, la operación se coloca en pausa con fines de verificación. En este momento, debe verificar si todos los agregados que no son raíz y los LIF de datos no SAN se migran al nodo 3.



El propietario raíz de los agregados y las LIF no se modifica; solo se modifica el propietario actual.

Pasos

1. Verifique que todos los agregados que no son raíz estén en línea y su estado en el nodo 3:

```
storage aggregate show -node node3 -state online -root false
```

En el ejemplo siguiente, los agregados no raíz en el nodo 2 están en línea:

```
cluster::> storage aggregate show -node node3 state online -root false
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes
RAID	Status					
aggr_1	744.9GB	744.8GB	0%	online	5	node2
raid_dp	normal					
aggr_2	825.0GB	825.0GB	0%	online	1	node2
raid_dp	normal					

2 entries were displayed.

Si los agregados se han desconectado o se han vuelto externos del nodo 3, conectarlos mediante el uso del siguiente comando de nodo 3, una vez por cada agregado:

```
storage aggregate online -aggregate aggr_name
```

2. Verifique que todos los volúmenes estén en línea en el nodo 3. Para ello, use el siguiente comando en el nodo 3 y examine el resultado:

```
volume show -node node3 -state offline
```

Si alguno de los volúmenes se encuentra sin conexión en el nodo 3, debe volver a estar en línea mediante el siguiente comando de nodo 3, una vez para cada volumen:

```
volume online -vserver vserver_name -volume volume_name
```

La *vserver_name* para utilizarlo con este comando se encuentra en el resultado del anterior `volume show` comando.

3. Compruebe que las LIF se han movido a los puertos correctos y que tienen el estado de `up`. Si alguna LIF está inactiva, establezca el estado administrativo de las LIF en `up` Con el siguiente comando, una vez para cada LIF:

```
network interface modify -vserver vserver_name -lif LIF_name -home-node node_name -status-admin up
```

4. Si los puertos que alojan actualmente las LIF de datos no existen en el nuevo hardware, elimínelas del dominio de retransmisión:

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

5. Compruebe que no quedan LIF de datos en el nodo 2 introduciendo el comando siguiente y examinando el resultado:

```
network interface show -curr-node node2 -role data
```

Retire el nodo 2

Para retirar node2, primero debe apagar node2 correctamente y quitarlo del rack o el chasis.

Pasos

1. Reanude la operación:

```
system controller replace resume
```

El nodo se detiene automáticamente.

Después de terminar

Puede retirar el nodo 2 una vez completada la actualización. Consulte ["Retire el sistema antiguo"](#).

Etapa 5. Instale y arranque el nodo 4

Descripción general de la etapa 5

Durante la fase 5, debe instalar y arrancar el nodo 4, compruebe que los puertos de gestión del clúster y de los nodos del nodo 2 estén en línea en el nodo 4 y verifique la instalación del nodo 4. Si utiliza NVE, debe restaurar la configuración del gestor de claves. También se deben reubicar los LIF de datos NAS 2 y los agregados no raíz de nodo 3 a nodo 4, y verificar que las LIF SAN existan en el nodo 4.

Pasos

1. ["Instale y arranque el nodo 4"](#)
2. ["Verifique la instalación del nodo 4"](#)
3. ["Restaure la configuración de gestor de claves en el nodo 4"](#)
4. ["Mueva agregados no raíz y LIF de datos NAS que pertenecen al nodo 2 desde el nodo 3 al nodo 4"](#)

Instale y arranque el nodo 4

Instale node4 en el rack, transfiera las conexiones de node2 a node4, arranque node4 e instale ONTAP. A continuación, se reasignan cualquiera de los discos de reserva de node2, los discos que pertenezcan al volumen raíz y los agregados que no sean raíz que no se reubicaron en la versión node3 anteriormente en el proceso, como se explica en esta sección.

Acerca de esta tarea

La operación de reubicación se detiene al principio de esta etapa. Este proceso está prácticamente automatizado; la operación se pausa para permitir comprobar su estado. Debe reanudar manualmente la operación.

Es necesario reiniciar el nodo 4 si no tiene la misma versión de ONTAP 9 que está instalada en el nodo 2. Después de instalar el nodo 4, arranque desde la imagen ONTAP 9 almacenada en el servidor web. A continuación, puede descargar los archivos correctos en el dispositivo multimedia de arranque para posteriores arranques del sistema, siguiendo las instrucciones en ["Prepárese para el arranque desde el red"](#).

Pasos

1. Asegúrese de que el nodo 4 tenga suficiente espacio en rack.

Si el nodo 4 se encuentra en un chasis separado del nodo 2, es posible colocar el nodo 4 en la misma ubicación que el nodo 3. Si el nodo 2 y el nodo 4 están en el mismo chasis, el nodo 4 ya se encuentra en la ubicación de rack adecuada.

2. Instale el nodo 4 en el rack, siguiendo las instrucciones de *Installation and Setup* para el modelo de nodo.
3. Cablee el nodo 4, mueva las conexiones del nodo 2 al nodo 4.

Conecte los cables siguientes, siguiendo las instrucciones de *Installation and Setup Instructions* o de *FlexArray Virtualization Installation reactions and Reference* para la plataforma node4, el documento de la bandeja de discos correspondiente y *High Availability Management*.

Consulte "[Referencias](#)" Para enlazar con *FlexArray Virtualization Installation requisitos y Reference* y *High Availability Management*.

- Consola (puerto de gestión remota)
- Clúster y puertos de alta disponibilidad
- Puertos de datos
- Puertos de gestión de clústeres y nodos
- SCSI con conexión en serie (SAS) y puertos de almacenamiento Ethernet
- Configuraciones SAN: Puertos Ethernet iSCSI, FC y switch NVMe/FC

Es posible que deba cambiar los cables de interconexión entre las controladoras antigua y nueva para permitir la interoperabilidad entre los distintos modelos de controladora y de tarjeta. Consulte la "[procedimientos de instalación del sistema](#)" para obtener un mapa de cableado de las bandejas de almacenamiento Ethernet de los sistemas.



Para las controladoras incluidas en ONTAP 9.15.1 y versiones posteriores, las interconexiones de clúster y alta disponibilidad utilizan los mismos puertos. Para las configuraciones conectadas por switch, es necesario conectar puertos similares al mismo switch de clúster. Por ejemplo, al actualizar a un AFF A1K desde una controladora existente, debe conectar los puertos e1a de ambos nodos a un switch y los puertos e7a de ambos nodos en el segundo switch.

4. Encienda el nodo 4 y, a continuación, interrumpa el proceso de arranque pulsando `Ctrl-C` en el terminal de la consola para acceder al aviso del entorno de arranque.



Cuando se arranca el nodo 4, es posible que se muestre el siguiente mensaje de advertencia:

```

WARNING: The battery is unfit to retain data during a power outage. This
is likely
    because the battery is discharged but could be due to other
temporary
    conditions.
    When the battery is ready, the boot process will complete
and services will be engaged. To override this delay, press 'c'
followed
    by 'Enter'

```

5. Si aparece el mensaje de advertencia en el paso 4, realice las siguientes acciones:

- a. Compruebe todos los mensajes de la consola que puedan indicar un problema distinto a una batería NVRAM baja y, si es necesario, realice las acciones correctivas necesarias.
- b. Deje que la batería se cargue y finalice el proceso de arranque.



Atención: No anular el retardo; si no se permite que la batería se cargue, se podrían producir pérdidas de datos.



Consulte "[Prepárese para el arranque desde el red](#)".

6. Configure la conexión para reiniciar el sistema eligiendo una de las siguientes acciones.



Se deben utilizar el puerto e IP de gestión como conexión para reiniciar el sistema. No utilice una IP de LIF de datos ni una interrupción del servicio de datos mientras se realiza la actualización.

Si el protocolo de configuración dinámica de hosts (DHCP) es...	Realice lo siguiente...
Ejecutando	Configure la conexión automáticamente mediante el siguiente comando en el símbolo del sistema del entorno de arranque: ifconfig e0M -auto

Si el protocolo de configuración dinámica de hosts (DHCP) es...	Realice lo siguiente...
No se está ejecutando	<p>Configure manualmente la conexión introduciendo el siguiente comando en el símbolo del sistema del entorno de arranque:</p> <pre>ifconfig e0M -addr=<i>filer_addr</i> -mask=<i>netmask</i> -gw=<i>gateway</i> -dns=<i>dns_addr</i> -domain=<i>dns_domain</i></pre> <p><i>filer_addr</i> Es la dirección IP del sistema de almacenamiento (obligatorio). <i>netmask</i> es la máscara de red del sistema de almacenamiento (obligatoria). <i>gateway</i> es la puerta de enlace del sistema de almacenamiento (obligatorio). <i>dns_addr</i> Es la dirección IP de un servidor de nombres en la red (opcional). <i>dns_domain</i> Es el nombre de dominio DNS (opcional).</p> <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;">  <p>Es posible que sean necesarios otros parámetros para la interfaz. Introduzca <code>help ifconfig</code> en el símbolo del sistema del firmware para obtener detalles.</p> </div>

7. Reiniciar el sistema en el nodo 4:

```
netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz
```

La <path_to_the_web-accessible_directory> debería conducir al lugar en el que se ha descargado el <ontap_version>_image.tgz En el paso 1 de la sección "[Prepárese para el arranque desde el red](#)".

 No interrumpa el arranque.

8. En el menú de inicio, seleccione opción (7) `Install new software first`.

Esta opción del menú descarga e instala la nueva imagen de ONTAP en el dispositivo de arranque.

Ignore el siguiente mensaje:

```
This procedure is not supported for Non-Disruptive Upgrade on an HA pair
```

La nota se aplica a las actualizaciones no disruptivas de ONTAP, no a las actualizaciones de controladoras.

 Utilice siempre netboot para actualizar el nodo nuevo a la imagen deseada. Si utiliza otro método para instalar la imagen en la nueva controladora, podría instalarse la imagen incorrecta. Este problema se aplica a todas las versiones de ONTAP. El procedimiento para reiniciar el sistema combinado con la opción (7) `Install new software` Limpia el soporte de arranque y coloca la misma versión ONTAP en ambas particiones de imagen.

9. Si se le solicita que continúe el procedimiento, introduzca `y`, Y cuando se le solicite el paquete, escriba la dirección URL:

```
http://<web_server_ip/path_to_web-  
accessible_directory>/<ontap_version>_image.tgz
```

10. Lleve a cabo los siguientes pasos para reiniciar el módulo del controlador:

- a. Introduzca `n` para omitir la recuperación del backup cuando aparezca la siguiente solicitud:

```
Do you want to restore the backup configuration now? {y|n}
```

- b. Reinicie introduciendo `y` cuando vea el siguiente símbolo del sistema:

```
The node must be rebooted to start using the newly installed  
software. Do you want to reboot now? {y|n}
```

El módulo del controlador se reinicia pero se detiene en el menú de inicio porque el dispositivo de arranque se ha reformateado y los datos de configuración deben restaurarse.

11. Seleccione el modo de mantenimiento 5 desde el menú de inicio y entrar `y` cuando se le pida que continúe con el arranque.
12. Compruebe que la controladora y el chasis están configurados como ha:

```
ha-config show
```

En el siguiente ejemplo, se muestra el resultado del `ha-config show` comando:

```
Chassis HA configuration: ha  
Controller HA configuration: ha
```



El sistema graba en una PROM tanto si se encuentran en un par ha como en una configuración independiente. El estado debe ser el mismo en todos los componentes del sistema independiente o del par de alta disponibilidad.

13. Si la controladora y el chasis no están configurados como alta disponibilidad, utilice los siguientes comandos para corregir la configuración:

```
ha-config modify controller ha
```

```
ha-config modify chassis ha
```

14. Confirme que todos los puertos Ethernet utilizados para conectarse a las bandejas Ethernet están configurados como almacenamiento:

```
storage port show
```

La salida mostrada depende de la configuración del sistema. El siguiente ejemplo de salida es para un

nodo con una única tarjeta de almacenamiento en slot11. La salida del sistema puede ser diferente:

```
*> storage port show
Port Type Mode      Speed(Gb/s) State      Status  VLAN ID
-----
e11a ENET storage 100 Gb/s    enabled  online  30
e11b ENET storage 100 Gb/s    enabled  online  30
```

15. Modifique los puertos que no están configurados en el almacenamiento:

```
storage port modify -p <port> -m storage
```

Todos los puertos Ethernet conectados a las bandejas de almacenamiento deben estar configurados como almacenamiento para permitir el acceso a los discos y las bandejas.

16. Salga del modo de mantenimiento:

```
halt
```

Interrumpa el arranque automático pulsando Ctrl-C en el símbolo del sistema del entorno de arranque.

17. en el nodo 3, compruebe la fecha, la hora y la zona horaria del sistema:

```
date
```

18. El nodo 4, compruebe la fecha mediante el siguiente comando en el símbolo del sistema del entorno de arranque:

```
show date
```

19. Si es necesario, configure la fecha del nodo 4:

```
set date <mm/dd/yyyy>
```

20. En el nodo 4, compruebe la hora mediante el siguiente comando en el símbolo del sistema del entorno de arranque:

```
show time
```

21. Si es necesario, configure la hora del nodo 4:

```
set time <hh:mm:ss>
```

22. En el cargador de arranque, establezca el ID del sistema del partner en el nodo 4:

```
setenv partner-sysid <node3_sysid>
```

Para el nodo 4, `partner-sysid` debe ser el del nodo 3.

Guarde los ajustes:

```
saveenv
```

23. Compruebe el `partner-sysid` para el nodo 4:

```
printenv partner-sysid
```

24. Si tiene unidades de cifrado de almacenamiento de NetApp (NSE) instaladas, realice los pasos siguientes.



Si aún no lo ha hecho anteriormente en el procedimiento, consulte el artículo de la base de conocimientos "[Cómo saber si una unidad tiene la certificación FIPS](#)" para determinar el tipo de unidades de autocifrado que están en uso.

a. Configurado `bootarg.storageencryption.support` para `true` o `false`.

Si están en uso las siguientes unidades...	Entonces...
Unidades NSE que cumplen con los requisitos de autocifrado de FIPS 140-2 de nivel 2	<code>setenv bootarg.storageencryption.support true</code>
SED de NetApp no con FIPS	<code>setenv bootarg.storageencryption.support false</code>

b. Vaya al menú de inicio especial y seleccione la opción (10) Set Onboard Key Manager recovery secrets.

Introduzca la frase de acceso y la información de copia de seguridad registrada anteriormente. Consulte "[Gestione el cifrado del almacenamiento con el gestor de claves incorporado](#)".

25. Nodo de arranque en el menú de arranque:

```
boot_ontap menu.
```

26. En `node4`, vaya al menú de inicio y, usando `22/7`, seleccione la opción oculta `boot_after_controller_replacement`. En el símbolo del sistema, introduzca el nodo 2 para reasignar los discos del nodo 2 al nodo 4, como en el ejemplo siguiente.

Expanda el ejemplo de salida de consola

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
.
<output truncated>
.
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 22/7
(22/7)                                     Print this secret List
(25/6)                                     Force boot with multiple filesystem
disks missing.
(25/7)                                     Boot w/ disk labels forced to clean.
(29/7)                                     Bypass media errors.
(44/4a)                                    Zero disks if needed and create new
flexible root volume.
(44/7)                                     Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                               Clean all configuration on boot
device
(boot_after_controller_replacement) Boot after controller upgrade
```

```

(boot_after_mcc_transition)      Boot after MCC transition
(9a)                             Unpartition all disks and remove
their ownership information.
(9b)                             Clean configuration and
initialize node with partitioned disks.
(9c)                             Clean configuration and
initialize node with whole disks.
(9d)                             Reboot the node.
(9e)                             Return to main boot menu.
The boot device has changed. System configuration information could
be lost. Use option (6) to
restore the system configuration, or option (4) to initialize all
disks and setup a new system.
Normal Boot is prohibited.
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? boot_after_controller_replacement
This will replace all flash-based configuration with the last backup
to disks. Are you sure
you want to continue?: yes
.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:
<nodename of the node being replaced>
Changing sysid of node node2 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.

```

```

.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote
    key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>
System rebooting...
.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:

```



En el ejemplo de resultado de la consola anterior, ONTAP le solicitará el nombre del nodo asociado si el sistema utiliza discos de partición avanzada de disco (ADP).

27. En el prompt del CARGADOR, arranque:

boot_ontap menu

Ahora, en el arranque, el nodo puede detectar todos los discos que se le habían asignado previamente y puede arrancar según se esperaba.

Cuando los nodos de clúster que desea reemplazar utilizan cifrado de volumen raíz, ONTAP no puede leer la información de los volúmenes desde los discos. Restaure las claves del volumen raíz:

Si el volumen raíz está cifrado, recupere los secretos de gestión de claves incorporados para que el sistema pueda encontrar el volumen raíz.

a. Vuelva al menú de inicio especial:

```
LOADER> boot_ontap menu
```

```
Please choose one of the following:
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.

Selection (1-11)? 10
```

b. Seleccione **(10) establecer secretos de recuperación de Onboard Key Manager**

c. Introduzca `y` en el siguiente símbolo del sistema:

```
This option must be used only in disaster recovery procedures. Are you sure?
(y or n): y
```

d. En la solicitud de, introduzca la frase de contraseña del gestor de claves.

e. Introduzca los datos de copia de seguridad cuando se le solicite.



Debe haber obtenido la clave de acceso y los datos de backup en la "[Prepare los nodos para la actualización](#)" sección de este procedimiento.

f. Después de que el sistema se inicie de nuevo en el menú de inicio especial, ejecute la opción **(1) Inicio normal**



Es posible que se encuentre un error en este momento. Si se produce un error, repita los subpasos de [Paso 27](#) hasta que el sistema arranque normalmente.

Verifique la instalación del nodo 4

Debe verificar que los puertos físicos del nodo 2 se asignan correctamente a los puertos físicos del nodo 4. Esto permitirá que el nodo 4 se comunique con otros nodos del clúster y con la red después de la actualización.

Acerca de esta tarea

Consulte "[Referencias](#)" Para enlazar con *Hardware Universe* y obtener información acerca de los puertos en los nuevos nodos. Utilizará la información más adelante en esta sección.

La distribución del puerto físico puede variar según el modelo de los nodos. Cuando se arranque el nuevo nodo, ONTAP intentará determinar qué puertos deberían alojar las LIF del clúster para que quoren automáticamente.

Si los puertos físicos del nodo 2 no se asignan directamente a los puertos físicos del nodo 4, en la sección posterior [Restaurar la configuración de red en el nodo 4](#) se debe utilizar para reparar la conectividad de red.

Después de instalar y arrancar el nodo 4, es necesario verificar que esté instalado correctamente. Debe esperar a que el nodo 4 se una al quórum y, a continuación, reanudar la operación de reubicación.

En este momento del procedimiento, la operación se pausó debido a que el quórum de node4 se une.

Pasos

1. Verifique que el nodo 4 se haya Unido al quórum:

```
cluster show -node node4 -fields health
```

El resultado del `health` el campo debe ser `true`.

2. Verifique que el nodo 4 forme parte del mismo clúster que el nodo 3 y que sea correcto:

```
cluster show
```

3. Cambie al modo de privilegio avanzado:

```
set advanced
```

4. Compruebe el estado del funcionamiento de sustitución de la controladora y compruebe que esté en pausa y que esté en el mismo estado en antes de que se detenga el nodo 2 para realizar las tareas físicas de instalación de nuevas controladoras y mover cables:

```
system controller replace show
```

```
system controller replace show-details
```

5. Reanude la operación de sustitución de la controladora:

```
system controller replace resume
```

6. La sustitución de la controladora se detendrá por la intervención indicando el siguiente mensaje:

```

Cluster::*> system controller replace show
Node                Status                Error-Action
-----
Node2(now node4) Paused-for-intervention  Follow the instructions
given in
Node2                Step Details

Step Details:
-----
To complete the Network Reachability task, the ONTAP network
configuration must be
manually adjusted to match the new physical network configuration of the
hardware.
This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For
detailed
commands and instructions, refer to the "Re-creating VLANs, ifgrps, and
broadcast
domains" section of the upgrade controller hardware guide for the ONTAP
version
running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show"
to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement
network displaced-vlans restore" to restore the VLAN on the desired
port.
2 entries were displayed.

```



En este procedimiento, se ha cambiado el nombre de la sección *Re-creating VLAN, ifgrps y dominios de difusión restoring network Configuration on node4*.

7. Con el reemplazo de la controladora en estado de pausa, continúe a la siguiente sección de este documento para restaurar la configuración de red en el nodo.

Restaurar la configuración de red en el nodo 4

Una vez que se confirma que el nodo 4 está en quórum y se puede comunicar con el nodo 3, verifique que las VLAN, los grupos de interfaces y los dominios de retransmisión del nodo 4. Además, verifique que todos los puertos de red de nodo 4 estén configurados en los dominios de retransmisión correctos.

Acerca de esta tarea

Para obtener más información sobre la creación y recreación de VLAN, grupos de interfaces y dominios de retransmisión, consulte ["Referencias"](#) Para establecer un vínculo con *Network Management*.

Pasos

1. Enumera todos los puertos físicos en el nodo 2 actualizado (conocido como nodo 4):

```
network port show -node node4
```

Se muestran todos los puertos de red física, los puertos VLAN y los puertos del grupo de interfaces en el nodo. A partir de esta salida puede ver los puertos físicos que se han movido al Cluster Dominio de difusión por ONTAP. Puede usar esta salida para decidir qué puertos se deben usar como puertos miembro de grupo de interfaces, puertos base de VLAN o puertos físicos independientes para alojar LIF.

2. Enumere los dominios de retransmisión del clúster:

```
network port broadcast-domain show
```

3. Enumerar la accesibilidad del puerto de red de todos los puertos del nodo 4:

```
network port reachability show
```

El resultado del comando se parece similar al ejemplo siguiente:

```

ClusterA::*> network port reachability show
Node      Port      Expected Reachability      Reachability
Status
-----
node1_node3
    e0M      Default:Mgmt      ok
    e10a     Default:Default   ok
    e10b     -                 no-reachability
    e10c     Default:Default   ok
    e10d     -                 no-reachability
    e1a      Cluster:Cluster   ok
    e1b      -                 no-reachability
    e7a      Cluster:Cluster   ok
    e7b      -                 no-reachability
node2_node4
    e0M      Default:Mgmt      ok
    e10a     Default:Default   ok
    e10b     -                 no-reachability
    e10c     Default:Default   ok
    e10d     -                 no-reachability
    e1a      Cluster:Cluster   ok
    e1b      -                 no-reachability
    e7a      Cluster:Cluster   ok
    e7b      -                 no-reachability
18 entries were displayed.

```

En el ejemplo anterior, 2_nodo 4 solo arranca después de reemplazar la controladora. Tiene varios puertos que no tienen accesibilidad y están pendientes de un análisis de accesibilidad.

- repare la accesibilidad de cada uno de los puertos del nodo 4 con un estado de accesibilidad distinto de ok. Ejecute el siguiente comando, primero en cualquier puerto físico y, después, en todos los puertos VLAN, de uno en uno:

```
network port reachability repair -node <node_name> -port <port_name>
```

El resultado es como el ejemplo siguiente:

```
Cluster ::> reachability repair -node node2_node4 -port e10a
```

```
Warning: Repairing port "node2_node4: e10a" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Se espera un mensaje de advertencia, como se muestra anteriormente, para los puertos con un estado de accesibilidad que puede ser diferente del estado de accesibilidad del dominio de difusión en el que se encuentra actualmente.

Revise la conectividad del puerto y la respuesta y o. n según corresponda.

Verifique que todos los puertos físicos tengan la habilidad esperada:

```
network port reachability show
```

A medida que se realiza la reparación de accesibilidad, ONTAP intenta colocar los puertos en los dominios de retransmisión correctos. Sin embargo, si no se puede determinar la accesibilidad de un puerto y no pertenece a ninguno de los dominios de difusión existentes, ONTAP creará nuevos dominios de difusión para estos puertos.

5. Si la configuración del grupo de interfaces no coincide con la nueva distribución de puertos físicos de la controladora, modifíquela mediante los siguientes pasos.
 - a. Primero debe eliminar los puertos físicos que deben ser puertos miembro del grupo de interfaces de su pertenencia a dominio de retransmisión. Para ello, puede utilizar el siguiente comando:

```
network port broadcast-domain remove-ports -broadcast-domain  
<broadcast_domain_name> -ports <node_name:port_name>
```

- b. Añada un puerto miembro a un grupo de interfaces:

```
network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port  
<port_name>
```

- c. El grupo de interfaces se añade automáticamente al dominio de retransmisión aproximadamente un minuto después de añadir el primer puerto miembro.
 - d. Compruebe que el grupo de interfaces se ha agregado al dominio de retransmisión apropiado:

```
network port reachability show -node <node_name> -port <ifgrp>
```

Si el estado de accesibilidad del grupo de interfaces no es `ok`, asígnelo al dominio de difusión apropiado:

```
network port broadcast-domain add-ports -broadcast-domain  
<broadcast_domain_name> -ports <node:port>
```

6. Asigne puertos físicos adecuados a `Cluster` dominio de retransmisión:

- a. Determine qué puertos tienen la posibilidad de recurrir al `Cluster` dominio de retransmisión:

```
network port reachability show -reachable-broadcast-domains Cluster:Cluster
```

- b. Repare cualquier puerto con la accesibilidad al `Cluster` dominio de retransmisión, si su estado de accesibilidad no es `ok`:

```
network port reachability repair -node <node_name> -port <port_name>
```

7. Mueva los puertos físicos restantes a sus dominios de retransmisión correctos mediante uno de los siguientes comandos:

```
network port reachability repair -node <node_name> -port <port_name>
```

```
network port broadcast-domain remove-port
```

```
network port broadcast-domain add-port
```

Compruebe que no hay puertos inesperados o inaccesibles presentes. Compruebe el estado de la accesibilidad de todos los puertos físicos mediante el siguiente comando y examine el resultado para confirmar que el estado es `ok`:

```
network port reachability show -detail
```

8. Restaure cualquier VLAN que pueda haberse desplazado siguiendo los pasos siguientes:

a. Enumerar las VLAN desplazadas:

```
cluster controller-replacement network displaced-vlans show
```

Se debe mostrar una salida como la siguiente:

```
Cluster::*> displaced-vlans show
(cluster controller-replacement network displaced-vlans show)
      Original
Node   Base Port   VLANs
-----
Node1  a0a         822, 823
      e10a         822, 823
```

b. Restaure las VLAN desplazadas de sus puertos base anteriores:

```
cluster controller-replacement network displaced-vlans restore
```

A continuación se muestra un ejemplo de restauración de VLAN que se han desplazado del grupo de interfaces `a0a` al mismo grupo de interfaces:

```
Cluster::*> displaced-vlans restore -node node2_node4 -port a0a
-destination-port a0a
```

Este es un ejemplo de restauración de VLAN desplazadas en el puerto "e10a" a "e10b":

```
Cluster::*> displaced-vlans restore -node node2_node4 -port e10a
-destination-port e10b
```

Cuando una restauración VLAN se realiza correctamente, las VLAN desplazadas se crean en el puerto de destino especificado. Se produce un error en la restauración de VLAN si el puerto de destino es miembro de un grupo de interfaces o si el puerto de destino está inactivo.

Espere aproximadamente un minuto para que las VLAN recién restauradas se coloquen en sus dominios de retransmisión correspondientes.

- a. Cree nuevos puertos VLAN según sea necesario para los puertos VLAN que no se encuentran en el `cluster controller-replacement network displaced-vlans show` salida pero se debe configurar en otros puertos físicos.

9. Elimine todos los dominios de retransmisión vacíos después de que se hayan completado todas las reparaciones de puertos:

```
network port broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

10. Compruebe la accesibilidad del puerto:

```
network port reachability show
```

Cuando todos los puertos se configuran y se añaden correctamente a los dominios de retransmisión correctos, el `network port reachability show` el comando debería informar el estado de la accesibilidad como `ok` para todos los puertos conectados y el estado como `no-reachability` para puertos sin conectividad física. Si alguno de los puertos presenta un estado distinto a estos dos, realice la reparación de accesibilidad y añada o quite puertos de sus dominios de retransmisión según se indica en [Paso 4](#).

11. Compruebe que todos los puertos se han colocado en dominios de retransmisión:

```
network port show
```

12. Compruebe que todos los puertos de los dominios de retransmisión tengan la unidad de transmisión máxima (MTU) correcta configurada:

```
network port broadcast-domain show
```

13. Restablezca los puertos de inicio de LIF, especificando los puertos de inicio de Vserver y LIF, si los hubiera, que deben restaurarse:

- a. Enumere las LIF que están desplazadas:

```
displaced-interface show
```

- b. Restablezca los puertos de inicio de LIF:

```
displaced-interface restore-home-node -node <node_name> -vserver  
<vserver_name> -lif-name <LIF_name>
```

14. Verifique que todas las LIF tienen un puerto doméstico y que están administrativamente más arriba:

```
network interface show -fields home-port, status-admin
```

Restablezca la configuración de gestor de claves en el nodo 4

Si utiliza el cifrado de volúmenes de NetApp (NVE) y el cifrado de agregados de NetApp (NAE) para cifrar volúmenes en el sistema que se está actualizando, la configuración de cifrado debe sincronizarse con los nodos nuevos. Si no se sincroniza el gestor de claves, cuando se reinstalan los agregados del nodo 2 desde el nodo 3 al nodo 4 mediante ARL,

es posible que se produzcan fallos, ya que el nodo 4 no tiene las claves de cifrado necesarias para poner en línea volúmenes y agregados cifrados.

Acerca de esta tarea

Para sincronizar la configuración de cifrado con los nuevos nodos, realice los siguientes pasos:

Pasos

1. Ejecute el siguiente comando desde no4:

```
security key-manager onboard sync
```

2. Verifique que la clave SVM-KEK se restaure en "TRUE" en el nodo 4 antes de reubicar los agregados de datos:

```
::> security key-manager key query -node node4 -fields restored -key  
-type SVM-KEK
```

Ejemplo

```
::> security key-manager key query -node node4 -fields restored -key  
-type SVM-KEK
```

node	vserver	key-server	key-id
restored			
-----	-----	-----	-----
node4	svm1	""	00000000000000000000200000000000a008a81976
true			2190178f9350e071fbb90f00000000000000000

Mueva agregados no raíz y LIF de datos NAS que pertenecen al nodo 2 desde el nodo 3 al nodo 4

Después de verificar la configuración de red en el nodo 4 y antes de reubicar agregados de nodo 3 al nodo 4, es necesario verificar que los LIF de datos NAS que pertenecen al nodo 2 que actualmente son de nodo 3 se reubicen de nodo 3 a nodo 4. También debe verificar que las LIF SAN existan en el nodo 4.

Acerca de esta tarea

Las LIF remotas gestionan el tráfico a LUN DE SAN durante el procedimiento de actualización. No es necesario mover LIF DE SAN durante la actualización para el estado del clúster o del servicio. Los LIF SAN no se mueven a menos que tengan que asignarse a nuevos puertos. Verifique que las LIF estén en buen estado y ubicadas en puertos adecuados después de poner el nodo 4 en línea.

Pasos

1. Los LIF iSCSI encuentran de forma automática los puertos iniciales correctos mediante el análisis de accesibilidad. Los LIF SAN FC y NVMe/FC no se mueven automáticamente. Continúan mostrando el

puerto raíz en el que estaban antes de actualizar.

Compruebe los LIF SAN en node4:

- a. Modifique cualquier LIF de SAN iSCSI que informe de un estado de operación inactivo a los nuevos puertos de datos:

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif>
```

- b. Modifique todos los LIF FC y NVMe/FC SAN que residan en la nueva controladora e informen de un estado operativo «inactivo» en los puertos FCP de la nueva controladora:

```
network interface modify -vserver <vserver> -lif <fc_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif>
```

2. Reanude la operación de reubicación:

```
system controller replace resume
```

El sistema ejecuta las siguientes tareas:

- Comprobación de quórum del clúster
- Comprobación del ID del sistema
- Comprobación de la versión de la imagen
- Comprobación de la plataforma de destino
- Comprobación de accesibilidad de red

La operación se detiene en esta fase de la comprobación de accesibilidad de red.

3. Reanude la operación de reubicación:

```
system controller replace resume
```

El sistema realiza las siguientes comprobaciones:

- Comprobación del estado del clúster
- Comprobación del estado de LIF de clúster

Después de ejecutar estas comprobaciones, el sistema reubica los agregados que no son raíz y los LIF de datos NAS que pertenecen al nodo 2 en la nueva controladora, el nodo 4. La operación de reemplazo de la controladora se coloca en pausa una vez que se completa la reubicación de recursos.

4. Comprobar el estado de las operaciones de reubicación de agregados y movimiento de LIF de datos de NAS:

```
system controller replace show-details
```

Si el procedimiento de reemplazo de la controladora está en pausa, compruebe y corrija el error, si corresponde, y luego emita `resume` para continuar la operación.

5. Si es necesario, restaure y devuelva los LIF desplazados. Enumerar las LIF desplazadas:

```
cluster controller-replacement network displaced-interface show
```

Si alguna LIF se ha desplazado, restaure el nodo de inicio al nodo 4:

```
cluster controller-replacement network displaced-interface restore-home-node
```

6. Reanude la operación para solicitar que el sistema realice las comprobaciones previas necesarias:

```
system controller replace resume
```

El sistema realiza las siguientes comprobaciones posteriores:

- Comprobación de quórum del clúster
- Comprobación del estado del clúster
- Comprobación de reconstrucción de los agregados
- Comprobación del estado del agregado
- Comprobación del estado del disco
- Comprobación del estado de LIF de clúster
- Comprobación del volumen

Etapa 6. Complete la actualización

Descripción general de la etapa 6

Durante la fase 6, el usuario confirma que los nodos nuevos están configurados correctamente y, si los nodos nuevos tienen la función de cifrado habilitada, se configuran y se configuran el cifrado de almacenamiento o el cifrado de volúmenes de NetApp. También debe retirar los nodos antiguos y reanudar las operaciones de SnapMirror.

Pasos

1. ["Gestionar la autenticación mediante servidores KMIP"](#)
2. ["Confirmar que las nuevas controladoras están configuradas correctamente"](#)
3. ["Configure Storage Encryption en el nuevo módulo de la controladora"](#)
4. ["Configure el cifrado de volúmenes de NetApp o el cifrado de agregados en el nuevo módulo de la controladora"](#)
5. ["Retire el sistema antiguo"](#)
6. ["Reanudar las operaciones de SnapMirror"](#)

Gestionar la autenticación mediante servidores KMIP

Es posible usar servidores de protocolo de interoperabilidad de gestión de claves (KMIP) para gestionar las claves de autenticación.

Pasos

1. Añadir una nueva controladora:

```
security key-manager external enable
```

2. Añada el gestor de claves:

```
security key-manager external add-servers -key-servers  
key_management_server_ip_address
```

3. Verifique que los servidores de gestión de claves estén configurados y disponibles para todos los nodos del clúster:

```
security key-manager external show-status
```

4. Restaure las claves de autenticación de todos los servidores de gestión de claves vinculados al nuevo nodo:

```
security key-manager external restore -node new_controller_name
```

Confirmar que las nuevas controladoras están configuradas correctamente

Para confirmar la configuración correcta, debe habilitar la pareja de ha. También es necesario verificar que los nodos 3 y 4 pueden acceder al almacenamiento de cada uno de los demás y que ninguno de los dos posee LIF de datos que pertenecen a otros nodos del clúster. Además, debe confirmar que el nodo 3 tiene agregados del nodo 1 y que el nodo 4 tiene agregados del nodo 2, y que los volúmenes de ambos nodos están en línea.

Pasos

1. Después de las comprobaciones posteriores al nodo 2, se habilitan la conmutación por error de almacenamiento y la pareja de alta disponibilidad de clúster para el clúster 2. Una vez finalizada la operación, ambos nodos muestran como completados y el sistema realiza algunas operaciones de limpieza.
2. Compruebe que la recuperación tras fallos del almacenamiento está activada:

```
storage failover show
```

En el ejemplo siguiente se muestra el resultado del comando cuando la conmutación por error del almacenamiento está habilitada:

```
cluster::> storage failover show
```

		Takeover	
Node	Partner	Possible	State Description
node3	node4	true	Connected to node4
node4	node3	true	Connected to node3

3. Verifique que los nodos 3 y 4 pertenezcan al mismo clúster mediante el siguiente comando y examinando el resultado:

```
cluster show
```

4. Verifique que los nodos 3 y 4 puedan acceder al almacenamiento de los demás mediante el siguiente comando y examinando el resultado:

```
storage failover show -fields local-missing-disks, partner-missing-disks
```

5. Verifique que ni el nodo 3 ni el nodo 4 sean propiedad de las LIF de datos propias del hogar de otros nodos del clúster. Para ello, utilice el siguiente comando y examine la salida:

```
network interface show
```

Si ni el nodo 3 ni el nodo 4 son propiedad de los LIF de datos propiedad del hogar de otros nodos del clúster, revierte las LIF de datos a su propietario doméstico:

```
network interface revert
```

6. Verifique que el nodo 3 tenga los agregados del nodo 1 y que el nodo 4 sea propietario de los agregados del nodo 2:

```
storage aggregate show -owner-name <node3>
```

```
storage aggregate show -owner-name <node4>
```

7. Determine si alguno de los volúmenes está sin conexión:

```
volume show -node <node3> -state offline
```

```
volume show -node <node4> -state offline
```

8. Si alguno de los volúmenes se encuentra sin conexión, compárelo con la lista de volúmenes sin conexión que ha capturado en la sección "[Prepare los nodos para la actualización](#)", y conectar cualquiera de los volúmenes sin conexión, según sea necesario, mediante el siguiente comando, una vez para cada volumen:

```
volume online -vserver <vserver_name> -volume <volume_name>
```

9. Instale licencias nuevas para los nodos nuevos mediante el siguiente comando para cada nodo:

```
system license add -license-code <license_code,license_code,license_code...>
```

El parámetro `license-code` acepta una lista de 28 claves de caracteres alfabéticos en mayúsculas. Puede añadir una licencia cada vez, o bien puede añadir varias licencias a la vez, separando cada clave de licencia por una coma.

10. Quite todas las licencias antiguas de los nodos originales mediante uno de los siguientes comandos:

```
system license clean-up -unused -expired
```

```
system license delete -serial-number <node_serial_number> -package  
<licensable_package>
```

- Eliminar todas las licencias caducadas:

```
system license clean-up -expired
```

- Elimine todas las licencias no utilizadas:

```
system license clean-up -unused
```

- Elimine una licencia específica de un clúster mediante los siguientes comandos en los nodos:

```
system license delete -serial-number <node1_serial_number> -package *
```

```
system license delete -serial-number <node2_serial_number> -package *
```

Se muestra la siguiente salida:

```
Warning: The following licenses will be removed:  
<list of each installed package>  
Do you want to continue? {y|n}: y
```

Introduzca `y` para eliminar todos los paquetes.

11. Compruebe que las licencias se han instalado correctamente mediante el siguiente comando y examine el resultado:

```
system license show
```

Puede comparar la salida con la que ha capturado en la sección "[Prepare los nodos para la actualización](#)".

12. Si se están utilizando unidades de autocifrado en la configuración y se ha establecido la `kmip.init.maxwait` variable en `off` (por ejemplo, en "[Instale y arranque el nodo 4, Paso 24](#)"), debe anular la definición de la variable:

```
set diag; systemshell -node <node_name> -command sudo kenv -u -p  
kmip.init.maxwait
```

13. Configure los SPS utilizando el siguiente comando en ambos nodos:

```
system service-processor network modify -node <node_name>
```

Consulte "[Referencias](#)" Para establecer un vínculo a la *referencia de administración del sistema* para

obtener información sobre los SPS y los comandos *ONTAP 9.8: Referencia de página del manual* para obtener información detallada sobre el sistema `service-processor network modify` comando.

14. Si desea configurar un clúster sin switches en los nuevos nodos, consulte "[Referencias](#)" Para establecer un enlace al *sitio de soporte de NetApp* y siga las instrucciones que se indican en *Cambiar a un clúster sin switch de dos nodos*.

Después de terminar

Si el cifrado del almacenamiento está habilitado en los nodos 3 y 4, complete la sección "[Configure Storage Encryption en el nuevo módulo de la controladora](#)". De lo contrario, complete la sección "[Retire el sistema antiguo](#)".

Configure Storage Encryption en el nuevo módulo de la controladora

Si la controladora reemplazada o el asociado de alta disponibilidad de la nueva controladora utilizan Storage Encryption, debe configurar el nuevo módulo de controlador para Storage Encryption, que incluye la instalación de certificados SSL y la configuración de servidores de administración de claves.

Acerca de esta tarea

Este procedimiento incluye los pasos que se realizan en el nuevo módulo del controlador. Debe introducir el comando en el nodo correcto.

Pasos

1. Compruebe que los servidores de gestión de claves aún estén disponibles, su estado y la información de la clave de autenticación:

```
security key-manager external show-status
```

```
security key-manager onboard show-backup
```

2. Añada los servidores de gestión de claves que se enumeran en el paso anterior a la lista del servidor de gestión de claves de la nueva controladora.
 - a. Añada el servidor de gestión de claves:

```
security key-manager external add-servers -key-servers  
key_management_server_ip_address
```

- b. Repita el paso anterior para cada servidor de gestión de claves enumerado. Puede vincular hasta cuatro servidores de gestión de claves.
- c. Compruebe que los servidores de gestión de claves se han añadido correctamente:

```
security key-manager external show
```

3. En el nuevo módulo de controlador, ejecute el asistente de configuración de gestión de claves para configurar e instalar los servidores de gestión de claves.

Debe instalar los mismos servidores de gestión de claves que se instalan en el módulo de controladora existente.

- a. Inicie el asistente de configuración del servidor de gestión de claves en el nuevo nodo:

```
security key-manager external enable
```

- b. Complete los pasos del asistente para configurar los servidores de gestión de claves.
4. Restaure las claves de autenticación de todos los servidores de gestión de claves vinculados al nuevo nodo:

```
security key-manager external restore -node new_controller_name
```

Configure el cifrado de volúmenes de NetApp o el cifrado de agregados en el nuevo módulo de la controladora

Si la controladora reemplazada o el partner de alta disponibilidad (ha) de la nueva controladora utilizan el cifrado de volúmenes de NetApp (NVE) o el cifrado de agregados de NetApp (NAE), debe configurar el nuevo módulo de controladoras para NVE o NAE.

Acerca de esta tarea

Este procedimiento incluye los pasos que se realizan en el nuevo módulo del controlador. Debe introducir el comando en el nodo correcto.

Gestión de claves incorporada

Configure NVE o NAE con el gestor de claves incorporado.

Pasos

1. Restaure las claves de autenticación de todos los servidores de gestión de claves vinculados al nuevo nodo:

```
security key-manager onboard sync
```

Gestión de claves externas

Configure NVE o NAE mediante la gestión de claves externa.

Pasos

1. Compruebe que los servidores de gestión de claves aún estén disponibles, su estado y la información de la clave de autenticación:

```
security key-manager key query -node node
```

2. Añada los servidores de gestión de claves que se enumeran en el paso anterior a la lista del servidor de gestión de claves de la nueva controladora:

- a. Añada el servidor de gestión de claves:

```
security key-manager external add-servers -key-servers  
key_management_server_ip_address
```

- b. Repita el paso anterior para cada servidor de gestión de claves enumerado. Puede vincular hasta cuatro servidores de gestión de claves.

- c. Compruebe que los servidores de gestión de claves se han añadido correctamente:

```
security key-manager external show
```

3. En el nuevo módulo de controlador, ejecute el asistente de configuración de gestión de claves para configurar e instalar los servidores de gestión de claves.

Debe instalar los mismos servidores de gestión de claves que se instalan en el módulo de controladora existente.

- a. Inicie el asistente de configuración del servidor de gestión de claves en el nuevo nodo:

```
security key-manager external enable
```

- b. Complete los pasos del asistente para configurar los servidores de gestión de claves.

4. Restaure las claves de autenticación de todos los servidores de gestión de claves vinculados al nuevo nodo:

```
security key-manager external restore
```

Este comando necesita la clave de acceso de OKM

Para obtener más información, vea el artículo de la base de conocimientos ["Cómo restaurar la configuración del servidor del administrador de claves externo desde el menú de arranque de](#)

Después de terminar

Compruebe si algún volumen se desconectó debido a que no había claves de autenticación disponibles o a que no se pudo acceder a los servidores EKM. Vuelva a conectar esos volúmenes en línea mediante el `volume online` comando.

Retire el sistema antiguo

Tras la actualización, puede retirar el sistema antiguo a través del sitio de soporte de NetApp. Decomisionando el sistema indica a NetApp que el sistema ya no está en funcionamiento y lo elimina de las bases de datos de soporte.

Pasos

1. Consulte "[Referencias](#)" Para enlazar con el *sitio de soporte de NetApp* e iniciar sesión.
2. Seleccione **Productos > Mis productos** en el menú.
3. En la página **Ver sistemas instalados**, elija los **criterios de selección** que desea utilizar para mostrar información sobre su sistema.

Puede elegir una de las siguientes opciones para localizar su sistema:

- Número de serie (situado en la parte posterior de la unidad)
- Números de serie para Mi ubicación

4. Seleccione **Go!**

Una tabla muestra información del clúster, incluidos los números de serie.

5. Localice el clúster en la tabla y seleccione **DECOMmission este sistema** en el menú desplegable Product Tool Set (conjunto de herramientas del producto).

Reanudar las operaciones de SnapMirror

Puede reanudar las transferencias de SnapMirror que se pusieron en modo inactivo antes de la actualización y reanudar las relaciones de SnapMirror. Las actualizaciones se programan una vez finalizada la actualización.

Pasos

1. Compruebe el estado de SnapMirror en el destino:

```
snapmirror show
```

2. Reanude la relación de SnapMirror:

```
snapmirror resume -destination-vserver vserver_name
```

Solucionar problemas

Solucionar problemas

Es posible que aparezca un error mientras se actualiza la pareja de nodos. El nodo podría bloquearse, es posible que los agregados no se reubiquen o que los LIF no migren. La causa del fallo y su solución dependen de cuándo se produjo el fallo durante el procedimiento de actualización.

Consulte la tabla que describe las diferentes fases del procedimiento en la sección "[Descripción general de la actualización de ARL](#)". La información sobre los fallos que pueden producirse se enumera en la fase del procedimiento.

Fallos de reubicación de agregados

La reubicación de agregados (ARL) puede fallar en diferentes puntos durante la actualización.

Compruebe si se ha producido un error de reubicación de agregados

Durante el procedimiento, ARL podría fallar en la etapa 2, etapa 3 o etapa 5.

Pasos

1. Introduzca el siguiente comando y examine la salida:

```
storage aggregate relocation show
```

La `storage aggregate relocation show` el comando muestra qué agregados se han reubicado correctamente y cuáles no, junto con las causas del fallo.

2. Compruebe si hay mensajes EMS en la consola.
3. Realice una de las siguientes acciones:
 - Tome la acción correctiva adecuada, en función del resultado del `storage aggregate relocation show` Y el resultado del mensaje de EMS.
 - Fuerce la reubicación del agregado o de los agregados mediante el `override-vetoes` o la `override-destination-checks` opción de `storage aggregate relocation start` comando.

Para obtener información detallada acerca de `storage aggregate relocation start`, `override-vetoes`, y `override-destination-checks` opciones, consulte "[Referencias](#)" Para enlazar a los comandos *ONTAP 9.8: Manual Page Reference*.

Los agregados, originalmente del nodo 1, son propiedad del nodo 4 después de completar la actualización

Al final del procedimiento de actualización, el nodo 3 debe ser el nuevo nodo de inicio de los agregados que originalmente tenían el nodo 1 como nodo de inicio. Puede reubicarlos tras la actualización.

Acerca de esta tarea

Es posible que los agregados no puedan reubicar correctamente y tener el nodo 1 como nodo de origen en

lugar del nodo 3 en las siguientes circunstancias:

- En la fase 3, cuando los agregados se trasladan del nodo 2 al nodo 3. Algunos de los agregados que se están reubicando tienen el nodo 1 como nodo de origen. Por ejemplo, un agregado de este tipo podría llamarse `aggr_node_1`. Si la reubicación de `aggr_node_1` falla durante la etapa 3 y no se puede forzar la reubicación, el agregado se quedará detrás en el nodo 2.
- Después de la fase 4, cuando el nodo 2 se reemplaza por el nodo 4. Cuando se reemplaza el nodo 2, `aggr_node_1` estará en línea con el nodo 4 como su nodo principal en lugar del nodo 3.

Puede resolver el problema de propiedad incorrecto después de la fase 6 una vez que se haya habilitado la conmutación por error del almacenamiento siguiendo los pasos siguientes:

Pasos

1. Escriba el siguiente comando para obtener una lista de agregados:

```
storage aggregate show -nodes node4 -is-home true
```

Para identificar los agregados que no se han reubicado correctamente, consulte la lista de agregados con el propietario raíz del nodo 1 obtenido en la sección ["Prepare los nodos para la actualización"](#) y compárelo con el resultado del comando anterior.

2. Compare la salida del paso 1 con la salida capturada para el nodo 1 de la sección ["Prepare los nodos para la actualización"](#) y anote los agregados que no se hayan reubicado correctamente.
3. reubique los agregados que quedan detrás del nodo 4:

```
storage aggregate relocation start -node node4 -aggr aggr_node_1 -destination node3
```

No utilice la `-ndo-controller-upgrade` parámetro durante esta reubicación.

4. Verifique que el nodo 3 ahora sea el propietario principal de los agregados:

```
storage aggregate show -aggregate aggr1,aggr2,aggr3... -fields home-name
```

`aggr1,aggr2,aggr3...` es la lista de agregados que tienen el nodo 1 como propietario original del hogar.

Los agregados que no tienen nodo 3 como propietario principal se pueden reubicar a nodo 3 con el mismo comando de reubicación en [Paso 3](#).

Reinicios, pánicos o ciclos de alimentación

Se puede bloquear el sistema: Reinicio, alarma o interrupción de un ciclo de encendido, durante las diferentes etapas de la actualización.

La solución a estos problemas depende de cuándo se produzcan.

Se reinicia, produce un pánico o se enciende durante la fase de comprobación previa

Los nodos 1 o 2 se bloquean antes de la fase de comprobación previa con el par de alta disponibilidad, aún habilitado

Si el nodo 1 o el nodo 2 se bloquean antes de la fase de comprobación previa, aún no se han reubicado agregados y la configuración de pares de alta disponibilidad está habilitada.

Acerca de esta tarea

La toma de control y la devolución pueden proceder con normalidad.

Pasos

1. Compruebe la consola para ver los mensajes de EMS que el sistema podría haber emitido y realice la acción correctiva recomendada.
2. Continúe con el procedimiento de actualización de la pareja de nodos.

Los reinicios, los pánicos o los ciclos de encendido y apagado durante la primera fase de la versión de recursos

El nodo 1 se bloquea durante la primera fase del lanzamiento de recursos con el par de alta disponibilidad todavía habilitado

Algunos o todos los agregados se han reubicado del nodo 1 al nodo 2 y el par de alta disponibilidad sigue estando habilitado. El nodo 2 toma el volumen raíz del nodo 1 y todos los agregados que no sean raíz en la ubicación.

Acerca de esta tarea

La propiedad de los agregados que se reubicaron tiene el mismo aspecto que la propiedad de los agregados no raíz que se tomaron el control porque el propietario de la casa no ha cambiado.

Cuando el nodo 1 entra en el `waiting for giveback` estado, el nodo 2 devuelve todos los agregados del nodo 1 que no son raíz.

Pasos

1. Después de arrancar el nodo 1, todos los agregados que no son raíz del nodo 1 se han movido de nuevo al nodo 1. Debe ejecutar una reubicación manual de agregados de los nodos 1 a 2:

```
storage aggregate relocation start -node node1 -destination node2 -aggregate -list * -ndocontroller-upgrade true
```
2. Continúe con el procedimiento de actualización de la pareja de nodos.

El nodo 1 se bloquea durante la primera fase de lanzamiento de recursos mientras se deshabilita el par de alta disponibilidad

El nodo 2 no toma el relevo, pero intenta servir datos en todos los agregados que no son raíz.

Pasos

1. Coloque el nodo 1.
2. Continúe con el procedimiento de actualización de la pareja de nodos.

Se produce un error en el nodo 2 durante la primera fase de lanzamiento de recursos con el par de alta disponibilidad, de todos modos habilitado

El nodo 1 ha reubicado algunos de sus agregados, o todos ellos, al nodo 2. La pareja de alta disponibilidad está habilitada.

Acerca de esta tarea

El nodo 1 asume todos los agregados del nodo 2, así como todos sus propios agregados, que se habían reubicado en el nodo 2. Cuando el nodo 2 arranca, la reubicación de agregados se completa automáticamente.

Pasos

1. Sube el 2.
2. Continúe con el procedimiento de actualización de la pareja de nodos.

El nodo 2 se bloquea en la primera fase de lanzamiento de recursos y después de que se deshabilita el par de alta disponibilidad

El nodo 1 no toma el control.

Pasos

1. Sube el 2.

Se produce una interrupción del servicio del cliente en todos los agregados, mientras que el nodo 2 arranca.

2. Continúe con el resto del procedimiento de actualización de la pareja de nodos.

Reinicia, produce un pánico o ciclos de encendido durante la primera fase de verificación

El nodo 2 se bloquea en la primera fase de verificación con el par de alta disponibilidad deshabilitado

El nodo 3 no retoma después de un bloqueo del nodo 2, ya que la pareja de alta disponibilidad ya está deshabilitada.

Pasos

1. Sube el 2.

Se produce una interrupción del servicio del cliente en todos los agregados, mientras que el nodo 2 arranca.

2. Continúe con el procedimiento de actualización de la pareja de nodos.

El nodo 3 se bloquea durante la primera fase de verificación con la pareja de alta disponibilidad deshabilitada

El nodo 2 no toma el relevo, pero intenta servir datos en todos los agregados que no son raíz.

Pasos

1. Traiga el nodo 3.
2. Continúe con el procedimiento de actualización de la pareja de nodos.

Reinicios, pánicos o ciclos de alimentación durante la primera fase de recuperación de recursos

El nodo 2 se bloquea durante la primera fase de recuperación de recursos durante la reubicación de agregados

El nodo 2 ha reubicado algunos o todos sus agregados del nodo 1 al nodo 3. El nodo 3 proporciona datos de agregados que se reubicaron. El par de alta disponibilidad está deshabilitado y, por lo tanto, no hay toma de control.

Acerca de esta tarea

Hay una interrupción del cliente para los agregados que no se han reubicado. Cuando el nodo de arranque del nodo 2, los agregados del nodo 1 se reubican en nodo 3.

Pasos

1. Sube el 2.

2. Continúe con el procedimiento de actualización de la pareja de nodos.

El nodo 3 se bloquea durante la primera fase de recuperación de recursos durante la reubicación de agregados

Si el nodo 3 se bloquea mientras el nodo 2 se reubica los agregados en el nodo 3, la tarea continúa después de que se arranca el nodo 3.

Acerca de esta tarea

El nodo 2 sigue sirviendo agregados restantes, pero los agregados que ya se reubicaron en nodo 3 se encuentran en una interrupción de cliente, mientras que el nodo 3 se inicia.

Pasos

1. Traiga el nodo 3.
2. Continúe con la actualización de la controladora.

Reinicios, pánicos o ciclos de alimentación durante la fase posterior a la comprobación

El nodo 2 o 3 se bloquea durante la fase de comprobación posterior

El par de alta disponibilidad está deshabilitado, por lo que no se toma el control. Hay una interrupción del cliente para los agregados que pertenecen al nodo que se reinició.

Pasos

1. Suba el nodo.
2. Continúe con el procedimiento de actualización de la pareja de nodos.

Reinicios, pánicos o ciclos de encendido durante la segunda fase de lanzamiento de recursos

El nodo 3 se bloquea durante la segunda fase de versión de recursos

Si el nodo 3 se bloquea mientras el nodo 2 está reubicando agregados, la tarea continuará después de que se arranque el nodo 3.

Acerca de esta tarea

El nodo 2 sigue sirviendo agregados restantes, pero los agregados que ya se reubicaron en los agregados de nodo 3 y los propios de nodo 3 se encuentran en situación de interrupción del servicio del cliente, mientras que el nodo 3 se inicia.

Pasos

1. Traiga el nodo 3.
2. Continúe con el procedimiento de actualización de la controladora.

El nodo 2 se bloquea durante la segunda fase de publicación de recursos

Si el nodo 2 se bloquea durante la reubicación de agregados, el nodo 2 no se retoma.

Acerca de esta tarea

El nodo 3 sigue sirviendo los agregados que se reubicaron, pero los agregados propiedad del nodo 2 encuentran las interrupciones de servicio del cliente.

Pasos

1. Sube el 2.

2. Continúe con el procedimiento de actualización de la controladora.

Reinicia, produce un pánico o ciclos de encendido durante la segunda fase de verificación

El nodo 3 se bloquea durante la segunda fase de verificación

Si el nodo 3 se bloquea durante esta fase, la toma de control no se produce porque la pareja de alta disponibilidad ya está deshabilitada.

Acerca de esta tarea

Hay una interrupción del servicio del cliente de todos los agregados hasta que se reinicia el nodo 3.

Pasos

1. Traiga el nodo 3.
2. Continúe con el procedimiento de actualización de la pareja de nodos.

Node4 se bloquea durante la segunda fase de verificación

Si el nodo 4 se bloquea durante esta fase, la toma de control no se produce. El nodo 3 proporciona datos de los agregados.

Acerca de esta tarea

Existe una interrupción del servicio de los agregados que no son raíz que ya se removieron hasta reinicios de nodo 4.

Pasos

1. Traiga el nodo 4.
2. Continúe con el procedimiento de actualización de la pareja de nodos.

Problemas que pueden surgir en varias etapas del procedimiento

Algunos problemas pueden ocurrir durante diferentes etapas del procedimiento.

Resultado de comando "Storage Failover show" inesperado

Durante el procedimiento, si el nodo que aloja todos los agregados de datos produce una alarma o se reinicia por accidente, podría ver un resultado inesperado para el `storage failover show` comando antes y después del reinicio, la alarma o el ciclo de apagado y encendido.

Acerca de esta tarea

Puede que aparezca un resultado inesperado en el `storage failover show` Orden en la etapa 2, etapa 3, etapa 4 o etapa 5.

El siguiente ejemplo muestra el resultado esperado del `storage failover show` comando si no hay reinicios o produce una alarma en el nodo que aloja todos los agregados de datos:

```
cluster::> storage failover show
```

Node	Partner	Takeover	
		Possible	State Description
node1	node2	false	Unknown
node2	node1	false	Node owns partner aggregates as part of the non-disruptive head upgrade procedure. Takeover is not possible: Storage failover is disabled.

En el siguiente ejemplo, se muestra el resultado del `storage failover show` comando tras un reinicio o una alarma:

```
cluster::> storage failover show
```

Node	Partner	Takeover	
		Possible	State Description
node1	node2	-	Unknown
node2	node1	false	Waiting for node1, Partial giveback, Takeover is not possible: Storage failover is disabled

Aunque el resultado dice que un nodo está en una devolución parcial y que la conmutación al respaldo del almacenamiento está deshabilitada, puede ignorar este mensaje.

Pasos

No es necesario realizar ninguna acción; continúe con el procedimiento de actualización de la pareja de nodos.

Error de migración de LIF

Después de migrar las LIF, es posible que no entren en línea después de la migración en las fases 2, fase 3 o fase 5.

Pasos

1. Compruebe que el tamaño de MTU del puerto sea el mismo que el del nodo de origen.

Por ejemplo, si el tamaño de MTU de puerto de clúster es 9000 en el nodo de origen, debe ser 9000 en el nodo de destino.

2. Compruebe la conectividad física del cable de red si el estado físico del puerto es `down`.

Referencias

Al realizar los procedimientos de este contenido, es posible que deba consultar el contenido de referencia o ir a sitios web de referencia.

- [Contenido de referencia](#)
- [Sitios de referencia](#)

Contenido de referencia

El contenido específico de esta actualización se muestra en la siguiente tabla.

Contenido	Descripción
"Información general de administración con la interfaz de línea de comandos"	Describe cómo administrar sistemas ONTAP, muestra cómo usar la interfaz de línea de comandos, cómo acceder al clúster, cómo gestionar nodos y mucho más.
"Decidir si se debe usar System Manager o la CLI de ONTAP para la configuración del clúster"	Describe cómo instalar y configurar ONTAP.
"Gestión de discos y agregados con la interfaz de línea de comandos"	Describe cómo gestionar el almacenamiento físico de ONTAP mediante la interfaz de línea de comandos. Muestra cómo crear, expandir y gestionar agregados, cómo trabajar con agregados de Flash Pool, cómo gestionar discos y cómo gestionar políticas de RAID.
"Referencias y requisitos de instalación de la virtualización FlexArray"	Contiene instrucciones de cableado y otra información para los sistemas de virtualización FlexArray.
"Gestión de alta disponibilidad"	Describe cómo instalar y gestionar las configuraciones almacenadas en clúster de alta disponibilidad, incluidas la conmutación al nodo de respaldo y la toma de control/retorno al nodo primario de almacenamiento.
"Gestión de almacenamiento lógico con CLI"	Describe cómo gestionar de forma eficiente sus recursos de almacenamiento lógico mediante volúmenes, volúmenes de FlexClone, archivos y LUN Volúmenes FlexCache, deduplicación, compresión, qtrees y cuotas.
"Actualización y ampliación de MetroCluster"	Ofrece procedimientos para actualizar los modelos de controladora y de almacenamiento de la configuración de MetroCluster, realizar la transición de una configuración IP de MetroCluster FC a una MetroCluster y ampliar la configuración de MetroCluster añadiendo nodos adicionales.
"Gestión de redes"	Describe cómo configurar y gestionar puertos de red físicos y virtuales (VLAN y grupos de interfaces), LIF, enrutamiento y servicios de resolución de hosts en clústeres; además, describe cómo optimizar el tráfico de red con el equilibrio de carga y cómo supervisar el clúster mediante SNMP.
"Comandos de ONTAP 9.13.1: Referencia de páginas del manual"	Describe la sintaxis y el uso de los comandos de ONTAP 9.13.1 admitidos.
"Comandos de ONTAP 9.14.1: Referencia de páginas del manual"	Describe la sintaxis y el uso de los comandos de ONTAP 9.14.1 admitidos.
"Comandos de ONTAP 9.15.1: Referencia de páginas del manual"	Describe la sintaxis y el uso de los comandos de ONTAP 9.15.1 admitidos.

Contenido	Descripción
"Gestión DE SAN con CLI"	Describe cómo configurar y gestionar LUN, iGroups y objetivos mediante los protocolos iSCSI y FC, así como los espacios de nombres y subsistemas mediante el protocolo NVMe/FC.
"Referencia para la configuración DE SAN"	Contiene información sobre las topologías FC e iSCSI y las esquemas de cableado.
"Actualice trasladando volúmenes o almacenamiento"	Describe cómo actualizar rápidamente el hardware de la controladora en un clúster moviendo almacenamiento o volúmenes. También describe cómo convertir un modelo compatible en una bandeja de discos.
"Actualice ONTAP"	Contiene instrucciones para descargar y actualizar ONTAP.
"Utilice los comandos para sustituir la controladora del sistema para actualizar los modelos de controladora en el mismo chasis"	Describe los procedimientos de reubicación de agregados necesarios para actualizar un sistema de forma no disruptiva y mantener los antiguos chasis y discos del sistema.
"Utilice comandos para sustituir la controladora del sistema para actualizar el hardware de la controladora que ejecute ONTAP 9.8 o una versión posterior"	Describe los procedimientos de reubicación de agregados necesarios para actualizar sin interrupciones controladoras que ejecutan ONTAP 9.8 mediante los comandos de "reemplazo de controladora del sistema".
"Utilice la reubicación de agregados para actualizar manualmente el hardware de la controladora que ejecuta ONTAP 9.8 o una versión posterior"	Describe los procedimientos de reubicación de agregados necesarios para realizar actualizaciones manuales de controladoras sin interrupciones que ejecuten ONTAP 9.8 o una versión posterior.

Sitios de referencia

La "[Sitio de soporte de NetApp](#)" También contiene documentación sobre las tarjetas de interfaz de red (NIC) y otro hardware que puede utilizar con el sistema. También contiene la "[Hardware Universe](#)", que proporciona información acerca del hardware que admite el nuevo sistema.

Acceso "[Documentación de ONTAP 9](#)".

Acceda a "[Active IQ Config Advisor](#)" herramienta.

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.