Soporte de arranque

Install and maintain

NetApp
February 13, 2026

Tabla de contenidos

Soporte de arranque . . . 1
- Flujo de trabajo de sustitución de medios de arranque: ASA A70 y ASA A90 . . . 1
- Requisitos para reemplazar el medio de arranque - ASA A70 y ASA A90 . . . 1
- Apague el controlador para reemplazar el medio de arranque: ASA A70 o ASA A90 . . . 2
- Sustituya el soporte de arranque: ASA A70 y ASA A90 . . . 3
- Restaurar la imagen de ONTAP en el medio de arranque - ASA A70 y ASA A90 . . . 6
- Devuelva la pieza fallida a NetApp - ASA A70 y ASA A90 . . . 12

Soporte de arranque

Flujo de trabajo de sustitución de medios de arranque: ASA A70 y ASA A90

Comience a reemplazar los medios de arranque en su sistema de almacenamiento ASA A70 y ASA A90 revisando los requisitos de reemplazo, apagando la controladora, reemplazando el soporte de arranque, restaurando la imagen en el soporte de arranque y verificando la funcionalidad del sistema.

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

Revise los requisitos para la sustitución de medios de arranque.

2. **"Apague la controladora"**

Apague la controladora en el sistema de almacenamiento cuando necesite reemplazar el medio de arranque.

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. **"Restaure la imagen en el soporte de 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 para reemplazar el medio de arranque - ASA A70 y ASA A90

Antes de reemplazar el medio de arranque en su sistema ASA A70 o ASA A90, asegúrese de cumplir con los requisitos necesarios para un reemplazo exitoso. Esto incluye verificar que tenga el medio de arranque de reemplazo correcto, confirmar que los puertos del clúster en el controlador dañado funcionen correctamente y determinar si el Administrador de claves integrado (OKM) o el Administrador de claves externo (EKM) están habilitados.

Revise los siguientes requisitos.

- Debe sustituir el medio de arranque con errores por un medio de arranque de reemplazo que recibió desde NetApp.
- Los puertos del clúster se utilizan para la comunicación entre los dos controladores durante el proceso de recuperación de arranque automático. Asegúrese de que los puertos del clúster del controlador dañado funcionen correctamente.
- Para OKM, necesita la frase de contraseña de todo el clúster y también los datos de respaldo.
- Para EKM, necesita copias de los siguientes archivos del nodo asociado:
  - /cfcard/kmip/servers.cfg
  - /cfcard/kmip/certs/client.crt
  - /cfcard/kmip/certs/cliente.clave
  - /cfcard/kmip/certs/CA.pem
- Comprenda la terminología del controlador utilizada en este procedimiento:
  - El *controlador dañado* es el controlador en el que está realizando mantenimiento.
  - El *controlador saludable* es el socio HA del controlador dañado.

El futuro

Después de revisar los requisitos de soporte de arranque, usted "apague la controladora".

Apague el controlador para reemplazar el medio de arranque: ASA A70 o ASA A90

Apague la controladora deteriorada en su sistema de almacenamiento ASA A70 o ASA A90 para evitar la pérdida de datos y garantizar la estabilidad del sistema al sustituir los medios de arranque.

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, elimine 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. Desactivar devolución automática:
   a. Ingrese el siguiente comando desde la consola del controlador en buen estado:

      ```
      storage failover modify -node impaired_node_name -auto-giveback false
      ```

   b. Ingresar `y` cuando vea el mensaje "¿Desea desactivar la devolución automática?"
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 -halt true` El parámetro *-halt true* lleva al símbolo del sistema de Loader.

El futuro

Después de apagar el controlador defectuoso, usted "sustituya el soporte de arranque".

Sustituya el soporte de arranque: ASA A70 y ASA A90

El medio de arranque del sistema ASA A70 o ASA A90 almacena datos esenciales del firmware y de configuración. El proceso de sustitución implica la extracción del módulo de gestión del sistema, la extracción del soporte de arranque defectuoso, la instalación del soporte de arranque de repuesto en el módulo de gestión del sistema y, a continuación, la reinstalación del módulo de gestión del sistema.

Reemplace el medio de arranque, que se encuentra dentro del módulo de administración del sistema en la parte posterior del controlador.

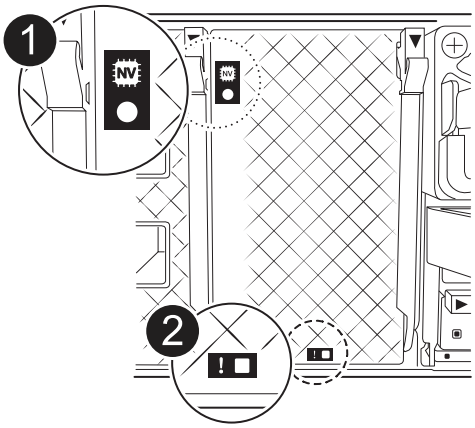
Antes de empezar

- Necesitas un medio de arranque de repuesto.
- Tenga a mano una alfombrilla antiestática para el módulo de gestión del sistema.

Pasos

1. Verifique que la descarga de la NVRAM se haya completado antes de continuar. Cuando el LED del módulo NV está apagado, la NVRAM se desactiva.

Si el LED parpadea, espere a que deje de parpadear. Si el parpadeo continúa durante más de 5 minutos, póngase en contacto con el soporte de NetApp para obtener ayuda.

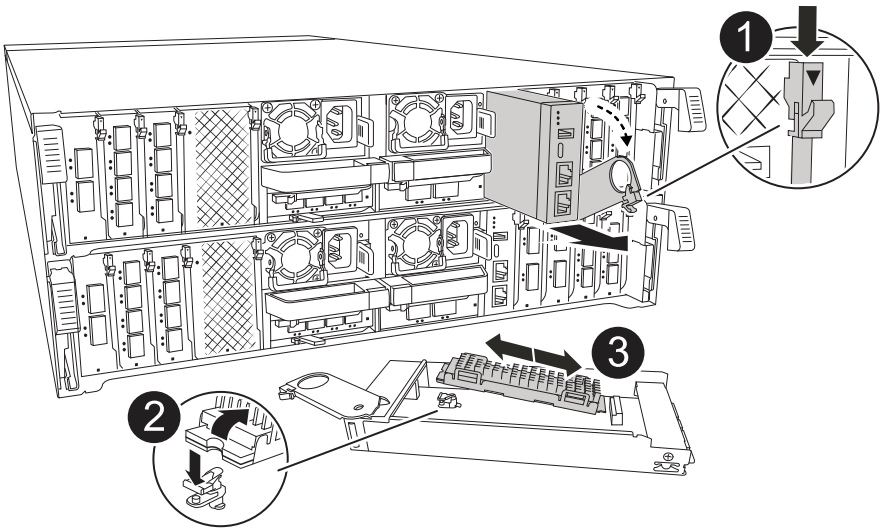


1	LED de estado de NVRAM
2	LED de alerta de NVRAM

2. Dirígete a la parte trasera del chasis y conéctate a tierra correctamente si aún no lo estás.
3. Desconectar la alimentación del controlador:
   - En el caso de fuentes de alimentación de CA, desconecte los cables de alimentación de las fuentes de alimentación.
   - Para fuentes de alimentación de CC, desconecte el bloque de alimentación de las fuentes de alimentación.
4. Retire el módulo Gestión del sistema:
   a. Retire todos los cables conectados al módulo de administración del sistema. Etiquete los cables para identificar sus puertos correctos para la reinstalación.
   b. Gire el brazo organizador de cables hacia abajo tirando de los botones situados a ambos lados del mismo.
   c. Pulse el botón de la leva de gestión del sistema.

      La palanca de levas se aleja del chasis.

   d. Gire la palanca de leva completamente hacia abajo y retire el módulo de administración del sistema del controlador.
   e. Coloque el módulo de administración del sistema sobre una alfombrilla antiestática con el medio de arranque accesible.
5. Retire el medio de arranque del módulo de administración del sistema:



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

a. Pulse el botón de bloqueo azul.

b. Gire el medio de arranque hacia arriba, deslícelo fuera del zócalo y déjelo a un lado.

6. 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.

7. Vuelva a instalar el módulo Gestión del sistema:

a. Alinee los bordes del módulo de administración del sistema con la abertura del chasis.

b. Deslice suavemente el módulo dentro del chasis hasta que el pestillo de leva comience a encajar.

c. Gire el pestillo de leva completamente hacia arriba para bloquear el módulo en su lugar.

d. Vuelva a conectar los cables al módulo de administración del sistema utilizando las etiquetas que creó durante la extracción.

e. Gire el ARM de gestión de cables hasta la posición cerrada.

8. Vuelva a conectar la alimentación al controlador:

◦ Para las fuentes de alimentación de CA, conecte los cables de alimentación a las fuentes de alimentación.

◦ Para fuentes de alimentación de CC, vuelva a conectar el bloque de alimentación a las fuentes de alimentación.

El controlador se reinicia automáticamente cuando se restablece la alimentación.

9. Interrumpa el proceso de arranque pulsando `Ctrl-C` para detenerse en el indicador CARGADOR.

El futuro

Después de sustituir físicamente el soporte de arranque defectuoso, "Restaure la imagen ONTAP desde el nodo del partner".

Restaurar la imagen de ONTAP en el medio de arranque - ASA A70 y ASA A90

Después de instalar el nuevo dispositivo multimedia de arranque en el sistema ASA A70 o ASA A90, puede iniciar el proceso de recuperación de medios de arranque automático para restaurar la configuración desde el nodo asociado.

Durante el proceso de recuperación, el sistema comprueba si el cifrado está habilitado y determina el tipo de cifrado de clave que se está usando. Si el cifrado de claves está activado, el sistema le guiará a través de los pasos adecuados para restaurarlo.

Antes de empezar

- Determine su tipo de gestor de claves:
  - Administrador de claves integrado (OKM): Requiere contraseña para todo el clúster y datos de respaldo.
  - Gestor de claves externo (EKM): Requiere los siguientes archivos del nodo asociado:
    - `/cfcard/kmip/servers.cfg`
    - `/cfcard/kmip/certs/client.crt`
    - `/cfcard/kmip/certs/client.key`
    - `/cfcard/kmip/certs/CA.pem`

Pasos

1. Desde el indicador LOADER, inicie el proceso de recuperación del medio de arranque:

   ```
   boot_recovery -partner
   ```

   La pantalla muestra el siguiente mensaje:

   ```
   Starting boot media recovery (BMR) process. Press Ctrl-C to abort…
   ```

2. Supervise el proceso de recuperación de instalación de medios de arranque.

   El proceso finaliza y muestra el `Installation complete` mensaje.

3. El sistema comprueba el cifrado y muestra uno de los siguientes mensajes:

Si ve este mensaje…	Realice lo siguiente…
`key manager is not configured. Exiting.`	El cifrado no está instalado en el sistema. a. Espere a que aparezca la pantalla de inicio de sesión. b. Inicia sesión en el nodo y devuelve el almacenamiento: `storage failover giveback -ofnode impaired_node_name` c. Ir a reactivación de la devolución automática Si estaba deshabilitado.
`key manager is configured.`	El cifrado está instalado. Vaya a restaurar el administrador de claves.

Si el sistema no puede identificar la configuración del gestor de claves, muestra un mensaje de error y le solicita que confirme si el gestor de claves está configurado y de qué tipo (integrado o externo). Responda a las preguntas para continuar.

4. Restaura el gestor de claves usando el procedimiento adecuado para tu configuración:

Gestión de claves incorporada (OKM)

El sistema muestra el siguiente mensaje y comienza a ejecutar la opción 10 del menú de arranque:

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

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

a. Ingresar `y` Cuando se le solicite, confirme que desea iniciar el proceso de recuperación de OKM.
b. Introduzca la contraseña para la gestión de llaves a bordo cuando se le solicite.
c. Vuelva a introducir la contraseña cuando se le solicite confirmación.
d. Introduzca los datos de copia de seguridad del gestor de claves integrado cuando se le solicite.

Mostrar ejemplo de solicitud de frase de contraseña y datos de respaldo

```
Enter the passphrase for onboard key management:
-----BEGIN PASSPHRASE-----
<passphrase_value>
-----END PASSPHRASE-----
Enter the passphrase again to confirm:
-----BEGIN PASSPHRASE-----
<passphrase_value>
-----END PASSPHRASE-----
Enter the backup data:
-----BEGIN BACKUP-----
<passphrase_value>
-----END BACKUP-----
```

e. Supervise el proceso de recuperación mientras restaura los archivos correspondientes desde el nodo asociado.

Cuando finaliza el proceso de recuperación, el nodo se reinicia. Los siguientes mensajes indican una recuperación exitosa:

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

Successfully recovered keymanager secrets.
```

f. Después de reiniciar el nodo, verifique que el sistema esté de nuevo en línea y operativo.

g. Devuelva la controladora afectada a su funcionamiento normal devolviendo su almacenamiento:

```
storage failover giveback -ofnode impaired_node_name
```

h. Una vez que el nodo asociado esté completamente operativo y proporcionando datos, sincronice las claves OKM en todo el clúster:

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

Ir a reactivación de la devolución automática Si estaba deshabilitado.

Gestor de claves externo (EKM)

El sistema muestra el siguiente mensaje y comienza a ejecutar la opción 11 del menú de arranque:

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

a. Introduzca los ajustes de configuración de EKM cuando se le solicite:

i. Introduzca el contenido del certificado de cliente desde el `/cfcard/kmip/certs/client.crt` archivo:

Mostrar ejemplo de contenido de certificado de cliente

```
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

ii. Introduzca el contenido del archivo de clave de cliente desde el `/cfcard/kmip/certs/client.key` archivo:

Muestra un ejemplo de contenido del archivo de clave de cliente

```
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
```

iii. Introduzca el contenido del archivo de CA(s) del servidor KMIP desde el `/cfcard/kmip/certs/CA.pem` archivo:

Muestra un ejemplo de contenido del archivo del servidor KMIP

```
-----BEGIN CERTIFICATE-----
<KMIP_certificate_CA_value>
-----END CERTIFICATE-----
```

iv. Introduzca el contenido del archivo de configuración del servidor desde el `/cfcard/kmip/servers.cfg` archivo:

Muestra un ejemplo del contenido del archivo de configuración del servidor

```
xxx.xxx.xxx.xxx:5696.host=xxx.xxx.xxx.xxx
xxx.xxx.xxx.xxx:5696.port=5696
xxx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xxx.xxx.xxx.xxx:5696.protocol=KMIP1_4
1xxx.xxx.xxx.xxx:5696.timeout=25
xxx.xxx.xxx.xxx:5696.nbio=1
xxx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.cr
t
xxx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key
xxx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:
!RC2:!RC4:!SEED:!eNULL:!aNULL"
xxx.xxx.xxx.xxx:5696.verify=true
xxx.xxx.xxx.xxx:5696.netapp_keystore_uuid=<id_value>
```

v. Si se le solicita, introduzca el UUID del clúster ONTAP del nodo asociado. Puedes comprobar el UUID del clúster desde el nodo asociado utilizando el `cluster identify show` dominio.

Mostrar ejemplo de solicitud UUID de clúster ONTAP

```
Notice: bootarg.mgwd.cluster_uuid is not set or is empty.
Do you know the ONTAP Cluster UUID? {y/n} y
Enter the ONTAP Cluster UUID: <cluster_uuid_value>


System is ready to utilize external key manager(s).
```

vi. Si se le solicita, introduzca la interfaz de red temporal y la configuración del nodo:

- La dirección IP del puerto
- La máscara de red para el puerto

- La dirección IP de la puerta de enlace predeterminada

Mostrar ejemplo de avisos de configuración de red temporales

```
In order to recover key information, a temporary network
interface needs to be
configured.

Select the network port you want to use (for example,
'e0a')
e0M

Enter the IP address for port : xxx.xxx.xxx.xxx
Enter the netmask for port : xxx.xxx.xxx.xxx
Enter IP address of default gateway: xxx.xxx.xxx.xxx
Trying to recover keys from key servers....
[discover_versions]
[status=SUCCESS reason= message=]
```

b. Verifique el estado de restauración de la clave:

- Si ves `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696` En la salida, se muestra que la configuración EKM se ha restaurado correctamente. El proceso restaura los archivos correspondientes del nodo asociado y reinicia el nodo. Pase al siguiente paso.
- Si la clave no se restaura correctamente, el sistema se detiene y muestra mensajes de error y advertencia. Vuelva a ejecutar el proceso de recuperación desde el símbolo del sistema del cargador: `boot_recovery -partner`

Muestre un ejemplo de mensajes de error y advertencia de recuperación de claves

```
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>
```

c. Después de reiniciar el nodo, verifique que el sistema esté de nuevo en línea y operativo.

d. Devuelva el funcionamiento normal de la controladora y devuelva su almacenamiento:

```
storage failover giveback -ofnode impaired_node_name
```

Ir a reactivación de la devolución automática Si estaba deshabilitado.

5. Si la devolución automática estaba desactivada, vuelve a activarla:

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

6. Si AutoSupport está habilitado, restaure la creación automática de casos:

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

El futuro

Después de haber restaurado la imagen ONTAP y el nodo esté activo y sirviendo datos, usted"Devuelva la pieza fallida a NetApp".

Devuelva la pieza fallida a NetApp - ASA A70 y ASA A90

Si un componente de su sistema ASA 70-90 falla, devuelva la pieza defectuosa a NetApp. Consulte la "Devolución de piezas y sustituciones" página para más información.

Información de copyright

Información de la marca comercial