Soporte de arranque

Install and maintain

NetApp
September 25, 2024

Tabla de contenidos

Soporte de arranque

Descripción general de la sustitución del soporte de arranque - ASA A1K

Puede reemplazar manualmente un soporte de arranque fallido mediante el módulo USB para la imagen de arranque o mediante la opción de reemplazo de soporte de arranque automático (BMR).

- "Sustitución de soportes de arranque automatizado"

  La sustitución automática de medios de arranque utiliza la imagen de arranque del nodo asociado y ejecuta automáticamente la opción de menú de arranque correspondiente para instalar la imagen de arranque en el soporte de arranque de reemplazo.

- "Sustitución manual del soporte 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.

Método automatizado

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. **"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.

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

Retire el soporte de arranque fallido del módulo de gestión del sistema e instale el soporte de arranque de repuesto.

4. **"Recuperación automática tras arranque"**

Restaurar la imagen ONTAP de la controladora asociada.

5 **"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 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.
- No debe haber puertos de clúster defectuosos en la controladora dañada.

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, 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:

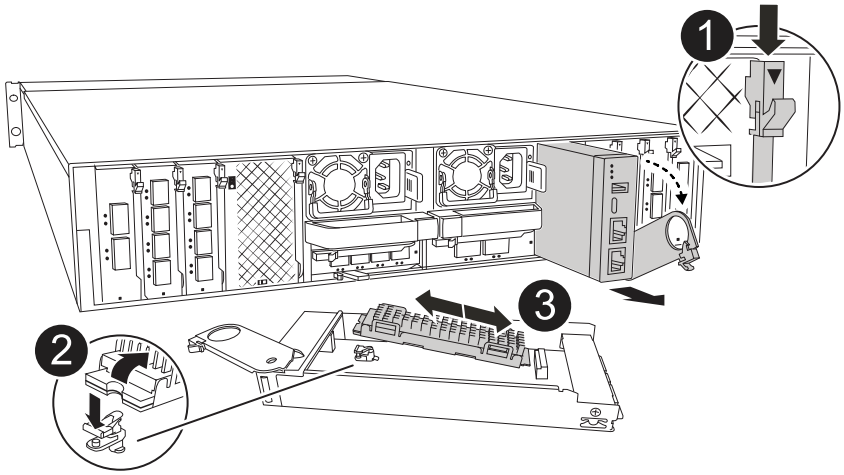
Si el controlador dañado está mostrando…	Realice lo siguiente…
El aviso del CARGADOR	Vaya al paso siguiente.
Esperando devolución…	Pulse Ctrl-C y, a continuación, responda `y` cuando se le solicite.
Solicitud del sistema o solicitud de contraseña	Retome o detenga el controlador dañado del controlador 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

Para sustituir el soporte de arranque, debe 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.

Pasos

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.

Recuperación automática de arranque - ASA A1K

Puede restaurar la imagen en el soporte de arranque desde el controlador asociado mediante el proceso de recuperación automática al arranque.

Seleccione la opción de recuperación automatizada de nodo único que se ajuste a la configuración.

Opción 1: Recuperación sin cifrado

Puede restaurar la imagen de ONTAP (recuperación del medio de arranque) desde el nodo del partner mediante `boot_recovery -partner` el comando en las plataformas ASA R2 que ejecuten ONTAP 9.16,0 y versiones posteriores.

Antes de empezar

Cuando arranca un nodo y el soporte de arranque de dicho nodo está dañado, verá los siguientes mensajes y el proceso de arranque con stop en el símbolo del sistema de Loader:

```
Can't find primary boot device u0a.0
Can't find backup boot device u0a.1
ACPI RSDP Found at 0x777fe014


Starting AUTOBOOT press Ctrl-C to abort...
Could not load fat://boot0/X86_64/freebsd/image1/kernel:Device not
found

ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/Linux/image1/vmlinuz (boot0,fat)


ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/freebsd/image1/kernel (boot0,fat)


Autoboot of PRIMARY image failed. Device not found (-6)
LOADER-A>
```

Si ve este mensaje, debe restaurar la imagen de ONTAP

Pasos

1. En el símbolo del sistema DE Loader, introduzca el comando *boot_recovery -partner*.

   La pantalla mostrará el mensaje `Starting boot media recovery (BMR) process press Ctrl-C to abort…` y comenzará las comprobaciones iniciales.

2. Supervise el proceso como Loader configura los puertos del clúster local y ejecuta netboot a través `\http://<remote-partner-IP>:65530/recoverydisk/image.tgz`de .

   Una vez que netboot se está ejecutando, `Starting BMR …` se muestra en la pantalla y el proceso completa el proceso de instalación.

   a. Si Key Manager no está configurado, verá el siguiente mensaje:

      ```
      key manager is not configured. Exiting.
      ```

b. Si aparece el siguiente mensaje, Onboard Key Manager (OKM) está configurado:

```
key manager is configured.
Entering Bootmenu Option 10...

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

Vaya a para completar el proceso de recuperación.

c. Si ve el siguiente mensaje, External Key Manager (EKM) está configurado. Vaya al tema de EKM y complete el proceso de recuperación:

```
Error when fetching key manager config from partner
169.254.139.209: 28
Has key manager been configured on this system? {y|n}
```

3. Supervisar el proceso BMR a medida que ejecuta la restauración de la configuración de copia de seguridad, el archivo env, mdb y rdb desde el partner.
4. El nodo se reinicia y la BMR se completa cuando observe lo siguiente:

```
varfs_backup_restore: update checksum for varfs.tgz
varfs_backup_restore: restore using /cfcard/x86_64/freebsd/oldvarfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: Rebooting to load the new varfs
.
Terminated
varfs_backup_restore: bootarg.abandon_varfs is set! Skipping /var
backup.
```

Opción 2: Recuperación con el gestor de claves incorporado presente

Es posible restaurar la imagen ONTAP (recuperación del medio de arranque) desde el nodo asociado mediante `boot_recovery -partner` las plataformas ASA R2 que ejecutan ONTAP 9.16,0 y versiones posteriores.

Antes de empezar

Cuando arranca un nodo y el soporte de arranque de dicho nodo está dañado, verá los siguientes mensajes y el proceso de arranque con stop en el símbolo del sistema de Loader:

```
Can't find primary boot device u0a.0
Can't find backup boot device u0a.1
ACPI RSDP Found at 0x777fe014


Starting AUTOBOOT press Ctrl-C to abort...
Could not load fat://boot0/X86_64/freebsd/image1/kernel:Device not
found

ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/Linux/image1/vmlinuz (boot0,fat)


ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/freebsd/image1/kernel (boot0,fat)


Autoboot of PRIMARY image failed. Device not found (-6)
LOADER-A>
```

Si ve este mensaje, debe restaurar la imagen de ONTAP

Pasos

1. En el símbolo del sistema DE Loader, introduzca el comando *boot_recovery -partner*.

   La pantalla mostrará el mensaje `Starting boot media recovery (BMR) process press Ctrl-C to abort…` e iniciará las comprobaciones iniciales y la instalación de los archivos de recuperación de arranque.

   a. Si Onboard Key Manager (OKM) está configurado, verá lo siguiente:

   ```
   key manager is configured.
   Entering Bootmenu Option 10...

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

2. Introduzca *y* en la petición de datos.
3. Introduzca la clave de acceso del gestor de claves incorporado cuando lo vea `Enter the passphrase for onboard key management:`
4. Introduzca de nuevo la frase de contraseña del gestor de claves incorporado cuando se le solicite que confirme la clave de acceso.

```
Enter the passphrase for onboard key management:
Enter the passphrase again to confirm:
Enter the backup data:
TmV0QXBwIEtleSBCbG9iAAECAAAEAAAAcAEAAAAAAAA3yR6UAAAAACEAAAAAAAAA
QAAAAAAAAACJz1u2AAAAAPX84XY5AU0p4Jcb9t8wiwOZoqyJPJ4L6/j5FHJ9yj/w
RVDO1sZB1E4HO79/zYc82nBwtiHaSPWCbkCrMWuQQDsiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAABHVFpxAAAAAHUgdVq0EKNp
.
.
.
.
```

Verá lo siguiente cuando se complete el proceso de recuperación:

```
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.
```

5. Supervisar el proceso BMR a medida que ejecuta la restauración de la configuración de copia de seguridad, el archivo env, mdb y rdb desde el partner.

   Cuando se completa la restauración, el nodo se reinicia para completar el proceso.

Opción 3: Recuperación con External Key Manager presente

Es posible restaurar la imagen ONTAP (recuperación del medio de arranque) desde el nodo asociado mediante `boot_recovery -partner` las plataformas ASA R2 que ejecutan ONTAP 9.16,0 y versiones posteriores.

Cuando arranca un nodo y el soporte de arranque de dicho nodo está dañado, verá los siguientes mensajes y el proceso de arranque con stop en el símbolo del sistema de Loader:

```
Can't find primary boot device u0a.0
Can't find backup boot device u0a.1
ACPI RSDP Found at 0x777fe014


Starting AUTOBOOT press Ctrl-C to abort...
Could not load fat://boot0/X86_64/freebsd/image1/kernel:Device not
found

ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/Linux/image1/vmlinuz (boot0,fat)


ERROR: Error booting OS on: 'boot0' file:
fat://boot0/X86_64/freebsd/image1/kernel (boot0,fat)


Autoboot of PRIMARY image failed. Device not found (-6)
LOADER-A>
```

Si ve este mensaje, debe restaurar la imagen de ONTAP.

Pasos

1. En el símbolo del sistema DE Loader, introduzca el comando *boot_recovery -partner*.

   La pantalla mostrará el mensaje `Starting boot media recovery (BMR) process press Ctrl-C to abort…` e iniciará las comprobaciones iniciales y la instalación de los archivos de recuperación de arranque.

   a. Si External Key Manager (EKM) está configurado, aparecerá lo siguiente:

   ```
   Error when fetching key manager config from partner
   169.254.139.209: 28
   Has key manager been configured on this system? {y|n}
   ```

   b. Introduzca *y* si se ha configurado un gestor de claves.

   ```
   key manager is configured.
   Entering Bootmenu Option 11...
   ```

   La opción bootmenu 11 solicitará al usuario toda la información de configuración de EKM para que los archivos de configuración puedan ser reconstruidos.

2. Introduzca la configuración de EKM en cada petición de datos.

   NOTA: La mayor parte de esta información fue ingresada cuando EKM fue originalmente habilitado.

Debe introducir la misma información que se introdujo durante la configuración inicial de EKM.

3. Compruebe que `Keystore UUID` los y `Cluster UUID` son correctos.

   a. En el nodo del partner, recupere el UUID de clúster con `cluster identity show`el comando.

   b. En el nodo asociado, recupere el UUID de almacén de claves con el `vserver show -type admin` comando y `key-manager keystore show -vserver <nodename>` el comando.

   c. Introduzca los valores para UUID del almacén de claves y UUID de clúster cuando se le solicite.

      NOTA: Si el nodo asociado no está disponible, el UUID de almacén de claves y el UUID de clúster se pueden obtener de la clave Mroot-AK ubicada en el servidor de claves configurado.

   Verifique `x-NETAPP-ClusterName: <cluster name>` para el UUID de clúster y `x-NETAPP-KeyUsage: "MROOT-AK"` los atributos de UUID de almacén de claves a fin de asegurarse de tener las claves correctas.

4. Supervise la recuperación y restauración de Mroot-AK en el nodo ONTAP.

5. Si el proceso no puede restaurar la clave, verá el siguiente mensaje y deberá configurar e0M desde el shell del sistema de menús:

```
ERROR: kmip_init: halting this system with encrypted mroot...
WARNING: kmip_init: authentication keys might not be available.
*********************************************************
*                  A T T E N T I O N                    *
*                                                       *
*       System cannot connect to key managers.          *
*                                                       *
*********************************************************
ERROR: kmip_init: halting this system with encrypted mroot...
.
Terminated

Uptime: 11m32s
System halting...

LOADER-B>
```

   a. Ejecute `boot_recovery -partner` el comando en el nodo de recuperación.

   b. Cuando se le solicite que realice (y o n) las opciones para EKM, seleccione *n* para todos.

      Después de seleccionar la opción *n* para las indicaciones de 8, el sistema se detendrá en el menú de inicio.

   c. Recopile la información del archivo /cfcard/kmip/servers.cfg de otro nodo del clúster. Usted recopilará la siguiente información:

      - La dirección del servidor KMIP.
      - El puerto KMIP.

- UUID del almacén de claves.
- Una copia del certificado de cliente del archivo /cfcard/kmip/certs/client.crt.
- Una copia de la clave de cliente del archivo /cfcard/kmip/certs/client.key.
- Una copia de las CA del servidor KMIP del archivo /cfcard/kmip/certs/CA.pem.

d. Introduzca systemshell desde el menú de inicio introduciendo *systemshell* en el prompt.

e. Configure la red desde el menú systemshell para e0M, máscara de red y puerta de enlace.

f. Salga del menú systemshell con el comando *exit*.

g. Verá el menú de arranque. Seleccione la opción `11` para continuar con la restauración de EKM.

h. Responda `y` a las siguientes preguntas e introduzca la información obligatoria que haya recopilado anteriormente cuando se le solicite:

- ¿Tiene una copia del archivo /cfcard/kmip/certs/client.crt? {s/n}
- ¿Tiene una copia del archivo /cfcard/kmip/certs/client.key? {s/n}
- ¿Tiene una copia del archivo /cfcard/kmip/certs/ca.pem? {s/n}
- ¿Tiene una copia del archivo /cfcard/kmip/servers.cfg? {s/n}

6. Si la clave se restaura correctamente, el proceso de recuperación continúa y reinicia el nodo.

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.

Método manual

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

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

"Revise los requisitos de medios de arranque"

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

"Compruebe las claves de cifrado incorporadas"

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

"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`.
- 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 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: ASA 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

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. Determine 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"

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".

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: 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, 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:

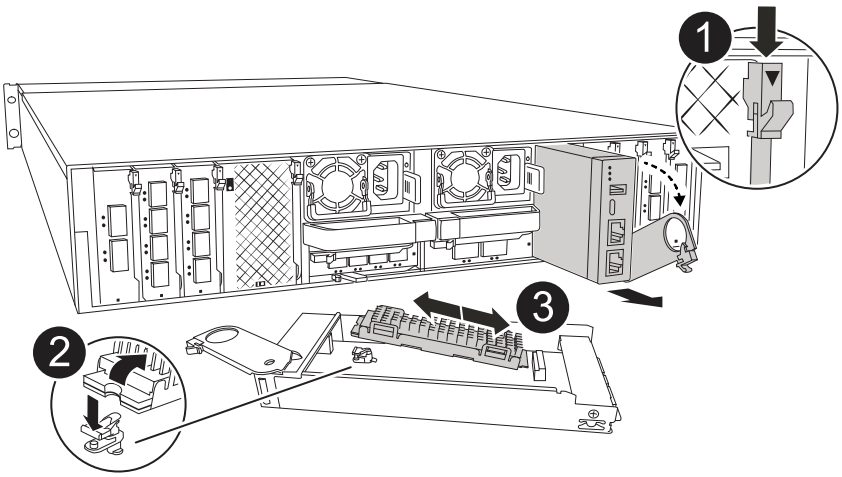
Si el controlador dañado está mostrando…	**Realice lo siguiente…**
El aviso del CARGADOR	Vaya al paso siguiente.
Esperando devolución…	Pulse Ctrl-C y, a continuación, responda `y` cuando se le solicite.
Solicitud del sistema o solicitud de contraseña	Retome o detenga el controlador dañado del controlador 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

Para sustituir el soporte de arranque, debe 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 soporte de arranque de repuesto que instaló no tiene 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.
- 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 - 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 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 se está ejecutando…	Realice lo siguiente…
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 afectado, pulse *Y* cuando se le solicite que sobrescriba `/etc/ssh/ssh_host_ecdsa_key`. c. En el controlador asociado en buen estado, establezca el controlador deficiente 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 administrador: *Set -privilege admin*. f. En el controlador afectado, pulse *y* cuando vea `Was the restore backup procedure successful?`. g. En el controlador afectado, pulse *y* cuando vea `…would you like to use this restored copy now?`. h. En el controlador afectado, pulse *y* cuando se le solicite reiniciar el controlador dañado y pulse *ctrl-c* para el menú de arranque. i. Si el sistema no utiliza encyption, seleccione *Opción 1 Arranque normal.*; de lo contrario, vaya a "Restaure gestores de claves". j. Conecte el cable de la consola al controlador asociado. k. Devuelva la controladora con el comando *storage failover giveback -fromnode local*. l. Restaure la devolución automática del control si la deshabilitó con el comando *storage failover modify -node local -auto-giveback true*. m. 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*. **NOTA:** Si el proceso falla, póngase en contacto con "Soporte de NetApp".

Si el sistema se está ejecutando…	Realice lo siguiente…
ONTAP 9.16.1 o posterior	a. En el controlador afectado, 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 realizó correctamente. c. En el controlador afectado, pulse *y* cuando se le solicite utilizar la configuración restaurada. d. En el controlador dañado, pulse *y* cuando se le solicite reiniciar el nodo. e. En el controlador afectado, pulse *y* cuando se le solicite reiniciar el controlador dañado y pulse *ctrl-c* para el menú de arranque. f. Si el sistema no utiliza encyption, seleccione *Opción 1 Arranque normal.*; de lo contrario, vaya a "Restaure gestores de claves". g. Conecte el cable de la consola al controlador asociado. h. Devuelva la controladora con el comando *storage failover giveback -fromnode local*. i. Restaure la devolución automática del control si la deshabilitó con el comando *storage failover modify -node local -auto-giveback true*. j. 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*. **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.

Paso 1: Restaure el gestor de claves incorporado

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.
2. Seleccione una de las siguientes opciones para restaurar la configuración del administrador de claves incorporado desde el menú de arranque ONATP.

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

Restaure 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.

```
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---------------------------
```

5. Se completará el proceso de recuperación.

```
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)`

8. Desde el nodo del partner, devolver la controladora asociada: *Storage failover giveback -fromnode local -only-cfo-aggregates true*
9. Una vez iniciado solo con CFO aggregate, ejecute el comando *security key-manager onboard sync*:
10. 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.
```

11. 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.

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

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

Restaure 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

1. Seleccione la opción 11 en el menú de inicio de ONTAP.

```
(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-----
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-----
MIIEpQIBAAKCAQEAoU1eajEG6QC2h2Zih0jEaGVtQUexNeoCFwKPoMSePmjDNtrU
MSB1SlX3VgCuElHk57XPdq6xSbYlbkIb4bAgLztHEmUDOkGmXYAkblQ=
-----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
```

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
```

Paso 2: 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 *storage failover show*.

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` columna = `yes/true`, ha finalizado y puede continuar con el proceso de sustitución.
   - Si `Key Manager type` = `external` y la `Restored` columna = 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` columna = 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` columna = `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 - 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.