Soporte de arranque

Install and maintain

NetApp
July 19, 2024

Tabla de contenidos

Soporte de arranque

Sustituya el soporte de arranque: ASA A900

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

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

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

- Ambos métodos no disruptivos y disruptivos para reemplazar medios de arranque requieren restaurar el `var` sistema de archivos:
  - Para reemplazar de forma no disruptiva, el par de alta disponibilidad no requiere una conexión a una red para restaurar el `var` sistema de archivos. El par de alta disponibilidad de un único chasis tiene una conexión e0S interna, que se utiliza para la transferencia `var` config. entre ellos.
  - Para el reemplazo disruptivo, no es necesaria una conexión de red para restaurar el `var` el sistema de archivos, pero el proceso requiere dos reinicios.
- Debe sustituir el componente con errores por un componente FRU de repuesto que haya recibido de su proveedor.
- Es importante que aplique los comandos en estos pasos en 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.

Comprobaciones previas al apagado para las claves de cifrado integradas: ASA A900

Antes de apagar la controladora deficiente y comprobar el estado de las claves de cifrado incorporadas, debe comprobar el estado de la controladora deficiente, deshabilitar la devolución automática y comprobar qué versión de ONTAP se está ejecutando en el sistema.

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 FALSE para tener derecho a recibir este tipo de servicios, debe corregir el problema antes de apagar la controladora con deficiencias; consulte la "Sincronice un nodo con el clúster".

Pasos

1. Compruebe el estado del controlador dañado:
   - Si el controlador dañado se encuentra en la solicitud de inicio de sesión, inicie sesión como `admin`.
   - Si la controladora dañada se encuentra en el aviso del CARGADOR y forma parte de la configuración de alta disponibilidad, inicie sesión como `admin` en el controlador en buen estado.
   - Si la controladora dañada se encuentra en una configuración independiente y en un aviso DEL

CARGADOR, póngase en contacto con "mysupport.netapp.com".

2. Si AutoSupport está habilitado, elimine la creación automática de casos invocando un mensaje de AutoSupport: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

   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`

3. Compruebe la versión de ONTAP que el sistema está funcionando en el controlador dañado si está activo, o en el controlador asociado si el controlador dañado está inactivo, usando el `version -v` comando:
   - Si se muestra <lno-DARE> o <1Ono-DARE> en el resultado del comando, el sistema no admite NVE, continúe para apagar la controladora.

ONTAP 9.6 y posteriores

Antes de apagar la controladora dañada, debe verificar si el sistema tiene habilitado el cifrado de volúmenes de NetApp (NVE) o el cifrado de almacenamiento de NetApp (NSE). Si es así, debe comprobar la configuración.

1. Verifique si el cifrado de volúmenes está en uso para cualquier volumen del clúster: `volume show -is-encrypted true`

   Si algún volumen aparece en la salida, NVE se configura y debe verificar la configuración NVE. Si no aparece ningún volumen en la lista, compruebe si NSE está configurado y en uso.

2. Compruebe si NSE está configurado y en uso: `storage encryption disk show`
   - Si el resultado del comando incluye los detalles de la unidad con información sobre el modo y el identificador de clave, NSE se configura y es necesario verificar la configuración de NSE y en uso.
   - Si no se muestra ningún disco, NSE no está configurado.
   - Si NVE y NSE no están configurados, no hay unidades protegidas con las claves NSE, es seguro apagar la controladora dañada.

Verifique la configuración de NVE

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves: `security key-manager key query`

   > Después de la versión ONTAP 9.6, es posible que tenga otros tipos de gestor de claves. Los tipos son `KMIP`, `AKV`, y. `GCP`. El proceso de confirmación de estos tipos es el mismo que el de confirmación `external` o. `onboard` tipos de gestor de claves.

   - Si la `Key Manager` aparece el tipo `external` y la `Restored` la columna muestra `yes`, es seguro apagar el controlador dañado.
   - Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, necesita completar algunos pasos adicionales.
   - Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.
   - Si la `Key Manager` aparece el tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.

2. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, Realizar una copia de seguridad manual de la información de OKM:
   a. Vaya al modo de privilegios avanzado e 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. Volver al modo admin: `set -priv admin`
   e. Apague el controlador dañado.
3. Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
   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.

   "mysupport.netapp.com"
   a. Compruebe que el `Restored` la columna es igual `yes` para todas las claves de autenticación: `security key-manager key query`
   b. Apague el controlador dañado.
4. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
   a. Introduzca el comando SYNC del gestor de claves de seguridad incorporado: `security key-manager onboard sync`

      Introduzca 32 la clave de acceso de gestión de claves incorporada y alfanumérica del cliente en el símbolo del sistema. Si no se puede proporcionar la clave de acceso, comuníquese con el soporte de NetApp. "mysupport.netapp.com"
   b. Compruebe el `Restored` la columna muestra `yes` para todas las claves de autenticación: `security key-manager key query`
   c. Compruebe que el `Key Manager` el tipo muestra `onboard`, Y a continuación, realice una copia de seguridad manual de la información de OKM.
   d. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
   e. Introduzca el comando para mostrar la información de backup para la gestión de claves: `security key-manager onboard show-backup`
   f. Copie el contenido de la información de la copia de seguridad en un archivo o archivo de registro separados. Lo necesitará en escenarios de desastres donde podría necesitar una recuperación manual de OKM.
   g. Volver al modo admin: `set -priv admin`

h. Puede apagar el controlador de forma segura.

Verifique la configuración de NSE

1. Muestre los ID de claves de las claves de autenticación que se almacenan en los servidores de gestión de claves: `security key-manager key query -key-type NSE-AK`

   Después de la versión ONTAP 9.6, es posible que tenga otros tipos de gestor de claves. Los tipos son `KMIP`, `AKV`, y. `GCP`. El proceso de confirmación de estos tipos es el mismo que el de confirmación `external` o. `onboard` tipos de gestor de claves.

   - Si la `Key Manager` aparece el tipo `external` y la `Restored` la columna muestra `yes`, es seguro apagar el controlador dañado.
   - Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, necesita completar algunos pasos adicionales.
   - Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.
   - Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`, necesita completar algunos pasos adicionales.

2. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` la columna muestra `yes`, Realizar una copia de seguridad manual de la información de OKM:
   a. Vaya al modo de privilegios avanzado e 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. Volver al modo admin: `set -priv admin`
   e. Puede apagar el controlador de forma segura.
3. Si la `Key Manager` aparece el tipo `external` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:
   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.

   "mysupport.netapp.com"

   a. Compruebe que el `Restored` la columna es igual `yes` para todas las claves de autenticación: `security key-manager key query`
   b. Puede apagar el controlador de forma segura.
4. Si la `Key Manager` aparece el tipo `onboard` y la `Restored` columna muestra cualquier otra cosa que no sea `yes`:

a. Introduzca el comando SYNC del gestor de claves de seguridad incorporado: `security key-manager onboard sync`

   Introduzca 32 la clave de acceso de gestión de claves incorporada y alfanumérica del cliente en el símbolo del sistema. Si no se puede proporcionar la clave de acceso, comuníquese con el soporte de NetApp.

"mysupport.netapp.com"

a. Compruebe el `Restored` la columna muestra `yes` para todas las claves de autenticación: `security key-manager key query`
b. Compruebe que el `Key Manager` el tipo muestra `onboard`, Y a continuación, realice una copia de seguridad manual de la información de OKM.
c. Vaya al modo de privilegios avanzado e introduzca `y` cuando se le solicite continuar: `set -priv advanced`
d. Introduzca el comando para mostrar la información de backup para la 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. Volver al modo admin: `set -priv admin`
g. Puede apagar el controlador de forma segura.

Apague el controlador defectuoso: ASA A900

Apague o retome el controlador dañado siguiendo el procedimiento adecuado para su configuración.

Mayoría de configuraciones

Después de completar las tareas de NVE o NSE, deberá completar el apagado 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`.

La controladora se encuentra en un MetroCluster

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

No use este procedimiento si el sistema está en una configuración de MetroCluster de dos nodos.

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.

- 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".
- Si tiene una configuración MetroCluster, debe haber confirmado que el estado de configuración de MetroCluster está configurado y que los nodos están en estado normal y habilitado (`metrocluster node show`).

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=number_of_hours_downh`

   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`
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 (introduzca la contraseña del sistema)	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 A900

Debe quitar y abrir el módulo de la controladora, localizar y sustituir los medios de arranque en la controladora y, a continuación, transferir la imagen al medio de arranque

de reemplazo.

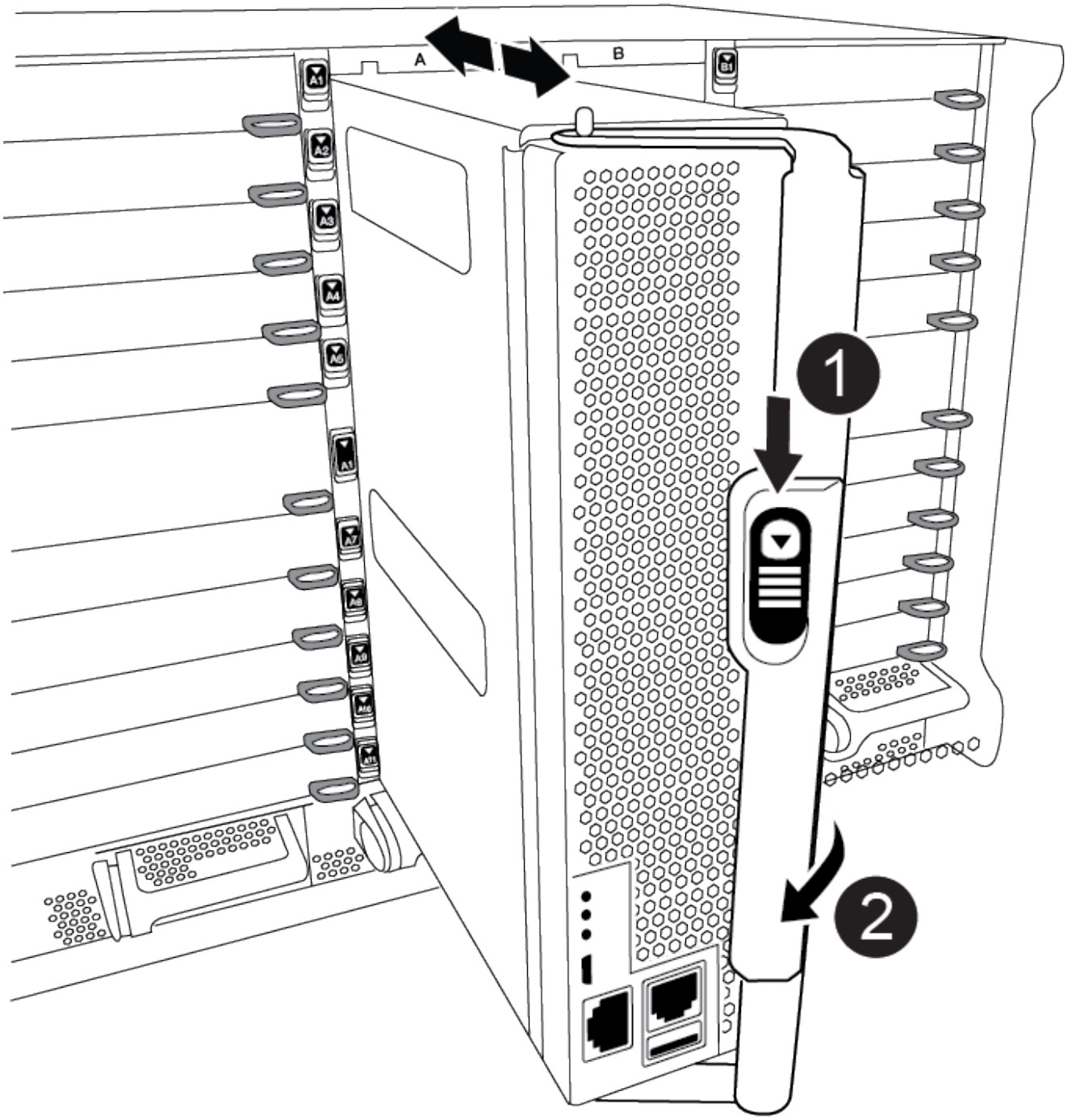
Paso 1: Extraiga el módulo del controlador

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

Pasos

1. Si usted no está ya conectado a tierra, correctamente tierra usted mismo.
2. Desenchufe los cables del módulo del controlador dañado y haga un seguimiento de dónde se conectaron los cables.
3. Deslice el botón terra cotta del asa de la leva hacia abajo hasta que se desbloquee.

   Animación: Retire el controlador



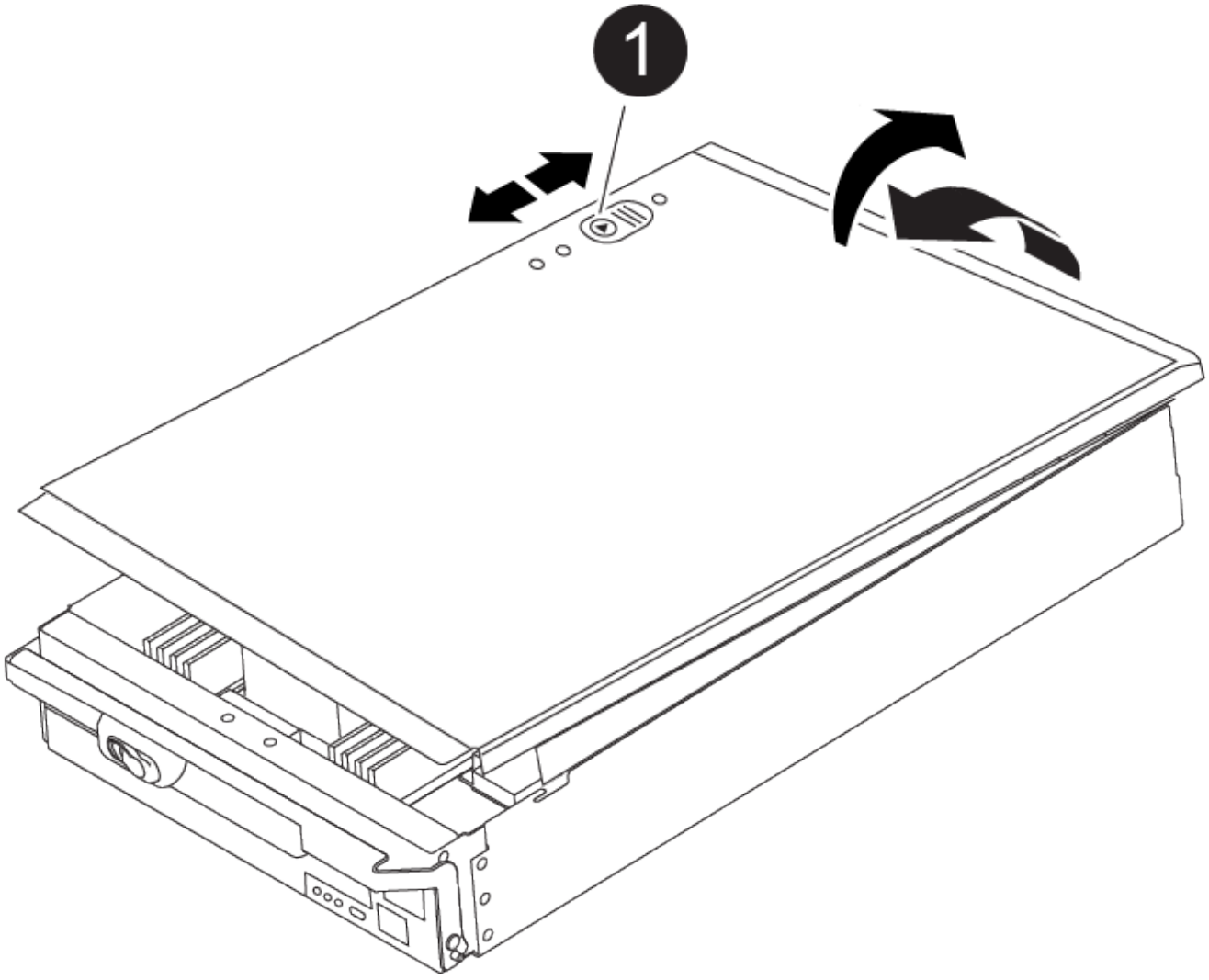
1	Botón de liberación de la palanca de leva
2	Mango de leva

4. Gire el asa de leva para que desacople completamente el módulo del controlador del chasis y, a continuación, deslice el módulo del controlador para sacarlo del chasis.

   Asegúrese de que admite la parte inferior del módulo de la controladora cuando la deslice para sacarlo del

chasis.

5. Coloque el lado de la tapa del módulo del controlador hacia arriba sobre una superficie plana y estable, pulse el botón azul de la cubierta, deslice la cubierta hacia la parte posterior del módulo del controlador y, a continuación, gire la cubierta hacia arriba y levántela fuera del módulo del controlador.



1	Botón de bloqueo de la cubierta del módulo del controlador

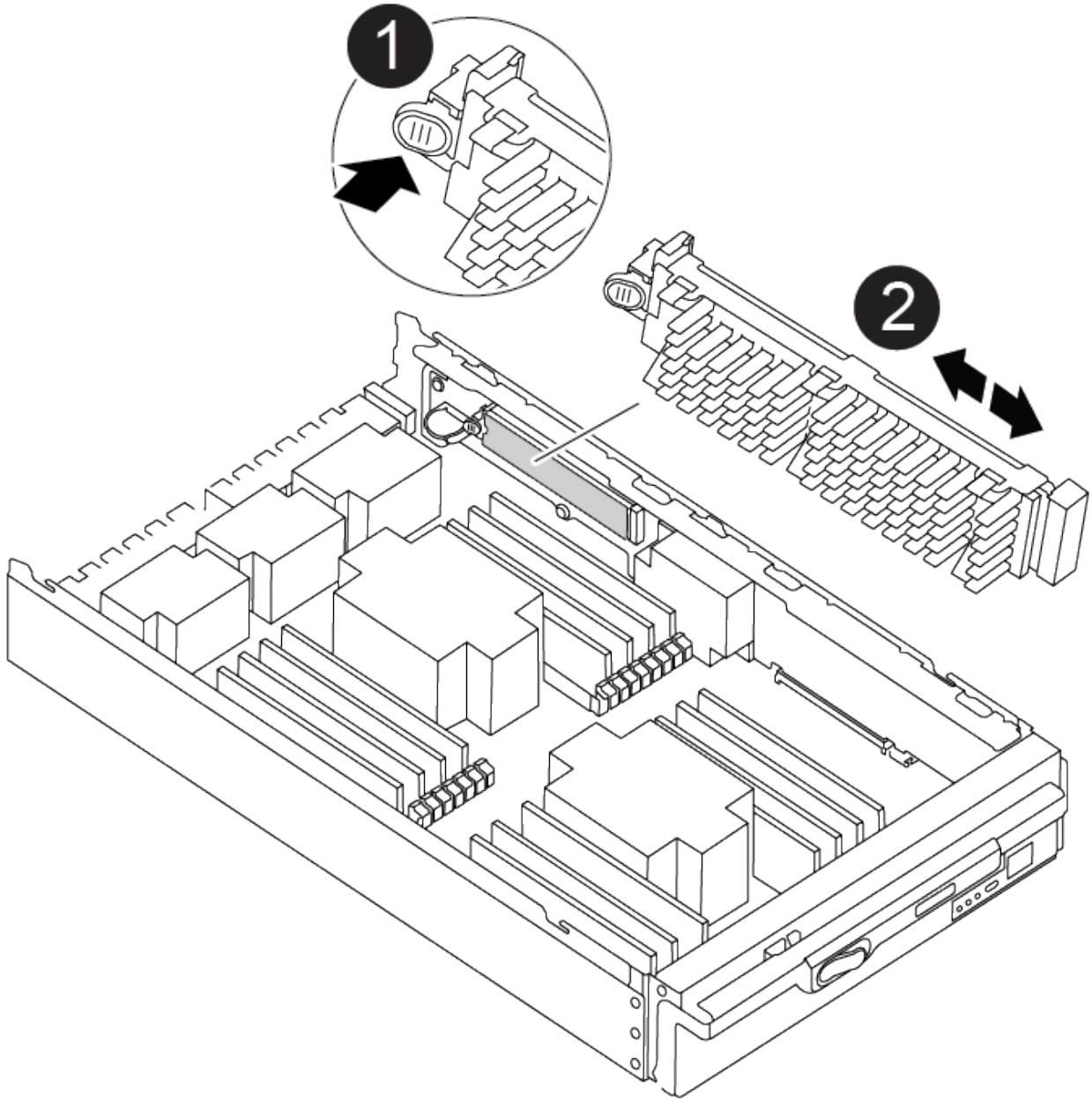
Paso 2: Sustituya el soporte de arranque

Debe localizar el soporte de arranque en la controladora y seguir las instrucciones para su reemplazo.

Pasos

1. Levante el conducto de aire negro situado en la parte posterior del módulo del controlador y, a continuación, localice el soporte del maletero mediante la siguiente ilustración o el mapa de FRU en el módulo del controlador:

   Animación: Reemplace el soporte de arranque



1	Presione la lengüeta de liberación
2	Soporte de arranque

2. Pulse el botón azul de la carcasa del soporte de arranque para liberar el soporte de arranque de su carcasa y, a continuación, tire suavemente de él hacia fuera del zócalo del soporte de arranque.

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

3. Alinee los bordes del soporte de arranque de repuesto con el zócalo del soporte de arranque y, a continuación, empújelo suavemente en el zócalo.
4. Compruebe el soporte del maletero para asegurarse de que está asentado completamente en la toma.

Si es necesario, extraiga el soporte de arranque y vuelva a colocarlo en la toma.

5. Empuje el soporte del maletero hacia abajo para activar el botón de bloqueo en la carcasa del soporte del maletero.
6. Vuelva a instalar la tapa del módulo del controlador alineando los pasadores de la tapa con las ranuras del soporte de la placa base y, a continuación, deslice la tapa en su lugar.

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

Puede instalar la imagen del sistema en el soporte de arranque de repuesto mediante una unidad flash USB con la imagen instalada en ella. No obstante, debe restaurar el sistema de archivos var durante este procedimiento.

Antes de empezar

- Debe tener una unidad flash USB, formateada con FAT32, con una capacidad mínima de 4 GB.
- Una copia de la misma versión de imagen de ONTAP que la controladora dañada en funcionamiento. Puede descargar la imagen adecuada en la sección Descargas del sitio de soporte de NetApp
  - Si NVE está habilitado, descargue la imagen con el cifrado de volúmenes de NetApp, como se indica en el botón de descarga.
  - Si el cifrado de volúmenes de NetApp no está habilitado, descargue la imagen sin el cifrado de volúmenes de NetApp, como se indica en el botón de descarga.
- Si el sistema es independiente, no necesita una conexión de red, pero debe realizar un reinicio adicional al restaurar el sistema de archivos var.

Pasos

1. Alinee el extremo del módulo del controlador con la abertura del chasis y, a continuación, empuje suavemente el módulo del controlador hasta la mitad del sistema.
2. Recuperar el módulo del controlador, según sea necesario.
3. Inserte la unidad flash USB en la ranura USB del módulo de controlador.

   Asegúrese de instalar la unidad flash USB en la ranura indicada para dispositivos USB, y no en el puerto de consola USB.

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

   La controladora comienza a arrancar en cuanto se ha instalado por completo en el chasis.

5. Interrumpa el proceso de arranque para que se detenga en el símbolo del SISTEMA DEL CARGADOR pulsando Ctrl-C cuando vea iniciando AUTOBOOT, pulse Ctrl-C para cancelar….

   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.

6. Configure el tipo de conexión de red en el símbolo del sistema del CARGADOR:

   - Si va a configurar DHCP: `ifconfig e0a -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 e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`
  - 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.
  - dns_addr es la dirección IP de un servidor de nombres de la red.
  - dns_Domain es el nombre de dominio del sistema de nombres de dominio (DNS).

    Si utiliza este parámetro opcional, no necesita un nombre de dominio completo en la URL del servidor para reiniciar el sistema. Solo necesita el nombre de host del servidor.

> 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.

7. Si la controladora está en una MetroCluster con ampliación o conexión a la estructura, debe restaurar la configuración del adaptador de FC:
   a. Arranque en modo de mantenimiento: `boot_ontap maint`
   b. Establezca los puertos MetroCluster como iniciadores: `ucadmin modify -m fc -t iniitator adapter_name`
   c. Detener para volver al modo de mantenimiento: `halt`

   Los cambios se implementarán al arrancar el sistema.

Inicie la imagen de recuperación - ASA A900

Debe arrancar la imagen de ONTAP desde la unidad USB, restaurar el sistema de archivos y verificar las variables del entorno.

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

   La imagen se descarga desde la unidad flash USB.

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

Si el sistema tiene…	Realice lo siguiente…
Una conexión de red	a. Pulse `y` cuando se le solicite que restaure la configuración de copia de seguridad. b. Pulse `y` cuando se le solicite sobrescribir `/etc/ssh/ssh_host_ecdsa_key`. c. Pulse `y` cuando se le solicite que confirme si la copia de seguridad de la restauración se realizó correctamente. d. Pulse `Y` cuando se le solicite la copia de configuración restaurada. e. Configure la controladora dañada al nivel de privilegio avanzado: `set -privilege advanced` f. Ejecute el comando restore backup: `system node restore-backup -node local -target-address impaired_node_IP_address` g. Devuelva la controladora dañada al nivel admin: `set -privilege admin` h. Pulse `y` cuando se le solicite que utilice la configuración restaurada. i. Pulse `y` cuando se le solicite reiniciar la controladora dañada.
No hay conexión de red	a. Pulse `n` cuando se le solicite que restaure la configuración de copia de seguridad. b. Reinicie el sistema cuando el sistema lo solicite. c. Seleccione la opción **Actualizar flash desde la configuración de copia de seguridad** (flash de sincronización) en el menú que se muestra. Si se le solicita que continúe con la actualización, pulse `y`.

Si el sistema tiene…	Realice lo siguiente…

No hay conexión de red y está en una configuración de IP de MetroCluster	a. Pulse `n` cuando se le solicite que restaure la configuración de copia de seguridad.
	b. Reinicie el sistema cuando el sistema lo solicite.
	c. Espere a que se conecten las conexiones de almacenamiento iSCSI.
	
	Puede continuar después de ver los siguientes mensajes:
	
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`
	
	d. Seleccione la opción **Actualizar flash desde la configuración de copia de seguridad** (flash de sincronización) en el menú que se muestra.
	
	Si se le solicita que continúe con la actualización, pulse `y`.

4. Asegurarse de que las variables medioambientales estén establecidas de la manera esperada:
   a. Lleve la controladora dañada al aviso DEL CARGADOR.
   b. Compruebe la configuración de la variable de entorno con el comando printenv.
   c. Si una variable de entorno no está establecida como se espera, modifíquela con el `setenv` *`environment_variable_name changed_value`* comando.
   d. Guarde los cambios con el comando saveenv.
5. El siguiente depende de la configuración del sistema:

- Si su sistema tiene configurado el gestor de claves incorporado, NSE o NVE, vaya a. Pasos de sustitución de medios posteriores al arranque para OKM, NSE y NVE
- Si su sistema no tiene configurado el gestor de claves incorporado, NSE o NVE, complete los pasos en esta sección.

6. Desde el aviso DEL CARGADOR, introduzca el comando boot_ontap.

Si ve…	Realice lo siguiente…
La solicitud de inicio de sesión de	Vaya al siguiente paso.
Esperando devolución…	a. Inicie sesión en el controlador asociado. b. Confirme que el destino está listo para la devolución con el `storage failover show` comando.

7. Conecte el cable de la consola al controlador asociado.
8. Dé vuelta a la controladora con el comando de recuperación tras fallos del almacenamiento -fromnode local.
9. En el símbolo del sistema del clúster, compruebe las interfaces lógicas con el comando net int -is-home false.

   Si alguna de las interfaces se muestra como "false", vuelva a revertir dichas interfaces a su puerto de inicio utilizando el comando net int revert.

10. Mueva el cable de la consola al apagado reparado o retome el controlador dañado siguiendo el procedimiento adecuado para su configuración. Y ejecute el comando version -v para comprobar las versiones de ONTAP.
11. Restaure la devolución automática si la deshabilitó con el comando Storage Failover modify -node local -auto-giveback true.

Pasos de sustitución de medios posteriores al arranque para OKM, NSE y NVE: ASA A900

Una vez comprobadas las variables de entorno, debe completar los pasos específicos para restaurar su gestor de claves incorporado (OKM), el cifrado del almacenamiento de NetApp (NSE) y el cifrado de volúmenes de NetApp (NVE).

Determine qué sección debe usar para restaurar sus configuraciones de OKM, NSE o NVE: Si NSE o NVE están habilitados junto con el gestor de claves incorporado debe restaurar la configuración capturada al principio de este procedimiento.

- Si NSE o NVE están habilitados y el gestor de claves incorporado está habilitado, vaya a. Restaure NVE o NSE cuando el gestor de claves incorporado está habilitado.
- Si NSE o NVE están habilitados para ONTAP 9.6, vaya a. Restaure NSE/NVE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores.

Restaure NVE o NSE cuando el gestor de claves incorporado está habilitado

Pasos

1. Conecte el cable de consola a la controladora de destino.
2. Utilice el comando boot_ontap en el símbolo del sistema DEL CARGADOR para arrancar la controladora.
3. Compruebe la salida de la consola:

Si la consola muestra…	Realice lo siguiente…
El aviso del CARGADOR	Arranque el controlador en el menú de arranque: `boot_ontap menu`
Esperando devolución	a. Introduzca `Ctrl-C` en el prompt de b. En el mensaje: ¿Desea detener este nodo en lugar de esperar [y/n]? , introduzca: `y` c. En el aviso del CARGADOR, introduzca el `boot_ontap menu` comando.

4. En Boot Menu (Menú de inicio), introduzca el comando oculto, `recover_onboard_keymanager`, y conteste `y` en el prompt de.
5. Introduzca la frase de acceso para el administrador de claves incorporado que haya obtenido del cliente al principio de este procedimiento.
6. Cuando se le solicite que introduzca los datos de copia de seguridad, pegue los datos de copia de seguridad que capturó al principio de esta sección, cuando se le solicite. Pegue la salida de `security key-manager backup show` O. `security key-manager onboard show-backup` comando.

   Los datos se emiten desde cualquiera de los dos `security key-manager backup show` o el comando «show-backup» de la gestión de claves de seguridad integrada.

   Ejemplo de datos de backup:

   Introduzca los datos de backup:

   ```
   ---------- COMIENCE COPIA DE SEGURIDAD----------
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA3AAAAAAAAAAAAAAAAAYAYAY
   AYAYAYAYAYAYAYAYAYAYZYAYAYAYAYAYZYAYAYAYAYAYAYAYAYAYAYAYAYAYAYA
   YAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAY
   AYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAYAY . . .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

   ---------- BACKUP FINAL----------
   ```

7. En Boot Menu (Menú de inicio), seleccione la opción para el inicio normal.

   El sistema arranca esperando la devolución… prompt.

8. Mueva el cable de la consola a la controladora correspondiente e inicie sesión como administrador.
9. Confirme que la controladora de destino está lista para la devolución con el `storage failover show` comando.
10. Entorno sólo los agregados del director financiero con la `storage failover giveback -fromnode local -only-cfo-aggregates true` comando.
    - 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 debido a una sesión CIFS abierta, compruebe con el cliente cómo se cierran las sesiones CIFS.

      Los terminación CIFS pueden provocar la pérdida de datos.

    - Si el comando falla porque el asociado "no está listo", espere 5 minutos para que los NVRAMS se sincronicen.
    - Si se produce un error en el comando debido a un proceso de NDMP, SnapMirror o SnapVault, deshabilite el proceso. Consulte el contenido adecuado para obtener más información.
11. Una vez que se haya completado la devolución, compruebe el estado de la conmutación al nodo de respaldo y la devolución con el `storage failover show` y.. `storage failover show-giveback` comandos.

    Solo se mostrarán los agregados CFO (agregados raíz y datos en estilo CFO).

12. Si ejecuta ONTAP 9.6 o una versión posterior, ejecute la sincronización integrada del gestor de claves de seguridad:
    a. Ejecute el `security key-manager onboard sync` y, a continuación, introduzca la frase de acceso cuando se le solicite.
    b. Introduzca el `security key-manager key-query` comando para ver una vista detallada de todas las claves almacenadas en el gestor de claves incorporado y verificar que el `Restored` columna = `yes/true` para todas las claves de autenticación.

       Si la `Restored` columna = cualquier otra cosa que no sea `yes/true`, Póngase en contacto con el servicio de atención al cliente

    c. Espere 10 minutos hasta que la clave se sincronice en el clúster.
13. Mueva el cable de la consola al controlador correspondiente.
14. Proporcione a la controladora objetivo mediante el `storage failover giveback -fromnode local` comando.
15. Compruebe el estado de devolución, tres minutos después de que haya completado el informe, utilizando la `storage failover show` comando.

    Si la devolución no está completa tras 20 minutos, póngase en contacto con el soporte de cliente.

16. En el símbolo del sistema clustershell, introduzca el comando net int show -is-home false para enumerar las interfaces lógicas que no están en su controlador y puerto de casa.

    Si alguna interfaz aparece como `false`, vuelva a revertir estas interfaces a su puerto de inicio mediante el `net int revert -vserver Cluster -lif` *`nodename`* comando.

17. Mueva el cable de la consola a la controladora de destino y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.
18. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

Restaure NSE/NVE en sistemas que ejecutan ONTAP 9.6 y versiones posteriores

Pasos

1. Conecte el cable de consola a la controladora de destino.
2. Utilice el comando boot_ontap en el símbolo del sistema DEL CARGADOR para arrancar la controladora.
3. Compruebe la salida de la consola:

Si la consola muestra…	Realice lo siguiente…
La solicitud de inicio de sesión de	Vaya al paso 7.
Esperando devolución…	a. Inicie sesión en el controlador asociado. b. Confirme que la controladora de destino está lista para la devolución con el `storage failover show` comando.

4. Mueva el cable de la consola a la controladora del partner y rebase el almacenamiento de la controladora de destino mediante el comando local de recuperación tras fallos del almacenamiento -fromnode -only-cfo -agents true local.
   - 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 debido a una sesión CIFS abierta, compruebe con el cliente cómo cerrar sesiones CIFS.

     Los terminación CIFS pueden provocar la pérdida de datos.

   - Si el comando falla porque el partner está "no listo", espere 5 minutos para que los NVMems se sincronicen.
   - Si se produce un error en el comando debido a un proceso de NDMP, SnapMirror o SnapVault, deshabilite el proceso. Consulte el contenido adecuado para obtener más información.
5. Espere 3 minutos y compruebe el estado de la conmutación al respaldo con el comando Storage Failover show.
6. En el símbolo del sistema clustershell, introduzca el `net int show -is-home false` comando para mostrar las interfaces lógicas que no están en su controladora y puerto de inicio.

   Si alguna interfaz aparece como `false`, vuelva a revertir estas interfaces a su puerto de inicio mediante el `net int revert -vserver Cluster -lif` *nodename* comando.

7. Mueva el cable de la consola a la controladora de destino y ejecute el `version -v` Comando para comprobar las versiones de ONTAP.
8. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

9. Utilice la `storage encryption disk show` en el símbolo del sistema clustershell, para revisar el resultado.
10. Utilice la `security key-manager key-query` comando para mostrar las claves de cifrado y 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 la `Key Manager type` = `external` y la `Restored` columna = cualquier otra cosa que no sea `yes/true`, utilice la `security key-manager external restore` Comando para restaurar los ID de claves de las claves de autenticación.

      Si el comando falla, póngase en contacto con el servicio de atención al cliente.

    - Si la `Key Manager type` = `onboard` y la `Restored` columna = cualquier otra cosa que no sea `yes/true`, utilice la `security key-manager onboard sync` Comando para volver a sincronizar el tipo de gestor de claves.

      Utilice la `security key-manager key-query` para comprobar que el `Restored` columna = `yes/true` para todas las claves de autenticación.
11. Conecte el cable de la consola al controlador asociado.
12. Dé vuelta a la controladora con el comando de recuperación tras fallos del almacenamiento -fromnode local.
13. Restaure la devolución automática si la ha desactivado mediante el `storage failover modify -node local -auto-giveback true` comando.

Devuelva la pieza fallida a NetApp - ASA A900

Devuelva la pieza que ha fallado a NetApp, como se describe en las instrucciones de RMA que se suministran con el kit. Consulte "Retorno de artículo sustituciones" para obtener más información.