



Soporte de arranque

Install and maintain

NetApp

February 13, 2026

This PDF was generated from <https://docs.netapp.com/es-es/ontap-systems/fas9000/bootmedia-replace-overview.html> on February 13, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Soporte de arranque	1
Descripción general de la sustitución de soportes de arranque - FAS9000	1
Compruebe la compatibilidad y el estado de la clave de cifrado	1
Paso 1: Compruebe la compatibilidad con NVE y descargue la imagen ONTAP correcta.....	2
Paso 2: Verifique el estado del administrador de claves y la configuración de copia de seguridad.....	2
Apague el controlador averiado - FAS9000	5
Opción 1: La mayoría de los sistemas	6
Opción 3: La controladora se encuentra en un MetroCluster de dos nodos	7
Sustituya el soporte de arranque - FAS9000	8
Paso 1: Quite la controladora	8
Paso 2: Sustituya el soporte de arranque	10
Paso 3: Transfiera la imagen de arranque al soporte de arranque	11
Inicie la imagen de recuperación - FAS9000	13
Opción 1: Inicia la imagen de recuperación en la mayoría de los sistemas	13
Opción 2: Arrancar la imagen de recuperación en una configuración MetroCluster de dos nodos	16
Vuelva a cambiar los agregados en una configuración MetroCluster de dos nodos: FAS9000	17
Restaurar cifrado - FAS9000	18
Devuelva la pieza fallida a NetApp - FAS9000	28

Soporte de arranque

Descripción general de la sustitución de soportes de arranque - FAS9000

El medio de arranque almacena un conjunto primario y secundario de archivos de sistema (imagen de arranque) que el sistema utiliza cuando arranca. El sistema FAS9000 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

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`.

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 reemplazar de forma no disruptiva, el par de alta disponibilidad no requiere una conexión a una red para restaurar el `var` sistema de archivos. El par de alta disponibilidad de un único chasis tiene una conexión e0S interna, que se utiliza para la transferencia `var config` entre ellos.
 - 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 *drivated* 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

Para garantizar la seguridad de los datos en su sistema de almacenamiento, debe verificar la compatibilidad y el estado de la clave de cifrado en su medio de arranque. Verifique si su versión de ONTAP admite NetApp Volume Encryption (NVE) y, antes de apagar el controlador, verifique si el administrador de claves está activo. El sistema FAS9000 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

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:

- 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:

- 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.

Apague el controlador averiado - FAS9000

Apague o tome el control del controlador dañado utilizando el procedimiento apropiado para su configuración. El sistema FAS9000 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

Opción 1: La mayoría de los sistemas

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

Después de completar las tareas de NVE o NSE, necesita completar el apagado del nodo dañado. NOTA: No utilice este procedimiento si el sistema está en una configuración 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. Des habilite 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)	<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>

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

Después de completar las tareas de NVE o NSE, necesita completar el apagado del nodo dañado.



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. Des habilite 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)	<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 y.</p>

Sustituya el soporte de arranque - FAS9000

Para reemplazar el medio de arranque, debe quitar el módulo del controlador dañado, instalar el medio de arranque de reemplazo y transferir la imagen de arranque a una unidad flash USB. El sistema FAS9000 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

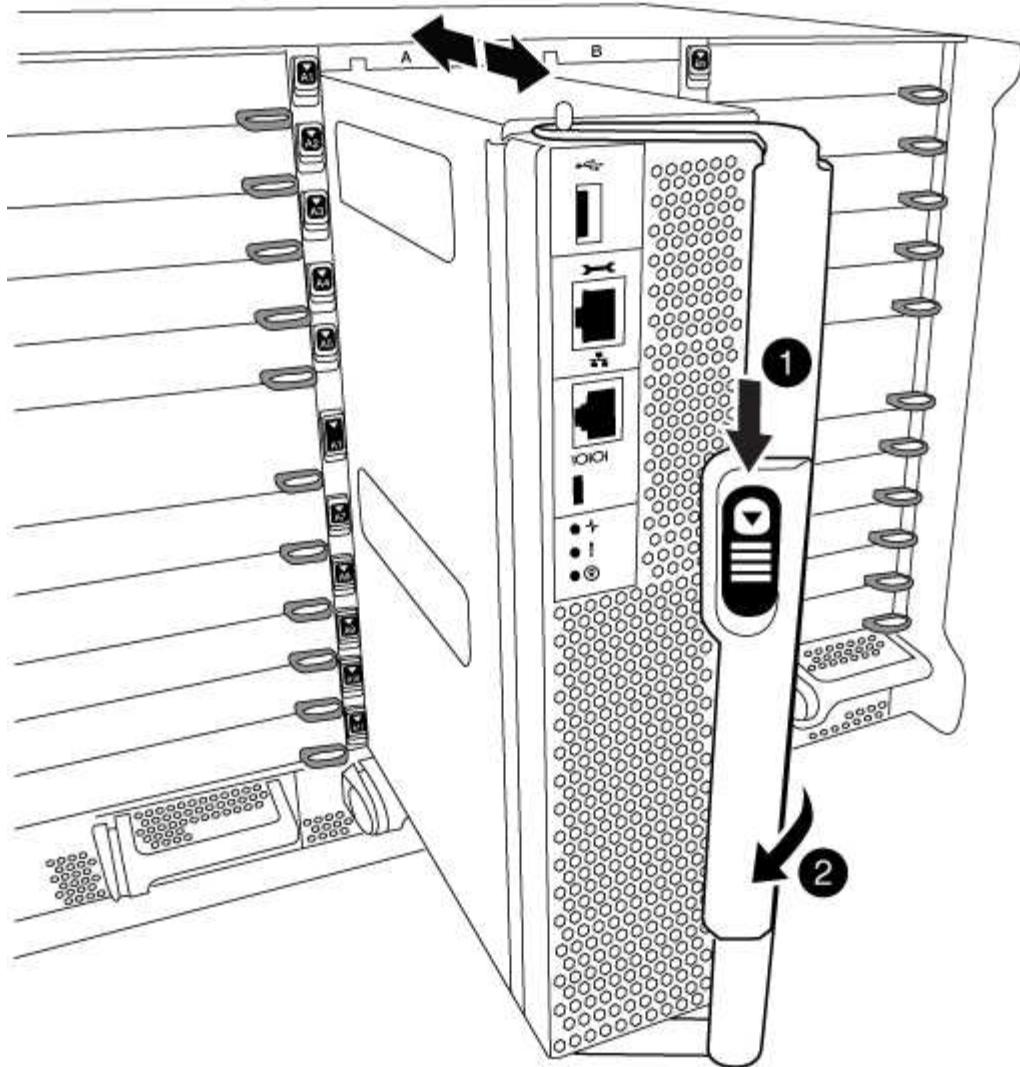
Para sustituir el soporte de arranque, debe retirar el módulo del controlador dañado, instalar el soporte de arranque de repuesto y transferir la imagen de inicio a una unidad flash USB.

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.

Pasos

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Desenchufe los cables del módulo del controlador dañado y haga un seguimiento de dónde se conectaron los cables.
3. Deslice el botón naranja del asa de la leva hacia abajo hasta que se desbloquee.



1

Botón de liberación de la palanca de leva

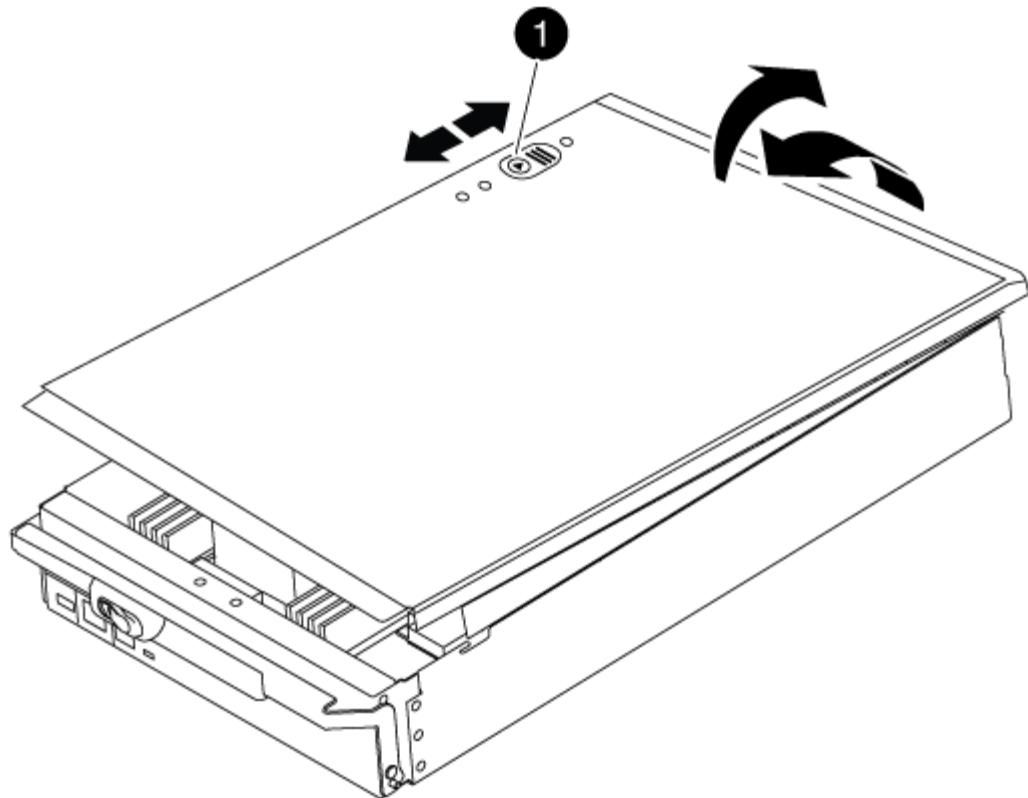
2

Mango de leva

4. Gire el asa de leva para que desacople completamente el módulo del controlador del chasis y, a continuación, deslice el módulo del controlador para sacarlo del chasis.

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

5. Coloque el lado de la tapa del módulo del controlador hacia arriba sobre una superficie plana y estable, pulse el botón azul de la cubierta, deslice la cubierta hacia la parte posterior del módulo del controlador y, a continuación, gire la cubierta hacia arriba y levántela fuera del módulo del controlador.

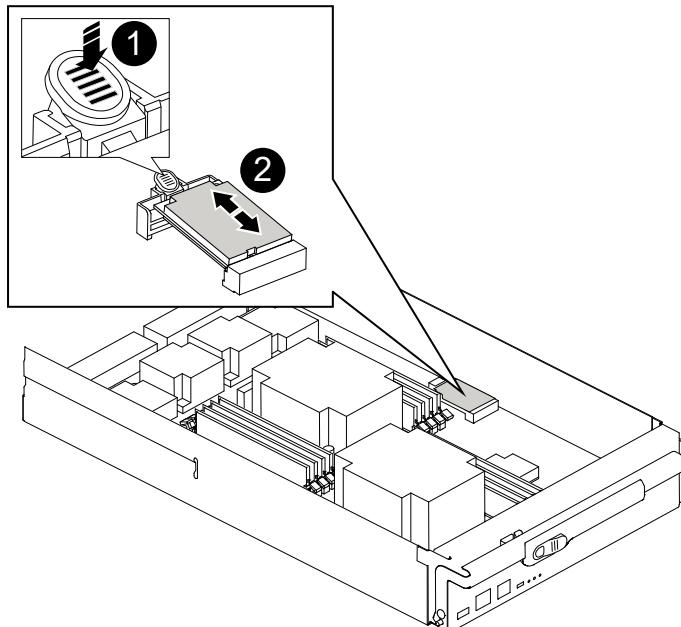


1

Botón de bloqueo de la cubierta del módulo del controlador

Paso 2: Sustituya el soporte de arranque

Localice el medio de arranque con la siguiente ilustración o el mapa de FRU en el módulo de la controladora:



1

Presione la lengüeta de liberación

2

Soporte de arranque

1. 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.

2. Alinee los bordes del soporte de arranque de repuesto con el zócalo del soporte de arranque y, a continuación, empújelo suavemente en el zócalo.
3. 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.

4. Empuje el soporte del maletero hacia abajo para activar el botón de bloqueo en la carcasa del soporte del maletero.
5. Vuelva a instalar la tapa del módulo del controlador alineando los pasadores de la tapa con las ranuras del soporte de la placa base y, a continuación, deslice la tapa en su lugar.

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. Sin embargo, debe restaurar el `var` sistema de archivos durante este

procedimiento.

- Debe tener una unidad flash USB, formateada con 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 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 independiente, no necesita una conexión de red, pero debe realizar un reinicio adicional al restaurar el `var` sistema de archivos.

Pasos

1. 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.
 2. Recuperar el módulo del controlador, según sea necesario.
 3. 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.
4. 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 sentarse el módulo del controlador y, a continuación, empuje el asa de la leva hasta la posición cerrada.

El nodo empieza a arrancar en cuanto se instala por completo en el chasis.

5. 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 pierde este mensaje, pulse Ctrl-C, seleccione la opción de arrancar en modo de mantenimiento y, a continuación, detenga el nodo para arrancar en EL CARGADOR.

6. 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 configura es el puerto de destino que utiliza para comunicarse con el nodo dañado del nodo en buen estado durante `var` restauración del sistema de archivos 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.

7. 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.

Inicie la imagen de recuperación - FAS9000

El procedimiento para iniciar el nodo dañado desde la imagen de recuperación depende de si el sistema está en una configuración MetroCluster de dos nodos. El sistema FAS9000 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

El procedimiento para arrancar el nodo dañado desde la imagen de recuperación depende de si el sistema está en una configuración de MetroCluster de dos nodos.

Opción 1: Inicia la imagen de recuperación en la mayoría de los sistemas

Debe arrancar la imagen de ONTAP desde la unidad USB, restaurar el sistema de archivos y verificar las variables del 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 `var` sistema de archivos:

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

Si el sistema tiene...	Realice lo siguiente...
No hay conexión de red y está en una configuración de IP de MetroCluster	<p>a. Pulse n 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 Actualizar flash desde la configuración de copia de seguridad (flash de sincronización) en el menú que se muestra.</p> <p>Si se le solicita que continúe con la actualización, pulse y.</p>

4. Asegurarse de que las variables medioambientales estén establecidas de la manera 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 `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.

*Si ve...	Entonces... *
La solicitud de inicio de sesión de	Vaya al siguiente paso.
Esperando devolución...	<ol style="list-style-type: none"> Inicie sesión en el nodo del partner. Confirme que el nodo de destino está listo para la devolución con el <code>storage failover show</code> comando.

7. Conecte el cable de consola al nodo compañero.

8. Vuelva a dar el nodo mediante 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 consola al nodo 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.

Opción 2: Arrancar la imagen de recuperación en una configuración 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 **savenv** comando.
 - e. Reiniciar el nodo.

Vuelva a cambiar los agregados en una configuración MetroCluster de dos nodos: FAS9000

Después de completar el reemplazo del medio de arranque, realice la operación de retroceso de MetroCluster. El sistema FAS9000 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

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 - FAS9000

Restaurar el cifrado en el medio de arranque de reemplazo. El sistema FAS9000 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

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

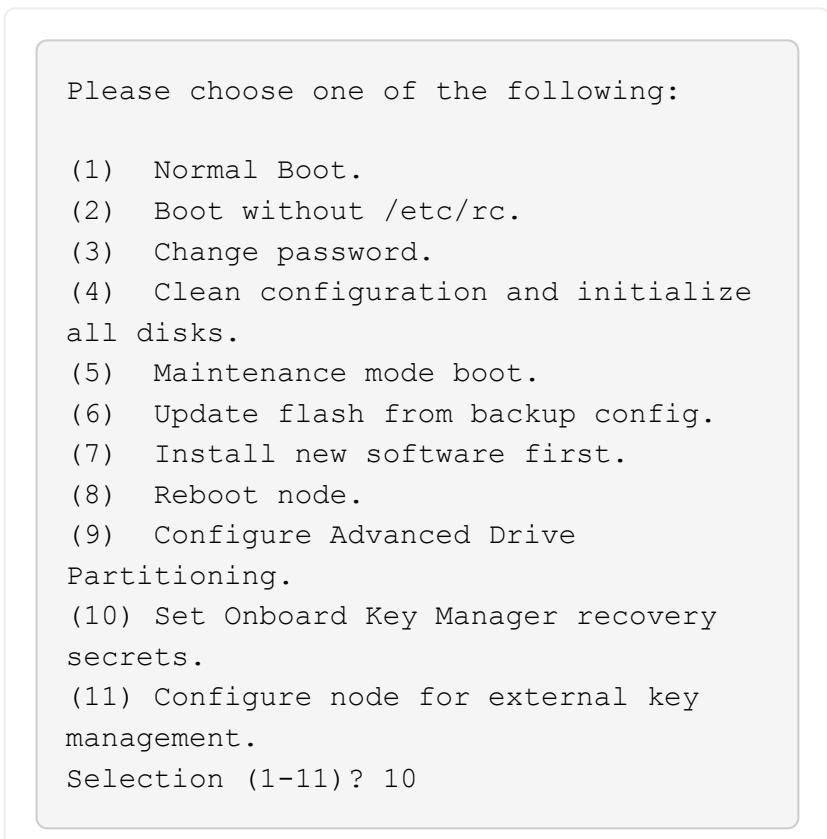
Asegúrese de tener disponible la siguiente información:

- 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 data-bbox="638 297 1437 973" style="border: 1px solid #ccc; padding: 10px;"> <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:

- a. 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
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
0123456789012345678901234567890123456789012345678901
23
1234567890123456789012345678901234567890123456789012
34
2345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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 fallida a NetApp - FAS9000

Devuelva la pieza defectuosa a NetApp, como se describe en las instrucciones de RMA enviadas con el kit. Ver el ["Devolución de piezas y sustituciones"](#) página para más información. El sistema FAS9000 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Impreso 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.