# Soporte de arranque

## Install and maintain

NetApp
March 22, 2024

# Tabla de contenidos

# Soporte de arranque

## Descripción general de la sustitución de medios de arranque - AFF A320

El soporte de arranque almacena un conjunto principal y secundario de archivos del sistema (imagen de arranque) que el sistema utiliza cuando arranca. En función de la configuración de red, puede realizar una sustitución no disruptiva o disruptiva.

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

También debe copiar el `image_xxx.tgz` Archivo a la unidad flash USB para su uso posterior en este procedimiento.

- Ambos métodos no disruptivos y disruptivos para reemplazar medios de arranque requieren restaurar el `var` sistema de archivos:
  - Para poder realizar sustituciones de forma no disruptiva, el par de alta disponibilidad debe estar conectado a una red para restaurar el `var` sistema de archivos.
  - Para el reemplazo disruptivo, no es necesaria una conexión de red para restaurar el `var` el sistema de archivos, pero el proceso requiere dos reinicios.
- Debe sustituir el componente con errores por un componente FRU de repuesto que haya recibido de su proveedor.
- Es importante que aplique los comandos en estos pasos en el nodo correcto:
  - El nodo *drinated* es el nodo en el que realiza tareas de mantenimiento.
  - El *heated node* es el partner de alta disponibilidad del nodo dañado.

## Compruebe las claves de cifrado integradas: AFF A320

Antes de apagar la controladora deficiente y comprobar el estado de las claves de cifrado incorporadas, debe comprobar el estado de la controladora deficiente, deshabilitar la devolución automática y comprobar qué versión de ONTAP se está ejecutando en el sistema.

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 FALSE para tener derecho a recibir este tipo de servicios, debe corregir el problema antes de apagar la controladora con deficiencias; consulte la "Sincronice un nodo con el clúster".

**Pasos**

1. Compruebe el estado del controlador dañado:
   - Si el controlador dañado se encuentra en la solicitud de inicio de sesión, inicie sesión como `admin`.
   - Si la controladora dañada se encuentra en el aviso del CARGADOR y forma parte de la configuración de alta disponibilidad, inicie sesión como `admin` en el controlador en buen estado.
   - Si la controladora dañada se encuentra en una configuración independiente y en un aviso DEL CARGADOR, póngase en contacto con "mysupport.netapp.com".

2. 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`

3. Compruebe la versión de ONTAP que el sistema está funcionando en el controlador dañado si está activo, o en el controlador asociado si el controlador dañado está inactivo, usando el `version -v` comando:
   - Si se muestra <lno-DARE> o <1Ono-DARE> en el resultado del comando, el sistema no admite NVE, continúe para apagar la controladora.
   - Si <lno-DARE> no aparece en el resultado del comando y el sistema está ejecutando ONTAP 9.6 o una versión posterior, vaya a la sección siguiente.

## Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.6 y posterior

Antes de apagar la controladora dañada, debe verificar si el sistema tiene habilitado el cifrado de volúmenes de NetApp (NVE) o el cifrado de almacenamiento de NetApp (NSE). Si es así, debe comprobar la configuración.

1. Verifique si el cifrado de volúmenes está en uso para cualquier volumen del clúster: `volume show -is -encrypted true`

   Si algún volumen aparece en la salida, NVE se configura y debe verificar la configuración NVE. Si no aparece ningún volumen en la lista, compruebe si NSE está configurado y en uso.

2. Compruebe si NSE está configurado y en uso: `storage encryption disk show`
   - Si el resultado del comando incluye los detalles de la unidad con información sobre el modo y el identificador de clave, NSE se configura y es necesario verificar la configuración de NSE y en uso.
   - Si no se muestra ningún disco, NSE no está configurado.
   - Si NVE y NSE no están configurados, no hay unidades protegidas con las claves NSE, es seguro apagar la controladora dañada.

## Verifique la configuración de NVE

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves: `security key-manager key query`

   > Después de la versión ONTAP 9.6, es posible que tenga otros tipos de gestor de claves. Los tipos son `KMIP`, `AKV`, y. `GCP`. El proceso de confirmación de estos tipos es el mismo que el de confirmación `external` o. `onboard` tipos de gestor de claves.

   - Si la `Key Manager` aparece el tipo `external` y la `Restored` la columna muestra `yes`, es seguro apagar el controlador dañado.
   - Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, necesita completar algunos pasos adicionales.
   - Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.

- Si la `Key Manager` aparece el tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.

2. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, Realizar una copia de seguridad manual de la información de OKM:
   a. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
   b. Introduzca el 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. Volver al modo admin: `set -priv admin`
   e. Apague el controlador dañado.
3. Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
   a. Restaure las claves de autenticación de gestión de claves externas a todos los nodos del clúster: `security key-manager external restore`

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

   "mysupport.netapp.com"

   a. Compruebe que el `Restored` la columna es igual `yes` para todas las claves de autenticación: `security key-manager key query`
   b. Apague el controlador dañado.
4. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
   a. Introduzca el comando SYNC del gestor de claves de seguridad incorporado: `security key-manager onboard sync`

      > Introduzca 32 la clave de acceso de gestión de claves incorporada y alfanumérica del cliente en el símbolo del sistema. Si no se puede proporcionar la clave de acceso, comuníquese con el soporte de NetApp. "mysupport.netapp.com"

   b. Compruebe el `Restored` la columna muestra `yes` para todas las claves de autenticación: `security key-manager key query`
   c. Compruebe que el `Key Manager` el tipo muestra `onboard`, Y a continuación, realice una copia de seguridad manual de la información de OKM.
   d. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
   e. Introduzca el comando para mostrar la información de backup para la gestión de claves: `security key-manager onboard show-backup`
   f. 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.

g. Volver al modo admin: `set -priv admin`

h. Puede apagar el controlador de forma segura.

## Verifique la configuración de NSE

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves: `security key-manager key query -key-type NSE-AK`

> Después de la versión ONTAP 9.6, es posible que tenga otros tipos de gestor de claves. Los tipos son `KMIP`, `AKV`, y. `GCP`. El proceso de confirmación de estos tipos es el mismo que el de confirmación `external` o. `onboard` tipos de gestor de claves.

   - Si la `Key Manager` aparece el tipo `external` y la `Restored` la columna muestra `yes`, es seguro apagar el controlador dañado.
   - Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, necesita completar algunos pasos adicionales.
   - Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.
   - Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.

2. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, Realizar una copia de seguridad manual de la información de OKM:

   a. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`

   b. Introduzca el 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. Volver al modo admin: `set -priv admin`

   e. Puede apagar el controlador de forma segura.

3. Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:

   a. Restaure las claves de autenticación de gestión de claves externas a todos los nodos del clúster: `security key-manager external restore`

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

   "mysupport.netapp.com"

   a. Compruebe que el `Restored` la columna es igual `yes` para todas las claves de autenticación: `security key-manager key query`

   b. Puede apagar el controlador de forma segura.

4. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:

   a. Introduzca el comando SYNC del gestor de claves de seguridad incorporado: `security key-manager onboard sync`

      Introduzca 32 la clave de acceso de gestión de claves incorporada y alfanumérica del cliente en el símbolo del sistema. Si no se puede proporcionar la clave de acceso, comuníquese con el soporte de NetApp.

   "mysupport.netapp.com"

   a. Compruebe el `Restored` la columna muestra `yes` para todas las claves de autenticación: `security key-manager key query`
   b. Compruebe que el `Key Manager` el tipo muestra `onboard`, Y a continuación, realice una copia de seguridad manual de la información de OKM.
   c. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
   d. Introduzca el comando para mostrar la información de backup para la gestión de claves: `security key-manager onboard show-backup`
   e. 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.
   f. Volver al modo admin: `set -priv admin`
   g. Puede apagar el controlador de forma segura.

# Apague el nodo - AFF A320

Después de completar las tareas de NVE o NSE, necesita completar el apagado del nodo dañado. Apague o retome el controlador dañado siguiendo el procedimiento adecuado para su configuración.

## 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. |

| Si el controlador dañado muestra… | Realice lo siguiente… |
|---|---|
| Solicitud del sistema o solicitud de contraseña (introduzca la contraseña del sistema) | Retome o detenga el controlador dañado del controlador en buen estado: `storage failover takeover -ofnode impaired_node_name`<br><br>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: El sistema está en una 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. |

| Si el controlador dañado está mostrando… | Realice lo 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: `storage failover takeover -ofnode` *`impaired_node_name`*<br><br>Cuando el controlador dañado muestre esperando devolución…, pulse Ctrl-C y, a continuación, responda `y`. |

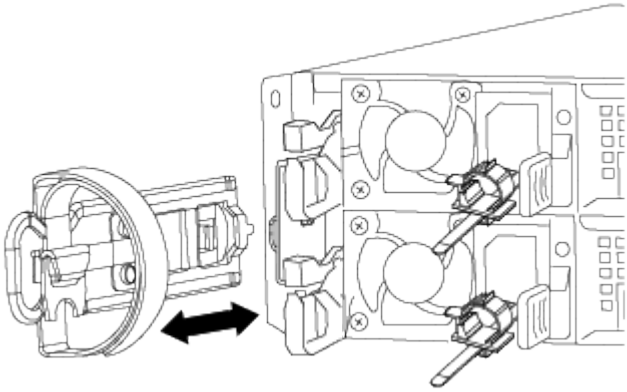
# Reemplace el soporte de arranque - AFF A320

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

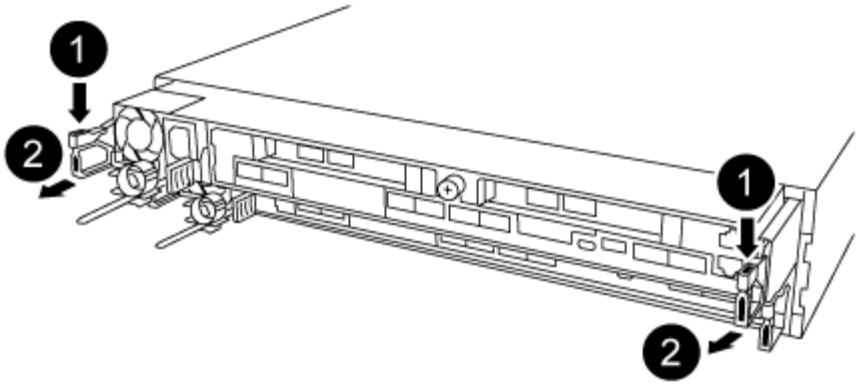
Para acceder a los componentes internos del módulo de controlador, debe extraer el módulo de controlador del chasis.

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



   Deje los cables en el dispositivo de administración de cables de manera que cuando vuelva a instalar el dispositivo de administración de cables, los cables estén organizados.

4. Retire y retire los dispositivos de administración de cables de los lados izquierdo y derecho del módulo del controlador.
5. Extraiga el módulo de la controladora del chasis:




a. Inserte el índice en el mecanismo de bloqueo a ambos lados del módulo del controlador.
b. Presione hacia abajo la lengüeta naranja de la parte superior del mecanismo de bloqueo hasta que se separe el pasador de bloqueo del chasis.

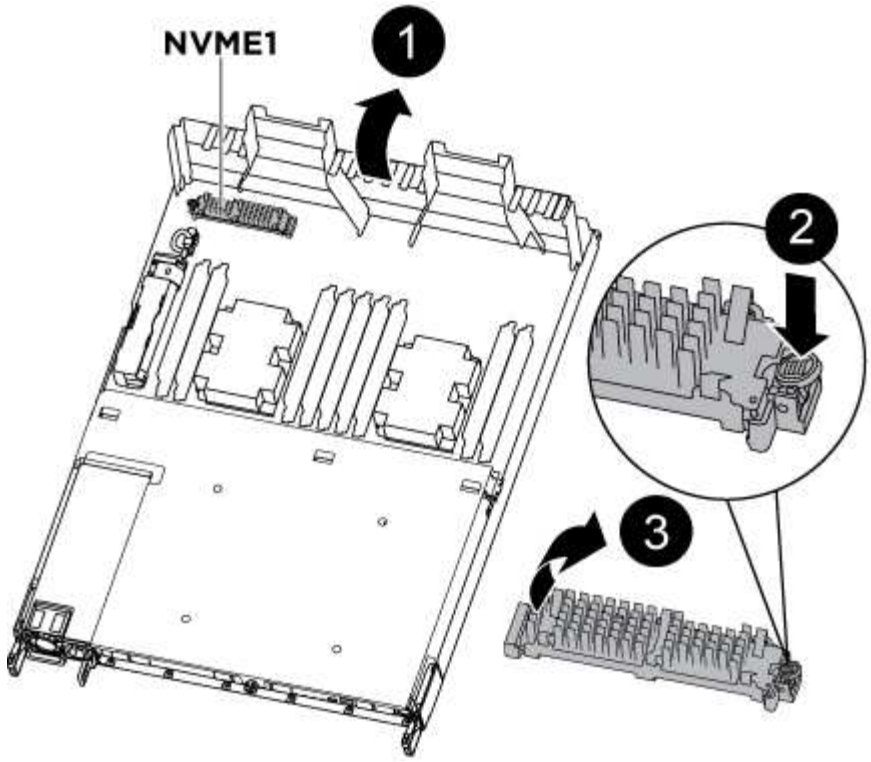
   El gancho del mecanismo de bloqueo debe estar casi en vertical y debe estar alejado del pasador del chasis.

c. Tire suavemente del módulo del controlador unas pulgadas hacia usted para que pueda agarrar los lados del módulo del controlador.
d. Con ambas manos, tire suavemente del módulo del controlador para sacarlo del chasis y configúrelo en una superficie plana y estable.

## Paso 2: Sustituya el soporte de arranque

Debe localizar el medio de arranque en el módulo de la controladora y, a continuación, seguir las instrucciones para reemplazarlo.

1. Abra el conducto de aire y localice el soporte de arranque con la siguiente ilustración o el mapa de FRU en el módulo del controlador:
2. Localice y retire el soporte de arranque del módulo de la controladora:




a. Pulse el botón azul al final del soporte de arranque hasta que el labio del soporte de arranque desaparezca el botón azul.

b. Gire el soporte del maletero hacia arriba y tire con cuidado del soporte del maletero para sacarlo del zócalo.

   i. 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.

3. Bloquee el soporte de arranque en su sitio:

   a. Gire el soporte de arranque hacia abajo hacia la placa base.

   b. Con el botón azul, coloque un dedo en el extremo del soporte de arranque y presione el extremo del soporte de inicio para activar el botón azul de bloqueo.

   c. Mientras presiona el soporte del maletero, levante el botón de bloqueo azul para bloquear el soporte del maletero en su sitio.

4. Cierre el conducto de aire.

## Paso 3: Transfiera la imagen de inicio al soporte de arranque mediante una unidad flash USB

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 adecuada en la sección Descargas del sitio de soporte de NetApp
  - Si NVE está habilitado, descargue la imagen con el cifrado de volúmenes de NetApp, como se indica en el botón de descarga.

- Si el cifrado de volúmenes de NetApp no está habilitado, descargue la imagen sin el cifrado de volúmenes de NetApp, como se indica en el botón de descarga.

- Si el sistema es un par de alta disponibilidad, debe tener una conexión de red.
- Si el sistema es independiente, no necesita una conexión de red, pero debe realizar un reinicio adicional al restaurar el sistema de archivos var.

a. Descargue y copie la imagen del servicio adecuada del sitio de soporte de NetApp en la unidad flash USB.

   i. Descargue la imagen de servicio en su espacio de trabajo en su portátil.

   ii. Descomprima la imagen de servicio.

   > Si va a extraer el contenido mediante 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:

   - arranque
   - efi

   iii. Copie la carpeta 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.

   iv. Extraiga la unidad flash USB del ordenador portátil.

b. Si aún no lo ha hecho, cierre el conducto de aire.

c. 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.

d. Vuelva a instalar el dispositivo de administración de cables y vuelva a instalar el sistema, según sea necesario.

   Al realizar la copia, recuerde volver a instalar los convertidores de medios (SFP o QSFP) si se retiraron.

e. Enchufe el cable de alimentación en la fuente de alimentación y vuelva a instalar el retenedor del cable de alimentación.

f. 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.

g. Complete la reinstalación del módulo del controlador:

   i. Asegúrese de que los brazos del pestillo están bloqueados en la posición extendida.

   ii. Con los brazos del pestillo, empuje el módulo del controlador hacia el compartimiento del chasis hasta que se detenga.

   > No empuje hacia abajo el mecanismo de bloqueo en la parte superior de los brazos del pestillo. Si lo hace, levante el mecanismo de bloqueo y prohíba deslizar el módulo del controlador en el chasis.

iii. Presione y sostenga las lengüetas naranjas en la parte superior del mecanismo de bloqueo.

iv. Empuje suavemente el módulo de la controladora en el compartimento del chasis hasta que quede alineado con los bordes del chasis.

> Los brazos del mecanismo de bloqueo se deslizan en el chasis.

El módulo de la controladora comienza a arrancar tan pronto como se asienta completamente en el chasis.

i. Suelte los pestillos para bloquear el módulo del controlador en su lugar.

ii. Si aún no lo ha hecho, vuelva a instalar el dispositivo de administración de cables.

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

      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.

   b. 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.

   c. 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.

   d. Después de instalar la imagen, inicie el proceso de restauración:

iii. Registre la dirección IP del nodo dañado que se muestra en la pantalla.

iv. Pulse `y` cuando se le solicite que restaure la configuración de copia de seguridad.

v. Pulse `y` cuando se le solicite sobrescribir /etc/ssh/ssh_host_dsa_key.

   a. En el nodo asociado en el nivel de privilegio avanzado, inicie la sincronización de configuración con la dirección IP registrada en el paso anterior: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`*

   b. Si la restauración se realiza correctamente, pulse `y` en el nodo dañado cuando se le solicite que utilice la copia restaurada?.

   c. Pulse `y` cuando vea que el procedimiento de confirmación de copia de seguridad se ha realizado correctamente y, a continuación, pulse `y` cuando se le solicite reiniciar el nodo.

   d. Compruebe que las variables de entorno están establecidas de la forma esperada.

vi. Lleve el nodo al aviso DEL CARGADOR.

   En el símbolo del sistema de ONTAP, puede emitir el comando system node halt -Skip-lif-migration -before-shutdown true -ignore-quorum-warnings true -inhibition-takeover true.

vii. Compruebe la configuración de la variable de entorno con el `printenv` comando.

viii. Si una variable de entorno no está establecida como se espera, modifíquela con el `setenv` *`environment-variable-name changed-value`* comando.

ix. Guarde los cambios mediante `savenv` comando.

x. Reiniciar el nodo.

a. Con el nodo reiniciado dañado, se muestra el `Waiting for giveback…` mensaje, realice una devolución del nodo en buen estado:

| Si el sistema está en… | Realice lo siguiente… |
|---|---|
| Un par de alta disponibilidad | Después de que el nodo dañado muestre el `Waiting for giveback…` mensaje, realice una devolución del nodo en buen estado:<br><br>i. Desde el nodo en buen estado: `storage failover giveback -ofnode partner_node_name`<br><br>El nodo dañado vuelve a tomar su almacenamiento, termina de arrancarse y, a continuación, se reinicia y el nodo vuelve a tomar el control en buen estado.<br><br>ⓘ Si el retorno se vetó, puede considerar la sustitución de los vetos.<br><br>"Gestión de parejas de HA"<br><br>ii. Supervise el progreso de la operación de devolución mediante el `storage failover show-giveback` comando.<br><br>iii. Una vez completada la operación de devolución, confirme que el par de alta disponibilidad esté en buen estado y que la toma de control sea posible gracias al uso de `storage failover show` comando.<br><br>iv. Restaure la devolución automática si la deshabilitó con el comando Storage Failover modify. |

b. Salga del nivel de privilegio avanzado en el nodo en buen estado.

# Arranque la imagen de recuperación - AFF A320

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

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 | a. Pulse `y` cuando se le solicite que restaure la configuración de copia de seguridad.<br>b. Configure el nodo en buen estado como nivel de privilegio avanzado: `set -privilege advanced`<br>c. Ejecute el comando restore backup: `system node restore-backup -node local -target-address impaired_node_IP_address`<br>d. Devuelva el nodo al nivel de administrador: `set -privilege admin`<br>e. Pulse `y` cuando se le solicite que utilice la configuración restaurada.<br>f. Pulse `y` cuando se le solicite reiniciar el nodo. |
| No hay conexión de red | a. Pulse `n` cuando se le solicite que restaure la configuración de copia de seguridad.<br>b. Reinicie el sistema cuando el sistema lo solicite.<br>c. Seleccione la opción **Actualizar flash desde la configuración de copia de seguridad** (flash de sincronización) en el menú que se muestra.<br><br>Si se le solicita que continúe con la actualización, pulse **`y`**. |

| Si el sistema tiene… | Realice lo siguiente… |
| --- | --- |
| No hay conexión de red y está en una configuración de IP de MetroCluster | a. Pulse `n` cuando se le solicite que restaure la configuración de copia de seguridad.<br>b. Reinicie el sistema cuando el sistema lo solicite.<br>c. Espere a que se conecten las conexiones de almacenamiento iSCSI.<br><br>Puede continuar después de ver los siguientes mensajes:<br><br>`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).`<br>`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).`<br>`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).`<br>`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).`<br><br>d. Seleccione la opción **Actualizar flash desde la configuración de copia de seguridad** (flash de sincronización) en el menú que se muestra.<br><br>Si se le solicita que continúe con la actualización, pulse **`y`**. |

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. Pasos de sustitución de medios posteriores al arranque para OKM, NSE y NVE
- Si su sistema no tiene configurado el gestor de claves incorporado, NSE o NVE, complete los pasos en esta sección.

6. Desde el aviso del CARGADOR, introduzca el `boot_ontap` comando.

| Si ve… | Realice lo siguiente… |
|---|---|
| La solicitud de inicio de sesión de | Vaya al siguiente paso. |
| Esperando devolución… | a. Inicie sesión en el nodo del partner.<br>b. Confirme que el nodo de destino está listo para la devolución con el `storage failover show` 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.

# Restauración de OKM, NSE y NVE según sea necesario: AFF A320

Una vez marcadas las variables de entorno, debe completar los pasos específicos de los sistemas que tienen activada la opción Onboard Key Manager (OKM), el cifrado en almacenamiento de NetApp (NSE) o el cifrado de volúmenes de NetApp (NVE).

1. Determine qué sección debe usar para restaurar sus configuraciones de OKM, NSE o NVE: Si NSE o NVE están habilitados junto con el gestor de claves incorporado debe restaurar la configuración capturada al principio de este procedimiento.
   - Si NSE o NVE están habilitados y el gestor de claves incorporado está habilitado, vaya a. Restaure NVE o NSE cuando el gestor de claves incorporado está habilitado.
   - Si NSE o NVE están habilitados para ONTAP 9.6, vaya a. Restaure NSE/NVE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores.

## Restaure NVE o NSE cuando el gestor de claves incorporado está habilitado

**Pasos**

1. Conecte el cable de consola a la controladora de destino.

2. Utilice la `boot_ontap` Comando en el símbolo del sistema del CARGADOR para arrancar la controladora.
3. Compruebe la salida de la consola:

| Si la consola muestra… | Entonces… |
|---|---|
| El aviso del CARGADOR | Arranque el controlador en el menú de arranque: `boot_ontap menu` |
| Esperando devolución | a. Introduzca `Ctrl-C` en el prompt de<br>b. En el mensaje: ¿Desea detener este nodo en lugar de esperar [y/n]? , introduzca: `y`<br>c. En el aviso del CARGADOR, introduzca el `boot_ontap menu` comando. |

4. En Boot Menu (Menú de inicio), introduzca el comando oculto, `recover_onboard_keymanager` y responda `y` en el prompt de
5. Introduzca la frase de acceso para el administrador de claves incorporado que haya obtenido del cliente al principio de este procedimiento.
6. Cuando se le solicite que introduzca los datos de copia de seguridad, pegue los datos de copia de seguridad que capturó al principio de este procedimiento, cuando se le solicite. Pegue la salida de `security key-manager backup show` O. `security key-manager onboard show-backup` comando

   > Los datos se emiten desde cualquiera de los dos `security key-manager backup show` o. `security key-manager onboard show-backup` comando.

   Ejemplo de datos de backup:

   ```
   ------------------------------ COMIENCE COPIA DE SEGURIDAD-------------------------------------------------------
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA3AAAAAAAAAAAAAAAAAAAAAYAYAY
   AYAYAYAYAYAYAYAYAYAYZYAYAYAYAYAYZYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYA
   YAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAY
   AYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAY . . .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

   ------------------------------ BACKUP FINAL----------------------------------------------------------
   ```

7. En Boot Menu (Menú de inicio), seleccione la opción para el inicio normal.

   El sistema arranca esperando la devolución… prompt.

8. Mueva el cable de la consola a la controladora asociada e inicie sesión como "admin".
9. Confirme que la controladora de destino está lista para la devolución con el `storage failover show` comando.

10. Restauración únicamente de los agregados del director financiero con la `storage failover giveback -fromnode local -only-cfo-aggregates true` comando.
    - Si el comando falla debido a un disco fallido, desactive físicamente el disco que ha fallado, pero deje el disco en la ranura hasta que se reciba un reemplazo.
    - Si el comando falla debido a una sesión CIFS abierta, compruebe con el cliente cómo cerrar sesiones CIFS.

      Los terminación CIFS pueden provocar la pérdida de datos.

    - Si el comando falla porque el partner "no está listo", espere 5 minutos para que los NVMems se sincronicen.
    - Si se produce un error en el comando debido a un proceso de NDMP, SnapMirror o SnapVault, deshabilite el proceso. Consulte el centro de documentación adecuado para obtener más información.
11. Una vez que se haya completado la devolución, compruebe el estado de la conmutación al nodo de respaldo y la devolución con el `storage failover show` y.. ``storage failover show`comandos -giveback'.

    Solo se mostrarán los agregados CFO (agregados raíz y datos en estilo CFO).

12. Mueva el cable de la consola a la controladora de destino.
    a. Si ejecuta ONTAP 9.6 o una versión posterior, ejecute la sincronización integrada del gestor de claves de seguridad:
    b. Ejecute el `security key-manager onboard sync` y, a continuación, introduzca la frase de acceso cuando se le solicite.
    c. Introduzca el `security key-manager key query` comando para ver una vista detallada de todas las claves almacenadas en el gestor de claves incorporado y verificar que el `Restored` columna = `yes/true` para todas las claves de autenticación.

       Si la `Restored` columna = cualquier otra cosa que no sea `yes/true`, Póngase en contacto con el servicio de atención al cliente

    d. Espere 10 minutos hasta que la clave se sincronice en el clúster.
13. Mueva el cable de la consola al controlador correspondiente.
14. Proporcione a la controladora objetivo mediante el `storage failover giveback -fromnode local` comando.
15. Compruebe el estado de devolución, 3 minutos después de que el informe haya finalizado, utilizando la `storage failover show` comando.

    Si la devolución no está completa tras 20 minutos, póngase en contacto con el soporte de cliente.

16. En el símbolo del sistema clustershell, introduzca el `net int show -is-home false` comando para mostrar las interfaces lógicas que no están en su controladora y puerto de inicio.

    Si alguna interfaz aparece como `false`, vuelva a revertir estas interfaces a su puerto de inicio mediante el `net int revert -vserver Cluster -lif` *`nodename`* comando.

17. Mueva el cable de la consola a la controladora de destino y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.

18. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

## Restaure NSE/NVE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores

**Pasos**

1. Conecte el cable de consola a la controladora de destino.
2. Utilice la `boot_ontap` Comando en el símbolo del sistema del CARGADOR para arrancar la controladora.
3. Compruebe la salida de la consola:

| Si la consola muestra… | Entonces… |
|---|---|
| La solicitud de inicio de sesión de | Vaya al paso 7. |
| Esperando devolución… | a. Inicie sesión en el controlador asociado.<br>b. Confirme que la controladora de destino está lista para la devolución con el `storage failover show` comando. |

4. Mueva el cable de la consola a la controladora correspondiente y regrese el almacenamiento de la controladora objetivo mediante el `storage failover giveback -fromnode local -only-cfo -aggregates true local` comando.
   - Si el comando falla debido a un disco fallido, desactive físicamente el disco que ha fallado, pero deje el disco en la ranura hasta que se reciba un reemplazo.
   - Si el comando falla debido a una sesión CIFS abierta, compruebe con el cliente cómo cerrar sesiones CIFS.

     Los terminación CIFS pueden provocar la pérdida de datos.

   - Si el comando falla porque el partner "no está listo", espere 5 minutos para que los NVMems se sincronicen.
   - Si se produce un error en el comando debido a un proceso de NDMP, SnapMirror o SnapVault, deshabilite el proceso. Consulte el centro de documentación adecuado para obtener más información.
5. Espere 3 minutos y compruebe el estado de la conmutación al nodo de respaldo con el `storage failover show` comando.
6. En el símbolo del sistema clustershell, introduzca el `net int show -is-home false` comando para mostrar las interfaces lógicas que no están en su controladora y puerto de inicio.

   Si alguna interfaz aparece como `false`, vuelva a revertir estas interfaces a su puerto de inicio mediante el `net int revert -vserver Cluster -lif` *`nodename`* comando.

7. Mueva el cable de la consola a la controladora de destino y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.
8. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.
9. Utilice la `storage encryption disk show` en el símbolo del sistema clustershell, para revisar el

resultado.

10. Utilice la `security key-manager key query` Comando para mostrar los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves.
    - Si la `Restored` columna = `yes/true`, ha finalizado y puede continuar con el proceso de sustitución.
    - Si la `Key Manager type` = `external` y la `Restored` columna = cualquier otra cosa que no sea `yes/true`, utilice la `security key-manager external restore` Comando para restaurar los ID de claves de las claves de autenticación.

      Si el comando falla, póngase en contacto con el servicio de atención al cliente.

    - Si la `Key Manager type` = `onboard` y la `Restored` columna = cualquier otra cosa que no sea `yes/true`, utilice la `security key-manager onboard sync` Comando para volver a sincronizar el tipo de gestor de claves.

      Utilice la `security key-manager key query` para comprobar que el `Restored` columna = `yes/true` para todas las claves de autenticación.

11. Conecte el cable de la consola al controlador asociado.
12. Respalde la controladora con el `storage failover giveback -fromnode local` comando.
13. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

# Vuelva a colocar la pieza en la que se ha producido el fallo en NetApp - AFF A320

Devuelva la pieza que ha fallado a NetApp, como se describe en las instrucciones de RMA que se suministran con el kit. Consulte "Retorno de artículo sustituciones" para obtener más información.