Soporte de arranque: Recuperación manual

Install and maintain

NetApp
December 18, 2024

Tabla de contenidos

Soporte de arranque: Recuperación manual

Descripción general de la recuperación de medios de arranque manual - ASA A1K

Puede sustituir manualmente un soporte de arranque fallido mediante un módulo USB para la imagen de arranque.

La sustitución manual de soportes de arranque utiliza el método tradicional de descargar la imagen ONTAP del sitio de soporte de NetApp, transferir la imagen a una unidad USB, descargarla al soporte de arranque de reemplazo de destino y caminar manualmente por las opciones del menú de arranque para instalar la imagen ONTAP en el soporte de arranque de reemplazo.

Flujo de trabajo de sustitución de soportes de arranque: ASA A1K

Siga estos pasos del flujo de trabajo para sustituir el soporte de arranque.

1. **"Revise los requisitos de medios de arranque"**

Para sustituir el soporte de arranque, debe cumplir ciertos requisitos.

2. **"Compruebe las claves de cifrado incorporadas"**

Verifique si el sistema tiene discos cifrados o habilitados para el gestor de claves de seguridad.

3. **"Apague el controlador dañado"**

Apague o asuma el control de la controladora deteriorada para que la controladora en buen estado siga sirviendo datos del almacenamiento de la controladora dañado.

4. **"Sustituya el soporte de arranque"**

Retire el soporte de arranque fallido del módulo de administración del sistema e instale el soporte de arranque de reemplazo y, a continuación, transfiera una imagen ONTAP mediante una unidad flash USB al soporte de arranque de reemplazo.

5. **"Arranque la imagen de recuperación"**

Inicie la imagen ONTAP desde la unidad USB, restaure el sistema de archivos y verifique las variables de entorno.

6. **"Restaure el cifrado"**

Restaure la configuración del gestor de claves incorporado o el gestor de claves externo desde el menú de

arranque de ONATP.

7 **"Devuelve la pieza que ha fallado a NetApp"**

Devuelva la pieza que ha fallado a NetApp, como se describe en las instrucciones de RMA que se suministran con el kit.

Requisitos de sustitución de soportes de arranque - ASA A1K

Antes de sustituir el soporte de arranque, asegúrese de revisar los siguientes requisitos.

- Debe tener una unidad flash USB, formateada a FAT32, con la cantidad de almacenamiento adecuada para guardar el `image_xxx.tgz` archivo.
- Debe copiar `image_xxx.tgz` el archivo en la unidad flash USB para su uso posterior en este procedimiento.
- Debe sustituir el componente con errores por un componente de FRU de reemplazo que haya recibido NetApp.
- 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 la compatibilidad y el estado de la clave de cifrado - ASA A1K

Antes de apagar la controladora dañada, compruebe si su versión de ONTAP es compatible con cifrado de volúmenes de NetApp (NVE) y si el sistema de gestión de claves está configurado correctamente.

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.

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.

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

Versión de ONTAP	Ejecute este comando
ONTAP 9.14.1 o posterior	`security key-manager keystore show` • Si EKM está activado, `EKM` aparece en la salida del comando. • Si OKM está activado, `OKM` aparece en la salida del comando. • Si no hay ningún gestor de claves activado, `No key manager keystores configured` aparece en el resultado del comando.
ONTAP 9.13.1 o anterior	`security key-manager show-key-store` • Si EKM está activado, `external` aparece en la salida del comando. • Si OKM está activado, `onboard` aparece en la salida del comando. • Si no hay ningún gestor de claves activado, `No key managers configured` aparece en el resultado del comando.

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

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`	Realice una copia de seguridad manual de la información de OKM. a. Vaya al modo avanzado introduciendo `set -priv advanced` y, a continuación, introdúzcalo `Y` cuando se le solicite. b. Introduzca el siguiente 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. Vaya a "apague el controlador dañado".

Valor de salida en `Restored` la columna	Siga estos pasos…

Cualquier otra cosa que no sea `true`	a. Introduzca el comando SYNC del gestor de claves de seguridad incorporado:
	
	`security key-manager onboard sync`
	
	b. Introduzca los 32 caracteres y la clave de acceso alfanumérica de gestión de claves incorporada cuando se le solicite.
	
	Si no se puede proporcionar la contraseña, póngase en contacto con "Soporte de NetApp".
	
	c. Compruebe que `Restored` se muestra la columna `true` para todas las claves de autenticación:
	
	`security key-manager key query`
	
	d. Compruebe que se muestra el `Key Manager` tipo `onboard`y, a continuación, realice una copia de seguridad manual de la información de OKM.
	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. Puede apagar el controlador defectuoso de forma segura. Vaya a "apague el controlador dañado".

Apague el controlador defectuoso: ASA A1K

Debe completar el apagado de la controladora dañada. Apague o tome el control de la controladora dañada.

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, "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. Desactive 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:

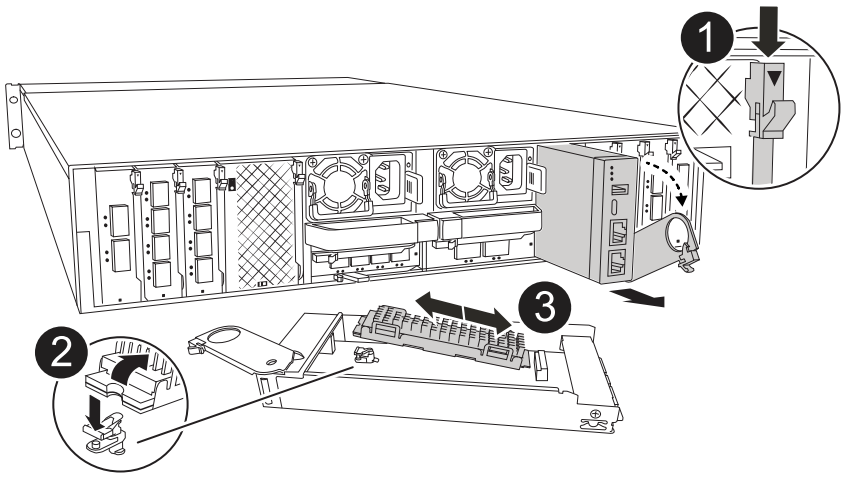
Si el controlador dañado está mostrando…	**Realice lo siguiente…**
El aviso del CARGADOR	Vaya al paso siguiente.
Esperando devolución…	Pulse Ctrl-C y, a continuación, responda `y` cuando se le solicite.
Solicitud del sistema o solicitud de contraseña	Retome o detenga el controlador dañado del controlador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

Sustituya el soporte de arranque: ASA A1K

Debe desconectar el módulo del controlador, extraer el módulo de gestión del sistema de la parte posterior del sistema, retirar el soporte de arranque defectuoso e instalar el soporte de arranque de repuesto en el módulo de gestión del sistema.

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.



1	Bloqueo de leva del módulo de gestión del sistema
2	Botón de bloqueo del soporte de arranque
3	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.
   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 medio de arranque de reemplazo que instaló se encuentra sin una imagen ONTAP. Puede transferir la imagen ONTAP al soporte de arranque de reemplazo descargando la imagen de servicio ONTAP adecuada de "Sitio de soporte de NetApp" a una unidad flash USB y, a continuación, al soporte de arranque de reemplazo.

Antes de empezar

- Debe tener una unidad flash USB vacía, formateada a FAT32, con al menos 4GB GB de capacidad.
- Descargue una copia de la misma versión de imagen de ONTAP que la que se estaba ejecutando la controladora afectada. Puede descargar la imagen adecuada en la sección Descargas del sitio de soporte de NetApp. Utilice `version -v` el comando para mostrar si su versión de ONTAP es compatible con NVE. Si aparece el resultado del comando `<10no- DARE>` , su versión de ONTAP no admite NVE.
  - Si NVE es compatible con su versión de ONTAP, descargue la imagen con el cifrado de volúmenes de NetApp, 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.
   a. 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 - ASA 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 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. En el controlador dañado, pulse `Y` cuando se le solicite 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".

Restaurar cifrado - ASA A1K

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	Seleccione la opción 10. **Mostrar ejemplo de menú de inicio** ``` Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. (10) Set Onboard Key Manager recovery secrets. (11) Configure node for external key management. Selection (1-11)? 10 ```

Versión de ONTAP	Seleccione esta opción

ONTAP 9,7 y anteriores	Seleccione la opción oculta `recover_onboard_keymanager`
	
	Mostrar ejemplo de menú de inicio
	
	`Please choose one of the following:`
	
	`(1) Normal Boot.`
	`(2) Boot without /etc/rc.`
	`(3) Change password.`
	`(4) Clean configuration and initialize all disks.`
	`(5) Maintenance mode boot.`
	`(6) Update flash from backup config.`
	`(7) Install new software first.`
	`(8) Reboot node.`
	`(9) Configure Advanced Drive Partitioning.`
	`Selection (1-19)?`
	`recover_onboard_keymanager`

3. 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
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

---------------------------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-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUbQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxciLJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----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-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
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
```

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....
[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.

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 deshabilitó, introduciendo el siguiente comando.

```
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
```

Devuelva la pieza fallida a NetApp - ASA A1K

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.