



# **Soporte de arranque**

Install and maintain

NetApp

February 02, 2026

This PDF was generated from <https://docs.netapp.com/es-es/ontap-systems/fas500f/bootmedia-replace-overview.html> on February 02, 2026. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Tabla de contenidos

Soporte de arranque .....	1
Descripción general de la sustitución del soporte de arranque - FAS500f .....	1
Compruebe la compatibilidad y el estado de la clave de cifrado - FAS500f .....	1
Paso 1: Compruebe la compatibilidad con NVE y descargue la imagen ONTAP correcta.....	1
Paso 2: Verifique el estado del administrador de claves y la configuración de copia de seguridad.....	2
Apague el controlador - FAS500f .....	4
Opción 1: Mayoría de las configuraciones .....	5
Opción 2: La controladora se encuentra en un MetroCluster .....	5
Sustituya el soporte de arranque - FAS500f .....	6
Paso 1: Extraiga el módulo del controlador .....	6
Paso 2: Sustituya el soporte de arranque .....	9
Paso 3: Transfiera la imagen de arranque al soporte de arranque .....	10
Inicie la imagen de recuperación - FAS500f .....	13
Restaurar cifrado - FAS500f .....	16
Devuelva la pieza con error a NetApp - FAS500f .....	26

# Soporte de arranque

## Descripción general de la sustitución del soporte de arranque - FAS500f

El soporte de arranque almacena un conjunto principal y secundario de archivos del sistema (imagen de arranque) que el sistema utiliza cuando arranca.

Debe tener una unidad flash USB, formateada a MBR/FAT32, con la cantidad de almacenamiento adecuada para contener el `image_xxx.tgz` archivo.

- 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 la controladora correcta:
  - El controlador *drinated* es el controlador en el que está realizando tareas de mantenimiento.
  - El controlador *heated* es el compañero de alta disponibilidad del controlador dañado.

## Compruebe la compatibilidad y el estado de la clave de cifrado - FAS500f

Para garantizar la seguridad de los datos en el sistema de almacenamiento, debe verificar el estado y la compatibilidad 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

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

- 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):

- 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
```

- 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.

- 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:**

- 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 .

- 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.

- 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:**

- 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.

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

- a. 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 .

- 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 y la Key Manager El tipo muestra onboard .

- c. 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
```

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

## **Apague el controlador - FAS500f**

Después de completar las tareas de NVE o NSE, deberá completar el apagado de la controladora dañada. Apague o retome el controlador dañado siguiendo el procedimiento adecuado para su configuración.

## Opción 1: Mayoría de las configuraciones

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)	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 y.

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 se encuentra en un 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 y 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 y.

## Sustituya el soporte de arranque - FAS500f

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: Extraiga el módulo del controlador

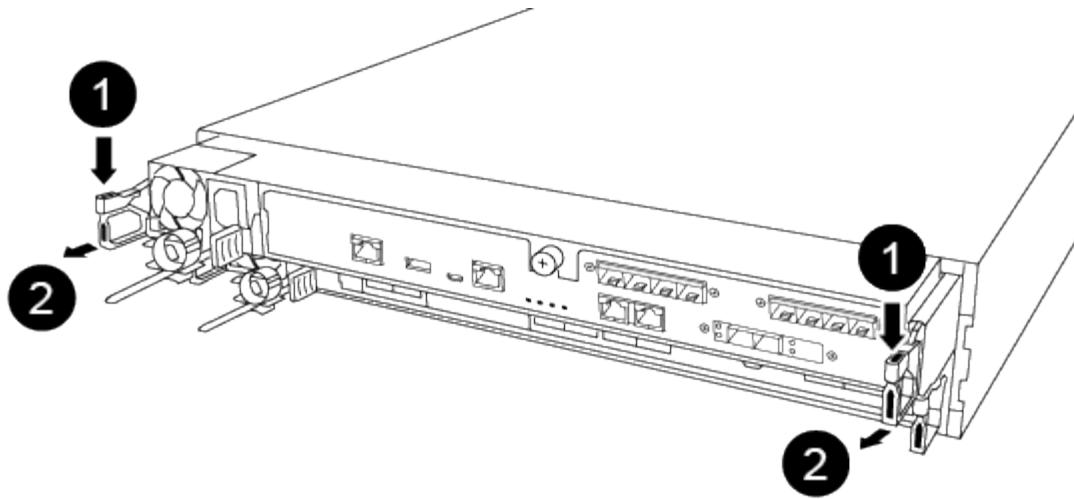
Debe quitar el módulo de la controladora del chasis cuando sustituya un componente dentro del módulo de la controladora.

Asegúrese de etiquetar los cables para saber de dónde proceden.

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Desconecte las fuentes de alimentación del módulo del controlador de la fuente.
3. Suelte los retenes del cable de alimentación y, a continuación, desenchufe los cables de las fuentes de alimentación.
4. Inserte el índice en el mecanismo de bloqueo de ambos lados del módulo del controlador, presione la palanca con el pulgar y tire suavemente del controlador a unas pocas pulgadas del chasis.



Si tiene dificultades para extraer el módulo del controlador, coloque los dedos de índice a través de los orificios para los dedos desde el interior (cruzando los brazos).



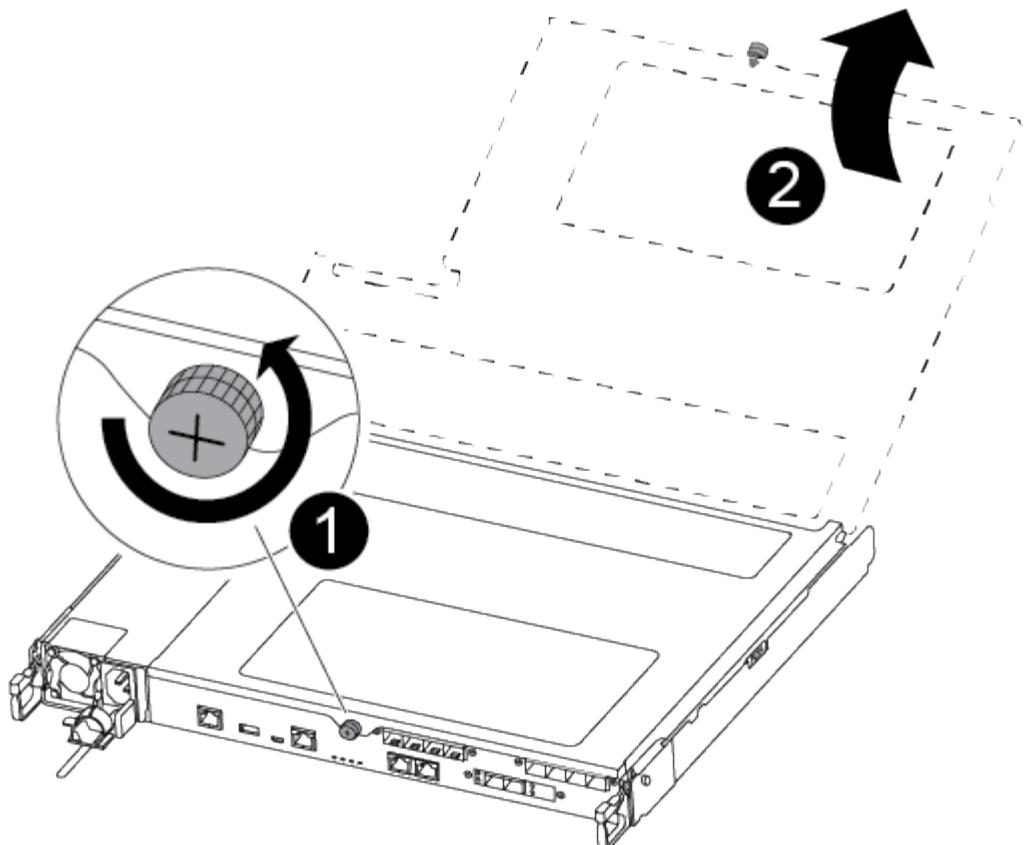
1

Palanca

2

Mecanismo de cierre

5. Con ambas manos, sujeté los lados del módulo del controlador y extrágalo suavemente del chasis y configúrelo sobre una superficie plana y estable.
6. Gire el tornillo de mano de la parte frontal del módulo del controlador hacia la izquierda y abra la cubierta del módulo del controlador.



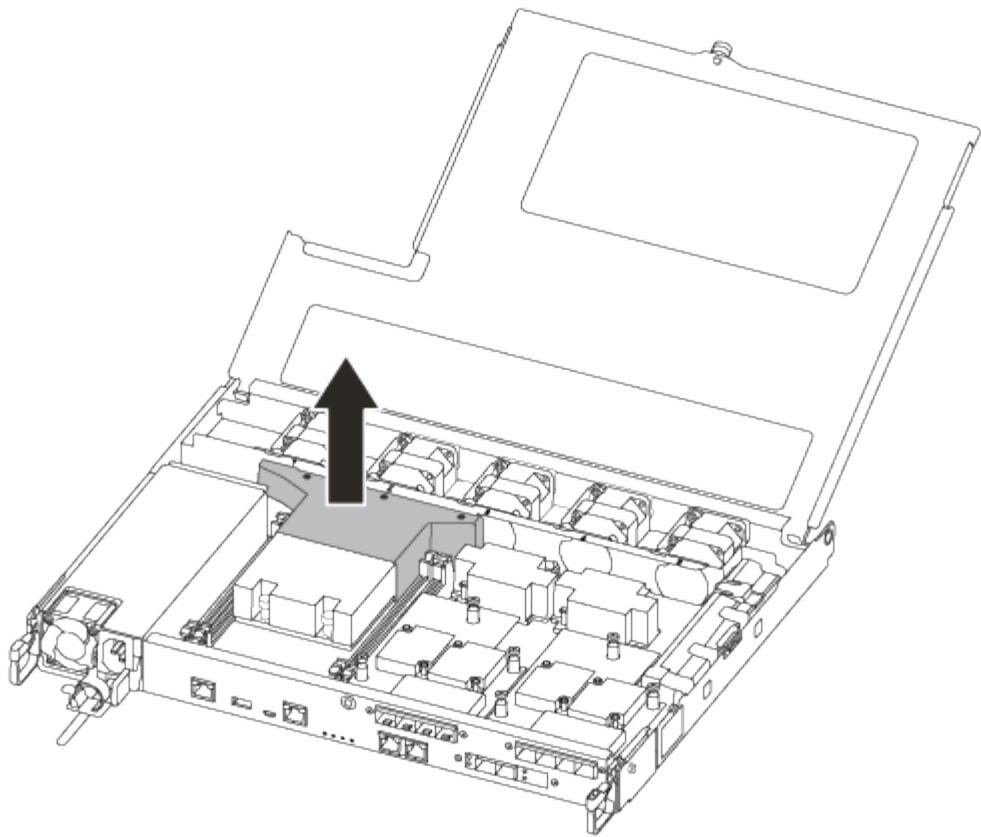
1

Tornillo de apriete manual

2

Cubierta del módulo del controlador.

7. Levantar la tapa del conducto de aire.



## Paso 2: Sustituya el soporte de arranque

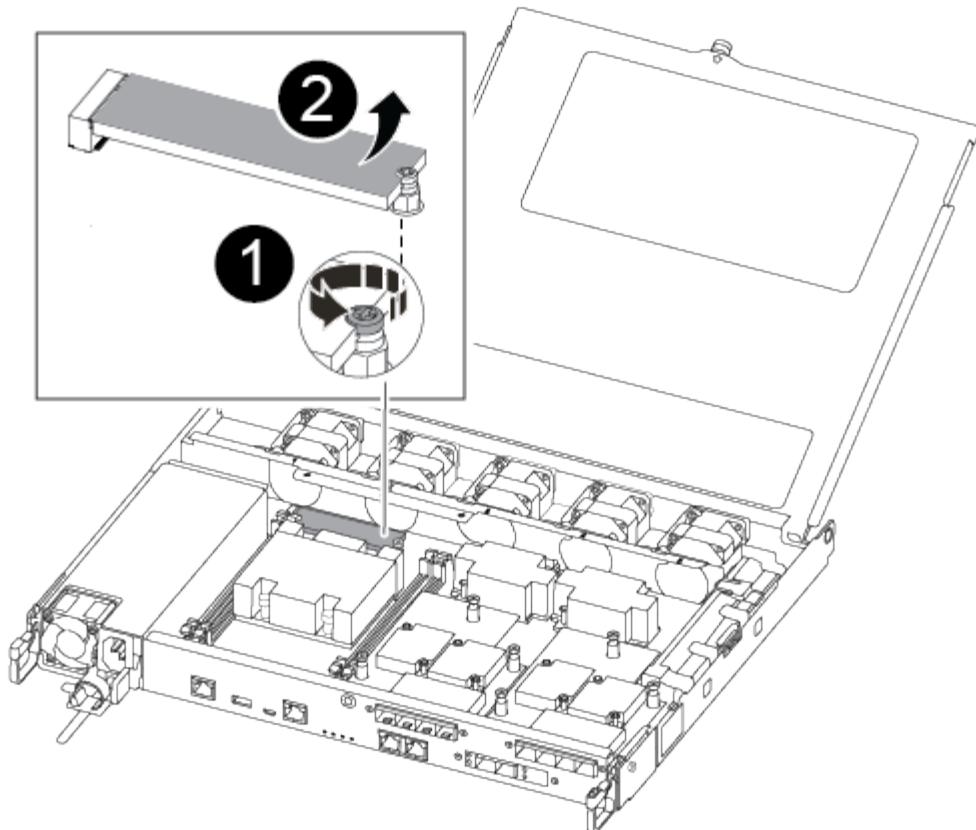
Localice el soporte de arranque con errores en el módulo del controlador quitando el conducto de aire del módulo del controlador antes de sustituir el soporte de arranque.

Necesita un destornillador Phillips magnético número 1 para quitar el tornillo que sujetá el soporte del maletero en su lugar. Debido a las limitaciones de espacio del módulo del controlador, también debe tener un imán para transferir el tornillo a para que no lo suelte.

Puede usar el siguiente vídeo o los pasos tabulados para reemplazar el soporte de arranque:

[Animación: Reemplace el soporte de arranque](#)

1. Localice y sustituya el soporte de arranque dañado del módulo del controlador.



**1**

Retire el tornillo que fija el soporte de arranque a la placa base en el módulo del controlador.

**2**

Levante el soporte del maletero para extraerlo del módulo del controlador.

- Con el destornillador magnético número 1, retire el tornillo del soporte del maletero dañado y colóquelo a un lado de forma segura en el imán.
- Levante suavemente el soporte del maletero dañado y colóquelo a un lado.
- Retire el soporte del maletero de repuesto de la bolsa de transporte antiestática y alinéelo en su sitio en el módulo del controlador.
- Con el destornillador magnético número 1, inserte y apriete el tornillo del soporte de arranque.



No aplique fuerza al apretar el tornillo en el soporte del maletero; puede que lo agriete.

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

El soporte de arranque de repuesto que ha instalado no tiene una imagen de arranque, por lo que debe transferir una imagen de arranque mediante una unidad flash USB.

- Debe tener una unidad flash USB, formateada a MBR/FAT32, con una capacidad mínima de 4 GB
- Una copia de la misma versión de imagen de ONTAP que la controladora dañada en funcionamiento. Puede descargar la imagen que corresponda 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.

## Pasos

1. Descargue y copie la imagen del servicio adecuada del sitio de soporte de NetApp en la unidad flash USB.
2. Descargue la imagen de servicio en su espacio de trabajo en su portátil.
3. 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.

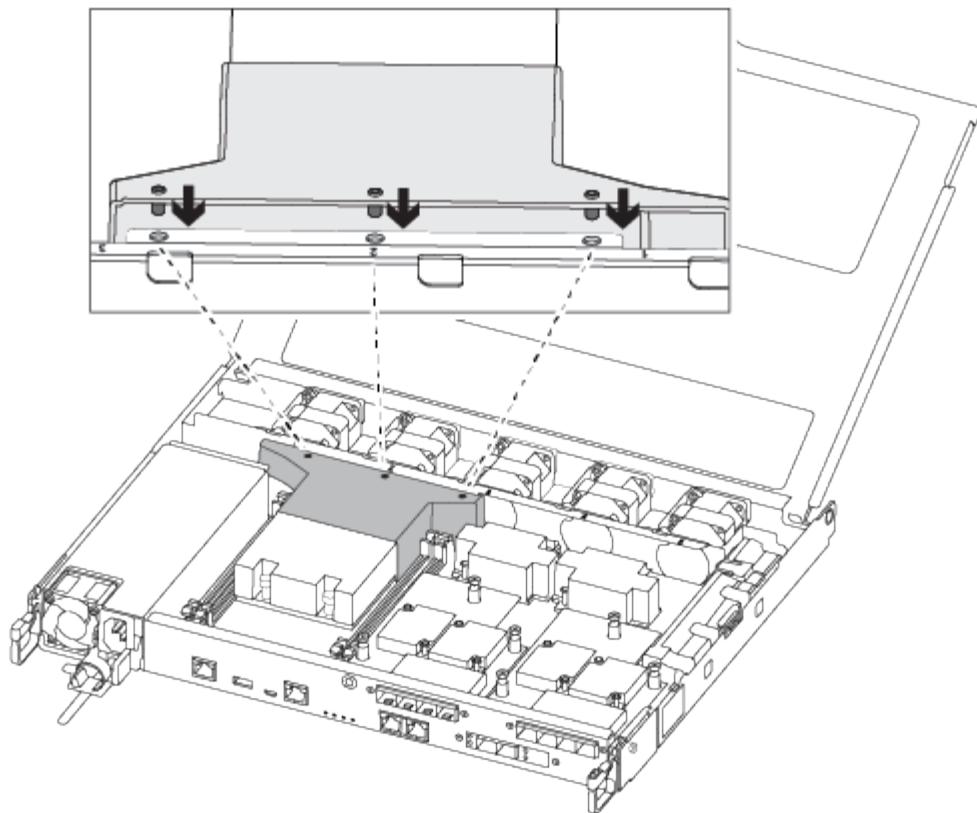
Hay dos carpetas en el archivo de imagen del servicio descomprimido:

- boot
- efi

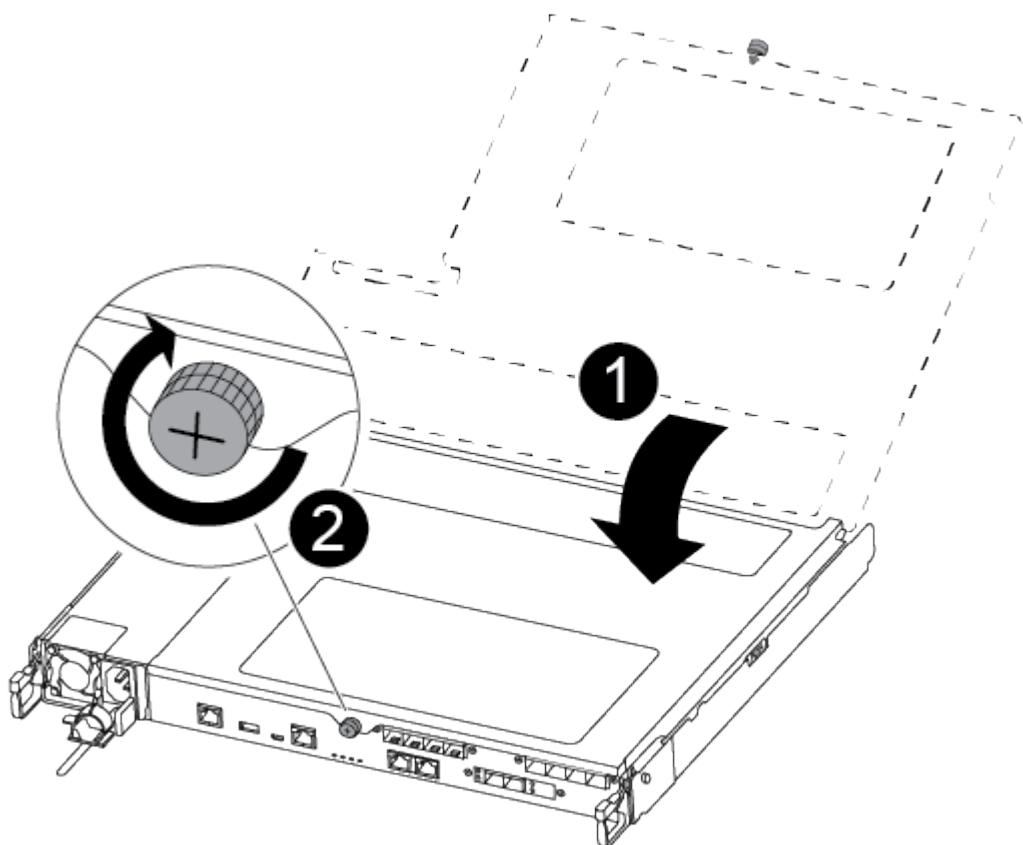
4. Copie el `efi` En el directorio superior de la unidad flash USB.

La unidad flash USB debe tener la carpeta `efi` y la misma versión de la imagen de servicio (BIOS) de la que se ejecuta el controlador dañado.

5. Extraiga la unidad flash USB del ordenador portátil.
6. Si aún no lo ha hecho, instale el conducto de aire.



7. Cierre la cubierta del módulo del controlador y apriete el tornillo de mariposa.



1	Cubierta del módulo del controlador
2	Tornillo de apriete manual

8. 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.
9. Enchufe el cable de alimentación en la fuente de alimentación y vuelva a instalar el retenedor del cable de alimentación.
10. 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.

11. Inserte completamente el módulo del controlador en el chasis:
12. Coloque los dedos de índice a través de los orificios de los dedos desde el interior del mecanismo de bloqueo.
13. Presione los pulgares hacia abajo en las lengüetas naranjas situadas en la parte superior del mecanismo de bloqueo y empuje suavemente el módulo del controlador sobre el tope.
14. Suelte los pulgares de la parte superior de los mecanismos de bloqueo y siga presionando hasta que los mecanismos de bloqueo encajen en su lugar.

El módulo de la controladora comienza a arrancar tan pronto como se asienta completamente en el chasis. Esté preparado para interrumpir el proceso de arranque.

El módulo del controlador debe estar completamente insertado y alineado con los bordes del chasis.

## Inicie la imagen de recuperación - FAS500f

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

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

Si el sistema tiene...	Realice lo siguiente...
No hay conexión de red y está en una configuración de IP de MetroCluster	<p>a. Pulse <b>n</b> cuando se le solicite que restaure la configuración de copia de seguridad.</p> <p>b. Reinicie el sistema cuando el sistema lo solicite.</p> <p>c. Espere a que se conecten las conexiones de almacenamiento iSCSI.</p> <p>Puede continuar después de ver los siguientes mensajes:</p> <pre data-bbox="703 502 1470 1305">date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).</pre> <p>d. Seleccione la opción <b>Actualizar flash desde la configuración de copia de seguridad</b> (flash de sincronización) en el menú que se muestra.</p> <p>Si se le solicita que continúe con la actualización, pulse <b>y</b>.</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 `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. [Restaure 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.

<b>Si ve...</b>	<b>Realice lo siguiente...</b>
La solicitud de inicio de sesión de	Vaya al siguiente paso.
Esperando devolución...	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. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

## Restaurar cifrado - FAS500f

Restaure el cifrado en el soporte de arranque de reemplazo.

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

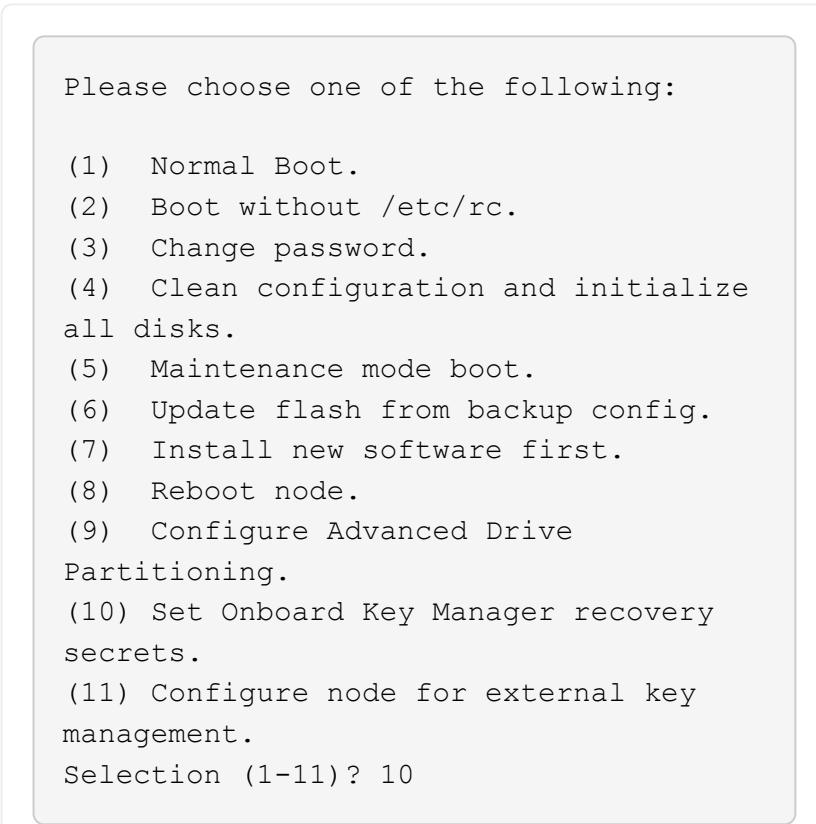
Asegúrese de tener disponible la siguiente información:

- 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.  <b>Mostrar ejemplo de menú de inicio</b>   <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><b>Mostrar ejemplo de menú de inicio</b></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"> <li>(1) Normal Boot.</li> <li>(2) Boot without /etc/rc.</li> <li>(3) Change password.</li> <li>(4) Clean configuration and initialize all disks.</li> <li>(5) Maintenance mode boot.</li> <li>(6) Update flash from backup config.</li> <li>(7) Install new software first.</li> <li>(8) Reboot node.</li> <li>(9) Configure Advanced Drive Partitioning.</li> </ul> <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
```

## Devuelva la pieza con error a NetApp - FAS500f

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 © 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.