



Medios de arranque: recuperación manual

Install and maintain

NetApp
February 13, 2026

Tabla de contenidos

Medios de arranque: recuperación manual	1
Flujo de trabajo de recuperación manual de medios de arranque: FAS70 y FAS90	1
Requisitos para la recuperación manual de medios de arranque: FAS70 y FAS90	2
Compruebe la compatibilidad con cifrado para la recuperación manual de medios de arranque: FAS70 y FAS90	2
Paso 1: Compruebe la compatibilidad con NVE y descargue la imagen ONTAP correcta.....	3
Paso 2: Verifique el estado del administrador de claves y la configuración de copia de seguridad.....	3
Apague el controlador para la recuperación manual del medio de arranque - FAS70 y FAS90	6
Reemplace el medio de arranque y prepárese para la recuperación de arranque manual - FAS70 y FAS90	10
Paso 1: Sustituya el soporte de arranque	10
Paso 2: Transfiera la imagen ONTAP al soporte de arranque	11
Recuperación manual de medios de arranque desde una unidad USB - FAS70 y FAS90	13
Restaurar claves de cifrado después de la recuperación de arranque manual - FAS70 y FAS90	15
Devuelva la pieza fallida a NetApp - FAS70 y FAS90	25

Medios de arranque: recuperación manual

Flujo de trabajo de recuperación manual de medios de arranque: FAS70 y FAS90

La recuperación manual de la imagen de arranque implica usar una unidad USB para reinstalar ONTAP en el medio de arranque de reemplazo del sistema FAS70 o FAS90. Debe descargar la imagen de recuperación de ONTAP correspondiente del sitio web de soporte de NetApp y copiarla a una unidad USB. Esta unidad USB preparada se utiliza para realizar la recuperación y restaurar el sistema a su estado operativo.

Si su sistema se ejecuta en ONTAP 9.17.1 y posterior, utilice el "["procedimiento de recuperación de arranque automático"](#)" .

Para comenzar, revise los requisitos de recuperación, apague el controlador, reemplace el medio de arranque, use la unidad USB para restaurar la imagen y vuelva a aplicar la configuración de cifrado si es necesario.

1

["Revise los requisitos de sustitución de soportes de arranque"](#)

Revise los requisitos para sustituir el soporte de arranque.

2

["Compruebe las claves de cifrado incorporadas"](#)

Determine si el sistema tiene discos cifrados o habilitados para el gestor de claves de seguridad.

3

["Apague el controlador dañado"](#)

Apague la controladora cuando necesite sustituir el soporte de arranque.

4

["Sustituya el soporte de arranque"](#)

Retire el soporte de arranque fallido del módulo de administración del sistema e instale el soporte de arranque de repuesto y, a continuación, transfiera una imagen ONTAP mediante una unidad flash USB.

5

["Arranque la imagen de recuperación"](#)

Inicie la imagen ONTAP desde la unidad USB, restaure el sistema de archivos y verifique las variables de entorno.

6

["Restaure el cifrado"](#)

Restaure la configuración del administrador de claves integrado o del administrador de claves externo desde el menú de arranque de ONTAP .

"Devuelve la pieza que ha fallado a NetApp"

Devuelva la pieza que ha fallado a NetApp, como se describe en las instrucciones de RMA que se suministran con el kit.

Requisitos para la recuperación manual de medios de arranque: FAS70 y FAS90

Antes de sustituir los medios de arranque en el sistema FAS70 o FAS90, asegúrese de cumplir con los requisitos necesarios para un reemplazo correcto. Esto incluye asegurarse de que tiene una unidad flash USB con la cantidad adecuada de almacenamiento y verificar que tiene el dispositivo de arranque de reemplazo correcto.

unidad flash USB

- Asegúrese de tener una unidad flash USB formateada en FAT32.
- El USB debe tener suficiente capacidad de almacenamiento para contener el `image_xxx.tgz` archivo.

Preparación de archivos

Copiar el `image_xxx.tgz` Archivo a la memoria USB. Este archivo se usará al transferir la imagen de ONTAP mediante la memoria USB.

Reemplazo de componentes

Reemplace el componente fallado con el componente de reemplazo proporcionado por NetApp.

Identificación del controlador

Es fundamental aplicar los comandos al controlador correcto cuando se reemplaza el medio de arranque dañado:

- El *controlador dañado* es el controlador en el que está realizando mantenimiento.
- El *controlador saludable* es el socio HA del controlador dañado.

El futuro

Después de revisar los requisitos para reemplazar el soporte de arranque, debe "[compruebe la compatibilidad y el estado de la clave de cifrado en el soporte de arranque](#)".

Compruebe la compatibilidad con cifrado para la recuperación manual de medios de arranque: FAS70 y FAS90

Para garantizar la seguridad de los datos en su sistema de almacenamiento FAS70 o FAS90, debe verificar la compatibilidad y el estado de la clave de cifrado en el soporte de arranque. Compruebe si la versión de ONTAP es compatible con el cifrado de volúmenes de NetApp (NVE) y antes de apagar la controladora compruebe si el gestor de claves está activo.

Paso 1: Compruebe la compatibilidad con NVE y descargue la imagen ONTAP correcta.

Determine si su versión de ONTAP admite NetApp Volume Encryption (NVE) para que pueda descargar la imagen de ONTAP correcta para el reemplazo del medio de arranque.

Pasos

1. Comprueba si tu versión de ONTAP admite cifrado:

```
version -v
```

Si la salida incluye `10no-DARE`, NVE no es compatible con la versión del clúster.

2. Descargue la imagen ONTAP apropiada según la compatibilidad con NVE:

- Si NVE es compatible: Descargue la imagen ONTAP con NetApp Volume Encryption.
- Si NVE no es compatible: Descargue la imagen de ONTAP sin NetApp Volume Encryption.



Descargue la imagen ONTAP desde el sitio de soporte de NetApp a su servidor HTTP o FTP o a una carpeta local. Necesitará este archivo de imagen durante el procedimiento de reemplazo del medio de arranque.

Paso 2: Verifique el estado del administrador de claves y la configuración de copia de seguridad.

Antes de apagar el controlador averiado, verifique la configuración del administrador de claves y haga una copia de seguridad de la información necesaria.

Pasos

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. Dependiendo de si hay un administrador de claves configurado en su sistema, realice una de las siguientes acciones:

Si no hay ningún gestor de claves configurado:

Puede apagar de forma segura el controlador averiado y proceder al procedimiento de apagado.

Si se ha configurado un gestor de claves (EKM u OKM):

- a. Introduzca el siguiente comando de consulta para mostrar el estado de las claves de autenticación en su gestor de claves:

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

- b. Revise la salida y verifique el valor en el Restored columna. Esta columna indica si las claves de autenticación para su gestor de claves (ya sea EKM u OKM) se han restaurado correctamente.

3. Complete el procedimiento correspondiente según su tipo de gestor de claves:

Gestor de claves externo (EKM)

Complete estos pasos según el valor en el Restored columna.

Si se muestran todas las teclas true en la columna Restaurado:

Puede apagar de forma segura el controlador averiado y proceder al procedimiento de apagado.

Si alguna clave muestra un valor distinto de true en la columna Restaurado:

- a. Restablecer las claves de autenticación de gestión de claves externas en todos los nodos del clúster:

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

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

- b. Verifique que todas las claves de autenticación se hayan restaurado:

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

Confirma que el Restored pantallas de columna true para todas las claves de autenticación.

- c. Si se restauran todas las claves, puede apagar de forma segura el controlador averiado y proceder al procedimiento de apagado.

Gestión de claves incorporada (OKM)

Complete estos pasos según el valor en el Restored columna.

Si se muestran todas las teclas true en la columna Restaurado:

- a. Realizar una copia de seguridad de la información de OKM:

- i. Cambiar al modo de privilegios avanzados:

```
set -priv advanced
```

Ingresar y cuando se le solicite continuar.

- i. Mostrar la información de copia de seguridad de gestión de claves:

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

- ii. Copie la información de la copia de seguridad a un archivo aparte o a su archivo de registro.

Necesitará esta información de respaldo si necesita recuperar OKM manualmente durante el procedimiento de reemplazo.

- iii. Volver al modo administrador:

```
set -priv admin
```

- b. Puede apagar de forma segura el controlador averiado y proceder al procedimiento de apagado.

Si alguna clave muestra un valor distinto de true en la columna Restaurado:

- Sincronizar el gestor de claves integrado:

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

Introduzca la contraseña alfanumérica de 32 caracteres para la gestión de la llave integrada cuando se le solicite.



Esta es la contraseña para todo el clúster que creó cuando configuró inicialmente el Administrador de claves integrado. Si no dispone de esta contraseña, póngase en contacto con el soporte de NetApp .

- Verifique que todas las claves de autenticación se hayan restaurado:

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

Confirma que el Restored pantallas de columna true para todas las claves de autenticación y la Key Manager El tipo muestra onboard .

- Realizar una copia de seguridad de la información de OKM:

- Cambiar al modo de privilegios avanzados:

```
set -priv advanced
```

Ingresar y cuando se le solicite continuar.

- Mostrar la información de copia de seguridad de gestión de claves:

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

- Copie la información de la copia de seguridad a un archivo aparte o a su archivo de registro.

Necesitará esta información de respaldo si necesita recuperar OKM manualmente durante el procedimiento de reemplazo.

- Volver al modo administrador:

```
set -priv admin
```

- Puede apagar de forma segura el controlador averiado y proceder al procedimiento de apagado.

El futuro

Después de comprobar la compatibilidad y el estado de la clave de cifrado en el soporte de arranque, debe ["apague la controladora"](#).

Apague el controlador para la recuperación manual del medio de arranque - FAS70 y FAS90

Apague el controlador dañado en su sistema de almacenamiento FAS70 o FAS90 para

evitar la pérdida de datos y mantener la estabilidad del sistema durante el proceso de recuperación del medio de arranque manual.

Opción 1: La mayoría de los sistemas

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.

Acerca de esta tarea

- Si dispone de un sistema SAN, debe haber comprobado los mensajes de evento cluster kernel-service show) para el blade SCSI de la controladora dañada. `cluster kernel-service show` El comando (desde el modo avanzado priv) muestra el nombre del nodo, "estado del quórum" de ese nodo, el estado de disponibilidad de ese nodo y el estado operativo de ese nodo.

Cada proceso SCSI-blade debe quórum con los otros nodos del clúster. Todos los problemas deben resolverse antes de continuar con el reemplazo.

- 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](#)".

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=<# of hours>h
```

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
```

- Desactivar devolución automática:

- Ingresar el siguiente comando desde la consola del controlador en buen estado:

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

- Ingresar y cuando vea el mensaje "¿Desea desactivar la devolución automática?"

- 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 y cuando se le solicite.

Si el controlador dañado está mostrando...	Realice lo siguiente...
Solicitud del sistema o solicitud de contraseña	<p>Retome o detenga el controlador dañado del controlador en buen estado:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>El parámetro <i>-halt true</i> lleva al símbolo del sistema de Loader.</p>

Opción 2: La controladora se encuentra en un MetroCluster

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](#)".
- Debe haber confirmado que el estado de configuración de MetroCluster está configurado y que los nodos están en un estado habilitado y normal:

```
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. Desactivar devolución automática:

- a. Ingrese el siguiente comando desde la consola del controlador en buen estado:

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

- b. Ingresar y cuando vea el mensaje "¿Desea desactivar la devolución automática?"

3. Lleve la controladora dañada al aviso DEL CARGADOR:

Si el controlador dañado está mostrando...	Realice lo siguiente...
El aviso del CARGADOR	Vaya a la siguiente sección.
Esperando devolución...	Pulse Ctrl-C y, a continuación, responda y cuando se le solicite.

Si el controlador dañado está mostrando...	Realice lo siguiente...
Solicitud del sistema o solicitud de contraseña (introduzca la contraseña del sistema)	<p>Retome o detenga el controlador dañado del controlador en buen estado:</p> <pre>storage failover takeover -ofnode impaired_node_name -halt true</pre> <p>El parámetro <i>-halt true</i> lleva al símbolo del sistema de Loader.</p>

El futuro

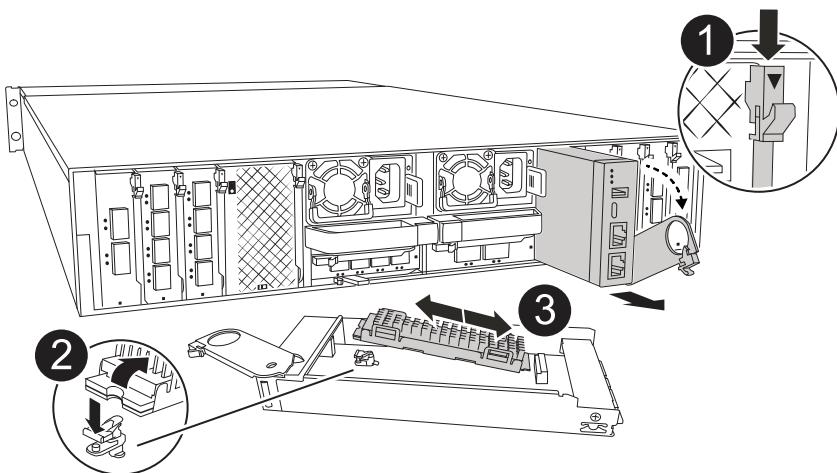
Después de apagar el controlador, debe ["sustituya el soporte de arranque"](#).

Reemplace el medio de arranque y prepárese para la recuperación de arranque manual - FAS70 y FAS90

El medio de arranque de su sistema FAS70 o FAS90 almacena datos esenciales de firmware y configuración. El proceso de reemplazo implica retirar el módulo de administración del sistema, retirar el medio de arranque dañado, instalar el nuevo medio de arranque y, a continuación, transferir manualmente la imagen de ONTAP al nuevo medio de arranque mediante una unidad flash USB.

Paso 1: Sustituya el soporte de arranque

El soporte de arranque se encuentra dentro del módulo de gestión del sistema y se accede a él quitando el módulo del sistema.



1	Bloqueo de leva del módulo de gestión del sistema
2	Botón de bloqueo del soporte de arranque

Pasos

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Desconecte los cables de alimentación de las fuentes de alimentación.



Si el sistema de almacenamiento tiene suministros de alimentación de CC, desconecte el bloque de cables de alimentación de las unidades de suministro de alimentación (PSU).

3. Retire el módulo Gestión del sistema:
 - a. Retire todos los cables conectados al módulo de gestión del sistema. Asegúrese de etiquetar dónde estaban conectados los cables, de modo que pueda conectarlos a los puertos correctos cuando vuelva a instalar el módulo.
 - b. Gire la bandeja de gestión de cables hacia abajo tirando de los botones situados en ambos lados del interior de la bandeja de gestión de cables y, a continuación, gire la bandeja hacia abajo.
 - c. Pulse el botón de leva de gestión del sistema.
 - d. Gire el pestillo de la leva hacia abajo hasta el tope.
 - e. Retire el módulo de gestión del sistema de la carcasa enganchando el dedo en la abertura de la palanca de leva y tirando del módulo para sacarlo de la carcasa.
 - f. Coloque el módulo de gestión del sistema en una alfombrilla antiestática, de forma que se pueda acceder al soporte de arranque.
4. Retire el soporte de arranque del módulo de gestión:
 - a. Pulse el botón de bloqueo azul.
 - b. Gire el soporte de arranque hacia arriba, deslícelo para extraerlo de la toma y déjelo a un lado.
5. Instale el soporte de arranque de repuesto en el módulo de gestión del sistema:
 - a. Alinee los bordes del soporte del maletero con el alojamiento del zócalo y, a continuación, empújelo suavemente en el zócalo.
 - b. Gire el soporte de arranque hacia abajo hacia el botón de bloqueo.
 - c. Pulse el botón de bloqueo, gire el soporte del maletero completamente hacia abajo y, a continuación, suelte el botón de bloqueo.
6. Vuelva a instalar el módulo Gestión del sistema.
 - a. Alinee el módulo con los bordes de la abertura de la ranura de la carcasa.
 - b. Deslice suavemente el módulo dentro de la ranura hasta el fondo de la carcasa y, a continuación, gire el pestillo de leva completamente hacia arriba para bloquear el módulo en su lugar.
7. Gire la bandeja de gestión de cables hasta la posición cerrada.
 - a. Vuelva a conectar el módulo Gestión del sistema.

Paso 2: Transfiera la imagen ONTAP al soporte de arranque

El medio de arranque de reemplazo que instaló se encuentra sin una imagen ONTAP. Puede transferir la imagen ONTAP al soporte de arranque de reemplazo descargando la imagen de servicio ONTAP adecuada de "[Sitio de soporte de NetApp](#)" a una unidad flash USB y, a continuación, al soporte de arranque de reemplazo.

Antes de empezar

- Debe tener una unidad flash USB vacía, formateada a FAT32, con al menos 4GB GB de capacidad.
- Descargue una copia de la misma versión de imagen de ONTAP que la que se estaba ejecutando la controladora afectada. Puede descargar la imagen adecuada en la sección Descargas del sitio de soporte de NetApp. Utilice `version -v` el comando para mostrar si su versión de ONTAP es compatible con NVE. Si aparece el resultado del comando <10no- DARE>, su versión de ONTAP no admite NVE.
 - Si NVE es compatible con su versión de ONTAP, descargue la imagen con el cifrado de volúmenes de NetApp, tal y como se indica en el botón de descarga.
 - Si NVE no es compatible, descargue la imagen sin cifrado de volúmenes NetApp, como se indica en el botón de descarga.
- Si el sistema es una pareja de alta disponibilidad, debe tener una conexión de red entre los puertos de gestión de nodos de las controladoras (normalmente las interfaces de e0M GbE).

Pasos

1. Descargue y copie la imagen de servicio adecuada desde el "[Sitio de soporte de NetApp](#)" a la unidad flash USB.
 - a. Descargue la imagen del servicio desde el enlace Descargas de la página, en su espacio de trabajo en su portátil.
 - b. Descomprima la imagen de servicio.



Si está extrayendo el contenido con Windows, no utilice WinZip para extraer la imagen netboot. Utilice otra herramienta de extracción, como 7-Zip o WinRAR.

La unidad flash USB debe tener la imagen ONTAP adecuada de lo que está ejecutando el controlador dañado.

- a. Extraiga la unidad flash USB del ordenador portátil.

2. Inserte la unidad flash USB en la ranura USB del módulo de administración del sistema.

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

3. Vuelva a enchufar los cables de alimentación a la fuente de alimentación.

El sistema comenzará a reiniciarse, normalmente en el aviso del CARGADOR.

4. Interrumpa el proceso de arranque pulsando Ctrl-C para detenerse en el símbolo del sistema DEL CARGADOR.

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.

El futuro

Después de reemplazar el soporte de arranque, debe "[inicie la imagen de recuperación](#)".

Recuperación manual de medios de arranque desde una unidad USB - FAS70 y FAS90

Después de instalar el nuevo dispositivo de medio de arranque en su sistema FAS70 o FAS90, puede arrancar la imagen de recuperación manualmente desde una unidad USB para restaurar la configuración desde el nodo asociado.

Antes de empezar

- Asegúrese de que su consola esté conectada al controlador averiado.
- Verifique que dispone de una unidad flash USB con la imagen de recuperación.
- Determina si tu sistema utiliza cifrado. Deberá seleccionar la opción apropiada en el paso 3 según si el cifrado está habilitado o no.

Pasos

1. Desde el indicador LOADER del controlador averiado, arranque la imagen de recuperación desde la unidad flash USB:

```
boot_recovery
```

La imagen de recuperación se descarga desde la unidad flash USB.

2. Cuando se le solicite, ingrese el nombre de la imagen o presione **Enter** para aceptar la imagen predeterminada que se muestra entre corchetes.
3. Restaure el sistema de archivos var siguiendo el procedimiento correspondiente a su versión de ONTAP :

ONTAP 9.16.0 o anterior

Complete los siguientes pasos en el controlador averiado y en el controlador asociado:

- a. **En el controlador averiado:** Pulse Y cuando ves Do you want to restore the backup configuration now?
- b. **En el controlador averiado:** Si se le solicita, pulse Y para sobrescribir /etc/ssh/ssh_host_ecdsa_key.
- c. **En el controlador asociado:** Configure el controlador afectado con el nivel de privilegios avanzado:

```
set -privilege advanced
```

- d. **En el controlador asociado:** Ejecute el comando de restauración de copia de seguridad:

```
system node restore-backup -node local -target-address  
impaired_node_IP_address
```



Si ve algún mensaje que no sea el de una restauración exitosa, póngase en contacto con el soporte de NetApp .

- e. **En el controlador asociado:** Volver al nivel de administrador:

```
set -privilege admin
```

- f. **En el controlador averiado:** Pulse Y cuando ves Was the restore backup procedure successful?
- g. **En el controlador averiado:** Pulse Y cuando ves ...would you like to use this restored copy now?
- h. **En el controlador averiado:** Pulse Y Cuando se le solicite reiniciar, pulse Ctrl-C cuando veas el menú de arranque.
- i. **En el controlador averiado:** Realice una de las siguientes acciones:
 - Si el sistema no utiliza cifrado, seleccione Opción 1 Arranque normal del menú de arranque.
 - Si el sistema utiliza cifrado, vaya a "[Restaure el cifrado](#)" .

ONTAP 9.16.1 o posterior

Complete los siguientes pasos en el controlador averiado:

- a. Pulse Y cuando se le solicite restaurar la configuración de copia de seguridad.

Una vez finalizado correctamente el proceso de restauración, aparece el siguiente mensaje:
syncflash_partner: Restore from partner complete

- b. Prensa Y cuando se le solicitó que confirmara que la restauración de la copia de seguridad se había realizado correctamente.
- c. Prensa Y cuando se le solicite utilizar la configuración restaurada.
- d. Prensa Y cuando se le solicite reiniciar el nodo.

- e. Prensa Y Cuando se le solicite reiniciar de nuevo, pulse Ctrl-C cuando veas el menú de arranque.
- f. Debe realizar una de las siguientes acciones:
 - Si el sistema no utiliza cifrado, seleccione *Opción 1 Arranque normal* del menú de arranque.
 - Si el sistema utiliza cifrado, vaya a "[Restaure el cifrado](#)" .

4. Conecte el cable de la consola al controlador asociado.
5. Devuelva el funcionamiento normal de la controladora y devuelva su almacenamiento:

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

6. Si desactivaste la devolución automática, vuelve a activarla:

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

7. Si AutoSupport está habilitado, restaure la creación automática de casos:

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

El futuro

Después de arrancar la imagen de recuperación, es necesario "[restaure el cifrado en el soporte de arranque](#)".

Restaurar claves de cifrado después de la recuperación de arranque manual - FAS70 y FAS90

Restaure el cifrado en los medios de arranque de reemplazo del sistema FAS70 o FAS90 para garantizar una protección de datos continua. El proceso de sustitución implica verificar la disponibilidad de claves, volver a aplicar la configuración de cifrado y confirmar el acceso seguro a sus datos.

Complete los pasos adecuados para restaurar el cifrado en su sistema según el tipo de administrador de claves que utilice. Si no está seguro de qué administrador de claves utiliza su sistema, revise la configuración que capturó al inicio del procedimiento de reemplazo del medio de arranque.

Gestión de claves incorporada (OKM)

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

Antes de empezar

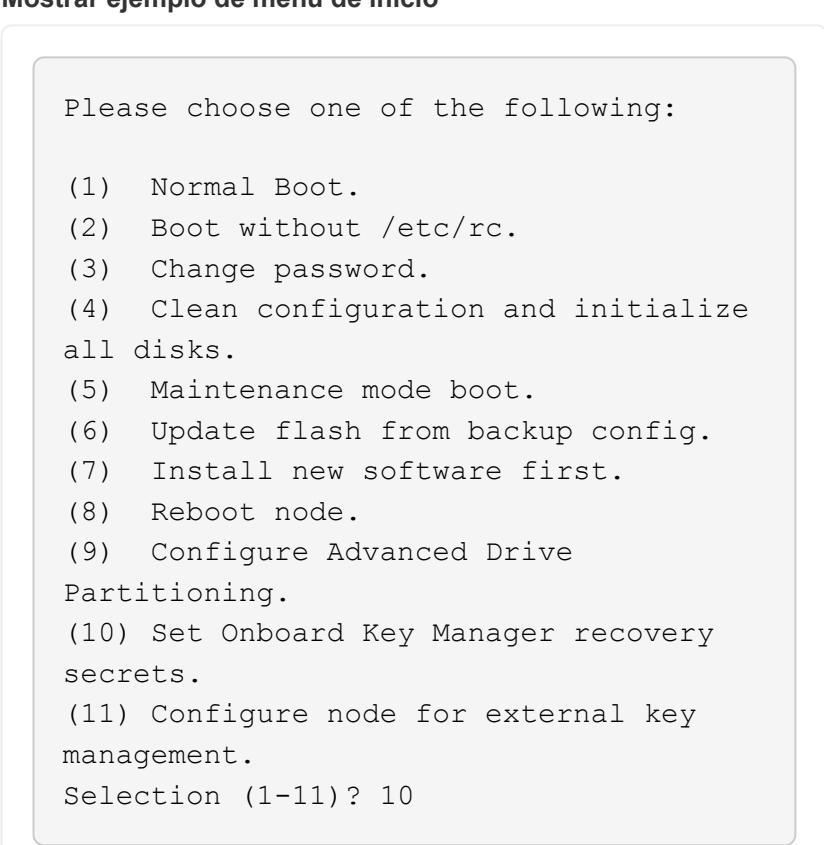
Asegúrese de tener disponible la siguiente información:

- Se introdujo la contraseña de todo el clúster mientras "[habilitación de la gestión de llaves a bordo](#)"
- "[Información de backup del gestor de claves incorporado](#)"
- Verificación de que dispone de la contraseña correcta y los datos de copia de seguridad utilizando el "[Cómo comprobar el backup de gestión de claves incorporada y la clave de acceso para todo el clúster](#)" procedimiento

Pasos

Sobre el controlador averiado:

1. Conecte el cable de la consola al controlador averiado.
2. Desde el menú de arranque de ONTAP , seleccione la opción adecuada:

Versión de ONTAP	Seleccione esta opción
ONTAP 9.8 o posterior	Seleccione la opción 10. Mostrar ejemplo de menú de inicio  <pre>Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. (10) Set Onboard Key Manager recovery secrets. (11) Configure node for external key management. Selection (1-11)? 10</pre>

Versión de ONTAP	Seleccione esta opción
ONTAP 9,7 y anteriores	<p>Seleccione la opción oculta <code>recover_onboard_keymanager</code></p> <p>Mostrar ejemplo de menú de inicio</p> <div style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p>Please choose one of the following:</p> <ul style="list-style-type: none"> (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. <p>Selection (1-19)?</p> <p><code>recover_onboard_keymanager</code></p> </div>

3. Confirma que deseas continuar con el proceso de recuperación cuando se te solicite:

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 contraseña, la consola no muestra 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 la copia de seguridad:

- Pegue todo el contenido desde la línea BEGIN BACKUP hasta la línea END BACKUP, incluyendo los guiones.

Mostrar símbolo del sistema de ejemplo

Enter the backup data:

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AA  
0123456789012345678901234567890123456789012345678901  
23  
1234567890123456789012345678901234567890123456789012  
34  
2345678901234567890123456789012345678901234567890123  
45  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AA  
AAAAAAAAAAAAAAAAAAAAAA  
AA  
AAAAAAAAAAAAAAAAAAAAAA  
AA
```

-----END
BACKUP-----

- b. Pulse la tecla Intro dos veces al final del texto introducido.

El proceso de recuperación finaliza y muestra el siguiente mensaje:

Successfully recovered keymanager secrets.

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 el resultado mostrado es diferente de Successfully recovered keymanager secrets . Realice la resolución de problemas para corregir el error.

6. Seleccionar opción 1 Desde el menú de arranque, continúe 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. Confirma que la consola del controlador muestra el siguiente mensaje:

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

En el controlador asociado:

8. Devuelva el controlador defectuoso:

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

Sobre el controlador averiado:

9. Tras arrancar únicamente con el agregado CFO, sincronice el gestor de claves:

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

10. Introduzca la contraseña de todo el clúster para el Administrador de claves integrado cuando se le solicite.

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

11. Verifique que todas las claves estén sincronizadas:

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

El comando no debería devolver ningún resultado. Si aparece algún resultado, repita el comando de sincronización hasta que no se devuelvan más resultados.

En el controlador asociado:

12. Devuelva el controlador defectuoso:

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

13. Restaure la devolución automática del control si la desactivó:

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

14. Si AutoSupport está habilitado, restaure la creación automática de casos:

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

Gestor de claves externo (EKM)

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

Antes de empezar

Reúna los siguientes archivos de otro nodo del clúster o de su copia de seguridad:

- `/cfcard/kmip/servers.cfg` archivo o la dirección y el puerto del servidor KMIP
- `/cfcard/kmip/certs/client.crt` archivo (certificado de cliente)
- `/cfcard/kmip/certs/client.key` archivo (clave de cliente)
- `/cfcard/kmip/certs/CA.pem` archivo (certificados CA del servidor KMIP)

Pasos

Sobre el controlador averiado:

1. Conecte el cable de la consola al controlador averiado.
2. Seleccionar opción 11 desde el menú de arranque 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. Confirma que has recopilado la información requerida cuando se te solicite:

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. Introduzca la información del cliente y del servidor cuando se le solicite:

- a. Introduzca el contenido del archivo de certificado de cliente (client.crt), incluidas las líneas BEGIN y END.
- b. Introduzca el contenido del archivo de clave de cliente (client.key), incluidas las líneas BEGIN y END.
- c. Ingrese el contenido del archivo CA(s) del servidor KMIP (CA.pem), incluidas las líneas BEGIN y END.
- d. Introduzca la dirección IP del servidor KMIP.
- e. Ingrese el puerto del servidor KMIP (presione Enter para usar el puerto predeterminado 5696).

Muestra el ejemplo

```
Enter the client certificate (client.crt) file contents:  
-----BEGIN CERTIFICATE-----  
<certificate_value>  
-----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-----  
<certificate_value>  
-----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
```

El proceso de recuperación finaliza y muestra el siguiente mensaje:

```
Successfully recovered keymanager secrets.
```

Muestra el ejemplo

```
System is ready to utilize external key manager(s).  
Trying to recover keys from key servers....  
Performing initialization of OpenSSL  
Successfully recovered keymanager secrets.
```

5. Seleccionar opción 1 Desde el menú de arranque, continúe 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 del control si la desactivó:

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

7. Si AutoSupport está habilitado, restaure la creación automática de casos:

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

El futuro

Después de restaurar el cifrado en el soporte de arranque, debe ["Devuelva la pieza fallida a NetApp"](#).

Devuelva la pieza fallida a NetApp - FAS70 y FAS90

Si un componente del sistema FAS70 o FAS90 falla, devuelva la pieza averiada a NetApp. Consulte ["Devolución de piezas y sustituciones"](#) la página para obtener más información.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.