



Soporte de arranque

Install and maintain

NetApp
July 19, 2024

Tabla de contenidos

- Soporte de arranque 1
 - Descripción general de la sustitución de medios de arranque: FAS8200 1
 - Compruebe el cifrado incorporado: FAS8200 1
 - Apague la controladora dañada - FAS8200 8
 - Sustituya el medio de arranque - FAS8200 12
 - Arranque la imagen de recuperación: FAS8200 16
 - Vuelva a cambiar los agregados en una configuración MetroCluster de dos nodos: FAS8200 19
 - Restaura OKM, NSE y NVE según sea necesario: FAS8200 20
 - Devuelva la parte con el error a NetApp - FAS8200 26

Soporte de arranque

Descripción general de la sustitución de medios de arranque: FAS8200

El soporte de arranque almacena un conjunto principal y secundario de archivos del sistema (imagen de arranque) que el sistema utiliza cuando arranca. En función de la configuración de red, puede realizar una sustitución no disruptiva o disruptiva.

Debe tener una unidad flash USB, formateada a FAT32, con la cantidad de almacenamiento adecuada para guardar el `image_XXX.tgz` archivo.

También debe copiar el `image_XXX.tgz` Archivo a la unidad flash USB para su uso posterior en este procedimiento.

- Ambos métodos no disruptivos y disruptivos para reemplazar medios de arranque requieren restaurar el `var` sistema de archivos:
 - Para poder realizar sustituciones de forma no disruptiva, el par de alta disponibilidad debe estar conectado a una red para restaurar el `var` sistema de archivos.
 - Para el reemplazo disruptivo, no es necesaria una conexión de red para restaurar el `var` el sistema de archivos, pero el proceso requiere dos reinicios.
- Debe sustituir el componente con errores por un componente FRU de repuesto que haya recibido de su proveedor.
- Es importante que aplique los comandos en estos pasos en el nodo correcto:
 - El nodo *drinated* es el nodo en el que realiza tareas de mantenimiento.
 - El *heated node* es el partner de alta disponibilidad del nodo dañado.

Compruebe el cifrado incorporado: FAS8200

Antes de apagar la controladora con deterioro y comprobar el estado de las claves de cifrado integradas, debe comprobar el estado de la controladora con deterioro, deshabilitar la devolución automática del control y comprobar la versión de ONTAP que el sistema está ejecutando.

Antes de apagar la controladora deficiente y comprobar el estado de las claves de cifrado incorporadas, debe comprobar el estado de la controladora deficiente, deshabilitar la devolución automática y comprobar qué versión de ONTAP se está ejecutando en el sistema.

Si tiene un clúster con más de dos nodos, debe estar en quórum. Si el clúster no tiene quórum o si una controladora en buen estado muestra FALSE para tener derecho a recibir este tipo de servicios, debe corregir el problema antes de apagar la controladora con deficiencias; consulte la ["Sincronice un nodo con el clúster"](#).

Pasos

1. Compruebe el estado del controlador dañado:
 - Si el controlador dañado se encuentra en la solicitud de inicio de sesión, inicie sesión como `admin`.
 - Si la controladora dañada se encuentra en el aviso del CARGADOR y forma parte de la configuración

de alta disponibilidad, inicie sesión como `admin` en el controlador en buen estado.

- Si la controladora dañada se encuentra en una configuración independiente y en un aviso DEL CARGADOR, póngase en contacto con "mysupport.netapp.com".

2. Si AutoSupport está habilitado, elimine la creación automática de casos invocando un mensaje de AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

El siguiente mensaje de AutoSupport suprime la creación automática de casos durante dos horas:

```
cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h
```

3. Compruebe la versión de ONTAP que el sistema está funcionando en el controlador dañado si está activo, o en el controlador asociado si el controlador dañado está inactivo, usando el `version -v` comando:
 - Si se muestra `<lno-DARE>` o `<1Ono-DARE>` en el resultado del comando, el sistema no admite NVE, continúe para apagar la controladora.
 - Si `<lno-DARE>` no se muestra en el resultado del comando y el sistema ejecuta ONTAP 9.5, vaya a. [Opción 1: Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.5 y versiones anteriores.](#)
 - Si `<lno-DARE>` no se muestra en el resultado del comando y el sistema está ejecutando ONTAP 9.6 o una versión posterior, vaya a. [Opción 2: Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores.](#)
4. Si la controladora dañada forma parte de una configuración de alta disponibilidad, deshabilite la recuperación automática de la controladora en buen estado: `storage failover modify -node local -auto-giveback false` o `storage failover modify -node local -auto-giveback -after-panic false`

Opción 1: Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.5 y versiones anteriores

Antes de apagar la controladora dañada, debe comprobar si el sistema tiene habilitado el cifrado de volúmenes de NetApp (NVE) o el cifrado de almacenamiento de NetApp (NSE). Si es así, debe comprobar la configuración.

Pasos

1. Conecte el cable de la consola al controlador dañado.
2. Compruebe si el cifrado de volúmenes está configurado para cualquier volumen del clúster: `volume show -is-encrypted true`

Si algún volumen aparece en la salida, NVE se configura y debe verificar la configuración NVE. Si no aparece ningún volumen en la lista, compruebe si NSE está configurado.

3. Compruebe si NSE está configurado: `storage encryption disk show`
 - Si el resultado del comando incluye los detalles de la unidad con información sobre el modo y el identificador de claves, se configura NSE y se debe verificar la configuración de NSE.
 - Si NVE y NSE no están configurados, es seguro apagar el controlador afectado.

Verifique la configuración de NVE

Pasos

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de

claves: `security key-manager query`

- Si la `Restored` la columna muestra `yes` y se muestran todos los gestores de claves `available`, es seguro apagar el controlador dañado.
- Si la `Restored` columna muestra cualquier otra cosa que no sea `yes` o si aparece algún gestor de claves `unavailable`, necesita completar algunos pasos adicionales.
- Si ve el mensaje este comando no es compatible con la gestión de claves incorporada, debe completar algunos pasos adicionales.

2. Si la `Restored` columna mostrada cualquier otra cosa que no sea `yes` o si aparece algún gestor de claves `unavailable`:

- a. Recupere y restaure todas las claves de autenticación y los ID de clave asociados: `security key-manager restore -address *`

Si el comando falla, póngase en contacto con el soporte de NetApp.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Compruebe que el `Restored` la columna muestra `yes` para todas las claves de autenticación y que se muestran todos los gestores de claves `available`: `security key-manager query`

- b. Apague el controlador dañado.

3. Si vio el mensaje este comando no es compatible cuando la gestión de claves incorporada está habilitada, muestre las claves almacenadas en el gestor de claves incorporado: `security key-manager key show -detail`

- a. Si la `Restored` la columna muestra `yes` realice un backup manual de la información de gestión de claves incorporada:

- Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
- Introduzca el comando para mostrar la información de backup de OKM: `security key-manager backup show`
- Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.
- Volver al modo admin: `set -priv admin`
- Apague el controlador dañado.

- b. Si la `Restored` columna muestra cualquier otra cosa que no sea `yes`:

- Ejecute el asistente de configuración Key-Manager: `security key-manager setup -node target/impaired node name`



Introduzca la clave de acceso de gestión de claves incorporada del cliente en el símbolo del sistema de. Si no se puede proporcionar la frase de contraseña, póngase en contacto con ["mysupport.netapp.com"](https://mysupport.netapp.com)

- Compruebe que el `Restored` la columna muestra `yes` para toda la clave de autenticación: `security key-manager key show -detail`
- Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv`

advanced

- Introduzca el comando para mostrar la información de backup de OKM: `security key-manager backup show`
- Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.
- Volver al modo admin: `set -priv admin`
- Puede apagar la controladora de forma segura.

Verifique la configuración de NSE

Pasos

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves: `security key-manager query`
 - Si la `Restored` la columna muestra `yes` y se muestran todos los gestores de claves `available`, es seguro apagar el controlador dañado.
 - Si la `Restored` columna muestra cualquier otra cosa que no sea `yes` o si aparece algún gestor de claves `unavailable`, necesita completar algunos pasos adicionales.
 - Si ve el mensaje este comando no es compatible con la gestión de claves incorporada, debe completar algunos pasos adicionales
2. Si la `Restored` columna mostrada cualquier otra cosa que no sea `yes` o si aparece algún gestor de claves `unavailable`:
 - a. Recupere y restaure todas las claves de autenticación y los ID de clave asociados: `security key-manager restore -address *`

Si el comando falla, póngase en contacto con el soporte de NetApp.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Compruebe que el `Restored` la columna muestra `yes` para todas las claves de autenticación y que se muestran todos los gestores de claves `available`: `security key-manager query`
 - b. Apague el controlador dañado.
3. Si vio el mensaje este comando no es compatible cuando la gestión de claves incorporada está habilitada, muestre las claves almacenadas en el gestor de claves incorporado: `security key-manager key show -detail`
 - a. Si la `Restored` la columna muestra `yes`, realice una copia de seguridad manual de la información de administración de claves integrada:
 - Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
 - Introduzca el comando para mostrar la información de backup de OKM: `security key-manager backup show`
 - Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.

- Volver al modo admin: `set -priv admin`
- Apague el controlador dañado.

b. Si la `Restored` columna muestra cualquier otra cosa que no sea `yes`:

- Ejecute el asistente de configuración Key-Manager: `security key-manager setup -node target/impaired node name`



Introduzca la frase de contraseña de OKM del cliente en la solicitud. Si no se puede proporcionar la frase de contraseña, póngase en contacto con ["mysupport.netapp.com"](https://mysupport.netapp.com)

- Compruebe que el `Restored` la columna muestra `yes` para todas las claves de autenticación: `security key-manager key show -detail`
- Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
- Introduzca el comando para realizar un backup de la información de OKM: `security key-manager backup show`



Asegúrese de que la información de OKM se guarda en su archivo de registro. Esta información será necesaria en situaciones de desastre en las que OKM podría necesitar recuperación manual.

- Copie el contenido de la información de la copia de seguridad en un archivo o registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.
- Volver al modo admin: `set -priv admin`
- Puede apagar el controlador de forma segura.

Opción 2: Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores

Antes de apagar la controladora dañada, debe verificar si el sistema tiene habilitado el cifrado de volúmenes de NetApp (NVE) o el cifrado de almacenamiento de NetApp (NSE). Si es así, debe comprobar la configuración.

1. Verifique si el cifrado de volúmenes está en uso para cualquier volumen del clúster: `volume show -is -encrypted true`

Si algún volumen aparece en la salida, NVE se configura y debe verificar la configuración NVE. Si no aparece ningún volumen en la lista, compruebe si NSE está configurado y en uso.

2. Compruebe si NSE está configurado y en uso: `storage encryption disk show`
 - Si el resultado del comando incluye los detalles de la unidad con información sobre el modo y el identificador de clave, NSE se configura y es necesario verificar la configuración de NSE y en uso.
 - Si no se muestra ningún disco, NSE no está configurado.
 - Si NVE y NSE no están configurados, no hay unidades protegidas con las claves NSE, es seguro apagar la controladora dañada.

Verifique la configuración de NVE

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves: `security key-manager key query`



Después de la versión ONTAP 9.6, es posible que tenga otros tipos de gestor de claves. Los tipos son KMIP, AKV, y GCP. El proceso de confirmación de estos tipos es el mismo que el de confirmación `external` o `onboard` tipos de gestor de claves.

- Si la `Key Manager` aparece el tipo `external` y la `Restored` la columna muestra `yes`, es seguro apagar el controlador dañado.
 - Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, necesita completar algunos pasos adicionales.
 - Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.
 - Si la `Key Manager` aparece el tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.
2. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, Realizar una copia de seguridad manual de la información de OKM:
 - a. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
 - b. Introduzca el comando para mostrar la información de gestión de claves: `security key-manager onboard show-backup`
 - c. Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.
 - d. Volver al modo `admin`: `set -priv admin`
 - e. Apague el controlador dañado.
 3. Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
 - a. Restaure las claves de autenticación de gestión de claves externas a todos los nodos del clúster: `security key-manager external restore`

Si el comando falla, póngase en contacto con el soporte de NetApp.

["mysupport.netapp.com"](https://mysupport.netapp.com)
 4. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
 - a. Introduzca el comando SYNC del gestor de claves de seguridad incorporado: `security key-manager onboard sync`



Introduzca 32 la clave de acceso de gestión de claves incorporada y alfanumérica del cliente en el símbolo del sistema. Si no se puede proporcionar la clave de acceso, comuníquese con el soporte de NetApp. "mysupport.netapp.com"

- b. Compruebe el Restored la columna muestra `yes` para todas las claves de autenticación: `security key-manager key query`
- c. Compruebe que el Key Manager el tipo muestra `onboard`, Y a continuación, realice una copia de seguridad manual de la información de OKM.
- d. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
- e. Introduzca el comando para mostrar la información de backup para la gestión de claves: `security key-manager onboard show-backup`
- f. Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.
- g. Volver al modo admin: `set -priv admin`
- h. Puede apagar el controlador de forma segura.

Verifique la configuración de NSE

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves: `security key-manager key query -key-type NSE-AK`



Después de la versión ONTAP 9.6, es posible que tenga otros tipos de gestor de claves. Los tipos son `KMIP`, `AKV`, y `GCP`. El proceso de confirmación de estos tipos es el mismo que el de confirmación `external` o `onboard` tipos de gestor de claves.

- Si la Key Manager aparece el tipo `external` y la Restored la columna muestra `yes`, es seguro apagar el controlador dañado.
 - Si la Key Manager aparece el tipo `onboard` y la Restored la columna muestra `yes`, necesita completar algunos pasos adicionales.
 - Si la Key Manager aparece el tipo `external` y la Restored columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.
 - Si la Key Manager aparece el tipo `external` y la Restored columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.
2. Si la Key Manager aparece el tipo `onboard` y la Restored la columna muestra `yes`, Realizar una copia de seguridad manual de la información de OKM:
 - a. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
 - b. Introduzca el comando para mostrar la información de gestión de claves: `security key-manager onboard show-backup`
 - c. Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.

- d. Volver al modo admin: `set -priv admin`
 - e. Puede apagar el controlador de forma segura.
3. Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
- a. Restaure las claves de autenticación de gestión de claves externas a todos los nodos del clúster:
`security key-manager external restore`

Si el comando falla, póngase en contacto con el soporte de NetApp.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Compruebe que el `Restored` la columna es igual `yes` para todas las claves de autenticación:
`security key-manager key query`
 - b. Puede apagar el controlador de forma segura.
4. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
- a. Introduzca el comando `SYNC` del gestor de claves de seguridad incorporado: `security key-manager onboard sync`

Introduzca 32 la clave de acceso de gestión de claves incorporada y alfanumérica del cliente en el símbolo del sistema. Si no se puede proporcionar la clave de acceso, comuníquese con el soporte de NetApp.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Compruebe el `Restored` la columna muestra `yes` para todas las claves de autenticación: `security key-manager key query`
- b. Compruebe que el `Key Manager` el tipo muestra `onboard`, Y a continuación, realice una copia de seguridad manual de la información de OKM.
- c. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
- d. Introduzca el comando para mostrar la información de backup para la gestión de claves: `security key-manager onboard show-backup`
- e. Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.
- f. Volver al modo admin: `set -priv admin`
- g. Puede apagar el controlador de forma segura.

Apague la controladora dañada - FAS8200

Opción 1: La mayoría de los sistemas

Después de completar las tareas de NVE o NSE, deberá completar el apagado de la controladora dañada. Después de completar las tareas de NVE o NSE, deberá completar

el apagado de la controladora dañada.

Pasos

1. Lleve la controladora dañada al aviso DEL CARGADOR:

Si el controlador dañado muestra...	Realice lo siguiente...
El aviso del CARGADOR	Vaya a Quitar módulo de controlador.
Waiting for giveback...	Pulse Ctrl-C y, a continuación, responda <code>y</code> cuando se le solicite.
Solicitud del sistema o solicitud de contraseña (introduzca la contraseña del sistema)	Retome o detenga el controlador dañado del controlador en buen estado: <code>storage failover takeover -ofnode impaired_node_name</code> Cuando el controlador dañado muestre esperando devolución..., pulse Ctrl-C y, a continuación, responda <code>y</code> .

2. Desde el aviso del CARGADOR, introduzca: `printenv` para capturar todas las variables ambientales de arranque. Guarde el resultado en el archivo de registro.



Es posible que este comando no funcione si el dispositivo de inicio está dañado o no funciona.

Opción 2: La controladora está en una configuración MetroCluster



No use este procedimiento si el sistema está en una configuración de MetroCluster de dos nodos.

Para apagar el controlador dañado, debe determinar el estado del controlador y, si es necesario, tomar el control para que el controlador sano siga sirviendo datos del almacenamiento del controlador dañado.

- Si tiene un clúster con más de dos nodos, debe estar en quórum. Si el clúster no tiene quórum o si una controladora en buen estado muestra falso según su condición, debe corregir el problema antes de apagar la controladora dañada; consulte "[Sincronice un nodo con el clúster](#)".
- Si tiene una configuración MetroCluster, debe haber confirmado que el estado de configuración de MetroCluster está configurado y que los nodos están en estado normal y habilitado (`metrocluster node show`).

Pasos

1. Si AutoSupport está habilitado, elimine la creación automática de casos invocando un mensaje de AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

El siguiente mensaje de AutoSupport suprime la creación automática de casos durante dos horas:

```
cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Deshabilite la devolución automática de la consola de la controladora en buen estado: `storage`

```
failover modify -node local -auto-giveback false
```

3. Lleve la controladora dañada al aviso DEL CARGADOR:

Si el controlador dañado está mostrando...	Realice lo siguiente...
El aviso del CARGADOR	Vaya al paso siguiente.
Esperando devolución...	Pulse Ctrl-C y, a continuación, responda <code>y</code> cuando se le solicite.
Solicitud del sistema o solicitud de contraseña (introduzca la contraseña del sistema)	Retome o detenga el controlador dañado del controlador en buen estado: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code> Cuando el controlador dañado muestre esperando devolución..., pulse Ctrl-C y, a continuación, responda <code>y</code> .

Opción 3: La controladora se encuentra en un MetroCluster de dos nodos

Para apagar el controlador dañado, debe determinar el estado del controlador y, si es necesario, cambiar el controlador para que el controlador correcto siga sirviendo datos del almacenamiento del controlador dañado.

Acerca de esta tarea

- Debe dejar las fuentes de alimentación encendidas al final de este procedimiento para proporcionar alimentación a la controladora en buen estado.

Pasos

1. Compruebe el estado de MetroCluster para determinar si el controlador dañado ha cambiado automáticamente al controlador en buen estado: `metrocluster show`
2. En función de si se ha producido una conmutación automática, proceda según la siguiente tabla:

Si el controlador está dañado...	Realice lo siguiente...
Se ha cambiado automáticamente	Continúe con el próximo paso.
No se ha cambiado automáticamente	Realice una operación de conmutación de sitios planificada desde el controlador en buen estado: <code>metrocluster switchover</code>
No se ha cambiado automáticamente, ha intentado efectuar una conmutación con el <code>metrocluster switchover</code> y se vetó la conmutación	Revise los mensajes de veto y, si es posible, resuelva el problema e inténtelo de nuevo. Si no puede resolver el problema, póngase en contacto con el soporte técnico.

3. Resincronice los agregados de datos ejecutando el `metrocluster heal -phase aggregates` comando del clúster superviviente.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

Si la curación es vetada, usted tiene la opción de reemitir el `metrocluster heal` con el `-override -vetoos` parámetro. Si utiliza este parámetro opcional, el sistema anula cualquier veto suave que impida la operación de reparación.

4. Compruebe que se ha completado la operación con el comando `MetroCluster operation show`.

```
controller_A_1::> metrocluster operation show
  Operation: heal-aggregates
  State: successful
Start Time: 7/25/2016 18:45:55
  End Time: 7/25/2016 18:45:56
  Errors: -
```

5. Compruebe el estado de los agregados mediante `storage aggregate show` comando.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes      RAID
Status
-----
...
aggr_b2       227.1GB   227.1GB   0% online    0 mcc1-a2
raid_dp, mirrored, normal...
```

6. Repare los agregados raíz mediante el `metrocluster heal -phase root-aggregates` comando.

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

Si la curación es vetada, usted tiene la opción de reemitir el `metrocluster heal` comando con el parámetro `-override-vetoos`. Si utiliza este parámetro opcional, el sistema anula cualquier veto suave que impida la operación de reparación.

7. Compruebe que la operación reparar se ha completado mediante el `metrocluster operation show` comando en el clúster de destino:

```
mccl1A::> metrocluster operation show
  Operation: heal-root-aggregates
    State: successful
  Start Time: 7/29/2016 20:54:41
  End Time: 7/29/2016 20:54:42
  Errors: -
```

8. En el módulo del controlador dañado, desconecte las fuentes de alimentación.

Sustituya el medio de arranque - FAS8200

Para sustituir el soporte de arranque, debe retirar el módulo del controlador dañado, instalar el soporte de arranque de repuesto y transferir la imagen de inicio a una unidad flash USB.

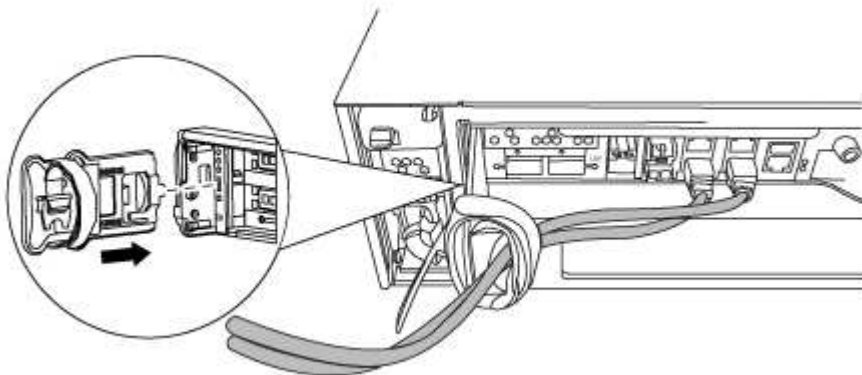
Paso 1: Quite la controladora

Para acceder a los componentes del interior del controlador, primero debe extraer el módulo del controlador del sistema y, a continuación, retirar la cubierta del módulo del controlador.

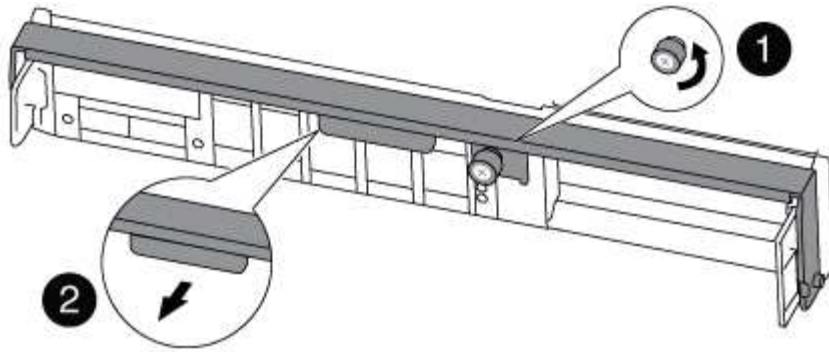
1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Afloje el gancho y la correa de bucle que sujetan los cables al dispositivo de administración de cables y, a continuación, desconecte los cables del sistema y los SFP (si fuera necesario) del módulo del controlador, manteniendo un seguimiento del lugar en el que estaban conectados los cables.

Deje los cables en el dispositivo de administración de cables de manera que cuando vuelva a instalar el dispositivo de administración de cables, los cables estén organizados.

3. Retire y retire los dispositivos de administración de cables de los lados izquierdo y derecho del módulo del controlador.



4. Afloje el tornillo de ajuste manual del asa de leva del módulo del controlador.



1

Tornillo de apriete manual

2

Mango de leva

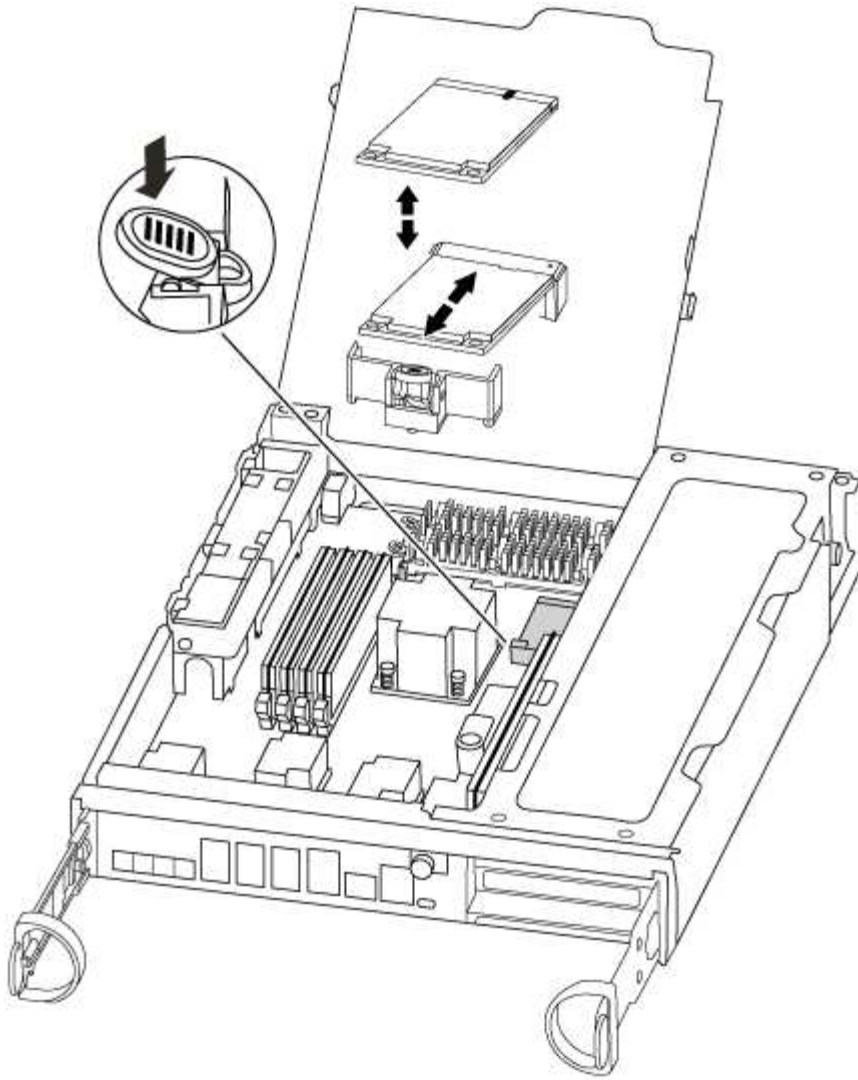
5. Tire del asa de leva hacia abajo y comience a sacar el módulo del controlador del chasis.

Asegúrese de que admite la parte inferior del módulo de la controladora cuando la deslice para sacarlo del chasis.

Paso 2: Sustituya el soporte de arranque

Debe localizar el soporte de arranque en la controladora y seguir las instrucciones para su reemplazo.

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Localice el medio de arranque con la siguiente ilustración o el mapa de FRU en el módulo de la controladora:



3. Pulse el botón azul de la carcasa del soporte de arranque para liberar el soporte de arranque de su carcasa y, a continuación, tire suavemente de él hacia fuera del zócalo del soporte de arranque.



No gire ni tire del soporte de arranque en línea recta, ya que podría dañar la toma o el soporte de arranque.

4. Alinee los bordes del soporte de arranque de repuesto con el zócalo del soporte de arranque y, a continuación, empújelo suavemente en el zócalo.
5. Compruebe el soporte del maletero para asegurarse de que está asentado completamente en la toma.

Si es necesario, extraiga el soporte de arranque y vuelva a colocarlo en la toma.

6. Empuje el soporte del maletero hacia abajo para activar el botón de bloqueo en la carcasa del soporte del maletero.
7. Cierre la cubierta del módulo del controlador.

Paso 3: Transfiera la imagen de arranque al soporte de arranque

Puede instalar la imagen del sistema en el soporte de arranque de repuesto mediante una unidad flash USB con la imagen instalada en ella. No obstante, debe restaurar el sistema de archivos var durante este procedimiento.

- Debe tener una unidad flash USB, formateada con FAT32, con una capacidad mínima de 4 GB.



El archivo tar.gz se debe colocar en una partición con formato FAT32 que tenga un mínimo de 4 GB. Aunque las particiones FAT32 pueden ser de hasta 2 TB, las herramientas integradas de Windows (por ejemplo, DiskPart) no pueden formatear particiones FAT32 de más de 32 GB.

- Una copia de la misma versión de imagen de ONTAP que la controladora dañada en funcionamiento. Puede descargar la imagen adecuada en la sección Descargas del sitio de soporte de NetApp
 - Si NVE está habilitado, descargue la imagen con el cifrado de volúmenes de NetApp, como se indica en el botón de descarga.
 - Si el cifrado de volúmenes de NetApp no está habilitado, descargue la imagen sin el cifrado de volúmenes de NetApp, como se indica en el botón de descarga.
- Si el sistema es un par de alta disponibilidad, debe tener una conexión de red.
- Si el sistema es independiente, no necesita una conexión de red, pero debe realizar un reinicio adicional al restaurar el sistema de archivos var.

- a. Alinee el extremo del módulo del controlador con la abertura del chasis y, a continuación, empuje suavemente el módulo del controlador hasta la mitad del sistema.
- b. Vuelva a instalar el dispositivo de administración de cables y vuelva a instalar el sistema, según sea necesario.

Al realizar la copia, recuerde volver a instalar los convertidores de medios (SFP) si se retiraron.

- c. Inserte la unidad flash USB en la ranura USB del módulo de controlador.

Asegúrese de instalar la unidad flash USB en la ranura indicada para dispositivos USB, y no en el puerto de consola USB.

- d. Empuje completamente el módulo del controlador en el sistema, asegurándose de que el mango de la leva borra la unidad flash USB, empuje firmemente el asa de la leva para terminar de colocar el módulo del controlador, empuje el asa de la leva hasta la posición cerrada y, a continuación, apriete el tornillo de mano.

La controladora comienza a arrancar en cuanto se ha instalado por completo en el chasis.

- e. Interrumpa el proceso de arranque para que se detenga en el símbolo del SISTEMA DEL CARGADOR pulsando Ctrl-C cuando vea iniciando AUTOBOOT, pulse Ctrl-C para cancelar....

Si omite este mensaje, pulse Ctrl-C, seleccione la opción de arrancar en modo de mantenimiento y detenga la controladora para arrancar en EL CARGADOR.

- f. En el caso de los sistemas con una controladora en el chasis, vuelva a conectar la alimentación y encienda las fuentes de alimentación.

El sistema empieza a arrancar y se detiene en el aviso del CARGADOR.

- g. Configure el tipo de conexión de red en el símbolo del sistema del CARGADOR:

- Si va a configurar DHCP: `ifconfig e0a -auto`



El puerto de destino que configure es el puerto de destino que utiliza para comunicarse con la controladora con la controladora con deterioro de la controladora en buen estado durante la restauración del sistema de archivos var con una conexión de red. También puede utilizar el puerto e0M en este comando.

- Si está configurando conexiones manuales: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
 - Filer_addr es la dirección IP del sistema de almacenamiento.
 - La máscara de red es la máscara de red de la red de gestión conectada al partner de alta disponibilidad.
 - gateway es la puerta de enlace de la red.
 - dns_addr es la dirección IP de un servidor de nombres de la red.
 - dns_Domain es el nombre de dominio del sistema de nombres de dominio (DNS).

Si utiliza este parámetro opcional, no necesita un nombre de dominio completo en la URL del servidor para reiniciar el sistema. Solo necesita el nombre de host del servidor.



Es posible que sean necesarios otros parámetros para la interfaz. Puede entrar `help ifconfig` en el símbolo del sistema del firmware para obtener detalles.

- h. Si la controladora está en una MetroCluster con ampliación o conexión a la estructura, debe restaurar la configuración del adaptador de FC:
 - i. Arranque en modo de mantenimiento: `boot_ontap maint`
 - ii. Establezca los puertos MetroCluster como iniciadores: `ucadmin modify -m fc -t initiator adapter_name`
 - iii. Detener para volver al modo de mantenimiento: `halt`

Los cambios se implementarán al arrancar el sistema.

Arranque la imagen de recuperación: FAS8200

El procedimiento para arrancar la controladora con deterioro de la imagen de recuperación depende de si el sistema está en una configuración MetroCluster de dos nodos.

Opción 1: La mayoría de los sistemas

: Debe arrancar la imagen ONTAP desde la unidad USB, restaurar el sistema de archivos y comprobar las variables de entorno.

Este procedimiento se aplica a los sistemas que no están en una configuración MetroCluster de dos nodos.

Pasos

1. Desde el símbolo DEL SISTEMA DEL CARGADOR, arranque la imagen de recuperación desde la unidad flash USB: `boot_recovery`

La imagen se descarga desde la unidad flash USB.

2. Cuando se le solicite, introduzca el nombre de la imagen o acepte la imagen predeterminada que se muestra dentro de los corchetes de la pantalla.
3. Restaure el sistema de archivos var:

Si el sistema tiene...	Realice lo siguiente...
Una conexión de red	<ol style="list-style-type: none"> a. Pulse <code>y</code> cuando se le solicite que restaure la configuración de copia de seguridad. b. Configure la controladora en buen estado como nivel de privilegio avanzado: <code>set -privilege advanced</code> c. Ejecute el comando <code>restore backup: system node restore-backup -node local -target-address <i>impaired_node_IP_address</i></code> d. Devuelva la controladora al nivel de administrador: <code>set -privilege admin</code> e. Pulse <code>y</code> cuando se le solicite que utilice la configuración restaurada. f. Pulse <code>y</code> cuando se le solicite reiniciar la controladora.
No hay conexión de red	<ol style="list-style-type: none"> a. Pulse <code>n</code> cuando se le solicite que restaure la configuración de copia de seguridad. b. Reinicie el sistema cuando el sistema lo solicite. c. Seleccione la opción Actualizar flash desde la configuración de copia de seguridad (flash de sincronización) en el menú que se muestra. <p>Si se le solicita que continúe con la actualización, pulse <code>y</code>.</p>

4. Asegurarse de que las variables medioambientales estén establecidas de la manera esperada:
 - a. Lleve la controladora al aviso del CARGADOR.
 - b. Compruebe la configuración de la variable de entorno con el `printenv` comando.
 - c. Si una variable de entorno no está establecida como se espera, modifíquela con el `setenv environment-variable-name changed-value` comando.
 - d. Guarde los cambios mediante `saveenv` comando.
5. El siguiente depende de la configuración del sistema:
 - Si su sistema tiene configurado el gestor de claves incorporado, NSE o NVE, vaya a [Restaura OKM, NSE y NVE según sea necesario](#)
 - Si su sistema no tiene configurado el gestor de claves incorporado, NSE o NVE, complete los pasos en esta sección.
6. Desde el aviso del CARGADOR, introduzca el `boot_ontap` comando.

Si ve...	Realice lo siguiente...
La solicitud de inicio de sesión de	Vaya al siguiente paso.
Esperando devolución...	<ol style="list-style-type: none"> Inicie sesión en el controlador asociado. Confirme que la controladora de destino está lista para la devolución con el <code>storage failover show</code> comando.

- Conecte el cable de la consola al controlador asociado.
- Respalde la controladora con el `storage failover giveback -fromnode local` comando.
- En el símbolo del sistema del clúster, compruebe las interfaces lógicas con el `net int -is-home false` comando.

Si alguna interfaz se muestra como "falsa", vuelva a revertir dichas interfaces a su puerto de inicio utilizando el `net int revert` comando.

- Mueva el cable de la consola al controlador reparado y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.
- Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

Opción 2: La controladora está en un MetroCluster de dos nodos

Debe arrancar la imagen de ONTAP desde la unidad USB y comprobar las variables de entorno.

Este procedimiento se aplica a los sistemas de una configuración MetroCluster de dos nodos.

Pasos

- Desde el símbolo DEL SISTEMA DEL CARGADOR, arranque la imagen de recuperación desde la unidad flash USB: `boot_recovery`

La imagen se descarga desde la unidad flash USB.

- Cuando se le solicite, introduzca el nombre de la imagen o acepte la imagen predeterminada que se muestra dentro de los corchetes de la pantalla.
- Después de instalar la imagen, inicie el proceso de restauración:
 - Pulse `n` cuando se le solicite que restaure la configuración de copia de seguridad.
 - Pulse `y` cuando se le pida que reinicie para empezar a utilizar el software recién instalado.

Debe estar preparado para interrumpir el proceso de arranque cuando se le solicite.

- Cuando se inicie el sistema, pulse `Ctrl-C` después de ver la `Press Ctrl-C for Boot Menu` Mensaje. Y cuando aparezca el menú Inicio, seleccione la opción 6.
- Compruebe que las variables de entorno están establecidas de la forma esperada.
 - Lleve el nodo al aviso DEL CARGADOR.
 - Compruebe la configuración de la variable de entorno con el `printenv` comando.

- c. Si una variable de entorno no está establecida como se espera, modifíquela con el `setenv environment-variable-name changed-value` comando.
- d. Guarde los cambios mediante `savenv` comando.
- e. Reiniciar el nodo.

Vuelva a cambiar los agregados en una configuración MetroCluster de dos nodos: FAS8200

Una vez que haya completado el reemplazo de FRU en una configuración de MetroCluster de dos nodos, podrá llevar a cabo la operación de conmutación de estado de MetroCluster. De este modo, la configuración vuelve a su estado operativo normal, con las máquinas virtuales de almacenamiento (SVM) sincronizada en el sitio anteriormente afectado que ahora están activas y sirviendo datos de los pools de discos locales.

Esta tarea solo se aplica a configuraciones MetroCluster de dos nodos.

Pasos

1. Compruebe que todos los nodos estén en el `enabled` provincia: `metrocluster node show`

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node              State          Mirroring Mode
-----
-----
1      cluster_A
      controller_A_1 configured      enabled      heal roots
completed
      cluster_B
      controller_B_1 configured      enabled      waiting for
switchback recovery
2 entries were displayed.
```

2. Compruebe que la resincronización se haya completado en todas las SVM: `metrocluster vserver show`
3. Compruebe que las migraciones LIF automáticas que realizan las operaciones de reparación se han completado correctamente: `metrocluster check lif show`
4. Lleve a cabo la conmutación de estado mediante el `metrocluster switchback` comando desde cualquier nodo del clúster superviviente.
5. Compruebe que la operación de conmutación de estado ha finalizado: `metrocluster show`

La operación de conmutación de estado ya está en ejecución cuando un clúster está en el `waiting-for-switchback` provincia:

```

cluster_B::> metrocluster show
Cluster           Configuration State      Mode
-----
Local: cluster_B configured      switchover
Remote: cluster_A configured     waiting-for-switchback

```

La operación de conmutación de estado se completa cuando los clústeres están en el `normal` estado:

```

cluster_B::> metrocluster show
Cluster           Configuration State      Mode
-----
Local: cluster_B configured      normal
Remote: cluster_A configured     normal

```

Si una conmutación de regreso tarda mucho tiempo en terminar, puede comprobar el estado de las líneas base en curso utilizando el `metrocluster config-replication resync-status show` comando.

6. Restablecer cualquier configuración de SnapMirror o SnapVault.

Restablecer OKM, NSE y NVE según sea necesario: FAS8200

Una vez marcadas las variables de entorno, debe completar los pasos específicos de los sistemas que tienen activada la opción Onboard Key Manager (OKM), el cifrado en almacenamiento de NetApp (NSE) o el cifrado de volúmenes de NetApp (NVE).

Determine qué sección debería usar para restaurar sus configuraciones de OKM, NSE o NVE:

Si NSE o NVE están habilitados junto con Onboard Key Manager, debe restaurar la configuración que capturó al principio de este procedimiento.

- Si NSE o NVE están habilitados y el gestor de claves incorporado está habilitado, vaya a [Opción 1: Restablecer NVE o NSE cuando el gestor de claves incorporado está habilitado](#).
- Si NSE o NVE están habilitados para NATP 9.5, vaya a [Opción 2: Restablecer NSE/NVE en sistemas que ejecutan ONTAP 9.5 y versiones anteriores](#).
- Si NSE o NVE están habilitados para ONTAP 9.6, vaya a [Opción 3: Restablecer NSE/NVE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores](#).

Opción 1: Restablecer NVE o NSE cuando el gestor de claves incorporado está habilitado

Pasos

1. Conecte el cable de consola a la controladora de destino.
2. Utilice la `boot_ontap` Comando en el símbolo del sistema del CARGADOR para arrancar la controladora.
3. Compruebe la salida de la consola:

- Si el comando falla debido a una sesión CIFS abierta, compruebe con el cliente cómo se cierran las sesiones CIFS.



Los terminación CIFS pueden provocar la pérdida de datos.

- Si el comando falla porque el partner está "no listo", espere 5 minutos para que los NVMMems se sincronicen.
- Si se produce un error en el comando debido a un proceso de NDMP, SnapMirror o SnapVault, deshabilite el proceso. Consulte el centro de documentación adecuado para obtener más información.

11. Una vez que se haya completado la devolución, compruebe el estado de la conmutación al nodo de respaldo y la devolución con el `storage failover show`. ``storage failover show`comandos -giveback`.

Solo se mostrarán los agregados CFO (agregados raíz y datos en estilo CFO).

12. Mueva el cable de la consola a la controladora de destino.
13. Si utiliza ONTAP 9.5 y versiones anteriores, ejecute el asistente de configuración de Key-Manager:
 - a. Inicie el asistente con `security key-manager setup -nodenodename` escriba la clave de acceso para la gestión de claves incorporada cuando se le solicite.
 - b. Introduzca el `key-manager key show -detail` comando para ver una vista detallada de todas las claves almacenadas en el gestor de claves incorporado y verificar que el `Restored` columna = `yes` para todas las claves de autenticación.



Si la `Restored` columna = cualquier otra cosa que no sea `yes`, Póngase en contacto con el servicio de atención al cliente

- c. Espere 10 minutos hasta que la clave se sincronice en el clúster.

14. Si utiliza ONTAP 9.6 o posterior:
 - a. Ejecute el `security key-manager onboard sync` y, a continuación, introduzca la frase de acceso cuando se le solicite.
 - b. Introduzca el `security key-manager key query` comando para ver una vista detallada de todas las claves almacenadas en el gestor de claves incorporado y verificar que el `Restored` columna = `yes/true` para todas las claves de autenticación.



Si la `Restored` columna = cualquier otra cosa que no sea `yes/true`, Póngase en contacto con el servicio de atención al cliente

- c. Espere 10 minutos hasta que la clave se sincronice en el clúster.

15. Mueva el cable de la consola al controlador correspondiente.
16. Proporcione a la controladora objetivo mediante el `storage failover giveback -fromnode local` comando.
17. Compruebe el estado de devolución, 3 minutos después de que el informe haya finalizado, utilizando la `storage failover show` comando.

Si la devolución no está completa tras 20 minutos, póngase en contacto con el soporte de cliente.

18. En el símbolo del sistema `clustershell`, introduzca el `net int show -is-home false` comando para

mostrar las interfaces lógicas que no están en su controladora y puerto de inicio.

Si alguna interfaz aparece como `false`, vuelva a revertir estas interfaces a su puerto de inicio mediante el `net int revert -vserver Cluster -lif nodename` comando.

19. Mueva el cable de la consola a la controladora de destino y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.
20. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

Opción 2: Restaure NSE/NVE en sistemas que ejecutan ONTAP 9.5 y versiones anteriores

Pasos

1. Conecte el cable de consola a la controladora de destino.
2. Utilice la `boot_ontap` Comando en el símbolo del sistema del CARGADOR para arrancar la controladora.
3. Compruebe la salida de la consola:

Si la consola muestra...	Entonces...
La solicitud de inicio de sesión de	Vaya al paso 7.
Esperando devolución...	<ol style="list-style-type: none">a. Inicie sesión en el controlador asociado.b. Confirme que la controladora de destino está lista para la devolución con el <code>storage failover show</code> comando.

4. Mueva el cable de la consola a la controladora correspondiente y regrese el almacenamiento de la controladora objetivo mediante el `storage failover giveback -fromnode local -only-cfo -aggregates true local` comando.
 - Si el comando falla debido a un disco fallido, desactive físicamente el disco que ha fallado, pero deje el disco en la ranura hasta que se reciba un reemplazo.
 - Si el comando falla debido a una sesión CIFS abierta, compruebe con el cliente cómo cerrar sesiones CIFS.



Los terminación CIFS pueden provocar la pérdida de datos.

- Si el comando falla porque el partner "no está listo", espere 5 minutos para que los NVMems se sincronicen.
 - Si se produce un error en el comando debido a un proceso de NDMP, SnapMirror o SnapVault, deshabilite el proceso. Consulte el centro de documentación adecuado para obtener más información.
5. Espere 3 minutos y compruebe el estado de la conmutación al nodo de respaldo con el `storage failover show` comando.
 6. En el símbolo del sistema `clustershell`, introduzca el `net int show -is-home false` comando para mostrar las interfaces lógicas que no están en su controladora y puerto de inicio.

Si alguna interfaz aparece como `false`, vuelva a revertir estas interfaces a su puerto de inicio mediante el

```
net int revert -vserver Cluster -lif nodename comando.
```

7. Mueva el cable de la consola a la controladora de destino y ejecute la versión `-v command` Para comprobar las versiones de ONTAP.
8. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.
9. Utilice la `storage encryption disk show` en el símbolo del sistema `clustershell`, para revisar el resultado.



Este comando no funciona si está configurado el cifrado de volúmenes de NetApp

10. Use la consulta del administrador de claves de seguridad para mostrar los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves.
 - Si la `Restored` columna = `yes` Y todos los gestores de claves informan en un estado disponible, vaya a *Complete el proceso de reemplazo*.
 - Si la `Restored` columna = cualquier otra cosa que no sea `yes`, y/o uno o más gestores de claves no están disponibles, utilice `security key-manager restore -address` Comando para recuperar y restaurar todas las claves de autenticación (AKS) e ID de clave asociados con todos los nodos de todos los servidores de administración de claves disponibles.

Compruebe de nuevo el resultado de la consulta del gestor de claves de seguridad para garantizar que el `Restored` columna = `yes` y todos los gestores de claves informan en un estado disponible
11. Si la gestión de claves incorporada está habilitada:
 - a. Utilice la `security key-manager key show -detail` para ver una vista detallada de todas las claves almacenadas en el gestor de claves incorporado.
 - b. Utilice la `security key-manager key show -detail` y compruebe que el `Restored` columna = `yes` para todas las claves de autenticación.

Si la `Restored` columna = cualquier otra cosa que no sea `yes`, utilice la `security key-manager setup -node Repaired(Target) node` Comando para restaurar la configuración de la gestión de claves incorporada. Vuelva a ejecutar el `security key-manager key show -detail` comando para verificar `Restored` columna = `yes` para todas las claves de autenticación.

12. Conecte el cable de la consola al controlador asociado.
13. Respalde la controladora con el `storage failover giveback -fromnode local` comando.
14. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

Opción 3: Restaure NSE/NVE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores

Pasos

1. Conecte el cable de consola a la controladora de destino.
2. Utilice la `boot_ontap` Comando en el símbolo del sistema del CARGADOR para arrancar la controladora.
3. Compruebe la salida de la consola:

Si la consola muestra...	Realice lo siguiente...
La solicitud de inicio de sesión de	Vaya al paso 7.
Esperando devolución...	<ul style="list-style-type: none"> a. Inicie sesión en el controlador asociado. b. Confirme que la controladora de destino está lista para la devolución con el <code>storage failover show</code> comando.

4. Mueva el cable de la consola a la controladora correspondiente y regrese el almacenamiento de la controladora objetivo mediante el `storage failover giveback -fromnode local -only-cfo -aggregates true local` comando.
 - Si el comando falla debido a un disco fallido, desactive físicamente el disco que ha fallado, pero deje el disco en la ranura hasta que se reciba un reemplazo.
 - Si el comando falla debido a una sesión CIFS abierta, compruebe con el cliente cómo se cierran las sesiones CIFS.



Los terminación CIFS pueden provocar la pérdida de datos.

- Si el comando falla porque el partner está "no listo", espere 5 minutos para que los NVMMems se sincronicen.
 - Si se produce un error en el comando debido a un proceso de NDMP, SnapMirror o SnapVault, deshabilite el proceso. Consulte el centro de documentación adecuado para obtener más información.
5. Espere 3 minutos y compruebe el estado de la conmutación al nodo de respaldo con el `storage failover show` comando.
 6. En el símbolo del sistema clustershell, introduzca el `net int show -is-home false` comando para mostrar las interfaces lógicas que no están en su controladora y puerto de inicio.

Si alguna interfaz aparece como `false`, vuelva a revertir estas interfaces a su puerto de inicio mediante el `net int revert -vserver Cluster -lif nodename` comando.
 7. Mueva el cable de la consola a la controladora de destino y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.
 8. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.
 9. Utilice la `storage encryption disk show` en el símbolo del sistema clustershell, para revisar el resultado.
 10. Utilice la `security key-manager key query` Comando para mostrar los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves.
 - Si la `Restored` columna = `yes/true`, ha finalizado y puede continuar con el proceso de sustitución.
 - Si la `Key Manager type` = `external` y la `Restored` columna = cualquier otra cosa que no sea `yes/true`, utilice la `security key-manager external restore` Comando para restaurar los ID de claves de las claves de autenticación.



Si el comando falla, póngase en contacto con el servicio de atención al cliente.

- Si la `Key Manager type = onboard` y la `Restored column = cualquier otra cosa que no sea yes/true`, utilice la `security key-manager onboard sync` Comando para volver a sincronizar el tipo de gestor de claves.

Utilice la consulta de claves del administrador de claves de seguridad para verificar que el `Restored column = yes/true` para todas las claves de autenticación.

11. Conecte el cable de la consola al controlador asociado.
12. Respalde la controladora con el `storage failover giveback -fromnode local` comando.
13. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.
14. Si AutoSupport está habilitado, restaure o desactive la creación automática de casos mediante el `system node autosupport invoke -node * -type all -message MAINT=END`

Devuelva la parte con el error a NetApp - FAS8200

Devuelva la pieza que ha fallado a NetApp, como se describe en las instrucciones de RMA que se suministran con el kit. Consulte "[Retorno de artículo sustituciones](#)" para obtener más información.

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 INTERRUPTIÓN 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.