Soporte de arranque

Install and maintain

NetApp
February 28, 2025

Tabla de contenidos

Soporte de arranque

Descripción general de la recuperación de medios de arranque - ASA A70 y ASA A90

La recuperación del medio físico de arranque utiliza la imagen de arranque del nodo asociado y ejecuta automáticamente la opción de menú de arranque adecuada para instalar la imagen de arranque en el soporte de arranque de reemplazo.

Cuando encuentre mensajes de error de arranque similares a los que se muestran a continuación, debe sustituir el soporte de arranque y restaurar la imagen ONTAP desde el nodo asociado.

```
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>
```

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

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

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

Revise los requisitos para la sustitución de medios de arranque.

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 **"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 de sustitución de soportes de arranque: ASA A70 y ASA A90

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

- Debe sustituir el medio de arranque con errores por un medio de arranque de reemplazo que recibió desde NetApp.
- No debe haber puertos de clúster defectuosos en la controladora dañada.
- Determine si Onboard Key Manager (OKM) o Eternal Key Manager (EKM) está configurado mediante uno de los siguientes métodos:
  - Puede preguntar al administrador del sistema si OKM o EKM están activados.
  - Para comprobar si OKM está activado, puede utilizar el `security key-manager onboard show`.
  - Para comprobar si EKM está activado, puede utilizar el `security key-manager external show`.
- Para OKM, necesita el contenido del archivo de contraseña de OKM.
- Para EKM, necesita copias de los siguientes archivos del nodo asociado:
  - archivo /cfcard/kmip/servers.cfg.
  - archivo /cfcard/kmip/certs/client.crt.
  - archivo /cfcard/kmip/certs/client.key.
  - Archivo /cfcard/kmip/certs/ca.pem.

El futuro

Después de revisar los requisitos de soporte de arranque, usted "apague el controlador defectuoso".

Apague el controlador defectuoso: ASA A70 y ASA A90

Apague o tome el control de la controladora afectada para poder realizar tareas de mantenimiento en el soporte 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, 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`.

El futuro

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

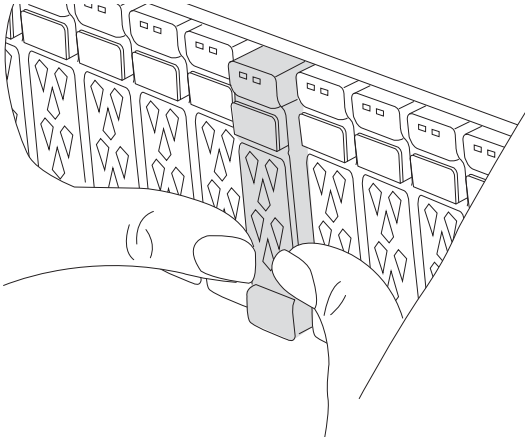
Sustituya el soporte de arranque: ASA A70 y ASA A90

Sustituya el soporte de arranque retirando el módulo de gestión del sistema de la parte posterior del sistema, retirando el soporte de arranque defectuoso, instalando el soporte de arranque de repuesto en el módulo de gestión del sistema y, a continuación, reinstalando el módulo de gestión del sistema.

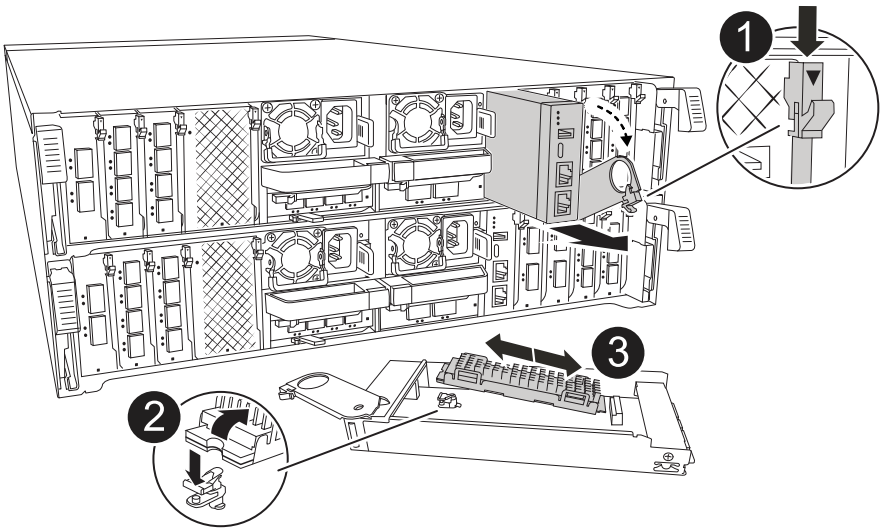
Pasos

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

1. En la parte frontal del chasis, utilice los pulgares para empujar con firmeza cada unidad hasta que sienta una parada positiva. De este modo se garantiza que las unidades se encuentren firmemente asentadas en el plano medio del chasis.



2. Vaya a la parte posterior del chasis. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
3. Desconecte la alimentación del módulo del controlador tirando del módulo del controlador hacia fuera unas tres pulgadas:
   a. Presione ambos pestillos de bloqueo del módulo del controlador y, a continuación, gire ambos pestillos hacia abajo al mismo tiempo.
   b. Extraiga el módulo del controlador unas 3 pulgadas del chasis para desconectar la alimentación.
   c. 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.
   d. 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.
   e. Pulse el botón de la leva de gestión del sistema. La palanca de leva se aleja del chasis.
   f. Gire la palanca de leva completamente hacia abajo y retire el módulo de gestión del sistema del módulo del controlador.
   g. Coloque el módulo de gestión del sistema en una alfombrilla antiestática, de forma que se pueda acceder al soporte de arranque.
4. Retire el soporte de arranque del módulo de gestión:



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 soporte de arranque hacia arriba, deslícelo para extraerlo de la toma y déjelo a un lado.

5. 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.

6. Vuelva a instalar el módulo Gestión del sistema:

a. Gire la bandeja de gestión de cables hasta la posición cerrada.

b. Vuelva a conectar el módulo Gestión del sistema.

7. Vuelva a instalar el controlador y vuelva a conectar la alimentación al módulo del controlador:

a. Empuje firmemente el módulo de la controladora en el chasis hasta que se ajuste al plano medio y esté totalmente asentado.

Los pestillos de bloqueo se elevan cuando el módulo del controlador está completamente asentado.

b. Gire los pestillos de bloqueo hacia arriba hasta la posición de bloqueo.

El controlador comienza a arrancar tan pronto como se asienta y se restablece la alimentación.

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

El futuro

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

Restaurar la imagen ONTAP - ASA A70 y ASA A90

Si el medio de arranque del sistema ASA A70 o ASA A90 está dañado, puede arrancar la imagen de recuperación y restaurar la configuración desde el nodo asociado.

Antes de empezar

- Determine si Onboard Key Manager (OKM) o Eternal Key Manager (EKM) está configurado mediante uno de los siguientes métodos:
  - Puede preguntar al cliente o al administrador del sistema si OKM o EKM están activados.
  - Para comprobar si OKM está activado, puede utilizar el `security key-manager onboard show`.
  - Para comprobar si EKM está activado, puede utilizar el `security key-manager external show`.
- Para OKM, necesita el contenido del archivo de contraseña de OKM.
- Para EKM, necesita copias de los siguientes archivos del nodo asociado:
  - archivo /cfcard/kmip/servers.cfg.
  - archivo /cfcard/kmip/certs/client.crt.
  - archivo /cfcard/kmip/certs/client.key.
  - Archivo /cfcard/kmip/certs/ca.pem.

Pasos

1. En el símbolo del SISTEMA de Loader, introduzca el comando:

   ```
   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 tipo de cifrado y cifrado y muestra uno de los dos mensajes. En función del mensaje que se muestre, realice una de las siguientes acciones:

   > En ocasiones, es posible que el proceso no pueda identificar si el gestor de claves está configurado en el sistema. Mostrará un mensaje de error, preguntará si el gestor de claves está configurado para el sistema y, a continuación, preguntará qué tipo de gestor de claves está configurado. El proceso se reanudará después de resolver el problema.

Mostrar ejemplo de error de configuración al buscar peticiones de datos

```
Error when fetching key manager config from partner ${partner_ip}:
${status}

Has key manager been configured on this system

Is the key manager onboard
```

Si ve este mensaje…	Realice lo siguiente…
`key manager is not configured. Exiting.`	El cifrado no está instalado en el sistema. Complete los siguientes pasos: a. Inicie sesión en el nodo cuando se muestre el aviso de inicio de sesión y devuelva el almacenamiento: `storage failover giveback -ofnode` *`impaired_node_name`* b. Vaya al paso 5 para activar la devolución automática del control si se deshabilitó.
`key manager is configured.`	Vaya al paso 4 para restaurar el administrador de claves adecuado. El nodo accede al menú de arranque y ejecuta lo siguiente: • Opción 10 para sistemas con gestor de claves incorporado (OKM). • Opción 11 para sistemas con External Key Manager (EKM).

4. Seleccione el proceso de restauración del gestor de claves adecuado.

Gestión de claves incorporada (OKM)

Si se detecta OKM, el sistema muestra el siguiente mensaje y comienza a ejecutar la opción de menú de inicio 10.

```
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. Introduzca `Y` en el prompt para confirmar que desea iniciar el proceso de recuperación de OKM.

b. Introduzca la frase de acceso del gestor de claves incorporado cuando se le solicite y vuelva a introducir la frase de acceso cuando se le solicite para confirmar.

Mostrar ejemplo de peticiones de contraseña

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

c. Seguir supervisando el proceso de recuperación mientras restaura los archivos adecuados desde el nodo asociado.

Cuando se complete el proceso de recuperación, el nodo se reiniciará. Los siguientes mensajes indican una recuperación correcta:

```
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.
```

d. Cuando el nodo se reinicia, compruebe que la recuperación del medio de arranque se haya realizado correctamente confirmando que el sistema vuelva a estar conectado y operativo.

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

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

f. Una vez que el nodo asociado esté completamente activo y sirviendo datos, sincronice las claves

OKM en todo el clúster.

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

Gestor de claves externo (EKM)

Si se detecta EKM, el sistema muestra el siguiente mensaje y comienza a ejecutar la opción de menú de inicio 11.

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

a. El siguiente paso depende de la versión de ONTAP que ejecute su sistema:

Si el sistema se está ejecutando…	Realice lo siguiente…
ONTAP 9.16.0	i. Pulse `Ctlr-C` para salir de la opción de menú de inicio 11. ii. Pulse `Ctlr-C` para salir del proceso de configuración de EKM y volver al menú de inicio. iii. Seleccione la opción de menú de inicio 8. iv. Reiniciar el nodo. Si `AUTOBOOT` está establecido, el nodo se reinicia y utiliza los archivos de configuración del nodo compañero. `` `AUTOBOOT`Si no está definido, introduzca el comando de inicio adecuado. El nodo reinicia y usa los archivos de configuración del nodo compañero. `` v. Reinicie el nodo para que EKM proteja la partición del medio de arranque. vi. Continúe con el paso c..
ONTAP 9.16.1	Continúe con el próximo paso.

b. Introduzca el siguiente ajuste de configuración de EKM cuando se le solicite:

Acción	Ejemplo

Introduzca el contenido del certificado de cliente desde `/cfcard/kmip/certs/client.crt` el archivo.	**Mostrar ejemplo de contenido de certificado de cliente**
	`-----BEGIN CERTIFICATE-----`
	`<certificate_value>`
	`-----END CERTIFICATE-----`

Introduzca el contenido del archivo de claves de cliente desde `/cfcard/kmip/certs/client.key` el archivo.	**Muestra un ejemplo de contenido del archivo de clave de cliente**
	`-----BEGIN RSA PRIVATE KEY-----`
	`<key_value>`
	`-----END RSA PRIVATE KEY-----`

Introduzca el contenido del archivo de CA del servidor KMIP desde `/cfcard/kmip/certs/CA.pem` el archivo.	**Muestra un ejemplo de contenido del archivo del servidor KMIP**
	`-----BEGIN CERTIFICATE-----`
	`<KMIP_certificate_CA_value>`
	`-----END CERTIFICATE-----`

Acción	Ejemplo

Introduzca el contenido del archivo de configuración del servidor del `/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.crt`
	`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>`

Acción	Ejemplo

Si se le solicita, introduzca el UUID de clúster ONTAP del partner.	**Muestra el ejemplo de 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).`

Acción	Ejemplo

Si se le solicita, introduzca la interfaz de red temporal y la configuración del nodo.	**Mostrar ejemplo de una configuración de red temporal**
	`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=]`

c. En función de si la clave se ha restaurado correctamente, realice una de las siguientes acciones:
   - Si la configuración de EKM se ha restaurado correctamente, el proceso intenta restaurar los archivos adecuados desde el nodo asociado y reinicia el nodo. Vaya al paso d.

Mostrar ejemplo de mensajes de restauración 9.16.0 correctos

```
kmip2_client: Importing keys from external key server:
xxx.xxx.xxx.xxx:5696
[Feb  6 04:57:43]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdUtils:
[locateMrootAkUuids]:420: Locating local cluster MROOT-AK
with keystore UUID: <uuid>
[Feb  6 04:57:43]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdBase: [doCmdImp]:79: Calling
KMIP Locate for the following attributes: [<x-NETAPP-
ClusterId, <uuid>>, <x-NETAPP-KeyUsage, MROOT-AK>, <x-
NETAPP-KeystoreUuid, <uuid>>, <x-NETAPP-Product, Data
ONTAP>]
[Feb  6 04:57:44]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdBase: [doCmdImp]:84: KMIP
Locate executed successfully!
[Feb  6 04:57:44]: 0x80cc09000: 0: DEBUG:
kmip2::kmipCmds::KmipLocateCmdBase: [setUuidList]:50: UUID
returned: <uuid>
...
kmip2_client: Successfully imported the keys from external
key server: xxx.xxx.xxx.xxx:5696

GEOM_ELI: Device nvd0s4.eli created.
GEOM_ELI: Encryption: AES-XTS 256
GEOM_ELI:     Crypto: software
Feb 06 05:02:37 [_server-name_]: crypto_get_mroot_ak:140
MROOT-AK is requested.
Feb 06 05:02:37 [_server-name_]: crypto_get_mroot_ak:162
Returning MROOT-AK.
```

Mostrar ejemplo de mensajes de restauración 9.16.1 correctos

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[discover_versions]
[status=SUCCESS reason= message=]
...
kmip2_client: Successfully imported the keys from external
key server: xxx.xxx.xxx.xxx:xxxx
Successfully recovered keymanager secrets.
```

- Si la clave no se restaura correctamente, el sistema se detendrá e indicará que no se pudo restaurar. Se muestran los mensajes de error y advertencia. Vuelva a ejecutar el proceso de recuperación introduciendo `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>
```

d. Cuando el nodo se reinicia, compruebe que la recuperación del medio de arranque se haya realizado correctamente confirmando que el sistema vuelva a estar en línea y operativo.

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

`storage failover giveback -ofnode impaired_node_name.`

5. Si la devolución automática está desactivada, vuelva a habilitarla:

`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

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.