



Soporte de arranque

Install and maintain

NetApp

October 25, 2024

Tabla de contenidos

- Soporte de arranque 1
 - Descripción general de la sustitución de medios de arranque: FAS8200 1
 - Compruebe la compatibilidad y el estado de la clave de cifrado - FAS8200 1
 - Apague la controladora dañada - FAS8200 6
 - Sustituya el medio de arranque - FAS8200 10
 - Arranque la imagen de recuperación: FAS8200 14
 - Vuelva a cambiar los agregados en una configuración MetroCluster de dos nodos: FAS8200 16
 - Restaurar cifrado - FAS8200 18
 - Devuelva la parte con el error a NetApp - FAS8200 28

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 la compatibilidad y el estado de la clave de cifrado - FAS8200

Antes de apagar la controladora dañada, compruebe si su versión de ONTAP es compatible con cifrado de volúmenes de NetApp (NVE) y si el sistema de gestión de claves está configurado correctamente.

Paso 1: Compruebe si su versión de ONTAP es compatible con el cifrado de volúmenes de NetApp

Compruebe si su versión de ONTAP es compatible con el cifrado de volúmenes de NetApp (NVE). Esta información es crucial para descargar la imagen ONTAP correcta.

1. Determine si la versión de ONTAP admite el cifrado ejecutando el siguiente comando:

```
version -v
```

Si la salida incluye `1Ono-DARE`, NVE no es compatible con la versión del clúster.

2. Según si NVE es compatible con el sistema, realice una de las siguientes acciones:
 - Si NVE es compatible, descargue la imagen ONTAP con NetApp Volume Encryption.
 - Si NVE no es compatible, descargue la imagen ONTAP **sin** Cifrado de volumen NetApp.

Paso 2: Determine si es seguro apagar el controlador

Para apagar de forma segura una controladora, primero identifique si el gestor de claves externo (EKM) o el gestor de claves incorporado (OKM) están activos. A continuación, verifique el administrador de claves en uso, muestre la información de clave adecuada y realice acciones en función del estado de las claves de autenticación.

1. Determine qué gestor de claves está activado en el sistema:

Versión de ONTAP	Ejecute este comando
ONTAP 9.14.1 o posterior	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none">• Si EKM está activado, EKM aparece en la salida del comando.• Si OKM está activado, OKM aparece en la salida del comando.• Si no hay ningún gestor de claves activado, No key manager keystores configured aparece en el resultado del comando.
ONTAP 9.13.1 o anterior	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none">• Si EKM está activado, external aparece en la salida del comando.• Si OKM está activado, onboard aparece en la salida del comando.• Si no hay ningún gestor de claves activado, No key managers configured aparece en el resultado del comando.

2. En función de si hay configurado un gestor de teclas en el sistema, seleccione una de las siguientes opciones.

No se ha configurado ningún gestor de claves

Puede apagar el controlador defectuoso de forma segura. Vaya a ["apague el controlador dañado"](#).

Se ha configurado el gestor de claves externo o incorporado

- a. Introduzca el siguiente comando query para mostrar el estado de las claves de autenticación en su administrador de claves.

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

- b. Compruebe la salida del valor de `Restored` la columna para su gestor de claves.

Esta columna indica si las claves de autenticación del gestor de claves (EKM u OKM) se han restaurado correctamente.

3. En función de si el sistema está utilizando el Administrador de claves externo o el Administrador de claves incorporado, seleccione una de las siguientes opciones.

Gestor de claves externo

En función del valor de salida mostrado en la `Restored` columna, siga los pasos adecuados.

Valor de salida en <code>Restored</code> la columna	Siga estos pasos...
<code>true</code>	Puede apagar el controlador defectuoso de forma segura. Vaya a "apague el controlador dañado" .
Cualquier otra cosa que no sea <code>true</code>	<p>a. Restaure las claves de autenticación de gestión de claves externas en todos los nodos del clúster mediante el siguiente comando:</p> <pre>security key-manager external restore</pre> <p>Si el comando falla, póngase en contacto con "Soporte de NetApp".</p> <p>b. Compruebe que <code>Restored</code> la columna se muestre <code>true</code> para todas las claves de autenticación introduciendo <code>`security key-manager key query`</code> el comando.</p> <p>Si todas las claves de autenticación son <code>true</code>, puede apagar de forma segura el controlador defectuoso. Vaya a "apague el controlador dañado".</p>

Gestión de claves incorporada

En función del valor de salida mostrado en la `Restored` columna, siga los pasos adecuados.

Valor de salida en Restored la columna	Siga estos pasos...
true	<p>Realice una copia de seguridad manual de la información de OKM.</p> <ol style="list-style-type: none"> Vaya al modo avanzado introduciendo <code>set -priv advanced</code> y, a continuación, introdúzcalo y cuando se le solicite. Introduzca el siguiente comando para mostrar la información de gestión de claves: <pre>security key-manager onboard show-backup</pre> Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. <p>Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.</p> Puede apagar el controlador defectuoso de forma segura. Vaya a "apague el controlador dañado".

Valor de salida en Restored la columna	Siga estos pasos...
Cualquier otra cosa que no sea true	<p>a. Introduzca el comando SYNC del gestor de claves de seguridad incorporado:</p> <pre>security key-manager onboard sync</pre> <p>b. Introduzca los 32 caracteres y la clave de acceso alfanumérica de gestión de claves incorporada cuando se le solicite.</p> <p>Si no se puede proporcionar la contraseña, póngase en contacto con "Soporte de NetApp".</p> <p>c. Compruebe que Restored se muestra la columna true para todas las claves de autenticación:</p> <pre>security key-manager key query</pre> <p>d. Compruebe que se muestra el Key Manager tipo `onboard`y, a continuación, realice una copia de seguridad manual de la información de OKM.</p> <p>e. Introduzca el comando para mostrar la información de backup para la gestión de claves:</p> <pre>security key-manager onboard show-backup</pre> <p>f. Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados.</p> <p>Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.</p> <p>g. Puede apagar el controlador defectuoso de forma segura. Vaya a "apague el controlador dañado".</p>

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 y cuando se le solicite.
Solicitud del sistema o solicitud de contraseña (introduzca la contraseña del sistema)	<p>Retome o detenga el controlador dañado del controlador en buen estado: <code>storage failover takeover -ofnode impaired_node_name</code></p> <p>Cuando el controlador dañado muestre esperando devolución..., pulse Ctrl-C y, a continuación, responda y.</p>

- 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

- 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
```

- Deshabilite la devolución automática de la consola de la controladora en buen estado: `storage failover modify -node local -auto-giveback false`
- 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)	<p>Retome o detenga el controlador dañado del controlador en buen estado: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code></p> <p>Cuando el controlador dañado muestre esperando devolución..., pulse Ctrl-C y, a continuación, responda <code>y</code>.</p>

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 -vetoes` 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-vetoes`. 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:

```
mcc1A:> 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.

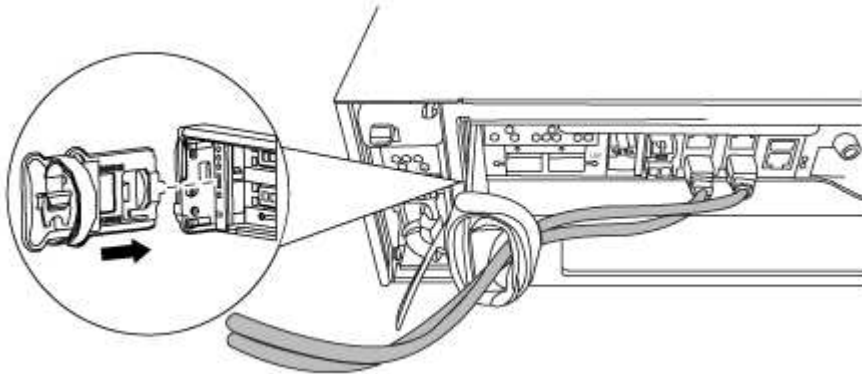
Paso 1: Quite la controladora

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.

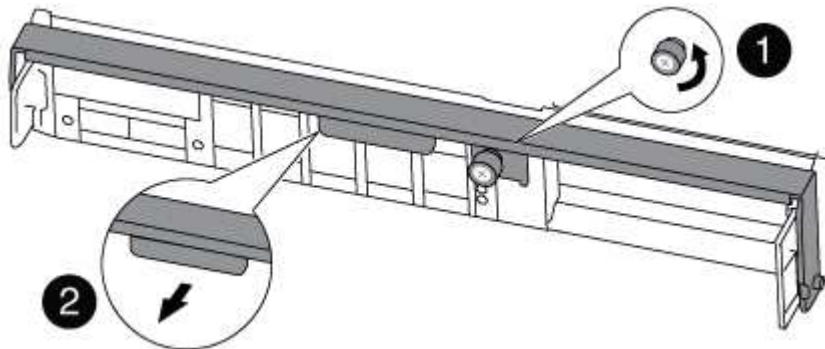
1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Afloje el gancho y la correa de bucle que sujetan los cables al dispositivo de administración de cables y, a continuación, desconecte los cables del sistema y los SFP (si fuera necesario) del módulo del controlador, manteniendo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

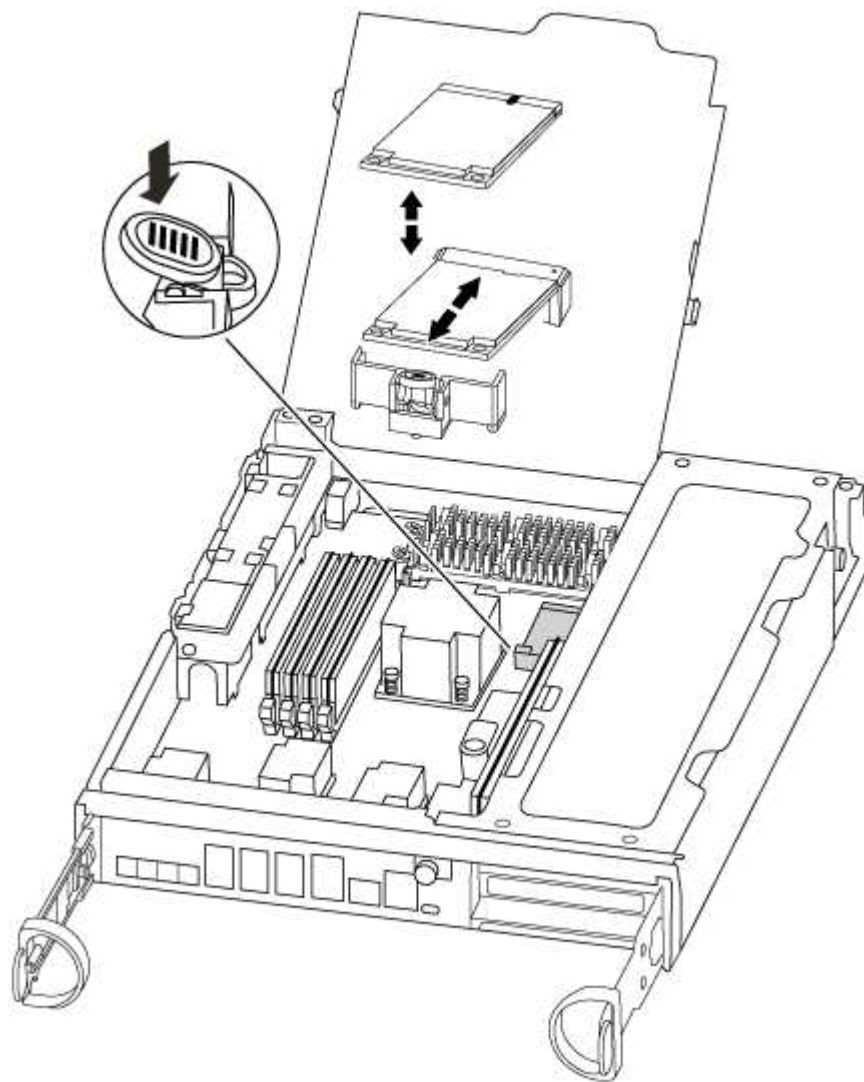
5. Tire del asa de leva hacia abajo y comience a sacar el módulo del controlador del chasis.

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, empujelo 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:

- Arranque en modo de mantenimiento: `boot_ontap maint`
- Establezca los puertos MetroCluster como iniciadores: `ucadmin modify -m fc -t initiator adapter_name`
- 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	<div><div>a. Pulse <code>y</code> cuando se le solicite que restaure la configuración de copia de seguridad.</div><div>b. Configure la controladora en buen estado como nivel de privilegio avanzado: <code>set -privilege advanced</code></div><div>c. Ejecute el comando <code>restore backup: system node restore-backup -node local -target-address <i>impaired_node_IP_address</i></code></div><div>d. Devuelva la controladora al nivel de administrador: <code>set -privilege admin</code></div><div>e. Pulse <code>y</code> cuando se le solicite que utilice la configuración restaurada.</div><div>f. Pulse <code>y</code> cuando se le solicite reiniciar la controladora.</div></div>
No hay conexión de red	<div><div>a. Pulse <code>n</code> cuando se le solicite que restaure la configuración de copia de seguridad.</div><div>b. Reinicie el sistema cuando el sistema lo solicite.</div><div>c. Seleccione la opción Actualizar flash desde la configuración de copia de seguridad (flash de sincronización) en el menú que se muestra.</div><div>Si se le solicita que continúe con la actualización, pulse <code>y</code>.</div></div>

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 `savenv` 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"> 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.

7. Conecte el cable de la consola al controlador asociado.
8. Respalde la controladora con el `storage failover giveback -fromnode local` comando.
9. 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.
10. Mueva el cable de la consola al controlador reparado y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.
11. Restaura 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

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. Después de instalar la imagen, inicie el proceso de restauración:
 - a. Pulse `n` cuando se le solicite que restaure la configuración de copia de seguridad.
 - b. 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.
4. 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.
5. Compruebe que las variables de entorno están establecidas de la forma esperada.
 - a. Lleve el nodo 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.
 - 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.

Restaurar cifrado - FAS8200

Restaure el cifrado en el soporte de arranque de reemplazo.

Se deben completar los pasos específicos de los sistemas que tengan habilitado el gestor de claves incorporado (OKM), el cifrado de almacenamiento de NetApp (NSE) o el cifrado de volúmenes de NetApp (NVE) mediante la configuración capturada al principio del procedimiento de reemplazo de medios de arranque.

En función del gestor de teclas configurado en el sistema, seleccione una de las siguientes opciones para restaurarlo desde el menú de inicio.

- ["Opción 1: Restaure la configuración del gestor de claves incorporado"](#)
- ["Opción 2: Restaure la configuración del gestor de claves externo"](#)

Opción 1: Restaure la configuración del gestor de claves incorporado

Restaure la configuración del Administrador de claves integrado (OKM) desde el menú de inicio de ONTAP.

Antes de empezar

- Asegúrese de que dispone de la siguiente información al restaurar la configuración de OKM:
 - Se ha introducido la clave de acceso para todo el clúster ["al tiempo que habilita la gestión de claves incorporada"](#).
 - ["Información de backup del gestor de claves incorporado"](#).
- Realice el ["Cómo comprobar el backup de gestión de claves incorporada y la clave de acceso para todo el clúster"](#) procedimiento antes de continuar.

Pasos

1. Conecte el cable de consola a la controladora de destino.
2. En el menú de inicio de ONTAP, seleccione la opción correspondiente en el menú de inicio.

Versión de ONTAP	Seleccione esta opción
ONTAP 9.8 o posterior	<p data-bbox="621 153 927 191">Seleccione la opción 10.</p> <p data-bbox="621 222 1058 254">Mostrar ejemplo de menú de inicio</p> <div data-bbox="654 296 1456 1081"> <p data-bbox="683 331 1294 363">Please choose one of the following:</p> <ul data-bbox="683 411 1369 1010" style="list-style-type: none"> <li data-bbox="683 411 971 443">(1) Normal Boot. <li data-bbox="683 453 1133 485">(2) Boot without /etc/rc. <li data-bbox="683 495 1045 527">(3) Change password. <li data-bbox="683 537 1369 600">(4) Clean configuration and initialize all disks. <li data-bbox="683 611 1149 642">(5) Maintenance mode boot. <li data-bbox="683 653 1328 684">(6) Update flash from backup config. <li data-bbox="683 695 1240 726">(7) Install new software first. <li data-bbox="683 737 976 768">(8) Reboot node. <li data-bbox="683 779 1192 842">(9) Configure Advanced Drive Partitioning. <li data-bbox="683 852 1333 915">(10) Set Onboard Key Manager recovery secrets. <li data-bbox="683 926 1317 989">(11) Configure node for external key management. <p data-bbox="683 1020 1032 1052">Selection (1-11)? 10</p> </div>

Versión de ONTAP	Seleccione esta opción
ONTAP 9,7 y anteriores	<p data-bbox="621 159 1489 199">Seleccione la opción oculta <code>recover_onboard_keymanager</code></p> <p data-bbox="621 226 1489 266">Mostrar ejemplo de menú de inicio</p> <div data-bbox="654 300 1456 966"> <pre data-bbox="683 338 1427 930">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. Selection (1-19)? recover_onboard_keymanager</pre> </div>

3. Confirme que desea continuar con el proceso de recuperación.

Mostrar símbolo del sistema de ejemplo

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

4. Introduzca dos veces la clave de acceso para todo el clúster.

Al introducir la frase de acceso, la consola no mostrará ninguna entrada.

Mostrar símbolo del sistema de ejemplo

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

5. Introduzca la información de backup.

- a. Pegue todo el contenido desde la línea de COPIA DE SEGURIDAD DE INICIO hasta la línea de COPIA DE SEGURIDAD FINAL.

Mostrar símbolo del sistema de ejemplo

Enter the backup data:

```
-----BEGIN BACKUP-----
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----
```

b. Pulse la tecla ENTER dos veces al final de la entrada.

El proceso de recuperación finaliza.

Mostrar símbolo del sistema de ejemplo

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.wkeydb file.

Successfully recovered keymanager secrets.

*****
*****
* Select option "(1) Normal Boot." to complete recovery process.
*
* Run the "security key-manager onboard sync" command to
synchronize the key database after the node reboots.
*****
*****
```



No continúe si la salida mostrada es otra cosa que `Successfully recovered keymanager secrets`. Realice la solución de problemas para corregir el error.

6. Seleccione la opción 1 en el menú de arranque para continuar arrancando en ONTAP.

Mostrar símbolo del sistema de ejemplo

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery process.
*
*****
*****

(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)? 1
```

7. Confirme que la consola de la controladora muestre el siguiente mensaje.

```
Waiting for giveback...(Press Ctrl-C to abort wait)
```

8. Desde el nodo del partner, devolver la controladora del partner introduciendo el siguiente comando.

```
storage failover giveback -fromnode local -only-cfo-aggregates true.
```

9. Después de arrancar solo con el agregado CFO, ejecute el siguiente comando.

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

10. Introduzca la clave de acceso en todo el clúster para la instancia de Onboard Key Manager.

Mostrar símbolo del sistema de ejemplo

```
Enter the cluster-wide passphrase for the Onboard Key Manager:
```

```
All offline encrypted volumes will be brought online and the
corresponding volume encryption keys (VEKs) will be restored
automatically within 10 minutes. If any offline encrypted volumes
are not brought online automatically, they can be brought online
manually using the "volume online -vserver <vserver> -volume
<volume_name>" command.
```



Si la sincronización se realiza correctamente, se devuelve el símbolo del sistema de clúster sin mensajes adicionales. Si la sincronización falla, aparecerá un mensaje de error antes de volver al símbolo del sistema del clúster. No continúe hasta que se corrija el error y la sincronización se ejecute correctamente.

11. Asegúrese de que todas las claves estén sincronizadas introduciendo el comando siguiente.

```
security key-manager key query -restored false.
```

```
There are no entries matching your query.
```



No deberían aparecer resultados al filtrar por false en el parámetro restaurado.

12. Realice la devolución del nodo del compañero introduciendo el comando siguiente.

```
storage failover giveback -fromnode local
```

13. Restaure la devolución automática, si la deshabilitó, introduciendo el siguiente comando.

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

14. Si AutoSupport está habilitado, restaure la creación automática de casos introduciendo el siguiente comando.

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Opción 2: Restaure la configuración del gestor de claves externo

Restaure la configuración del Administrador de claves externo desde el menú de inicio de ONTAP.

Antes de empezar

Necesita la siguiente información para restaurar la configuración de un gestor de claves externo (EKM).

- Una copia del archivo /cfcard/kmip/servers.cfg de otro nodo de cluster o de la siguiente información:
 - La dirección del servidor KMIP.
 - El puerto KMIP.

- Una copia del `/cfcard/kmip/certs/client.crt` archivo de otro nodo del clúster o del certificado de cliente.
- Una copia del `/cfcard/kmip/certs/client.key` archivo de otro nodo de clúster o la clave de cliente.
- Una copia `/cfcard/kmip/certs/CA.pem` del archivo de otro nodo del clúster o las CA del servidor KMIP.

Pasos

1. Conecte el cable de consola a la controladora de destino.
2. Seleccione la opción 11 en el menú de inicio de ONTAP.

Mostrar ejemplo de menú de inicio

```
(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)? 11
```

3. Cuando se le solicite, confirme que ha recopilado la información obligatoria.

Mostrar símbolo del sistema de ejemplo

```
Do you have a copy of the /cfcard/kmip/certs/client.crt file? {y/n}
Do you have a copy of the /cfcard/kmip/certs/client.key file? {y/n}
Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}
Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}
```

4. Cuando se le solicite, introduzca la información del cliente y del servidor.

Mostrar petición de datos

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

Muestra el ejemplo

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEWpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUwBQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----END CERTIFICATE-----

Enter the IP address for the KMIP server: 10.10.10.10
Enter the port for the KMIP server [5696]:

System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

Después de introducir la información del cliente y el servidor, el proceso de recuperación finaliza.

Muestra el ejemplo

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[Aug 29 21:06:28]: 0x808806100: 0: DEBUG: kmip2::main:
[initOpenssl]:460: Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Seleccione la opción 1 en el menú de arranque para continuar arrancando en ONTAP.

Mostrar símbolo del sistema de ejemplo

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery process.
*
*****
*****

(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)? 1
```

6. Restaure la devolución automática, si la deshabilitó, introduciendo el siguiente comando.

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

7. Si AutoSupport está habilitado, restaure la creación automática de casos introduciendo el siguiente comando.

```
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 ["Devolución de piezas y sustituciones"](#) la página 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 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.