



Soporte de arranque

Install and maintain

NetApp
August 18, 2025

This PDF was generated from <https://docs.netapp.com/es-es/ontap-systems/fas2800/bootmedia-replace-overview.html> on August 18, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Soporte de arranque 1
 - Descripción general de la sustitución de soportes de arranque - FAS2820 1
 - Compruebe la compatibilidad y el estado de la clave de cifrado - FAS2820 1
 - Paso 1: Compruebe si su versión de ONTAP es compatible con el cifrado de volúmenes de NetApp. . . . 1
 - Paso 2: Determine si es seguro apagar el controlador 2
 - Apague el controlador averiado - FAS2820 6
 - Sustituya el soporte de arranque - FAS2820 7
 - Paso 1: Extraiga el módulo del controlador 7
 - Paso 2: Sustituya el soporte de arranque 8
 - Paso 3: Transfiera la imagen de arranque al soporte de arranque 10
 - Inicie la imagen de recuperación - FAS2820 11
 - Restaurar cifrado - FAS2820 13
 - Opción 1: Restaure la configuración del gestor de claves incorporado. 13
 - Opción 2: Restaure la configuración del gestor de claves externo 19
 - Devuelva la pieza fallida a NetApp - FAS2820 23

Soporte de arranque

Descripción general de la sustitución de soportes de arranque - FAS2820

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

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

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

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

Compruebe la compatibilidad y el estado de la clave de cifrado - FAS2820

Para garantizar la seguridad de los datos en el sistema de almacenamiento, debe verificar el estado y la compatibilidad de la clave de cifrado en el soporte de arranque. Compruebe si la versión de ONTAP es compatible con el cifrado de volúmenes de NetApp (NVE) y antes de apagar la controladora compruebe si el gestor de claves está activo.

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

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

Pasos

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

```
version -v
```

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

2. Según si NVE es compatible con el sistema, realice una de las siguientes acciones:
 - Si NVE es compatible, descargue la imagen ONTAP con NetApp Volume Encryption.
 - Si NVE no es compatible, descargue la imagen ONTAP **sin** Cifrado de volumen NetApp.

Paso 2: Determine si es seguro apagar el controlador

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

Pasos

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

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

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

No se ha configurado ningún gestor de claves

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

Se ha configurado el gestor de claves externo o incorporado

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

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

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

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

3. En función de si el sistema utiliza el Administrador de claves externo o el Administrador de claves incorporado, seleccione una de las siguientes opciones.

Gestor de claves externo

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

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

Gestión de claves incorporada

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

Valor de salida en Restored la columna	Siga estos pasos...
true	<p>Realice una copia de seguridad manual de la información de OKM.</p> <ol style="list-style-type: none"> Vaya al modo avanzado introduciendo <code>set -priv advanced</code> y, a continuación, introdúzcalo y cuando se le solicite. Introduzca el siguiente comando para mostrar la información de gestión de claves: <pre>security key-manager onboard show-backup</pre> Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. <p>Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.</p> Puede apagar el controlador defectuoso de forma segura. Vaya a "apague el controlador dañado".

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

El futuro

Después de comprobar la compatibilidad y el estado de la clave de cifrado en el soporte de arranque, debe ["apague la controladora"](#).

Apague el controlador averiado - FAS2820

Apague o tome el control de la controladora dañada.

Después de completar las tareas de NVE o NSE, deberá completar el apagado de la controladora dañada.

Pasos

1. Lleve la controladora dañada al aviso DEL CARGADOR:

Si el controlador dañado muestra...	Realice lo siguiente...
El aviso del CARGADOR	Vaya a Quitar módulo de controlador.
Waiting for giveback...	Pulse Ctrl-C y, a continuación, responda y cuando se le solicite.
Solicitud del sistema o solicitud de contraseña (introduzca la contraseña del sistema)	<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 y.</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.

El futuro

Después de apagar el controlador, debe ["sustituya el soporte de arranque"](#).

Sustituya el soporte de arranque - FAS2820

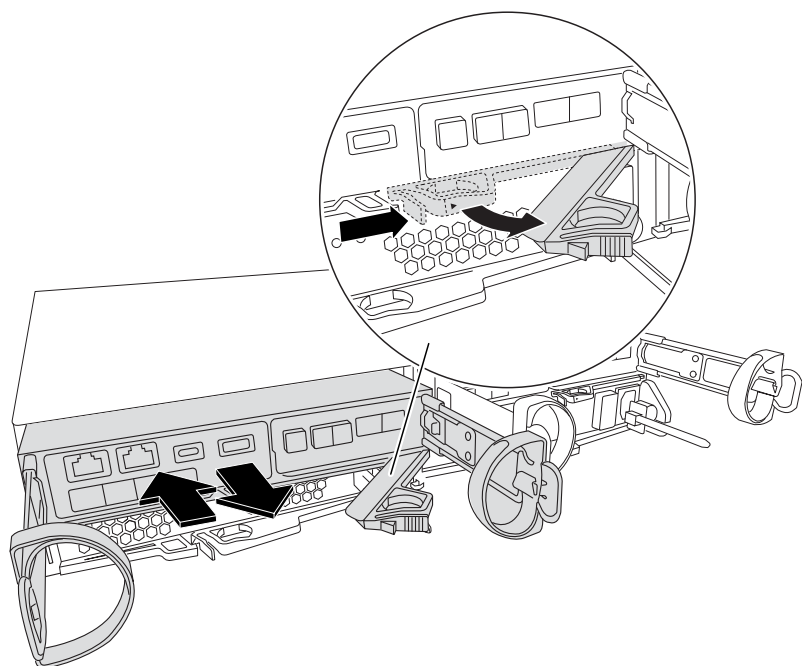
Debe quitar y abrir el módulo del controlador dañado, ubicar y reemplazar el medio de arranque en el controlador, transferir la imagen de arranque a una unidad USB, insertar la unidad USB en el controlador y luego arrancar el controlador.

Paso 1: Extraiga el módulo del controlador

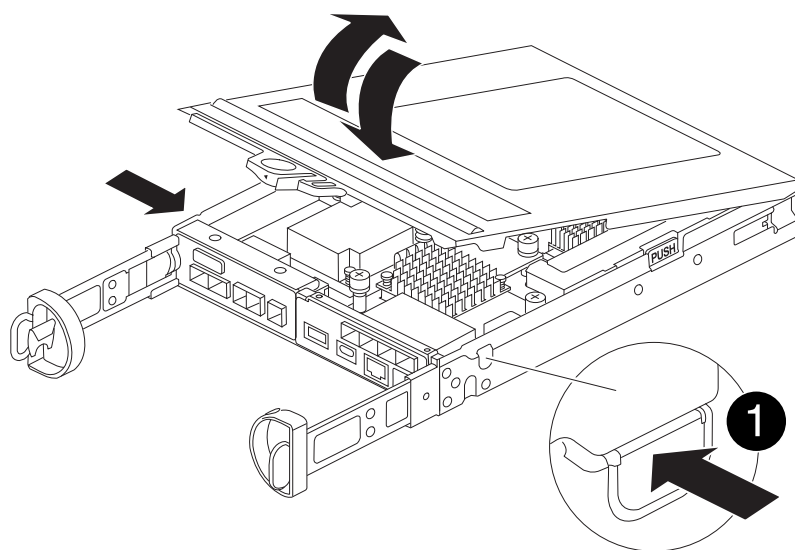
Pasos

Para acceder a los componentes del interior del controlador, primero debe extraer el módulo del controlador del sistema y, a continuación, retirar la cubierta del módulo del controlador.

- 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.
- Apriete el pestillo del mango de la leva hasta que se suelte, abra el mango de la leva completamente para liberar el módulo del controlador del plano medio y, a continuación, tire con dos manos del módulo del controlador para extraerlo del chasis.



4. Dé la vuelta al módulo del controlador y colóquelo sobre una superficie plana y estable.
5. Abra la cubierta pulsando los botones azules de los laterales del módulo del controlador para liberar la cubierta y, a continuación, gire la cubierta hacia arriba y hacia fuera del módulo del controlador.

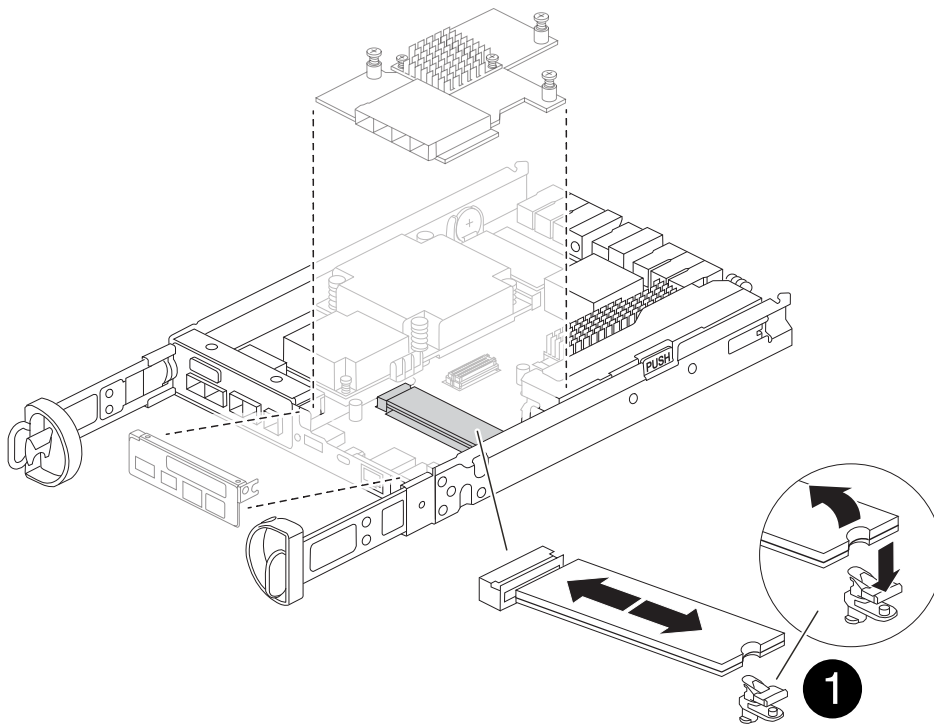


1

Botón de liberación de la cubierta del módulo del controlador

Paso 2: Sustituya el soporte de arranque

Localice el medio de arranque en el módulo del controlador, que se encuentra debajo de la tarjeta intermedia y siga las instrucciones para reemplazarlo.



1

Lengüeta de bloqueo del soporte de arranque

Pasos

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Retire la tarjeta intermedia utilizando la siguiente ilustración o el mapa de FRU del módulo del controlador:
 - a. Retire la placa de E/S deslizándola directamente hacia fuera del módulo del controlador.
 - b. Afloje los tornillos de la tarjeta mezzanine.



Puede aflojar los tornillos con los dedos o con un destornillador. Si utiliza los dedos, es posible que necesite girar la batería NV hacia arriba para una mejor compra de dedos en el tornillo de apriete manual junto a ella.

- c. Levante la tarjeta mezzanine en línea recta.
3. Sustituya el soporte de arranque:
 - a. Pulse el botón azul de la carcasa del soporte de arranque para liberar el soporte de arranque de su carcasa, gire el soporte de arranque hacia arriba y, a continuación, tire suavemente de él para extraerlo de la toma del soporte de arranque.



No gire ni tire del soporte de arranque en línea recta, ya que podría dañar la toma o el soporte de arranque.

- b. Alinee los bordes del soporte de arranque de repuesto con el zócalo del soporte de arranque y, a continuación, empújelo suavemente en el zócalo. Compruebe el soporte de arranque para asegurarse de que está bien asentado y completamente en la toma y, si es necesario, retire el soporte de arranque y vuelva a colocarlo en la toma.
 - c. Pulse el botón azul de bloqueo, gire el soporte de arranque completamente hacia abajo y, a continuación, suelte el botón de bloqueo para bloquear el soporte de arranque en su lugar.

4. Vuelva a instalar la tarjeta mezzanine:
 - a. Alinee la toma de la placa base con la toma de la tarjeta mezzanine y, a continuación, coloque suavemente la tarjeta en la toma.
 - b. Apriete los tres tornillos de apriete manual de la tarjeta mezzanine.
 - c. Vuelva a instalar la placa IO.
5. Vuelva a instalar la cubierta del módulo del controlador y bloquéela en su lugar.

Paso 3: Transfiera la imagen de arranque al soporte de arranque

Instale la imagen del sistema en el soporte de arranque de repuesto mediante una unidad flash USB con la imagen instalada en él. Debe restaurar el sistema de archivos var durante este procedimiento.

Antes de empezar

- Debe tener una unidad flash USB, formateada a MBR/FAT32, con una capacidad de al menos 4GB.
- Debe tener una conexión de red.

Pasos

1. Descargue la versión de imagen adecuada de ONTAP en la unidad flash USB formateada:
 - a. Uso ["Cómo determinar si la versión de ONTAP en ejecución es compatible con el cifrado de volúmenes de NetApp \(NVE\)"](#) para determinar si se admite actualmente el cifrado de volúmenes.
 - Si el clúster es compatible con NVE, descargue la imagen con NetApp Volume Encryption.
 - Si NVE no es compatible con el clúster, descargue la imagen sin el cifrado de volúmenes de NetApp. Consulte ["¿Qué imagen de ONTAP debo descargar? ¿Con o sin cifrado de volumen?"](#) para obtener más detalles.
2. Extraiga la unidad flash USB del ordenador portátil.
3. Instale el módulo del controlador:
 - a. 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.
 - b. Vuelva a conectar el módulo del controlador.

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

4. 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.

5. Empuje completamente el módulo del controlador en el sistema, asegurándose de que el mango de la leva borra la unidad flash USB, empuje firmemente el asa de la leva para terminar de colocar el módulo del controlador, empuje el asa de la leva hasta la posición cerrada y, a continuación, apriete el tornillo de mano.

El controlador comienza a arrancar tan pronto como está completamente instalado en el chasis y se detiene en el mensaje LOADER.

El futuro

Después de reemplazar el soporte de arranque, debe ["inicie la imagen de recuperación"](#).

Inicie la imagen de recuperación - FAS2820

Después de instalar el nuevo dispositivo multimedia de arranque en el sistema, puede iniciar la imagen de recuperación desde una unidad USB y restaurar la configuración desde el nodo asociado.

Pasos

1. Desde el símbolo DEL SISTEMA DEL CARGADOR, arranque la imagen de recuperación desde la unidad flash USB: `boot_recovery`

La imagen se descarga desde la unidad flash USB.

2. Cuando se le solicite, introduzca el nombre de la imagen o acepte la imagen predeterminada que se muestra dentro de los corchetes de la pantalla.
3. Restaure el sistema de archivos var:

Opción 1: ONTAP 9.16,0 o anterior

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

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

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

Opción 2: ONTAP 9.16,1 o posterior

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

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

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

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

7. Si AutoSupport está habilitado, restaurar/desactivar la creación automática de casos mediante el `system node autosupport invoke -node * -type all -message MAINT=END` comando.

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

El futuro

Después de arrancar la imagen de recuperación, es necesario ["restaure el cifrado en el soporte de arranque"](#).

Restaurar cifrado - FAS2820

Restaure el cifrado en el soporte de arranque de reemplazo.

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

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

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

Opción 1: Restaure la configuración del gestor de claves incorporado

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

Antes de empezar

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

Pasos

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

Versión de ONTAP	Seleccione esta opción
ONTAP 9.8 o posterior	<p data-bbox="621 153 927 191">Seleccione la opción 10.</p> <p data-bbox="621 222 1057 260">Mostrar ejemplo de menú de inicio</p> <div data-bbox="654 296 1456 1081"> <p data-bbox="683 333 1294 367">Please choose one of the following:</p> <ul data-bbox="683 411 1369 1010" style="list-style-type: none"> <li data-bbox="683 411 971 445">(1) Normal Boot. <li data-bbox="683 453 1133 487">(2) Boot without /etc/rc. <li data-bbox="683 495 1045 529">(3) Change password. <li data-bbox="683 537 1369 606">(4) Clean configuration and initialize all disks. <li data-bbox="683 615 1154 648">(5) Maintenance mode boot. <li data-bbox="683 657 1328 690">(6) Update flash from backup config. <li data-bbox="683 699 1240 732">(7) Install new software first. <li data-bbox="683 741 976 774">(8) Reboot node. <li data-bbox="683 783 1192 852">(9) Configure Advanced Drive Partitioning. <li data-bbox="683 861 1333 930">(10) Set Onboard Key Manager recovery secrets. <li data-bbox="683 938 1317 1008">(11) Configure node for external key management. <p data-bbox="683 1016 1032 1050">Selection (1-11)? 10</p> </div>

Versión de ONTAP	Seleccione esta opción
ONTAP 9,7 y anteriores	<p data-bbox="621 159 1489 199">Seleccione la opción oculta <code>recover_onboard_keymanager</code></p> <p data-bbox="621 226 1057 262">Mostrar ejemplo de menú de inicio</p> <div data-bbox="654 304 1456 966"> <pre data-bbox="683 338 1369 930">Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager</pre> </div>

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

Mostrar símbolo del sistema de ejemplo

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

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

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

Mostrar símbolo del sistema de ejemplo

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

5. Introduzca la información de backup.

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

Mostrar símbolo del sistema de ejemplo

Enter the backup data:

```
-----BEGIN BACKUP-----
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
-----END BACKUP-----
```

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

El proceso de recuperación finaliza.

Mostrar símbolo del sistema de ejemplo

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

Successfully recovered keymanager secrets.

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



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

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

Mostrar símbolo del sistema de ejemplo

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

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

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

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

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

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

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

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

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

Mostrar símbolo del sistema de ejemplo

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

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



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

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

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

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



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

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

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

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

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

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

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

Opción 2: Restaure la configuración del gestor de claves externo

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

Antes de empezar

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

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

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

Pasos

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

Mostrar ejemplo de menú de inicio

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

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

Mostrar símbolo del sistema de ejemplo

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

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

Mostrar petición de datos

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

Muestra el ejemplo

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

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

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

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

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

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

Muestra el ejemplo

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

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

Mostrar símbolo del sistema de ejemplo

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

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

6. Restaure la devolución automática si la ha desactivado.

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

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

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

El futuro

Después de restaurar el cifrado en el soporte de arranque, debe ["Devuelva la pieza fallida a NetApp"](#).

Devuelva la pieza fallida a NetApp - FAS2820

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

Información de copyright

Copyright © 2025 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 INTERRUPCIÓN 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.