



# Soporte de arranque

Install and maintain

NetApp  
July 01, 2024

# Tabla de contenidos

- Soporte de arranque ..... 1
  - Descripción general de la sustitución de soportes de arranque - AFF A1K ..... 1
  - Compruebe las claves de cifrado integradas: AFF A1K ..... 1
  - Apague el controlador defectuoso: AFF A1K ..... 3
  - Sustituya el soporte de arranque: AFF A1K ..... 5
  - Inicie la imagen de recuperación - AFF A1K ..... 8
  - Restauración de cifrado - AFF A1K ..... 10
  - Devuelva la pieza fallida a NetApp - AFF A1K ..... 18

# Soporte de arranque

## Descripción general de la sustitución de soportes de arranque - AFF A1K

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

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

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

- 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 A1K

Antes de apagar la controladora con deterioro y comprobar el estado de las claves de cifrado integradas, debe comprobar el estado de la controladora con deterioro, deshabilitar la devolución automática del control y comprobar la versión de ONTAP que se está ejecutando.

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"](#).

## Compruebe NVE o NSE en sistemas que ejecutan ONTAP 9.15 y posterior

Antes de apagar la controladora deteriorada, debe verificar si el sistema tiene el administrador de claves de seguridad habilitado o discos cifrados.

## Verifique la configuración del gestor de claves de seguridad


### Pasos

1. Deserme si Key Manager está activo con el comando `security key-manager keystore show`. Para obtener más información, consulte ["Almacén de claves de seguridad gestor de claves mostrar página DEL COMANDO MAN"](#)



Es posible que tenga tipos de gestor de claves adicionales. Los tipos son KMIP AKV, y GCP. El proceso de confirmación de estos tipos es el mismo que el de confirmación `external` o `onboard` el de los tipos de gestor de claves.

- Si no se muestra ninguna salida, vaya a "apague el controlador dañado" para apagar el nodo defectuoso.
  - Si el comando muestra resultados, el sistema tiene `security key-manager` activo y necesita mostrar el Key Manager tipo y el estado.
2. Visualice la información de los activos Key Manager mediante el comando `security key-manager key query`.
    - Si aparece el Key Manager tipo `external` y aparece la `Restored` columna `true`, es seguro apagar el controlador defectuoso.
    - Si aparece el Key Manager tipo `onboard` y aparece la `Restored` columna `true`, deberá realizar algunos pasos adicionales.
    - Si aparece el Key Manager tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `true`, deberá realizar algunos pasos adicionales.
    - Si aparece el Key Manager tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `true`, deberá realizar algunos pasos adicionales.
  3. Si aparece el Key Manager tipo `onboard` y aparece la `Restored` columna `true`, realice una copia de seguridad manual de la información de OKM:
    - a. 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. Puede apagar el controlador defectuoso de forma segura.
  4. Si aparece el Key Manager tipo `onboard` y la `Restored` columna muestra cualquier cosa que no sea `true`:
    - a. Introduzca el comando `sync` del gestor de claves de seguridad incorporado: `Security key-manager onboard sync`

 Introduzca la clave de acceso 32 caracteres alfanumérica integrada en el símbolo del sistema. Si no se puede proporcionar la contraseña, comuníquese con el soporte de NetApp. "[mysupport.netapp.com](https://mysupport.netapp.com)"
    - b. Compruebe que `Restored` se muestra la columna `true` para todas las claves de autenticación: `security key-manager key query`
    - c. Compruebe que se muestra el Key Manager tipo ``onboard`` y, a continuación, realice una copia de seguridad manual de la información de OKM.
    - d. Introduzca el comando para mostrar la información de backup de 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. Puede apagar el controlador de forma segura.
  5. Si aparece el Key Manager tipo `external` y la `Restored` columna muestra cualquier cosa que no sea `true`:

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

- b. Compruebe que la `Restored` columna se muestra `true` para todas las claves de autenticación:  
`Security key-manager key query`
- c. Puede apagar el controlador defectuoso de forma segura.

## Apague el controlador defectuoso: AFF A1K

Después de completar las tareas de NVE o NSE, deberá completar el apagado de la controladora dañada. Apague o retome el controlador dañado siguiendo el procedimiento adecuado para su configuración.

### Opción 1: La mayoría de los sistemas

Para apagar el controlador dañado, debe determinar el estado del controlador y, si es necesario, tomar el control para que el controlador sano siga sirviendo datos del almacenamiento del controlador dañado.

#### Acerca de esta tarea

- Si dispone de un sistema SAN, debe haber comprobado los mensajes de evento `cluster kernel-service show`) para el blade SCSI de la controladora dañada. `cluster kernel-service show``El comando (desde el modo avanzado `priv`) muestra el nombre del nodo, el estado del quórum de ese nodo, el estado de disponibilidad de ese nodo y el estado operativo de ese nodo.

Cada proceso SCSI-blade debe quórum con los otros nodos del clúster. Todos los problemas deben resolverse antes de continuar con el reemplazo.

- Si tiene un clúster con más de dos nodos, debe estar en quórum. Si el clúster no tiene quórum o si una controladora en buen estado muestra falso según su condición, debe corregir el problema antes de apagar la controladora dañada; consulte "[Sincronice un nodo con el clúster](#)".

#### Pasos

1. Si AutoSupport está habilitado, suprima la creación automática de casos invocando un mensaje de AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=<# of hours>h`

El siguiente mensaje de AutoSupport suprime la creación automática de casos durante dos horas:  
`cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h`

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



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

3. Lleve la controladora dañada al aviso DEL CARGADOR:

Si el controlador dañado está mostrando...	Realice lo siguiente...
El aviso del CARGADOR	Vaya al paso siguiente.
Esperando devolución...	Pulse Ctrl-C y, a continuación, responda <code>y</code> cuando se le solicite.
Solicitud del sistema o solicitud de contraseña	Retome o detenga el controlador dañado del controlador en buen estado: <code>storage failover takeover -ofnode impaired_node_name</code>  Cuando el controlador dañado muestre esperando devolución..., pulse Ctrl-C y, a continuación, responda <code>y</code> .

### Opción 2: La controladora se encuentra en un MetroCluster

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:

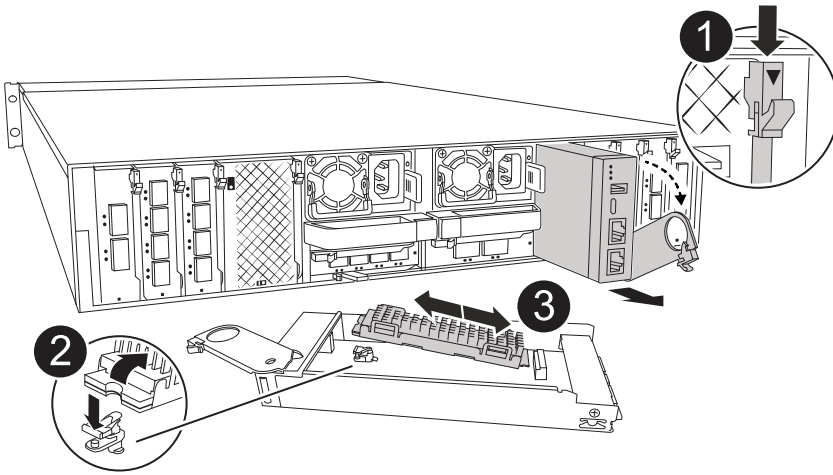
Si el controlador dañado está mostrando...	Realice lo siguiente...
El aviso del CARGADOR	Vaya al paso siguiente.
Esperando devolución...	Pulse Ctrl-C y, a continuación, responda y cuando se le solicite.
Solicitud del sistema o solicitud de contraseña (introduzca la contraseña del sistema)	Retome o detenga el controlador dañado del controlador en buen estado: <code>storage failover takeover -ofnode impaired_node_name</code>  Cuando el controlador dañado muestre esperando devolución..., pulse Ctrl-C y, a continuación, responda y.

## Sustituya el soporte de arranque: AFF A1K

Para sustituir el soporte de arranque, debe extraer el módulo de gestión del sistema de la parte posterior del sistema, extraer el soporte de arranque defectuoso, instalar el soporte de arranque de repuesto en el módulo de gestión del sistema y transferir la imagen ONTAP de una unidad flash USB al soporte de arranque de repuesto.

### Paso 1: Sustituya el soporte de arranque

El soporte de arranque se encuentra dentro del módulo de gestión del sistema y se accede a él quitando el módulo del sistema.



	Bloqueo de leva del módulo de gestión del sistema
	Botón de bloqueo del soporte de arranque
	Soporte de arranque

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Desconecte los cables de la fuente de alimentación de las PSU del controlador.



Si el sistema de almacenamiento tiene suministros de alimentación de CC, desconecte el bloque de cables de alimentación de las unidades de suministro de alimentación (PSU).

- a. Retire todos los cables conectados al módulo de gestión del sistema. Asegúrese de etiquetar dónde estaban conectados los cables, de modo que pueda conectarlos a los puertos correctos cuando vuelva a instalar el módulo.
- b. Gire la bandeja de gestión de cables hacia abajo tirando de los botones situados en ambos lados del interior de la bandeja de gestión de cables y, a continuación, gire la bandeja hacia abajo.



- c. Pulse el botón de leva de gestión del sistema. La palanca de leva se aleja de la carcasa.
  - d. Gire el pestillo de la leva hacia abajo hasta el tope.
  - e. Retire el módulo de gestión del sistema de la carcasa enganchando el dedo en la abertura de la palanca de leva y tirando del módulo para sacarlo de la carcasa.
  - f. Coloque el módulo de gestión del sistema en una alfombrilla antiestática, de forma que se pueda acceder al soporte de arranque.
3. Retire el soporte de arranque del módulo de gestión:
    - a. Pulse el botón de bloqueo azul.
    - b. Gire el soporte de arranque hacia arriba, deslícelo para extraerlo de la toma y déjelo a un lado.
  4. Instale el soporte de arranque de repuesto en el módulo de gestión del sistema:
    - a. Alinee los bordes del soporte del maletero con el alojamiento del zócalo y, a continuación, empújelo suavemente en el zócalo.
    - b. Gire el soporte de arranque hacia abajo hacia el botón de bloqueo.
    - c. Pulse el botón de bloqueo, gire el soporte del maletero completamente hacia abajo y, a continuación, suelte el botón de bloqueo.
  5. Vuelva a instalar el módulo Gestión del sistema.
    - a. Alinee el módulo con los bordes de la abertura de la ranura de la carcasa.
    - b. Deslice suavemente el módulo dentro de la ranura hasta el fondo de la carcasa y, a continuación, gire el pestillo de leva completamente hacia arriba para bloquear el módulo en su lugar.
  6. Gire la bandeja de gestión de cables hasta la posición cerrada.
    - a. Vuelva a conectar el módulo Gestión del sistema.

## Paso 2: Transfiera la imagen ONTAP al soporte de arranque

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

### Antes de empezar

- Debe tener una unidad flash USB vacía, formateada a FAT32, con al menos 4GB GB de capacidad.
- Debe tener una copia de la misma versión de imagen de ONTAP que se estaba ejecutando la controladora dañada. Puede descargar la imagen adecuada de "[Descargas](#)" la sección del sitio de soporte de NetApp
  - Si NVE es compatible, descargue la imagen con NetApp Volume Encryption, tal y como se indica en el botón de descarga.
  - Si NVE no es compatible, descargue la imagen sin cifrado de volúmenes NetApp, como se indica en el botón de descarga.
- Si el sistema es una pareja de alta disponibilidad, debe tener una conexión de red entre los puertos de gestión de nodos de las controladoras (normalmente las interfaces de e0M GbE).

### Pasos

1. Descargue y copie la imagen de servicio adecuada desde el "[Sitio de soporte de NetApp](#)" a la unidad flash USB.
  - a. Descargue la imagen del servicio desde el enlace Descargas de la página, en su espacio de trabajo en su portátil.
  - b. Descomprima la imagen de servicio.



Si está extrayendo el contenido con Windows, no utilice WinZip para extraer la imagen netboot. Utilice otra herramienta de extracción, como 7-Zip o WinRAR.

La unidad flash USB debe tener la imagen ONTAP adecuada de lo que está ejecutando el controlador dañado.

c. Extraiga la unidad flash USB del ordenador portátil.

2. Inserte la unidad flash USB en la ranura USB del módulo de administración del sistema.

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

3. Conecte los cables de alimentación a las fuentes de alimentación y vuelva a instalar el retén del cable de alimentación.

La controladora comienza a arrancar en cuanto se vuelve a conectar la alimentación al sistema.

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

Si omite este mensaje, pulse Ctrl-C, seleccione la opción de arrancar en modo de mantenimiento y detenga la controladora para arrancar en EL CARGADOR.

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

◦ Si va a configurar DHCP: `ifconfig e0M -auto`



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

◦ Si está configurando conexiones manuales: `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway`

- Filer\_addr es la dirección IP del sistema de almacenamiento.
- La máscara de red es la máscara de red de la red de gestión conectada al partner de alta disponibilidad.
- gateway es la puerta de enlace de la red.



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

## Inicie la imagen de recuperación - AFF A1K


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

### Pasos

1. Desde el aviso del CARGADOR, inicie 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	<p>a. En el controlador defectuoso, pulse <b>Y</b> cuando vea <code>Do you want to restore the backup configuration now?</code></p> <p>b. En el controlador afectado, pulse <b>Y</b> cuando se le solicite que sobrescriba <code>/etc/ssh/ssh_host_ecdsa_key</code>.</p> <p>c. En el controlador asociado en buen estado, establezca el controlador deficiente en el nivel de privilegio avanzado: <code>Set -privilege advanced</code>.</p> <p>d. En la controladora asociada en buen estado, ejecute el comando <code>restore backup: System node restore-backup -node local -target -address impaired_node_ip_address</code>.</p> <div style="border-left: 1px solid #ccc; padding-left: 10px; margin: 10px 0;">  Si ve algún mensaje que no sea una restauración correcta, póngase en contacto con <a href="#">"Soporte de NetApp"</a>.         </div> <p>e. En la controladora asociada en buen estado, devuelva la controladora afectada al nivel de administrador: <code>Set -privilege admin</code>.</p> <p>f. En el controlador afectado, pulse <b>y</b> cuando vea <code>Was the restore backup procedure successful?</code>.</p> <p>g. En el controlador afectado, pulse <b>y</b> cuando vea <code>...would you like to use this restored copy now?</code>.</p> <p>h. En el controlador afectado, pulse <b>y</b> cuando se le solicite reiniciar el controlador dañado y pulse <code>ctrl-c</code> para el menú de arranque.</p> <p>i. Si el sistema no utiliza encryption, seleccione <i>Opción 1 Arranque normal.</i>; de lo contrario, vaya a <a href="#">"Restaure gestores de claves"</a>.</p> <p>j. Conecte el cable de la consola al controlador asociado.</p> <p>k. Devuelva la controladora con el comando <code>storage failover giveback -fromnode local</code>.</p> <p style="padding-left: 20px;">i. Restaure la devolución automática del control si la deshabilitó con el comando <code>storage failover modify -node local -auto -giveback true</code>.</p> <p>l. Si AutoSupport está habilitado, restaure/anule la supresión de la creación automática de casos mediante el comando <code>system node AutoSupport invoke -node * -type all -message MAINT=END</code>.</p>
No hay conexión de red	Contacto <a href="#">"Soporte de NetApp"</a> .

Si el sistema tiene...	Realice lo siguiente...
No hay conexión de red y está en una configuración de IP de MetroCluster	Contacto " <a href="#">Soporte de NetApp</a> ".

## Restauración de cifrado - AFF A1K

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



Si se habilitan NSE o NVE junto con el gestor de claves incorporado o externo, debe restaurar la configuración capturada al principio de este procedimiento.

### Pasos

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

## Opción 1: Sistemas con configuración del servidor de gestión de claves incorporada

Restaurar la configuración del gestor de claves incorporado desde el menú de arranque de ONATP.

### Antes de empezar

Necesita la siguiente información al restaurar la configuración de OKM:

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

### Pasos

1. En el menú de arranque de ONTAP, seleccione la opción 10:

```
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_
```

2. Confirme la continuación del proceso. This option must be used only in disaster recovery procedures. Are you sure? (y or n): **y**
3. Introduzca dos veces la clave de acceso para todo el clúster.



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

```
Enter the passphrase for onboard key management:
```

```
Enter the passphrase again to confirm:
```

4. Introduzca la información de backup. Pegue todo el contenido desde la línea de COPIA DE SEGURIDAD DE INICIO hasta la línea de COPIA DE SEGURIDAD FINAL.

Pulse la tecla ENTER dos veces al final de la entrada.



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

```
Successfully recovered keymanager secrets.
```

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



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

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

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

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

7. Confirme que se muestre la consola de la controladora `Waiting for giveback...(Press Ctrl-C to abort wait)`

- Desde el nodo del partner, devolver la controladora asociada: *Storage failover giveback -fromnode local -only-cfo-aggregates true*
- Una vez iniciado solo con CFO aggregate, ejecute el comando *security key-manager onboard sync*:
- Introduzca la clave de acceso para todo el clúster de Onboard Key Manager:

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.

- Asegúrese de que todas las claves estén sincronizadas: *Security key-manager key query -restored false*

There are no entries matching your query.



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

- Devolución del nodo del partner: *Storage failover giveback -fromnode local*

## Opción 2: Sistemas con configuración de servidor de gestor de claves externo

Restablezca la configuración del gestor de claves externo desde el menú de arranque de ONATP.

### Antes de empezar

Necesitará la siguiente información para restaurar la configuración del gestor de claves externo (EKM):

- Necesita una copia del archivo */cfcard/kmip/servers.cfg* de otro nodo de cluster o la siguiente información:
- La dirección del servidor KMIP.
- El puerto KMIP.
- Una copia del archivo */cfcard/kmip/certs/client.crt* de otro nodo del clúster o del certificado de cliente.
- Una copia del archivo */cfcard/kmip/certs/client.key* de otro nodo del clúster o la clave de cliente.
- Una copia del archivo */cfcard/kmip/certs/CA.pem* de otro nodo del clúster o de las CA del servidor KMIP.

### Pasos

- Seleccione la opción 11 en el menú de inicio de ONATP.



```
(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
```

2. Cuando se le solicite, confirme que ha recopilado la información necesaria:

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

En su lugar, también puede realizar estas indicaciones:

- e. Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n} *n*
  - i. Do you know the KMIP server address? {y/n} *y*
  - ii. Do you know the KMIP Port? {y/n} *y*

3. Proporcione la información para cada una de estas peticiones de datos:

- a. Enter the client certificate (client.crt) file contents:
- b. Enter the client key (client.key) file contents:
- c. Enter the KMIP server CA(s) (CA.pem) file contents:
- d. Enter the server configuration (servers.cfg) file contents:

## Example

Enter the client certificate (client.crt) file contents:

```
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk51
MSUubQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxp bz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----
```

Enter the client key (client.key) file contents:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAOUleaajEG6QC2h2Zih0jEaGVtQUexNeoCFwKPoMSePmjDNtrU
MSB1SlX3VgCuElHk57XPdq6xSbYl b kIb4bAgLztHEmUDOkGmXYAkblQ=
-----END RSA PRIVATE KEY-----
```

Enter the KMIP server CA(s) (CA.pem) file contents:

```
-----BEGIN CERTIFICATE-----
MIIEIzCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMVCVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----END CERTIFICATE-----
```

Enter the IP address for the KMIP server: 10.10.10.10

Enter the port for the KMIP server [5696]:

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

#### 4. El proceso de recuperación se completará:

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

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

```
*****
*****
* 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
```

## Complete la sustitución del soporte de arranque

Complete el proceso de sustitución de medios de arranque después del arranque normal realizando las comprobaciones finales y devolviendo almacenamiento.

1. Compruebe la salida de la consola:

Si la consola muestra...	Realice lo siguiente...
La solicitud de inicio de sesión de	Vaya al paso 6.
Esperando devolución...	a. Inicie sesión en el controlador asociado. b. Confirme que la controladora de destino está lista para la devolución con el comando <i>storage failover show</i> .

2. Mueva el cable de consola a la controladora asociada y devuelva el almacenamiento de la controladora de destino mediante el comando *storage failover giveback -fromnode local -only-cfo-aggregates true*.

- 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 porque el partner no está listo, espere 5 minutos hasta que el subsistema HA se sincronice entre los partners.

- 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.
3. Espere 3 minutos y compruebe el estado de la conmutación por error con el comando `storage failover show`.
  4. En el símbolo del sistema de clustershell, introduzca el comando `network interface show -is-home false` para mostrar las interfaces lógicas que no están en su controlador principal y su puerto.

Si alguna interfaz se muestra `false` como , revierta esas interfaces de nuevo a su puerto raíz mediante el comando `net int revert -vserver Cluster -lif _nodename`.

5. Mueva el cable de la consola al controlador de destino y ejecute el comando `version -v` para comprobar las versiones de ONTAP.
6. Utilice el `storage encryption disk show` para revisar la salida.
7. Utilice el comando `security key-manager key query` para mostrar los identificadores de claves de las claves de autenticación almacenadas en los servidores de gestión de claves.
  - Si la `Restored column = yes/true`, ha finalizado y puede continuar con el proceso de sustitución.
  - Si `Key Manager type = external` y la `Restored column = cualquier otra cosa que no sea yes/true`, utilice el comando `security key-manager external restore` para restaurar los ID de clave de las claves de autenticación.



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

- Si `Key Manager type = onboard` y la `Restored column = cualquier otra cosa que no sea yes/true`, utilice el comando `security key-manager onboard sync` para sincronizar las claves integradas que faltan en el nodo reparado.

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

8. Conecte el cable de la consola al controlador asociado.
9. Respalde la controladora con el `storage failover giveback -fromnode local` comando.
10. Restaure la devolución automática del control si la deshabilitó con el comando `storage failover modify -node local -auto-giveback true`.
11. Si AutoSupport está habilitado, restaure/anule la supresión de la creación automática de casos mediante el comando `system node AutoSupport invoke -node * -type all -message MAINT=END`.

## Devuelva la pieza fallida a NetApp - AFF A1K

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.