Soporte de arranque

Install and maintain

NetApp
February 13, 2026

Tabla de contenidos

Soporte de arranque

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

El sistema AFF A320 solo admite procedimientos de recuperación de medios de arranque manuales.

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 la compatibilidad y el estado de la clave de cifrado: AFF A320

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 AFF A320 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 `1Ono-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	`security key-manager keystore show` • 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	`security key-manager show-key-store` • Si EKM está activado, `external` aparece en la salida del comando. • Si OKM está activado, `onboard` aparece en la salida del comando. • Si no hay ningún gestor de claves activado, `No key managers configured` aparece en el resultado del comando.

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

   Si no hay ningún gestor de claves configurado:

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

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

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

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

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

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

Gestor de claves externo (EKM)

Complete estos pasos según el valor en el `Restored` columna.

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

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

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

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

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

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

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

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

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

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

Gestión de claves incorporada (OKM)

Complete estos pasos según el valor en el `Restored` columna.

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

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

   i. Cambiar al modo de privilegios avanzados:

      ```
      set -priv advanced
      ```

   Ingresar `y` cuando se le solicite continuar.

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

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

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

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

   iii. Volver al modo administrador:

      ```
      set -priv admin
      ```

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

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

a. Sincronizar el gestor de claves integrado:

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

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

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

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

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

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

c. Realizar una copia de seguridad de la información de OKM:

i. Cambiar al modo de privilegios avanzados:

```
set -priv advanced
```

Ingresar `y` cuando se le solicite continuar.

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

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

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

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

iii. Volver al modo administrador:

```
set -priv admin
```

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

Apague el nodo - AFF A320

Después de completar las tareas NVE o NSE, debe completar el apagado del nodo dañado. Apague o tome el control del controlador dañado utilizando el procedimiento apropiado para su configuración. El sistema AFF A320 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: `storage failover takeover -ofnode impaired_node_name` 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.
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`* Cuando el controlador dañado muestre esperando devolución…, pulse Ctrl-C y, a continuación, responda `y`.

Reemplace el soporte de arranque - AFF A320

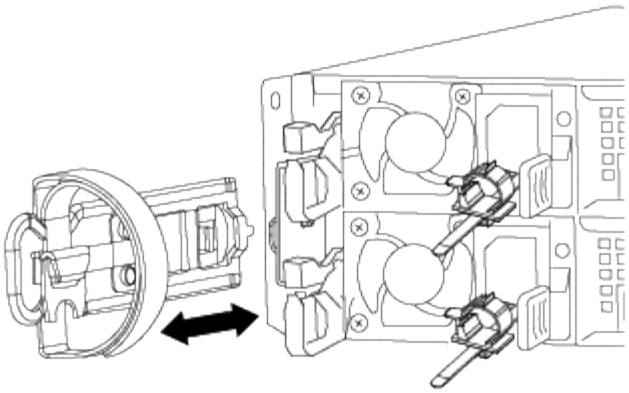
Para reemplazar el medio de arranque, debe quitar el módulo del controlador dañado, instalar el medio de arranque de reemplazo y transferir la imagen de arranque a una unidad flash USB. El sistema AFF A320 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

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.

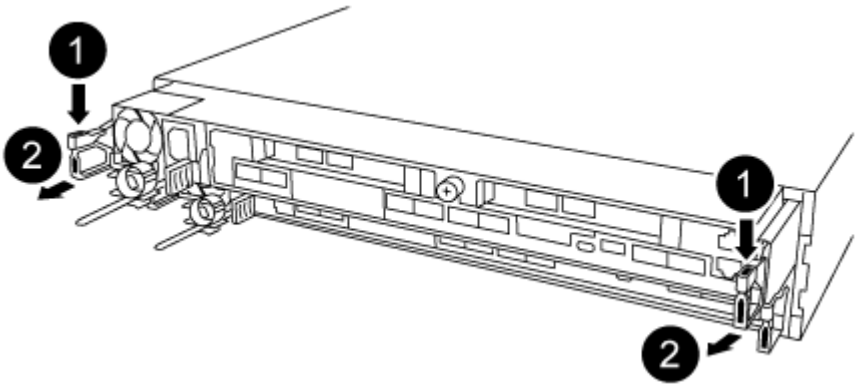
Pasos

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.

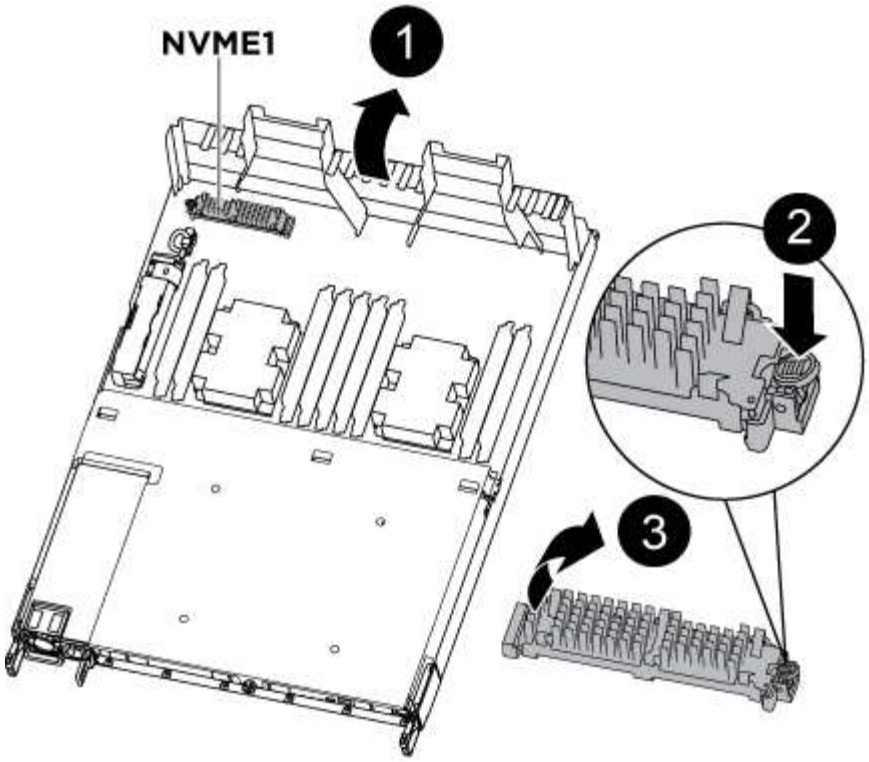
   c. Tire suavemente del módulo del controlador unas pulgadas hacia usted para que pueda agarrar los lados del módulo del controlador.
   d. Con ambas manos, tire suavemente del módulo del controlador para sacarlo del chasis y configúrelo en una superficie plana y estable.

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.

Pasos

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 arranque usando 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.

Pasos

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

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

   b. 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

   c. Copie la carpeta efi en el directorio superior de la unidad flash USB.

      Si la imagen de servicio no tiene carpeta efi, consulte "Falta la carpeta EFI del archivo de descarga de la imagen de servicio utilizada para la recuperación del dispositivo de arranque para los modelos FAS y AFF^".

   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.

   a. Extraiga la unidad flash USB del ordenador portátil.

2. Si aún no lo ha hecho, cierre el conducto de aire.
3. 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.
4. 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.

5. Enchufe el cable de alimentación en la fuente de alimentación y vuelva a instalar el retenedor del cable de alimentación.
6. 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.

7. Complete la reinstalación del módulo del controlador:

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

   b. 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.

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

d. 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.

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

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

8. 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.

9. 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.

10. 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.
11. Después de instalar la imagen, inicie el proceso de restauración:
    a. Registre la dirección IP del nodo dañado que se muestra en la pantalla.
    b. Pulse `y` cuando se le solicite que restaure la configuración de copia de seguridad.
    c. Pulse `y` cuando se le solicite sobrescribir /etc/ssh/ssh_host_dsa_key.
12. 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`*
13. Si la restauración se realiza correctamente, pulse `y` en el nodo dañado cuando se le solicite que utilice la copia restaurada?.
14. 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.
15. Compruebe que las variables de entorno están establecidas de la forma esperada.
    a. 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.

    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.

16. 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: a. Desde el nodo en buen estado: `storage failover giveback -ofnode partner_node_name` 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. Si el retorno se vetó, puede considerar la sustitución de los vetos. "Gestión de parejas de HA" b. Supervise el progreso de la operación de devolución mediante el `storage failover show-giveback` comando. c. 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. d. Restaure la devolución automática si la deshabilitó con el comando Storage Failover modify.

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

Arranque la imagen de recuperación - AFF A320

Debe iniciar la imagen ONTAP desde la unidad USB, restaurar el sistema de archivos y verificar las variables ambientales. El sistema AFF A320 solo admite procedimientos de recuperación de medios de arranque manuales. No se admite la recuperación automática de medios de arranque.

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. b. Configure el nodo en buen estado como nivel de privilegio avanzado: `set -privilege advanced` c. Ejecute el comando restore backup: `system node restore-backup -node local -target-address impaired_node_IP_address` d. Devuelva el nodo al nivel de administrador: `set -privilege admin` 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	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. 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.
	b. Reinicie el sistema cuando el sistema lo solicite.
	c. Espere a que se conecten las conexiones de almacenamiento iSCSI.
	
	Puede continuar después de ver los siguientes mensajes:
	
	`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).`
	
	d. Seleccione la opción **Actualizar flash desde la configuración de copia de seguridad** (flash de sincronización) en el menú que se muestra.
	
	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. 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.

Restaurar cifrado - AFF A320

Restaurar el cifrado en el medio de arranque de reemplazo. El sistema AFF A320 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
	
	`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`

Versión de ONTAP	Seleccione esta opción

ONTAP 9,7 y anteriores	Seleccione la opción oculta `recover_onboard_keymanager`
	
	Mostrar ejemplo de menú de inicio
	
	`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`

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:

--------------------------BEGIN
BACKUP--------------------------
012345678901234567890123456789012345678901234567890123456789012345678901
23
123456789012345678901234567890123456789012345678901234567890123456789012
34
234567890123456789012345678901234567890123456789012345678901234567890123
45
345678901234567890123456789012345678901234567890123456789012345678901234
56
456789012345678901234567890123456789012345678901234567890123456789012345
67
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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
   ```

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

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 AFF A320 solo admite procedimientos de recuperación de medios de arranque manuales.

Información de copyright

Información de la marca comercial