



Soporte de arranque

Install and maintain

NetApp
December 18, 2024

Tabla de contenidos

- Soporte de arranque 1
 - Flujo de trabajo de sustitución de medios de arranque: AFF C30 y AFF C60 1
 - Requisitos y consideraciones: AFF C30 y AFF C60 1
 - Compruebe las claves de cifrado integradas: AFF C30 y AFF C60 2
 - Apague el controlador defectuoso: AFF C30 y AFF C60 7
 - Sustituya el soporte de arranque: AFF C30 y AFF C60 8
 - Inicie la imagen de recuperación - AFF C30 y AFF C60 14
 - Restaurar cifrado: AFF C30 y AFF C60 16
 - Devuelva la pieza fallida a NetApp - AFF C30 and AFF C60 26

Soporte de arranque

Flujo de trabajo de sustitución de medios de arranque: AFF C30 y AFF C60

Siga estos pasos del flujo de trabajo para sustituir el soporte de arranque.

1

"Revise los requisitos de medios de arranque"

Para sustituir el soporte de arranque, debe cumplir ciertos requisitos.

2

"Compruebe las claves de cifrado incorporadas"

Verifique si su sistema de almacenamiento tiene el administrador de claves de seguridad habilitado o discos cifrados.

3

"Apague el controlador dañado"

Apague o asuma el control de la controladora deteriorada para que la controladora en buen estado siga sirviendo datos del almacenamiento de la controladora dañado.

4

"Sustituya el soporte de arranque"

Retire el soporte de arranque defectuoso del controlador defectuoso e instale el soporte de arranque de repuesto y, a continuación, transfiera una imagen ONTAP mediante una unidad flash USB al soporte de arranque de repuesto.

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 gestor de claves incorporado o el gestor de claves externo desde el menú de arranque de ONATP.

7

"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 y consideraciones: AFF C30 y AFF C60

Antes de sustituir el soporte de arranque, asegúrese de revisar los siguientes requisitos y

consideraciones.

Requisitos

- Debe tener una unidad flash USB, formateada a FAT32, con la cantidad de almacenamiento adecuada para guardar el `image_xxx.tgz`.
- Debe copiar `image_xxx.tgz` el archivo en la unidad flash USB para su uso posterior en este procedimiento.
- Debe sustituir el componente con fallos por un componente FRU de reemplazo con la misma capacidad que recibió de su proveedor.

Consideraciones

- 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.
- Si es necesario, puede encender los LED de ubicación del chasis de la plataforma (azules) para ayudar a localizar físicamente la plataforma afectada. Inicie sesión en BMC mediante SSH e introduzca `system location-led on` el comando.

Un chasis de plataforma tiene tres LED de ubicación: Uno en el panel de visualización del operador y otro en cada controlador. Los LED de ubicación permanecen encendidos durante 30 minutos.

Puede desactivarlos introduciendo `system location-led off` el comando. Si no está seguro de si los LED están encendidos o apagados, puede comprobar su estado introduciendo `system location-led show` el comando.

Compruebe las claves de cifrado integradas: AFF C30 y AFF C60

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

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

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

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

```
version -v
```

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

2. Según si NVE es compatible con el sistema, realice una de las siguientes acciones:
 - Si NVE es compatible, descargue la imagen ONTAP con NetApp Volume Encryption.

- Si NVE no es compatible, descargue la imagen ONTAP **sin** Cifrado de volumen NetApp.

Paso 2: Determine si es seguro apagar el controlador

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

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

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

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

No se ha configurado ningún gestor de claves

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

Se ha configurado el gestor de claves externo o incorporado

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

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

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

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

3. En función de si el sistema utiliza el Administrador de claves externo o el Administrador de claves

incorporado, seleccione una de las siguientes opciones.

Gestor de claves externo

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

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

Gestión de claves incorporada

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

Valor de salida en Restored la columna

Siga estos pasos...

true

Realice una copia de seguridad manual de la información de OKM.

- a. Vaya al modo avanzado introduciendo `set -priv advanced` y, a continuación, introdúzcalo y cuando se le solicite.
- b. Introduzca el siguiente comando para mostrar la información de gestión de claves:

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

- c. Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados.

Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.

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

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

Apague el controlador defectuoso: AFF C30 y AFF C60

Apague o tome el control de la controladora dañada.

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

1. Si AutoSupport está habilitado, suprima 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
```

2. Desactive la devolución automática de la consola de la controladora en buen estado: `storage failover modify -node local -auto-giveback false`



Cuando vea *do desea desactivar la devolución automática?*, introduzca *y*.

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

Sustituya el soporte de arranque: AFF C30 y AFF C60

Para sustituir el soporte de arranque, debe extraer el controlador deteriorado, extraer el soporte de arranque, instalar el soporte de arranque de repuesto y transferir la imagen de arranque a una unidad flash USB.

Paso 1: Quite la controladora

Es necesario quitar la controladora del chasis cuando se sustituye la controladora o se sustituye uno dentro de la controladora.

Antes de empezar

El resto de componentes del sistema de almacenamiento deben funcionar correctamente. De lo contrario,

debe ponerse en contacto ["Soporte de NetApp"](#) antes de continuar con este procedimiento.

Pasos

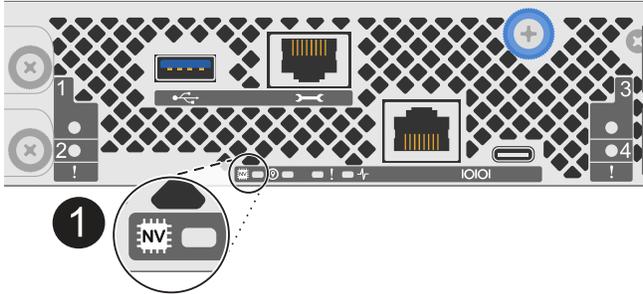
1. En el controlador deteriorado, asegúrese de que el LED NV está apagado.

Cuando el LED NV está apagado, la separación se completa y es seguro retirar el controlador defectuoso.



Si el LED NV parpadea (verde), la separación está en curso. Debe esperar a que se apague el LED NV. Sin embargo, si el parpadeo continúa durante más de cinco minutos, póngase en contacto con ["Soporte de NetApp"](#) antes de continuar con este procedimiento.

El LED NV se encuentra junto al icono de NV de la controladora.



1

Icono de NV y LED en el controlador

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Desconecte la alimentación del controlador dañado:



Las fuentes de alimentación (PSU) no tienen un interruptor de alimentación.

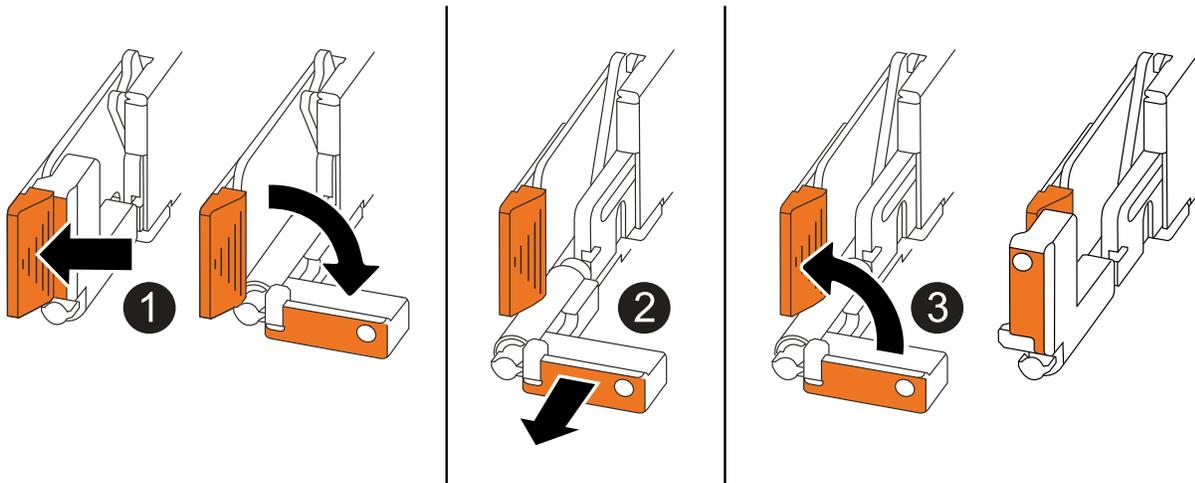
Si va a desconectar un...	Realice lo siguiente...
PSU DE CA	<ol style="list-style-type: none">a. Abra el retén del cable de alimentación.b. Desconecte el cable de alimentación de la fuente de alimentación y déjelo a un lado.
FUENTE DE ALIMENTACIÓN DE CC	<ol style="list-style-type: none">a. Desenrosque los dos tornillos de mariposa del conector del cable de alimentación de CC D-SUB.b. Desconecte el cable de alimentación de la fuente de alimentación y déjelo a un lado.

3. Desconecte todos los cables del controlador dañado.

Mantenga un registro de dónde se conectaron los cables.

4. Retire el controlador deteriorado:

En la siguiente ilustración, se muestra el funcionamiento de las asas de la controladora (desde el lado izquierdo de la controladora) al quitar una controladora:



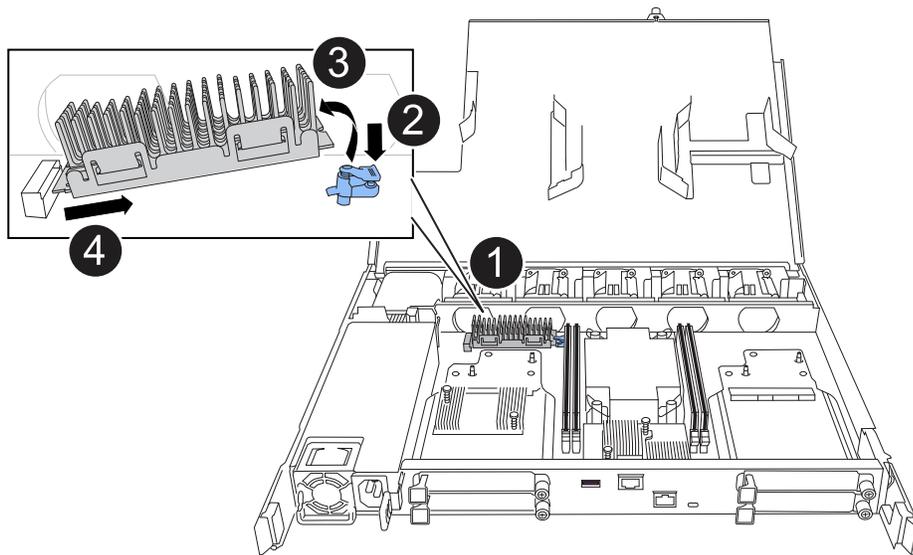
<p>1</p>	<p>En ambos extremos del controlador, empuje las lengüetas de bloqueo verticales hacia afuera para liberar las asas.</p>
<p>2</p>	<ul style="list-style-type: none"> • Tire de las asas hacia usted para desalojar el controlador del plano medio. <p>A medida que tira, las asas se extienden hacia fuera del controlador y luego siente algo de resistencia, siga tirando.</p> <ul style="list-style-type: none"> • Deslice el controlador para sacarlo del chasis mientras sostiene la parte inferior del controlador y colóquelo en una superficie plana y estable.
<p>3</p>	<p>Si es necesario, gire las asas hacia arriba (junto a las pestañas) para alejarlas.</p>

5. Coloque el controlador sobre una alfombrilla antiestática.
6. Abra la cubierta del controlador girando el tornillo de mariposa hacia la izquierda para aflojarla y, a continuación, abra la cubierta.

Paso 2: Sustituya el soporte de arranque

Para sustituir el medio de arranque, búsquelo dentro de la controladora y siga la secuencia de pasos específica.

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Retire el soporte de arranque:



1	Ubicación del soporte de arranque
2	Presione la pestaña azul hacia abajo para soltar el extremo derecho del soporte de arranque.
3	Levante el extremo derecho del soporte de arranque en un ángulo ligero para conseguir un buen agarre a lo largo de los laterales del soporte de arranque.
4	Tire suavemente del extremo izquierdo del soporte de arranque para extraerlo de su toma.

3. Instale el soporte de arranque de repuesto:

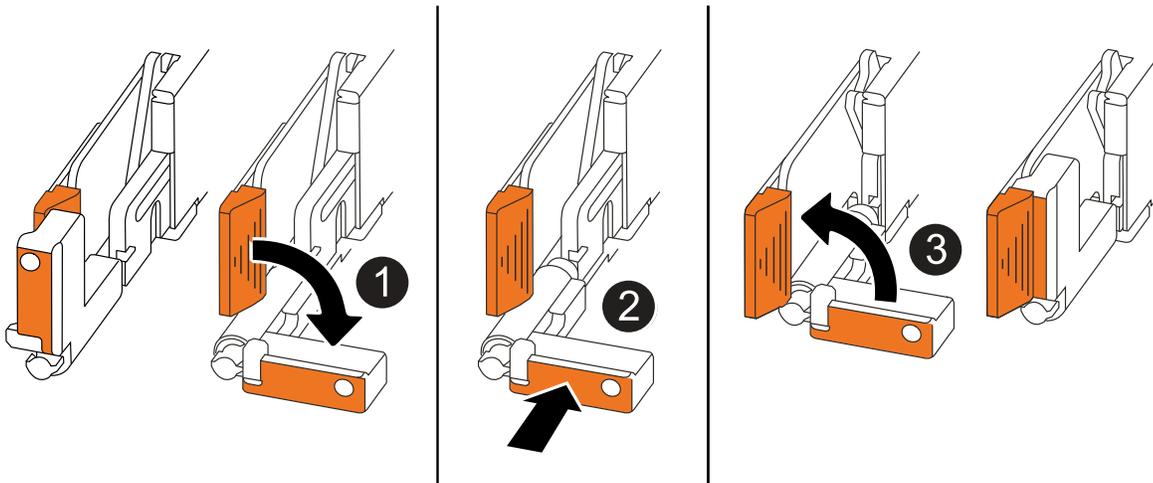
- a. Retire el soporte de arranque de su paquete.
- b. Deslice el extremo de la toma del soporte de arranque en su toma.
- c. En el extremo opuesto del soporte de arranque, presione y mantenga presionada la lengüeta azul (en la posición abierta), presione suavemente hacia abajo ese extremo del soporte de arranque hasta que se detenga, y luego suelte la pestaña para bloquear el soporte de arranque en su lugar.

Paso 3: Vuelva a instalar el controlador

Vuelva a instalar la controladora en el chasis, pero no la reinicie.

Acerca de esta tarea

La siguiente ilustración muestra el funcionamiento de las asas de la controladora (desde el lado izquierdo de una controladora) al reinstalar la controladora y se puede utilizar como referencia para el resto de los pasos de reinstalación de la controladora.



<p>1</p>	<p>Si giró las asas del controlador en posición vertical (junto a las pestañas) para alejarlas mientras realizaba el mantenimiento del controlador, gírelas hacia abajo hasta la posición horizontal.</p>
<p>2</p>	<p>Empuje las asas para volver a insertar el controlador en el chasis hasta la mitad y, a continuación, cuando se le indique, empuje hasta que el controlador esté completamente asentado.</p>
<p>3</p>	<p>Gire las asas hasta la posición vertical y bloquéelas en su lugar con las lengüetas de bloqueo.</p>

Pasos

1. Cierre la cubierta del controlador y gire el tornillo de mariposa hacia la derecha hasta que se apriete.
2. Inserte la controladora a la mitad en el chasis.

Alinee la parte posterior de la controladora con la apertura del chasis y empuje suavemente la controladora con las asas.



No inserte por completo la controladora en el chasis hasta que se le indique hacerlo más adelante en este procedimiento.

3. Vuelva a conectar los cables a la controladora; sin embargo, no conecte el cable de alimentación al suministro de alimentación (PSU) en este momento.



Asegúrese de que el cable de la consola está conectado a la controladora porque desea capturar y registrar la secuencia de arranque más adelante en el procedimiento de sustitución de medios de arranque cuando coloque completamente la controladora en el chasis y comience a arrancar.

Paso 4: Transfiera la imagen de arranque al soporte de arranque

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

Antes de empezar

- Debe tener una unidad flash USB, formateada con FAT32, con una capacidad mínima de 4 GB.
- Debe tener una copia de la misma versión de imagen de ONTAP que se estaba ejecutando la controladora dañada. Puede descargar la imagen adecuada de "[Descargas](#)" la sección del sitio de soporte de NetApp
 - Si NVE es compatible, descargue la imagen con NetApp Volume Encryption, 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.
- Debe tener una conexión de red entre los puertos de gestión de nodos de las controladoras (normalmente las interfaces e0M).

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 el puerto USB-A del controlador afectado.

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

3. Coloque completamente el controlador deteriorado en el chasis:

- a. Empuje firmemente las asas hasta que el controlador se encuentre con el plano medio y quede completamente asentado.



No ejerza demasiada fuerza al deslizar el controlador en el chasis, ya que podría dañar los conectores.



La controladora arranca cuando está completamente asentada en el chasis. Obtiene su poder del controlador asociado.

- a. Gire las asas del controlador hacia arriba y bloquéelas en su lugar con las lengüetas.

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.

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

- Si va a configurar DHCP:

```
ifconfig e0M -auto
```



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

- Si está configurando conexiones manuales:

```
ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway
```

- 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.



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

6. Vuelva a conectar el cable de alimentación a la fuente de alimentación (PSU) de la controladora dañada.

Una vez restaurada la alimentación de la fuente de alimentación, el LED de estado debería ser verde.

Si va a volver a conectar un...	Realice lo siguiente...
PSU DE CA	<ol style="list-style-type: none"> Conecte el cable de alimentación a la fuente de alimentación. Fije el cable de alimentación con el retén del cable de alimentación.
FUENTE DE ALIMENTACIÓN DE CC	<ol style="list-style-type: none"> Conecte el conector del cable de alimentación de CC D-SUB a la PSU. Apriete los dos tornillos de mariposa para fijar el conector del cable de alimentación de CC D-SUB a la PSU.

Inicie la imagen de recuperación - AFF C30 y AFF C60

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:

Opción 1: ONTAP 9.16,0 o anterior

- a. En el controlador defectuoso, pulse Y cuando vea `Do you want to restore the backup configuration now?`
- b. En el controlador dañado, pulse Y cuando se le solicite sobrescribir `/etc/ssh/ssh_HOST_ecdsa_KEY`.
- c. En el controlador asociado en buen estado, configure la controladora con deficiencias en el nivel de privilegio avanzado `set -privilege advanced:.`
- d. En la controladora asociada en buen estado, ejecute el comando `restore backup system node restore-backup -node local -target-address impaired_node_IP_address:.`

NOTA: Si ve cualquier mensaje que no sea una restauración exitosa, póngase en contacto con ["Soporte de NetApp"](#).

- e. En la controladora asociada en buen estado, devuelva la controladora afectada al nivel de administración `set -privilege admin:.`
- f. En el controlador deficiente, pulse Y cuando vea `Was the restore backup procedure successful?.`
- g. En el controlador deficiente, pulse Y cuando vea `...would you like to use this restored copy now?.`
- h. En el controlador dañado, pulse Y cuando se le solicite reiniciar el controlador dañado y pulse `ctrl-c` para acceder al menú de arranque.
- i. Si el sistema no utiliza cifrado, seleccione *Opción 1 Normal Boot.*; de lo contrario, vaya a ["Restaure el cifrado"](#).

Opción 2: ONTAP 9.16,1 o posterior

- a. En el controlador dañado, pulse Y cuando se le solicite restaurar la configuración de copia de seguridad.

Después de que el procedimiento de restauración se haya realizado correctamente, este mensaje se mostrará en la consola - `syncflash_partner: Restore from partner complete.`

- b. En la controladora deteriorada, pulse Y cuando se le solicite confirmar si la copia de seguridad de la restauración se ha realizado correctamente.
- c. En el controlador defectuoso, pulse Y cuando se le solicite utilizar la configuración restaurada.
- d. En la controladora defectuosa, pulse Y cuando se le solicite reiniciar el nodo.
- e. En el controlador dañado, pulse Y cuando se le solicite reiniciar el controlador dañado y pulse `ctrl-c` para acceder al menú de arranque.
- f. Si el sistema no utiliza cifrado, seleccione *Opción 1 Normal Boot.*; de lo contrario, vaya a ["Restaure el cifrado"](#).

4. Conecte el cable de la consola al controlador asociado.

5. Respalde la controladora con el `storage failover giveback -fromnode local` comando.

6. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.
7. Si AutoSupport está habilitado, restaurar/desactivar la creación automática de casos mediante el `system node autosupport invoke -node * -type all -message MAINT=END` comando.

NOTA: Si el proceso falla, póngase en contacto con ["Soporte de NetApp"](#).

Restaurar cifrado: AFF C30 y AFF C60

Restaure el cifrado en el soporte de arranque de reemplazo.

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

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

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

Opción 1: Restaure la configuración del gestor de claves incorporado

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

Antes de empezar

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

Pasos

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

Versión de ONTAP	Seleccione esta opción
ONTAP 9.8 o posterior	<p data-bbox="621 153 927 191">Seleccione la opción 10.</p> <p data-bbox="621 222 1060 260">Mostrar ejemplo de menú de inicio</p> <div data-bbox="654 296 1455 1079" style="border: 1px solid #ccc; padding: 10px;"><p data-bbox="683 331 1295 369">Please choose one of the following:</p><ul data-bbox="683 411 1370 1010" style="list-style-type: none"><li data-bbox="683 411 971 449">(1) Normal Boot.<li data-bbox="683 453 1133 491">(2) Boot without /etc/rc.<li data-bbox="683 495 1045 533">(3) Change password.<li data-bbox="683 537 1370 606">(4) Clean configuration and initialize all disks.<li data-bbox="683 611 1154 648">(5) Maintenance mode boot.<li data-bbox="683 653 1328 690">(6) Update flash from backup config.<li data-bbox="683 695 1240 732">(7) Install new software first.<li data-bbox="683 737 971 774">(8) Reboot node.<li data-bbox="683 779 1192 848">(9) Configure Advanced Drive Partitioning.<li data-bbox="683 852 1333 921">(10) Set Onboard Key Manager recovery secrets.<li data-bbox="683 926 1317 995">(11) Configure node for external key management.<p data-bbox="683 1010 1036 1047">Selection (1-11)? 10</p></div>

Versión de ONTAP	Seleccione esta opción
ONTAP 9,7 y anteriores	<p data-bbox="621 163 1404 195">Seleccione la opción oculta <code>recover_onboard_keymanager</code></p> <p data-bbox="621 233 1058 264">Mostrar ejemplo de menú de inicio</p> <div data-bbox="654 306 1455 968" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <pre data-bbox="683 342 1369 932"> Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager </pre> </div>

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

Mostrar símbolo del sistema de ejemplo

```

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

```

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

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

Mostrar símbolo del sistema de ejemplo

```

Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:

```

5. Introduzca la información de backup.

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

Mostrar símbolo del sistema de ejemplo

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

Successfully recovered keymanager secrets.

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



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

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

Mostrar símbolo del sistema de ejemplo

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

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

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

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

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

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

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

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

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

Mostrar símbolo del sistema de ejemplo

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

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



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

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

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

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



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

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

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

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

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

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

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

Opción 2: Restaure la configuración del gestor de claves externo

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

Antes de empezar

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

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

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

Pasos

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

Mostrar ejemplo de menú de inicio

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 11
```

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

Mostrar símbolo del sistema de ejemplo

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

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

Mostrar petición de datos

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

Muestra el ejemplo

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEWpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUobQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

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

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

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

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

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

Muestra el ejemplo

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

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

Mostrar símbolo del sistema de ejemplo

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

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

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

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

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

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

Devuelva la pieza fallida a NetApp - AFF C30 and AFF C60

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

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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