



## **Etapas 6. Arranque node2 con los módulos del sistema de sustitución**

Upgrade controllers

NetApp

February 22, 2024

# Tabla de contenidos

- Etapa 6. Arranque node2 con los módulos del sistema de sustitución . . . . . 1
  - Descripción general . . . . . 1
  - Arranque node2 con los módulos del sistema de sustitución . . . . . 1
  - Compruebe la instalación del nodo 2. . . . . 6
  - Restaurar la configuración de gestor de claves en el nodo 2 . . . . . 10
  - Vuelva a colocar los agregados que no son raíz y las LIF de datos NAS en el nodo 2. . . . . 10

# Etapa 6. Arranque node2 con los módulos del sistema de sustitución

## Descripción general

Durante la etapa 6, se inicia node2 con módulos de sistema actualizados y se verifica la instalación node2 actualizada. Si utiliza el cifrado de volúmenes de NetApp (NVE), debe restaurar la configuración del gestor de claves. También puede reubicar agregados que no sean raíz y LIF de datos NAS del nodo 1 al nodo 2 actualizado y verificar que las LIF DE SAN existan en el nodo 2.

1. ["Arranque node2 con los módulos del sistema de sustitución"](#)
2. ["Compruebe la instalación del nodo 2"](#)
3. ["Restaure la configuración de gestor de claves en el nodo 2"](#)
4. ["Vuelva a colocar los agregados que no son raíz y las LIF de datos NAS en el nodo 2"](#)

## Arranque node2 con los módulos del sistema de sustitución

node2 con los módulos de reemplazo está ahora listo para arrancar. La actualización mediante el intercambio de los módulos del sistema implica mover únicamente las conexiones de la consola y de gestión. Esta sección proporciona los pasos necesarios para arrancar node2 con los módulos de reemplazo para las siguientes configuraciones de actualización:

Controlador node2 antiguo	Sustitución de los módulos del sistema node2
AFF A220 configurado como ASA	Módulo de controlador ASA A150
AFF A220 AFF A200 C190 de AFF	Módulo de controlador AFF A150
FAS2620 FAS2720	Módulo del controlador FAS2820
AFF A700 configurado como ASA	Controladora ASA A900 y módulos NVRAM
AFF A700	Controladora AFF A900 y módulos NVRAM
FAS9000	Controladora FAS9500 y módulos NVRAM

### Pasos

1. Si tiene unidades de cifrado del almacenamiento de NetApp (NSE) instaladas, siga los pasos siguientes.



Si aún no lo ha hecho anteriormente en el procedimiento, consulte el artículo de la base de conocimientos ["Cómo saber si una unidad tiene la certificación FIPS"](#) para determinar el tipo de unidades de autocifrado que están en uso.

a. Configurado `bootarg.storageencryption.support` para `true` o `false`:

Si están en uso las siguientes unidades...	Entonces...
Unidades NSE que cumplen con los requisitos de autocifrado de FIPS 140-2 de nivel 2	<code>setenv bootarg.storageencryption.support true</code>
SED de NetApp no con FIPS	<code>setenv bootarg.storageencryption.support false</code>



No es posible mezclar unidades FIPS con otros tipos de unidades en el mismo nodo o la pareja de alta disponibilidad. Puede mezclar unidades de cifrado distinto de SED en el mismo nodo o par de alta disponibilidad.

b. Vaya al menú de inicio especial y seleccione la opción (10) Set Onboard Key Manager recovery secrets.

Introduzca la frase de acceso y la información de copia de seguridad registrada anteriormente. Consulte "[Gestione el cifrado del almacenamiento con el gestor de claves incorporado](#)".

2. Arranque el nodo en el menú de arranque:

```
boot_ontap menu
```

3. Para reasignar los discos antiguos de node2 al node2 de reemplazo, introduzca «22/7» y seleccione la opción oculta `boot_after_controller_replacement` cuando el nodo se detiene en el menú de arranque.

Tras un breve retraso, se le pedirá que introduzca el nombre del nodo que se va a reemplazar. Si hay discos compartidos (también llamados Advanced Disk Partitioning (ADP) o discos con particiones), se le pedirá que introduzca el nombre del nodo del compañero de alta disponibilidad.

Estos mensajes pueden aparecer ocultos en los mensajes de la consola. Si no introduce un nombre de nodo o introduce un nombre incorrecto, se le pedirá que vuelva a introducir el nombre.



Si `[localhost:disk.encryptNoSupport:ALERT]: Detected FIPS-certified encrypting drive y,` o `[localhost:diskown.errorDuringIO:error]: error 3 (disk failed)` on disk se producen errores, realice los pasos siguientes:

- Detenga el nodo en el símbolo del sistema del CARGADOR.
- Compruebe y restablezca los bootargs de cifrado de almacenamiento mencionados en [Paso 1](#).
- En el símbolo del sistema del cargador, arranque:

```
boot_ontap
```

Puede utilizar el siguiente ejemplo como referencia:

## Expanda el ejemplo de salida de consola

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*****
*                                     *
* Press Ctrl-C for Boot Menu. *
*                                     *
*****
.
<output truncated>
.
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)? 22/7

(22/7)                                Print this secret List
(25/6)                                Force boot with multiple filesystem
disks missing.
(25/7)                                Boot w/ disk labels forced to clean.
(29/7)                                Bypass media errors.
(44/4a)                               Zero disks if needed and create new
flexible root volume.
(44/7)                                Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                          Clean all configuration on boot
```

```

device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)          Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.

```

The boot device has changed. System configuration information could be lost. Use option (6) to restore the system configuration, or option (4) to initialize all disks and setup a new system. Normal Boot is prohibited.

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)? boot_after_controller_replacement

```

This will replace all flash-based configuration with the last backup to disks. Are you sure you want to continue?: yes

```

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id

```

```

= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.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: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...

.
System rebooting...

.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
.
Login:

```



Los ID del sistema que se muestran en el ejemplo anterior son ID de ejemplo. Los ID reales del sistema de los nodos que va a actualizar serán diferentes.

Entre introducir nombres de nodo en la solicitud de entrada y la solicitud de inicio de sesión, el nodo se reinicia unas cuantas veces para restaurar las variables de entorno, actualizar el firmware en las tarjetas del sistema y para otras actualizaciones de ONTAP.

## Compruebe la instalación del nodo 2

Debe verificar la instalación de node2 con los módulos del sistema de reemplazo. Como no hay ningún cambio en los puertos físicos, no es necesario asignar los puertos físicos del nodo 2 antiguo al nodo 2 de reemplazo.

### Acerca de esta tarea

Después de arrancar node1 con el módulo del sistema de reemplazo, compruebe que está instalado correctamente. Debe esperar a que el nodo 2 se una al quórum y reanudar la operación de reemplazo de la controladora.

En este punto del procedimiento, la operación se detiene mientras el nodo 2 se une al quórum.

### Pasos

1. Verifique que el nodo 2 esté Unido al quórum:

```
cluster show -node node2 -fields health
```

El resultado del `health` el campo debe ser `true`.

2. Compruebe que el nodo 2 forme parte del mismo clúster que el nodo 1 y que esté en buen estado:

```
cluster show
```

3. Cambie al modo de privilegio avanzado:

```
set advanced
```

4. Compruebe el estado de la operación de reemplazo de la controladora y compruebe que esté en pausa y que esté en el mismo estado que antes de detener el nodo 2 para realizar las tareas físicas de instalación de nuevas controladoras y mover cables:

```
system controller replace show
```

```
system controller replace show-details
```

5. Reanude la operación de sustitución de la controladora:

```
system controller replace resume
```

6. La operación de reemplazo de la controladora se detiene para intervención con el siguiente mensaje:



```
Cluster::*> system controller replace show
```

Node	Status	Error-Action
Node2	Paused-for-intervention	Follow the instructions given in
Node1	None	Step Details

Step Details:

-----

To complete the Network Reachability task, the ONTAP network configuration must be manually adjusted to match the new physical network configuration of the hardware. This includes:

1. Re-create the interface group, if needed, before restoring VLANs. For detailed commands and instructions, refer to the "Re-creating VLANs, ifgrps, and broadcast domains" section of the upgrade controller hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-replacement network displaced-vlans restore" to restore the VLAN on the desired port.

2 entries were displayed.



En este procedimiento, la sección *Re-creating VLAN, ifgrps y dominios de difusión* se ha cambiado el nombre *Restore network Configuration on 2*.

7. Con el reemplazo de la controladora en estado de pausa, continúe a. [Restaurar la configuración de red en el nodo 2](#).

## Restaurar la configuración de red en el nodo 2

Después de confirmar que el nodo 2 tiene quórum y puede comunicarse con el nodo 1, compruebe que las VLAN del nodo 1, los grupos de interfaces y los dominios de retransmisión estén en el nodo 2. Además, verifique que todos los puertos de red 2 estén configurados en sus dominios de retransmisión correctos.

### Acerca de esta tarea

Para obtener más información sobre la creación y recreación de VLAN, grupos de interfaces y dominios de retransmisión, consulte ["Referencias"](#) Para vincular al contenido de *Network Management*.

### Pasos

1. Enumera todos los puertos físicos en el nodo 2 actualizado:

```
network port show -node node2
```

Se muestran todos los puertos de red física, los puertos VLAN y los puertos del grupo de interfaces en el nodo. A partir de esta salida, puede ver los puertos físicos que se han movido al `Cluster` Dominio de difusión por ONTAP. Puede usar esta salida para decidir qué puertos se deben usar como puertos miembro de grupo de interfaces, puertos base de VLAN o puertos físicos independientes para alojar LIF.

2. Enumere los dominios de retransmisión del clúster:

```
network port broadcast-domain show
```

3. Enumerar la posibilidad de cambio de puerto de red de todos los puertos en el nodo 2:

```
network port reachability show -node node2
```

Debería ver un resultado similar al siguiente ejemplo. Los nombres del puerto y de la difusión varían.

```
Cluster::*> network port reachability show -node local
Node      Port      Expected Reachability      Reachability
Status
-----
Node2
      e0M      Default:Mgmt      no-reachability
      e10a      Default:Default-3      ok
      e10b      Default:Default-4      ok
      e11a      Cluster:Cluster      no-reachability
      e11b      Cluster:Cluster      no-reachability
      e11c      -      no-reachability
      e11d      -      no-reachability
      e2a      Default:Default-1      ok
      e2b      Default:Default-2      ok
      e9a      Default:Default      no-reachability
      e9b      Default:Default      no-reachability
      e9c      Default:Default      no-reachability
      e9d      Default:Default      no-reachability
13 entries were displayed.
```

En el ejemplo anterior, el nodo 2 arranca y se unió al quórum después del reemplazo de la controladora. Tiene varios puertos que no tienen accesibilidad y están pendientes de un análisis de accesibilidad.

4. repare la accesibilidad de cada uno de los puertos del nodo 2 con un estado de accesibilidad distinto de `ok` utilizando el siguiente comando, en el siguiente orden:

```
network port reachability repair -node node_name -port port_name
```

- a. Puertos físicos
- b. Puertos VLAN

Debería ver un resultado como el siguiente ejemplo:

```
Cluster ::> reachability repair -node node2 -port e9d
```

```
Warning: Repairing port "node2:e9d" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

Se espera un mensaje de advertencia, como se muestra en el ejemplo anterior, para los puertos con un estado de accesibilidad que puede ser diferente del estado de accesibilidad del dominio de difusión en el que se encuentra actualmente. Revise la conectividad del puerto y la respuesta `y` o `n` según corresponda.

Verifique que todos los puertos físicos tengan la habilidad esperada:

```
network port reachability show
```

A medida que se realiza la reparación de accesibilidad, ONTAP intenta colocar los puertos en los dominios de retransmisión correctos. Sin embargo, si no se puede determinar la accesibilidad de un puerto y no pertenece a ninguno de los dominios de difusión existentes, ONTAP creará nuevos dominios de difusión para estos puertos.

5. Compruebe la accesibilidad del puerto:

```
network port reachability show
```

Cuando todos los puertos se configuran y se añaden correctamente a los dominios de retransmisión correctos, el `network port reachability show` el comando debería informar el estado de la accesibilidad como `ok` para todos los puertos conectados y el estado como `no-reachability` para puertos sin conectividad física. Si algún puerto informa de un estado distinto a estos dos, realice la reparación de accesibilidad y añada o quite puertos de sus dominios de retransmisión como se indica en [Paso 4](#).

6. Compruebe que todos los puertos se han colocado en dominios de retransmisión:

```
network port show
```

7. Compruebe que todos los puertos de los dominios de retransmisión tengan la unidad de transmisión máxima (MTU) correcta configurada:

```
network port broadcast-domain show
```

8. Restaure los puertos iniciales de LIF, especificando los puertos iniciales de Vserver y LIF, si los hay, que deben restaurarse mediante los siguientes pasos:

a. Enumere las LIF que están desplazadas:

```
displaced-interface show
```

b. Restaure los nodos de inicio de LIF y sus puertos iniciales:

```
displaced-interface restore-home-node -node node_name -vserver vserver_name
-lif-name LIF_name
```

9. Verifique que todas las LIF tienen un puerto doméstico y que están administrativamente más arriba:

```
network interface show -fields home-port,status-admin
```

## Restaurar la configuración de gestor de claves en el nodo 2

Si utiliza el cifrado de agregados de NetApp (NAE) o el cifrado de volúmenes de NetApp (NVE) para cifrar volúmenes en el sistema que desea actualizar, la configuración de cifrado debe sincronizarse con los nodos nuevos. Si no vuelve a sincronizar el gestor de claves, cuando se reinstalan los agregados del nodo 2 actualizados al nodo 2 actualizado mediante ARL, pueden producirse fallos, ya que el nodo 2 no tiene las claves de cifrado requeridas para poner en línea volúmenes y agregados cifrados.

### Acerca de esta tarea

Para sincronizar la configuración de cifrado con los nuevos nodos, realice los siguientes pasos:

### Pasos

1. Ejecute el siguiente comando en el nodo 2:

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

2. Compruebe que la clave SVM-KEK se restaure en "true" en el nodo 2 antes de reubicar los agregados de datos:

```
::> security key-manager key query -node node2 -fields restored -key  
-type SVM-KEK
```

### Ejemplo

```
::> security key-manager key query -node node2 -fields restored -key  
-type SVM-KEK
```

node	vserver	key-server	key-id
restored			
-----	-----	-----	-----
node2	svm1	""	0000000000000000020000000000a008a81976
true			2190178f9350e071fbb90f00000000000000000

## Vuelva a colocar los agregados que no son raíz y las LIF de datos NAS en el nodo 2

Después de verificar la configuración de red en node2 y antes de reubicar agregados de node1 a node2, debe verificar que los LIF de datos NAS que pertenecen a node2 y que

están actualmente en node1 se reubiquen de node1 a node2. También debe verificar si las LIF DE SAN existen en el nodo 2.

### Acerca de esta tarea

Las LIF remotas gestionan el tráfico a LUN DE SAN durante el procedimiento de actualización. No es necesario mover LIF DE SAN durante la actualización para el estado del clúster o del servicio. Los LIF SAN no se mueven a menos que tengan que asignarse a nuevos puertos. Después de conectar el nodo 2 en línea, debe verificar que las LIF están en buen estado y estén ubicadas en los puertos adecuados.

### Pasos

1. Reanude la operación de reubicación:

```
system controller replace resume
```

El sistema ejecuta las siguientes tareas:

- Comprobación de quórum del clúster
- Comprobación del ID del sistema
- Comprobación de la versión de la imagen
- Comprobación de la plataforma de destino
- Comprobación de accesibilidad de red

La operación se detiene en esta fase de la comprobación de accesibilidad de red.

2. Reanude la operación de reubicación:

```
system controller replace resume
```

El sistema realiza las siguientes comprobaciones:

- Comprobación del estado del clúster
- Comprobación del estado de LIF de clúster

Después de realizar estas comprobaciones, el sistema reubica los agregados no raíz y las LIF de datos NAS en node2, que ahora se está ejecutando en la controladora de reemplazo.

La operación de reemplazo de la controladora se coloca en pausa una vez que se completa la reubicación de recursos.

3. Comprobar el estado de las operaciones de reubicación de agregados y movimiento de LIF de datos de NAS:

```
system controller replace show-details
```

Si el procedimiento de reemplazo de la controladora está en pausa, compruebe y corrija el error, si corresponde, y luego emita `resume` para continuar la operación.

4. Si es necesario, restaure y devuelva los LIF desplazados. Enumerar las LIF desplazadas:

```
cluster controller-replacement network displaced-interface show
```

Si hay alguna LIF desplazada, restaurar el nodo inicial a 2:

cluster controller-replacement network displaced-interface restore-home-node

5. Reanude la operación para solicitar que el sistema realice las comprobaciones previas necesarias:

```
system controller replace resume
```

El sistema realiza las siguientes comprobaciones posteriores:

- Comprobación de quórum del clúster
- Comprobación del estado del clúster
- Comprobación de reconstrucción de los agregados
- Comprobación del estado del agregado
- Comprobación del estado del disco
- Comprobación del estado de LIF de clúster
- Comprobación del volumen

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.