



Soporte de arranque

Install and maintain

NetApp
April 19, 2024

This PDF was generated from <https://docs.netapp.com/es-es/ontap-systems/a700s/bootmedia-replace-overview.html> on April 19, 2024. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Soporte de arranque 1
 - Descripción general de la sustitución de medios de arranque: AFF A700s 1
 - Compruebe las claves de cifrado integradas: AFF A700s 1
 - Apague la controladora AFF A700s 8
 - Sustituya el medio de arranque - AFF A700s 9
 - Transfiera la imagen de arranque al medio de arranque - AFF A700s 13
 - Arranque la imagen de recuperación: AFF A700s 19
 - Restaura OKM, NSE y NVE según sea necesario: AFF A700s 21
 - Devuelva la pieza con el fallo a NetApp - AFF A700s 27

Soporte de arranque

Descripción general de la sustitución de medios de arranque: AFF A700s

El medio de arranque principal almacena la imagen de arranque ONTAP que utiliza el sistema cuando arranca. Puede restaurar la imagen del soporte de arranque principal utilizando la imagen ONTAP en el soporte de arranque secundario o, si es necesario, utilizando una unidad flash USB.

Si el soporte de arranque secundario ha fallado o le falta el archivo `image.tgz`, debe restaurar el soporte de arranque primario mediante una unidad flash USB. La unidad debe formatearse con FAT32 y debe disponer de la cantidad de almacenamiento adecuada para alojar el archivo `image_xxx.tgz`.

- El proceso de sustitución restaura el sistema de archivos var desde el soporte de arranque secundario o la unidad flash USB al medio de arranque principal.
- Debe sustituir el componente con errores por un componente FRU de repuesto que haya recibido de su proveedor.
- Es importante que aplique los comandos en estos pasos en la controladora correcta:
 - El controlador *drinated* es el controlador en el que está realizando tareas de mantenimiento.
 - El controlador *heated* es el compañero de alta disponibilidad del controlador dañado.

Compruebe las claves de cifrado integradas: AFF A700s

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"](https://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 <Ino-DARE> o <1Ono-DARE> en el resultado del comando, el sistema no admite NVE, continúe para apagar la controladora.
 - Si <Ino-DARE> no se muestra en el resultado del comando y el sistema ejecuta ONTAP 9.5, vaya a. [Opción 1: Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.5 y versiones anteriores.](#)
 - Si <Ino-DARE> no se muestra en el resultado del comando y el sistema está ejecutando ONTAP 9.6 o una versión posterior, vaya a. [Opción 2: Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores.](#)
4. Si la controladora dañada forma parte de una configuración de alta disponibilidad, deshabilite la recuperación automática de la controladora en buen estado: `storage failover modify -node local -auto-giveback false` o `storage failover modify -node local -auto-giveback -after-panic false`

Opción 1: Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.5 y versiones anteriores

Antes de apagar la controladora dañada, debe comprobar 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.

Pasos

1. Conecte el cable de la consola al controlador dañado.
2. Compruebe si el cifrado de volúmenes está configurado 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.

3. Compruebe si NSE está configurado: `storage encryption disk show`
 - Si el resultado del comando incluye los detalles de la unidad con información sobre el modo y el identificador de claves, se configura NSE y se debe verificar la configuración de NSE.
 - Si NVE y NSE no están configurados, es seguro apagar el controlador afectado.

Verifique la configuración de NVE

Pasos

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves: `security key-manager query`
 - Si la `Restored` columna muestra `yes` y se muestran todos los gestores de claves `available`, es seguro apagar el controlador dañado.
 - Si la `Restored` columna muestra cualquier otra cosa que no sea `yes` o si aparece algún gestor de claves `unavailable`, necesita completar algunos pasos adicionales.
 - Si ve el mensaje este comando no es compatible con la gestión de claves incorporada, debe completar algunos pasos adicionales.
2. Si la `Restored` columna mostrada cualquier otra cosa que no sea `yes` o si aparece algún gestor de claves `unavailable`:

- a. Recupere y restaure todas las claves de autenticación y los ID de clave asociados: `security key-manager restore -address *`

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

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Compruebe que el Restored la columna muestra `yes` para todas las claves de autenticación y que se muestran todos los gestores de claves `available: security key-manager query`
 - b. Apague el controlador dañado.
3. Si vio el mensaje este comando no es compatible cuando la gestión de claves incorporada está habilitada, muestre las claves almacenadas en el gestor de claves incorporado: `security key-manager key show -detail`
- a. Si la Restored la columna muestra `yes` realice un backup manual de la información de gestión de claves incorporada:
 - Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
 - Introduzca el comando para mostrar la información de backup de OKM: `security key-manager backup show`
 - 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.
 - Volver al modo admin: `set -priv admin`
 - Apague el controlador dañado.
 - b. Si la Restored columna muestra cualquier otra cosa que no sea `yes`:
 - Ejecute el asistente de configuración Key-Manager: `security key-manager setup -node target/impaired node name`



Introduzca la clave de acceso de gestión de claves incorporada del cliente en el símbolo del sistema de. Si no se puede proporcionar la frase de contraseña, póngase en contacto con ["mysupport.netapp.com"](https://mysupport.netapp.com)

- Compruebe que el Restored la columna muestra `yes` para toda la clave de autenticación: `security key-manager key show -detail`
- Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
- Introduzca el comando para mostrar la información de backup de OKM: `security key-manager backup show`
- 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.
- Volver al modo admin: `set -priv admin`
- Puede apagar la controladora de forma segura.

Verifique la configuración de NSE

Pasos

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves: `security key-manager query`
 - Si la `Restored` la columna muestra `yes` y se muestran todos los gestores de claves `available`, es seguro apagar el controlador dañado.
 - Si la `Restored` columna muestra cualquier otra cosa que no sea `yes` o si aparece algún gestor de claves `unavailable`, necesita completar algunos pasos adicionales.
 - Si ve el mensaje este comando no es compatible con la gestión de claves incorporada, debe completar algunos pasos adicionales
2. Si la `Restored` columna mostrada cualquier otra cosa que no sea `yes` o si aparece algún gestor de claves `unavailable`:
 - a. Recupere y restaure todas las claves de autenticación y los ID de clave asociados: `security key-manager restore -address *`

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

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Compruebe que el `Restored` la columna muestra `yes` para todas las claves de autenticación y que se muestran todos los gestores de claves `available`: `security key-manager query`
 - b. Apague el controlador dañado.
3. Si vio el mensaje este comando no es compatible cuando la gestión de claves incorporada está habilitada, muestre las claves almacenadas en el gestor de claves incorporado: `security key-manager key show -detail`
 - a. Si la `Restored` la columna muestra `yes`, realice una copia de seguridad manual de la información de administración de claves integrada:
 - Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
 - Introduzca el comando para mostrar la información de backup de OKM: `security key-manager backup show`
 - 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.
 - Volver al modo admin: `set -priv admin`
 - Apague el controlador dañado.
 - b. Si la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
 - Ejecute el asistente de configuración Key-Manager: `security key-manager setup -node target/impaired node name`



Introduzca la frase de contraseña de OKM del cliente en la solicitud. Si no se puede proporcionar la frase de contraseña, póngase en contacto con ["mysupport.netapp.com"](https://mysupport.netapp.com)

- Compruebe que el Restored la columna muestra *yes* para todas las claves de autenticación:
`security key-manager key show -detail`
- Vaya al modo de privilegios avanzado e introduzca *y* cuando se le solicite continuar: `set -priv advanced`
- Introduzca el comando para realizar un backup de la información de OKM: `security key-manager backup show`



Asegúrese de que la información de OKM se guarda en su archivo de registro. Esta información será necesaria en situaciones de desastre en las que OKM podría necesitar recuperación manual.

- Copie el contenido de la información de la copia de seguridad en un archivo o registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.
- Volver al modo admin: `set -priv admin`
- Puede apagar el controlador de forma segura.

Opción 2: Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores

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"](https://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"](https://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"](https://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"](https://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 la controladora AFF A700s

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.
<code>Waiting for giveback...</code>	Pulse Ctrl-C y, a continuación, responda <code>y</code> cuando se le solicite.

Si el controlador dañado muestra...	Realice lo siguiente...
Solicitud del sistema o solicitud de contraseña (introduzca la contraseña del sistema)	<p>Retome o detenga el controlador dañado del controlador en buen estado: <code>storage failover takeover -ofnode impaired_node_name</code></p> <p>Cuando el controlador dañado muestre esperando devolución..., pulse Ctrl-C y, a continuación, responda <code>y</code>.</p>

- 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.

Sustituya el medio de arranque - AFF A700s

Debe quitar el módulo de la controladora del chasis, abrirlo y luego sustituir el soporte de arranque con errores.

Paso 1: Extraiga el módulo del controlador

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

- Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
- 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.

- Desenchufe la fuente de alimentación del módulo del controlador y, a continuación, desconecte el cable de la fuente de alimentación.
- Retire el dispositivo de administración de cables del módulo del controlador y colóquelo aparte.
- Presione los dos pestillos de bloqueo hacia abajo y, a continuación, gire ambos pestillos hacia abajo al mismo tiempo.

El módulo de la controladora se mueve ligeramente fuera del chasis.



1

Pestillo de bloqueo

2

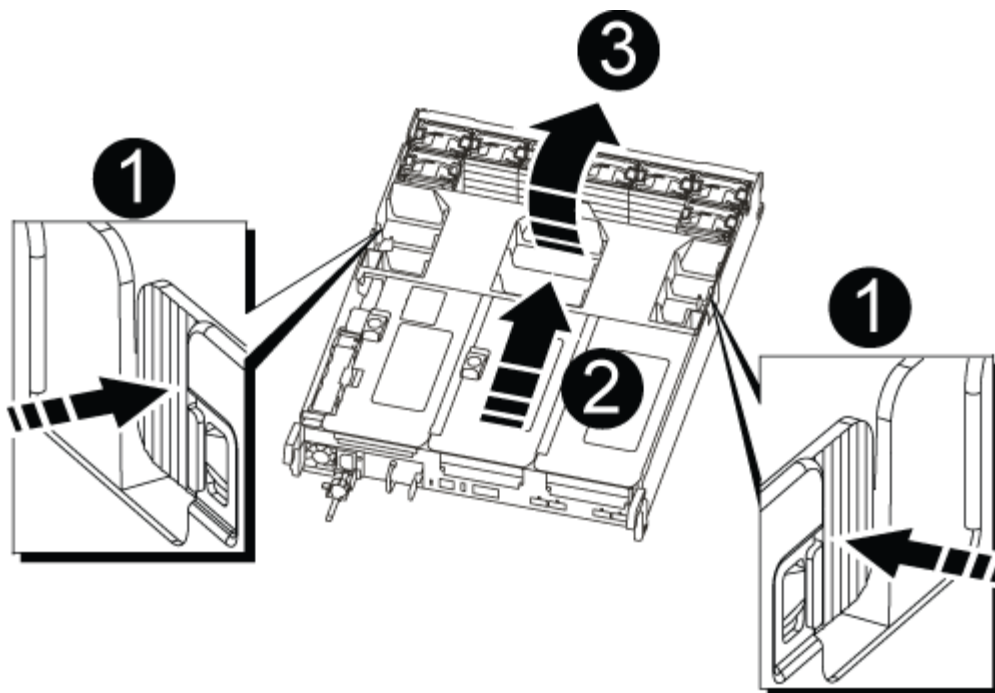
Pasador de bloqueo

1. Deslice el módulo de la controladora para sacarlo del chasis.

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

2. Coloque el módulo del controlador sobre una superficie plana y estable y, a continuación, abra el conducto de aire:

- a. Presione las lengüetas de bloqueo de los lados del conducto de aire hacia el centro del módulo del controlador.
- b. Deslice el conducto de aire hacia los módulos del ventilador y gírelo hacia arriba hasta su posición completamente abierta.



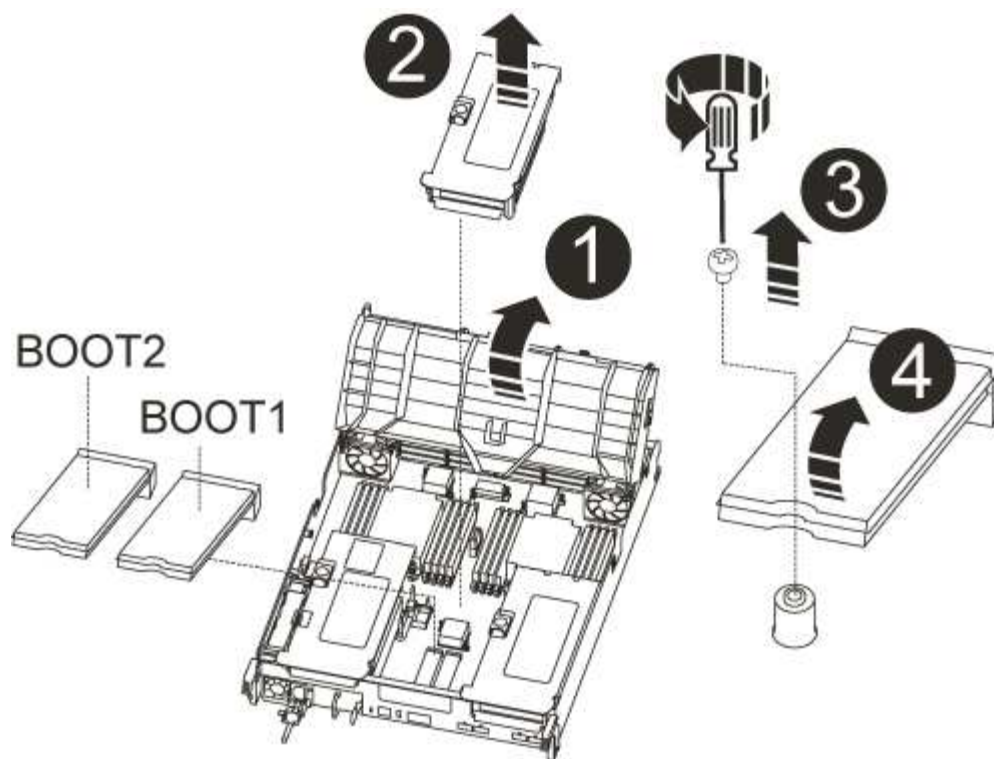
1	
Lengüetas de bloqueo del conducto de aire	
2	
Elevadores	
3	
Conducto de aire	

Paso 2: Sustituya el soporte de arranque - AFF A700s

Debe localizar el medio de arranque con fallos en el módulo de la controladora. Para ello, debe retirar el módulo PCIe central del módulo de la controladora, localizar el medio de arranque con fallos y, a continuación, sustituir el soporte de arranque.

Necesita un destornillador Phillips para quitar el tornillo que sujeta el soporte del maletero en su lugar.

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Busque el soporte de arranque:
 - a. Abra el conducto de aire, si es necesario.
 - b. Si es necesario, extraiga la tarjeta vertical 2, el módulo PCIe central, desbloqueando el pestillo de bloqueo y extrayendo la tarjeta vertical del módulo de la controladora.



1	
	Conducto de aire
2	
	Tarjeta «riser» 2 (módulo PCIe medio)
3	
	Tornillo del soporte del maletero
4	
	Soporte de arranque

3. Localice el medio de arranque con errores.
4. Extraiga el soporte de arranque del módulo del controlador:
 - a. Con un destornillador Phillips del número 1, retire el tornillo que sujeta el soporte del maletero y coloque el tornillo a un lado en un lugar seguro.
 - b. Sujetando los lados del soporte de arranque, gire suavemente el soporte de arranque hacia arriba, y luego tire del soporte de arranque directamente del zócalo y colóquelo a un lado.
5. Alinee los bordes del soporte de arranque de repuesto con el zócalo del soporte de arranque y, a

continuación, empújelo suavemente en el zócalo.

6. 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.

7. Gire el soporte de arranque hacia abajo hasta que esté alineado con la placa base.
8. Fije el soporte de la funda en su sitio con el tornillo.



No apriete demasiado el tornillo. Si lo hace, puede agrietar la placa de circuitos del soporte del maletero.

9. Vuelva a instalar la tarjeta vertical en el módulo de la controladora.
10. Cierre el conducto de aire:
 - a. Gire el conducto de aire hacia abajo.
 - b. Deslice el conducto de aire hacia los elevadores hasta que encaje en su sitio.

Transfiera la imagen de arranque al medio de arranque - AFF A700s

Puede instalar la imagen del sistema en el soporte de arranque de repuesto mediante la imagen del segundo soporte de arranque instalado en el módulo del controlador, el método principal para restaurar la imagen del sistema, O al transferir la imagen de inicio al soporte de arranque mediante una unidad flash USB cuando se produjo un error en la restauración del soporte de arranque secundario o si el archivo `image.tgz` no se encuentra en el soporte de arranque secundario.

Opción 1: Transfiera archivos al soporte de arranque mediante la recuperación de copia de seguridad desde el segundo soporte de arranque

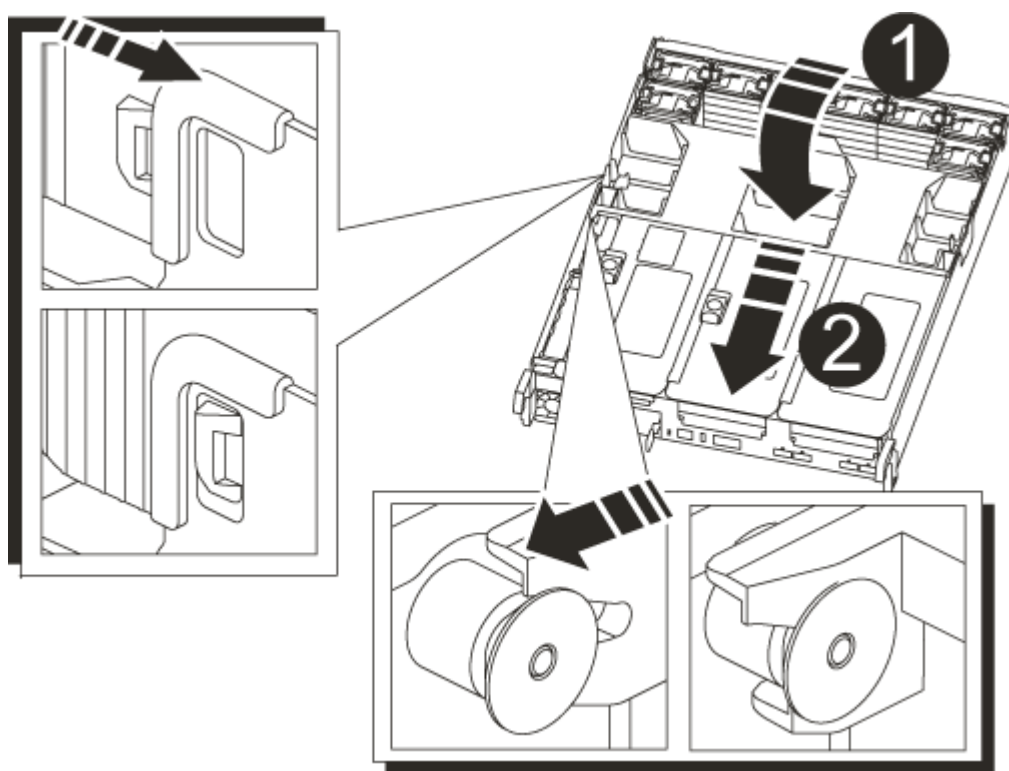
Puede instalar la imagen del sistema en el soporte de arranque de reemplazo mediante la imagen del segundo soporte de arranque instalado en el módulo de la controladora. Este es el método principal para transferir los archivos de medios de arranque al medio de arranque de reemplazo en sistemas con dos medios de arranque en el módulo del controlador.

La imagen del soporte de arranque secundario debe contener un `image.tgz` error de archivo y no debe ser informado. Si falta el archivo `image.tgz` o el soporte de arranque informa de fallos, no puede usar este procedimiento. Debe transferir la imagen de inicio al soporte de arranque de repuesto mediante el procedimiento de sustitución de la unidad flash USB.

Pasos

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Si aún no lo ha hecho, cierre el conducto de aire:
 - a. Gire el conducto de aire hacia abajo hasta el módulo del controlador.
 - b. Deslice el conducto de aire hacia los elevadores hasta que las lengüetas de bloqueo encajen en su lugar.
 - c. Inspeccione el conducto de aire para asegurarse de que está correctamente asentado y bloqueado en

su lugar.



1

Conducto de aire

2

Elevadores

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) si se retiraron.

5. Vuelva a conectar la fuente de alimentación y, a continuación, conéctela a la fuente de alimentación.

Asegúrese de volver a colocar el collarín de bloqueo del cable de alimentación en el cable de alimentación.

6. Empuje suavemente el módulo del controlador hasta que los ganchos de bloqueo del módulo del controlador empiecen a elevarse, empuje firmemente los ganchos de bloqueo para terminar de fijar el módulo del controlador y, a continuación, gire los ganchos de bloqueo a la posición de bloqueo sobre los pasadores del módulo del controlador.

La controladora comienza a arrancar en cuanto se ha instalado por completo en el chasis.

7. 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.

8. Desde el aviso del CARGADOR, arranque la imagen de recuperación desde el medio de arranque secundario: `boot_recovery`

La imagen se descarga desde el soporte de arranque secundario.

9. 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.
10. Después de instalar la imagen, inicie el proceso de restauración:
 - a. Registre la dirección IP del controlador 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 que confirme que el procedimiento de copia de seguridad se ha realizado correctamente.
11. En la controladora asociada 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`
12. Cuando la sincronización de la configuración se haya completado sin errores, pulse `y` cuando se le solicite que confirme que el procedimiento de copia de seguridad se ha realizado correctamente.
13. Pulse `y` cuando se le pregunte si desea utilizar la copia restaurada y, a continuación, pulse `y` cuando se le solicite reiniciar la controladora.
14. Salga del nivel de privilegio avanzado en la controladora en buen estado.

Opción 2: Transfiera la imagen de inicio al soporte de arranque mediante una unidad flash USB

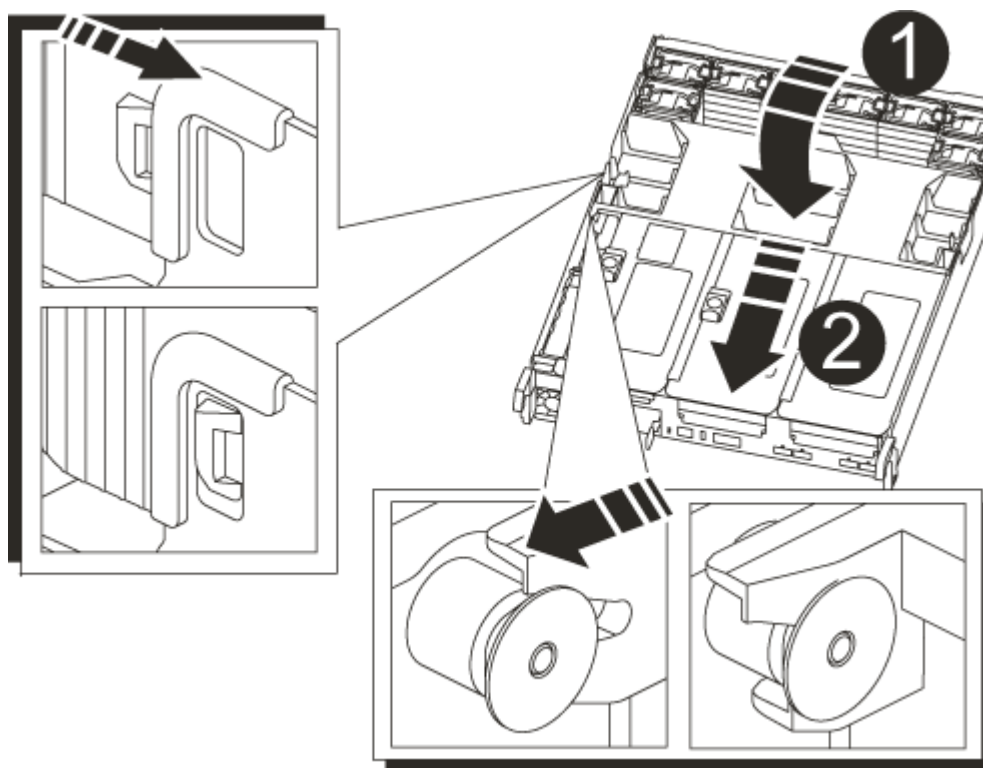
Este procedimiento solo debe usarse si falló la restauración de medios de arranque secundarios o si el archivo `image.tgz` no se encuentra en el medio de arranque secundario.

- Debe tener una unidad flash USB, formateada con FAT32, con una capacidad mínima de 4 GB.
- Una copia de la misma versión de imagen de ONTAP que la controladora dañada en funcionamiento. Puede descargar la imagen adecuada en la sección Descargas del sitio de soporte de NetApp
 - Si NVE está habilitado, descargue la imagen con el cifrado de volúmenes de NetApp, como se indica en el botón de descarga.
 - Si el cifrado de volúmenes de NetApp no está habilitado, descargue la imagen sin el cifrado de volúmenes de NetApp, como se indica en el botón de descarga.
- Si el sistema es 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. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Si aún no lo ha hecho, cierre el conducto de aire:

- a. Gire el conducto de aire hacia abajo hasta el módulo del controlador.
- b. Deslice el conducto de aire hacia los elevadores hasta que las lengüetas de bloqueo encajen en su lugar.
- c. Inspeccione el conducto de aire para asegurarse de que está correctamente asentado y bloqueado en su lugar.



1	Conducto de aire
2	Elevadores

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) si se retiraron.

5. Vuelva a conectar la fuente de alimentación y, a continuación, conéctela a la fuente de alimentación.

Asegúrese de volver a colocar el collarín de bloqueo del cable de alimentación en el 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. Empuje suavemente el módulo del controlador hasta que los ganchos de bloqueo del módulo del controlador empiecen a elevarse, empuje firmemente los ganchos de bloqueo para terminar de fijar el módulo del controlador y, a continuación, gire los ganchos de bloqueo a la posición de bloqueo sobre los pasadores del módulo del controlador.

La controladora comienza a arrancar en cuanto se ha instalado por completo en el chasis.

8. 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.

9. Aunque se conservan las variables de entorno y los bootargs, debe comprobar que todas las variables de entorno de arranque y los bootargs necesarios están correctamente definidos para el tipo de sistema y la configuración mediante el `printenv bootarg name` comando y corrija los errores mediante el `setenv variable-name <value>` comando.

- a. Compruebe las variables de entorno de arranque:

- `bootarg.init.boot_clustered`
- `partner-sysid`
- `bootarg.init.flash_optimized` Para C190 de AFF/AFF A220 (all-flash FAS)
- `bootarg.init.san_optimized` Para cabinas AFF A220 y SAN all-flash
- `bootarg.init.switchless_cluster.enable`

- b. Si el Administrador de claves externo está activado, compruebe los valores de bootarg que aparecen en la `kenv` Salida de ASUP:

- `bootarg.storageencryption.support <value>`
- `bootarg.keymanager.support <value>`
- `kmip.init.interface <value>`
- `kmip.init.ipaddr <value>`
- `kmip.init.netmask <value>`
- `kmip.init.gateway <value>`

- c. Si Onboard Key Manager está habilitado, compruebe los valores de bootarg que se muestran en la `kenv` Salida de ASUP:

- `bootarg.storageencryption.support <value>`
- `bootarg.keymanager.support <value>`
- `bootarg.onboard_keymanager <value>`

- d. Guarde las variables de entorno modificadas con el `savenv` comando

- e. Confirme los cambios mediante el `printenv variable-name` comando.


10. 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.

11. 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.
12. Después de instalar la imagen, inicie el proceso de restauración:
 - a. Registre la dirección IP del controlador 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 que confirme que el procedimiento de copia de seguridad se ha realizado correctamente.
13. Pulse `y` cuando se le pregunte si desea utilizar la copia restaurada y, a continuación, pulse `y` cuando se le solicite reiniciar la controladora.
14. En la controladora asociada 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`
15. Cuando la sincronización de la configuración se haya completado sin errores, pulse `y` cuando se le solicite que confirme que el procedimiento de copia de seguridad se ha realizado correctamente.
16. Pulse `y` cuando se le pregunte si desea utilizar la copia restaurada y, a continuación, pulse `y` cuando se le solicite reiniciar la controladora.
17. Compruebe que las variables de entorno están establecidas de la forma esperada.
 - a. Lleve la controladora 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. Reinicie la controladora.
18. Con el controlador deteriorado reiniciado que muestra el `Waiting for giveback...` mensaje, realice una devolución del control en buen estado:

Si el sistema está en...	Realice lo siguiente...
Un par de alta disponibilidad	<p>Después de que el controlador dañado muestre el <code>Waiting for giveback...</code> mensaje, realice una devolución del control en buen estado:</p> <p>a. Desde el controlador en buen estado: <code>storage failover giveback -ofnode partner_node_name</code></p> <p>El controlador dañado recupera su almacenamiento, termina el arranque, y luego reinicia y es tomado de nuevo por el controlador sano.</p> <div style="display: flex; align-items: center; margin-top: 10px;">  <div> <p>Si el retorno se vetó, puede considerar la sustitución de los vetos.</p> </div> </div> <p style="color: #0070C0; margin-top: 10px;">"Gestión de parejas de HA"</p> <p>b. Supervise el progreso de la operación de devolución mediante el <code>storage failover show-giveback</code> comando.</p> <p>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 <code>storage failover show</code> comando.</p> <p>d. Restaure la devolución automática si la ha desactivado mediante el <code>storage failover modify</code> comando.</p>

19. Salga del nivel de privilegio avanzado en la controladora en buen estado.

Arranque la imagen de recuperación: AFF A700s

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

- 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.

- 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.
- Restaure el sistema de archivos var:

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

4. Asegurarse de que las variables medioambientales estén establecidas de la manera esperada:
 - a. Lleve la controladora al aviso del CARGADOR.
 - b. Compruebe la configuración de la variable de entorno con el `printenv` comando.
 - c. Si una variable de entorno no está establecida como se espera, modifíquela con el `setenv environment-variable-name changed-value` comando.
 - d. Guarde los cambios mediante `savenv` comando.
5. El siguiente depende de la configuración del sistema:
 - Si su sistema tiene configurado el gestor de claves incorporado, NSE o NVE, vaya a. [Restaura OKM, NSE y NVE según sea necesario](#)
 - Si su sistema no tiene configurado el gestor de claves incorporado, NSE o NVE, complete los pasos en esta sección.
6. Desde el aviso del CARGADOR, introduzca el `boot_ontap` comando.

Si ve...	Realice lo siguiente...
La solicitud de inicio de sesión de	Vaya al siguiente paso.

Si ve...	Realice lo siguiente...
Esperando devolución...	a. Inicie sesión en el controlador asociado. b. Confirme que la controladora de destino está lista para la devolución con el <code>storage failover show</code> comando.

7. Conecte el cable de la consola al controlador asociado.
8. Respalde la controladora con el `storage failover giveback -fromnode local` comando.
9. En el símbolo del sistema del clúster, compruebe las interfaces lógicas con el `net int -is-home false` comando.

Si alguna interfaz se muestra como "falsa", vuelva a revertir dichas interfaces a su puerto de inicio utilizando el `net int revert` comando.

10. Mueva el cable de la consola al controlador reparado y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.
11. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

Restaure OKM, NSE y NVE según sea necesario: AFF A700s

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).

Determine qué sección debería usar para restaurar sus configuraciones de OKM, NSE o NVE:

Si NSE o NVE están habilitados junto con Onboard Key Manager, debe restaurar la configuración que capturó al principio de este procedimiento.

- Si NSE o NVE están habilitados y el gestor de claves incorporado está habilitado, vaya a. [Opción 1: Restaure NVE o NSE cuando el gestor de claves incorporado está habilitado.](#)
- Si NSE o NVE están habilitados para NATP 9.5, vaya a. [Opción 2: Restaure NSE/NVE en sistemas que ejecutan ONTAP 9.5 y versiones anteriores.](#)
- Si NSE o NVE están habilitados para ONTAP 9.6, vaya a. [Opción 3: Restaure NSE/NVE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores.](#)

Opción 1: 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: <code>boot_ontap menu</code>
Esperando devolución...	a. Introduzca <code>Ctrl-C</code> en el prompt de b. En el mensaje: ¿Desea detener este controlador en lugar de esperar [y/n]? , introduzca: <code>y</code> c. En el aviso del CARGADOR, introduzca el <code>boot_ontap menu</code> comando.

- En Boot Menu (Menú de inicio), introduzca el comando oculto, `recover_onboard_keymanager` y responda `y` en el prompt de.
- Introduzca la frase de acceso para el administrador de claves incorporado que haya obtenido del cliente al principio de este procedimiento.
- 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 0.security key-manager onboard show-backup` comando.



Los datos se emiten desde cualquiera de los dos `security key-manager backup show 0.security key-manager onboard show-backup` comando.

Ejemplo de datos de backup:

```

----- COMIENZE COPIA DE SEGURIDAD-----
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA3AAAAAAAAAAAAAAAAAYAYAY
AYAYAYAYAYAYAYAYAYAYZYAYAYAYAYAYZYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAY
YAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAY
AYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAY
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
----- BACKUP FINAL-----

```

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

El sistema se inicia a. `Waiting for giveback...` prompt.
- Mueva el cable de la consola a la controladora asociada e inicie sesión como `admin`.
- Confirme que la controladora de destino está lista para la devolución con el `storage failover show` comando.
- Entorno único de agregados CFO con recuperación tras fallos del almacenamiento `-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 se cierran las sesiones CIFS.



Los terminación CIFS pueden provocar la pérdida de datos.

- Si el comando falla porque el partner está "no listo", espere 5 minutos para que los NVMMems 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.

13. Si utiliza ONTAP 9.5 y versiones anteriores, ejecute el asistente de configuración de Key-Manager:

- a. Inicie el asistente con `security key-manager setup -nodenodename` escriba la clave de acceso para la gestión de claves incorporada cuando se le solicite.
- b. Introduzca el `key-manager key show -detail` comando para ver una vista detallada de todas las claves almacenadas en el gestor de claves incorporado y verificar que el `Restored` columna = `yes` para todas las claves de autenticación.



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

- c. Espere 10 minutos hasta que la clave se sincronice en el clúster.

14. Si utiliza ONTAP 9.6 o posterior:

- a. Ejecute el `security key-manager onboard sync` y, a continuación, introduzca la frase de acceso cuando se le solicite.
- b. 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

- c. Espere 10 minutos hasta que la clave se sincronice en el clúster.

15. Mueva el cable de la consola al controlador correspondiente.

16. Proporcione a la controladora objetivo mediante el `storage failover giveback -fromnode local` comando.

17. 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.

18. 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.

19. Mueva el cable de la consola a la controladora de destino y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.
20. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

Opción 2: Restaure NSE/NVE en sistemas que ejecutan ONTAP 9.5 y versiones anteriores

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...	<ol style="list-style-type: none">a. Inicie sesión en el controlador asociado.b. Confirme que la controladora de destino está lista para la devolución con el <code>storage failover show</code> comando.

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 NVMMems 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 la versión `-v command` 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.



Este comando no funciona si está configurado el cifrado de volúmenes de NetApp

10. Use la consulta del administrador de claves de seguridad para mostrar los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves.
 - Si la `Restored column` = `yes` Y todos los gestores de claves informan en un estado disponible, vaya a *Complete el proceso de reemplazo*.
 - Si la `Restored column` = cualquier otra cosa que no sea `yes`, y/o uno o más gestores de claves no están disponibles, utilice `security key-manager restore -address` Comando para recuperar y restaurar todas las claves de autenticación (AKS) e ID de clave asociados con todos los nodos de todos los servidores de administración de claves disponibles.

Compruebe de nuevo el resultado de la consulta del gestor de claves de seguridad para garantizar que el `Restored column` = `yes` y todos los gestores de claves informan en un estado disponible

11. Si la gestión de claves incorporada está habilitada:
 - a. Utilice la `security key-manager key show -detail` para ver una vista detallada de todas las claves almacenadas en el gestor de claves incorporado.
 - b. Utilice la `security key-manager key show -detail` y compruebe que el `Restored column` = `yes` para todas las claves de autenticación.

Si la `Restored column` = cualquier otra cosa que no sea `yes`, utilice la `security key-manager setup -node Repaired(Target) node` Comando para restaurar la configuración de la gestión de claves incorporada. Vuelva a ejecutar el `security key-manager key show -detail` comando para verificar `Restored column` = `yes` para todas las claves de autenticación.

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

Opción 3: 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...	Realice lo siguiente...
La solicitud de inicio de sesión de	Vaya al paso 7.
Esperando devolución...	a. Inicie sesión en el controlador asociado. b. Confirme que la controladora de destino está lista para la devolución con el <code>storage failover show</code> comando.

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 se cierran las sesiones CIFS.



Los terminación CIFS pueden provocar la pérdida de datos.

- Si el comando falla porque el partner está "no listo", espere 5 minutos para que los NVMMems 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 column = 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 consulta de claves del administrador de claves de seguridad para verificar que el `Restored column = 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.
14. Restaure AutoSupport si se deshabilitó mediante el `system node autosupport invoke -node * -type all -message MAINT=END`

Devuelva la pieza con el fallo a NetApp - AFF A700s

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.

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.