



Procedimientos de mantenimiento de las configuraciones IP de MetroCluster

ONTAP MetroCluster

NetApp
August 30, 2024

Tabla de contenidos

- Procedimientos de mantenimiento de las configuraciones IP de MetroCluster 1
 - Modificar las propiedades de una interfaz IP de MetroCluster 1
 - Mantenimiento y sustitución del switch IP 5
 - Identificar el almacenamiento en una configuración IP de MetroCluster 32
 - Adición de bandejas a una IP de MetroCluster mediante switches de MetroCluster de almacenamiento compartido 36
 - Configure el cifrado integral en una configuración IP de MetroCluster 52
 - Apagar y encender un sitio único en una configuración IP de MetroCluster 56
 - Apagado de una configuración de IP de MetroCluster completa 63

Procedimientos de mantenimiento de las configuraciones IP de MetroCluster

Modificar las propiedades de una interfaz IP de MetroCluster

A partir de ONTAP 9.10.1, puede cambiar las siguientes propiedades de una interfaz IP de MetroCluster: Dirección IP, máscara y puerta de enlace. Puede usar cualquier combinación de parámetros para actualizar.

Es posible que deba actualizar estas propiedades, por ejemplo, si se detecta una dirección IP duplicada o si una puerta de enlace necesita cambiar en el caso de una red de capa 3 debido a cambios en la configuración del enrutador.

Acerca de esta tarea

- Sólo puede cambiar una interfaz a la vez. Habrá interrupciones en el tráfico en esa interfaz hasta que se actualicen las otras interfaces y se restablezcan las conexiones.
- Utilice la `metrocluster configuration-settings interface modify` Comando para cambiar cualquier propiedad de interfaz IP de MetroCluster.



Estos comandos cambian la configuración de un nodo en particular para un puerto en particular. Para restaurar una conectividad de red completa, se necesitan comandos similares en otros puertos. De igual modo, los switches de red también deben actualizar su configuración. Por ejemplo, si la puerta de enlace se actualiza, lo ideal es que cambie en ambos nodos de un par de alta disponibilidad, ya que son los mismos. Además, el switch conectado a dichos nodos también debe actualizar su puerta de enlace.

- Utilice `metrocluster configuration-settings interface show metrocluster connection check`` los comandos `,` `,` y ``metrocluster connection show` para comprobar que toda la conectividad funciona en todas las interfaces.

Modifique la dirección IP, la máscara de red y la pasarela

Realice los siguientes pasos para modificar la dirección IP, la máscara de red y la pasarela de una interfaz MetroCluster IP.

Pasos

1. Actualice la dirección IP, la máscara de red y la pasarela de un solo nodo e interfaz: `metrocluster configuration-settings interface modify`

El siguiente comando muestra cómo actualizar la dirección IP, la máscara de red y la pasarela:

```

cluster_A::~* metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_1 -home-port e0a-10 -address
192.168.12.101 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Setting up iSCSI target configuration. (pass2:iscsil3:0:-1:0):
xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO not supported
[Job 28] Establishing iSCSI initiator connections.
(pass6:iscsil4:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass8:iscsil5:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
(pass9:iscsil6:0:-1:0): xpt_action_default: CCB type 0xe XPT_DEV_ADVINFO
not supported
[Job 28] Job succeeded: Interface Modify is successful.
cluster_A::~*> metrocluster configuration-settings interface modify
-cluster-name cluster_A -home-node node_A_2 -home-port e0a-10 -address
192.168.12.201 -gateway 192.168.12.1 -netmask 255.255.254.0
(metrocluster configuration-settings interface modify)
Warning: This operation will disconnect and reconnect iSCSI and RDMA
connections used for DR protection through port "e0a-10". Partner nodes
may need modifications for port "e0a-10" in order to completely
establish network connectivity.
Do you want to continue?" yes
[Job 28] Job succeeded: Interface Modify is successful

```

2. Compruebe que toda la conectividad funciona para todas las interfaces: metrocluster configuration-settings interface show

El siguiente comando muestra cómo comprobar que toda la conectividad funciona en todas las interfaces:

```

cluster_A::*> metrocluster configuration-settings interface show
(metrocluster configuration-settings interface show)
DR          Config
Group Cluster Node      Network Address Netmask      Gateway
State
-----
1          cluster_A node_A_2
          Home Port: e0a-10
          192.168.12.201 255.255.254.0 192.168.12.1
completed
          Home Port: e0b-20
          192.168.20.200 255.255.255.0 192.168.20.1
completed
          node_A_1
          Home Port: e0a-10
          192.168.12.101 255.255.254.0 192.168.12.1
completed
          Home Port: e0b-20
          192.168.20.101 255.255.255.0 192.168.20.1
completed
          cluster_B node_B_1
          Home Port: e0a-10
          192.168.11.151 255.255.255.0 192.168.11.1
completed
          Home Port: e0b-20
          192.168.21.150 255.255.255.0 192.168.21.1
completed
          node_B_2
          Home Port: e0a-10
          192.168.11.250 255.255.255.0 192.168.11.1
completed
          Home Port: e0b-20
          192.168.21.250 255.255.255.0 192.168.21.1
completed
8 entries were displayed.

```

3. Compruebe que todas las conexiones funcionan:

```
metrocluster configuration-settings connection show
```

El siguiente comando muestra cómo comprobar que todas las conexiones funcionan:

```

cluster_A::*> metrocluster configuration-settings connection show
(metrocluster configuration-settings connection show)
DR
Group Cluster Node      Source          Destination
Config State           Network Address Network Address Partner Type
-----
1      cluster_A node_A_2
      Home Port: e0a-10
      192.168.10.200 192.168.10.101 HA Partner
completed
      Home Port: e0a-10
      192.168.10.200 192.168.11.250 DR Partner
completed
      Home Port: e0a-10
      192.168.10.200 192.168.11.151 DR Auxiliary
completed
      Home Port: e0b-20
      192.168.20.200 192.168.20.100 HA Partner
completed
      Home Port: e0b-20
      192.168.20.200 192.168.21.250 DR Partner
completed
      Home Port: e0b-20
      192.168.20.200 192.168.21.150 DR Auxiliary
completed
      node_A_1
      Home Port: e0a-10
      192.168.10.101 192.168.10.200 HA Partner
completed
      Home Port: e0a-10
      192.168.10.101 192.168.11.151 DR Partner
completed
      Home Port: e0a-10
      192.168.10.101 192.168.11.250 DR Auxiliary
completed
      Home Port: e0b-20
      192.168.20.100 192.168.20.200 HA Partner
completed
      Home Port: e0b-20
      192.168.20.100 192.168.21.150 DR Partner
completed
      Home Port: e0b-20
      192.168.20.100 192.168.21.250 DR Auxiliary
completed

```

Mantenimiento y sustitución del switch IP

Sustituya un switch IP o cambie el uso de los switches IP de MetroCluster existentes

Es posible que deba sustituir un switch con errores, actualizar o degradar un switch, o cambiar el uso de switches IP de MetroCluster existentes.

Acerca de esta tarea

Este procedimiento se aplica cuando se utilizan switches validados por NetApp. Si utiliza switches compatibles con MetroCluster, consulte al proveedor de switches.

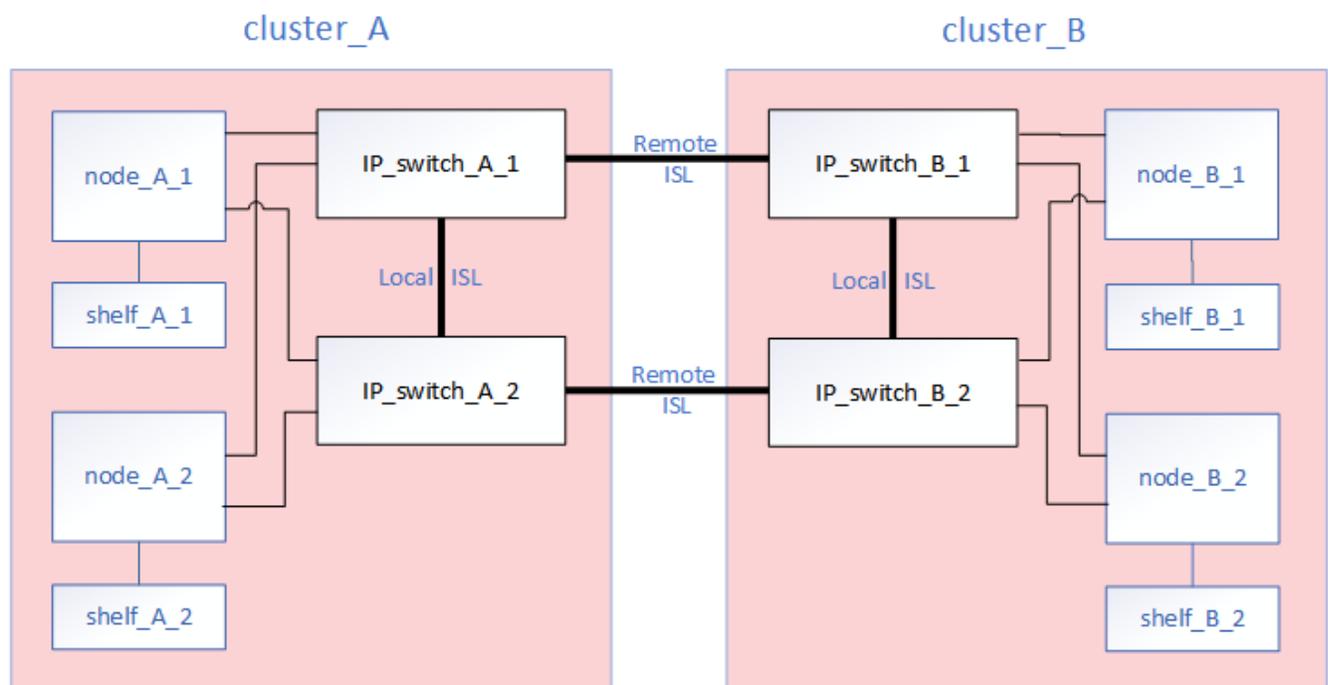
"[Active el registro de la consola](#)" antes de realizar esta tarea.

Este procedimiento admite las siguientes conversiones:

- Cambiando el proveedor del switch, el tipo o ambos. El nuevo conmutador puede ser el mismo que el antiguo cuando un conmutador ha fallado, o puede cambiar el tipo de conmutador (actualizar o degradar el conmutador).

Por ejemplo, para expandir una configuración IP de MetroCluster de una configuración individual de cuatro nodos mediante controladoras AFF A400 y switches BES-53248 a una configuración de ocho nodos mediante controladoras AFF A400, debe cambiar los switches a un tipo compatible para la configuración porque los switches BES-53248 no se admiten en la nueva configuración.

Si desea reemplazar un interruptor fallido por el mismo tipo de interruptor, solo debe reemplazar el interruptor fallido. Si desea actualizar o degradar un conmutador, debe ajustar dos switches que se encuentren en la misma red. Hay dos switches en la misma red cuando se conectan a un enlace entre switches (ISL) y no se encuentran en el mismo sitio. Por ejemplo, la Red 1 incluye IP_SWITCH_A_1 e IP_SWITCH_B_1, y la Red 2 incluye IP_SWITCH_A_2 e IP_SWITCH_B_2, como se muestra en el diagrama siguiente:





Si reemplaza un conmutador o actualiza a diferentes conmutadores, puede preconfigurar los conmutadores instalando el firmware del conmutador y el archivo RCF.

- Convierta una configuración de IP de MetroCluster en una configuración de IP de MetroCluster mediante switches MetroCluster de almacenamiento compartido.

Por ejemplo, si tiene una configuración IP MetroCluster regular con controladoras AFF A700 y desea volver a configurar MetroCluster para conectar las bandejas NS224 a los mismos switches.



- Si desea añadir o quitar bandejas en una configuración de IP de MetroCluster mediante switches IP de MetroCluster de almacenamiento compartido, siga los pasos de ["Añadir bandejas a una IP de MetroCluster mediante switches MetroCluster de almacenamiento compartido"](#)
- Es posible que la configuración IP de MetroCluster ya se conecte directamente a bandejas NS224 o a switches de almacenamiento dedicados.

Hoja de trabajo de uso del puerto

A continuación se muestra un ejemplo de hoja de datos para convertir una configuración de IP de MetroCluster en una configuración de almacenamiento compartido conectando dos bandejas NS224 con los switches existentes.

Definiciones de hoja de trabajo:

- Configuración existente: El cableado de la configuración de MetroCluster existente.
- Nueva configuración con NS224 bandejas: La configuración de destino donde los switches se comparten entre el almacenamiento y MetroCluster.

Los campos resaltados en esta hoja de trabajo indican lo siguiente:

- Verde: No es necesario cambiar el cableado.
- Amarillo: Debe mover los puertos con la misma configuración o con otra diferente.
- Azul: Puertos que son conexiones nuevas.

PORT USAGE OVERVIEW

Example of expanding an existing 4Node MetroCluster with 2x NS224 shelves and changing the ISL's from 10G to 40/100G

Switch port	Existing configuration			New configuration with NS224 shelves		
	Port use	IP_switch_x_1	IP_switch_x_2	Port use	IP_switch_x_1	IP_switch_x_2
1	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'	MetroCluster 1, Local Cluster Interface	Cluster Port 'A'	Cluster Port 'B'
2		Cluster Port 'A'	Cluster Port 'B'		Cluster Port 'A'	Cluster Port 'B'
3						
4						
5				Storage shelf 1 (9)	NSM-A, e0a	NSM-A, e0b
6					NSM-B, e0a	NSM-B, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8						
9	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'	MetroCluster 1, MetroCluster interface	Port 'A'	Port 'B'
10		Port 'A'	Port 'B'		Port 'A'	Port 'B'
11						
12						
13				ISL, MetroCluster, native speed 40G / 100G breakout mode 10G	Remote ISL, 2x 40/100G	Remote ISL, 2x 40/100G
14						
15						
16						
17				MetroCluster 1, Storage Interface	Storage Port 'A'	Storage Port 'B'
18					Storage Port 'A'	Storage Port 'B'
19						
20						
21	ISL, MetroCluster breakout mode 10G	Remote ISL, 10G	Remote ISL, 10G	Storage shelf 2 (8)	NSM-A, e0a	NSM-A, e0b
22					NSM-B, e0a	NSM-B, e0b
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						

Pasos

1. Compruebe el estado de la configuración.
 - a. Compruebe que la MetroCluster esté configurada y en modo normal de cada clúster: **metrocluster show**

```
cluster_A::> metrocluster show
Cluster                               Entry Name                               State
-----                               -
Local: cluster_A                       Configuration state configured
Mode                                    normal
AUSO Failure Domain auso-on-cluster-
disaster
Remote: cluster_B                       Configuration state configured
Mode                                    normal
AUSO Failure Domain auso-on-cluster-
disaster
```

- b. Compruebe que el mirroring está habilitado en cada nodo: **metrocluster node show**

```
cluster_A::> metrocluster node show
DR                                     Configuration  DR
Group Cluster Node                    State          Mirroring Mode
-----
-----
1      cluster_A
      node_A_1      configured    enabled    normal
      cluster_B
      node_B_1      configured    enabled    normal
2 entries were displayed.
```

- c. Compruebe que los componentes de MetroCluster sean los mismos en buen estado: **metrocluster check run**

```
cluster_A::> metrocluster check run
```

```
Last Checked On: 10/1/2014 16:03:37
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok

4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results.

To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

d. Compruebe que no hay alertas de estado: **system health alert show**

2. Configure el nuevo interruptor antes de instalarlo.

Si está reutilizando los interruptores existentes, vaya a [Paso 4](#).



Si está actualizando o degradando los switches, debe configurar todos los switches de la red.

Siga los pasos de la sección *Configuración de los switches IP* del ["Instalación y configuración de IP de MetroCluster."](#)

Asegúrese de aplicar el archivo RCF correcto para switch `_A_1`, `_A_2`, `_B_1` o `_B_2`. Si el nuevo conmutador es el mismo que el antiguo, deberá aplicar el mismo archivo RCF.

Si actualiza o degrada un conmutador, aplique el último archivo RCF admitido para el nuevo conmutador.

3. Ejecute el comando Port show para ver información acerca de los puertos de red:

network port show

a. Modifique todas las LIF del clúster para deshabilitar la reversión automática:

```
network interface modify -vserver <vserver_name> -lif <lif_name>
-auto-revert false
```

4. Desconecte las conexiones del interruptor antiguo.



Solo se desconectan las conexiones que no estén utilizando el mismo puerto en las configuraciones nuevas y antiguas. Si utiliza switches nuevos, debe desconectar todas las conexiones.

Quite las conexiones en el siguiente orden:

- a. Desconecte las interfaces del clúster local
- b. Desconecte los ISL del clúster local
- c. Desconecte las interfaces IP de MetroCluster
- d. Desconecte los ISL de MetroCluster

En el ejemplo [[port_usage_worksheet](#)], los interruptores no cambian. Los ISL de MetroCluster se reubican y deben desconectarse. No es necesario desconectar las conexiones marcadas en verde en la hoja de trabajo.

5. Si está utilizando interruptores nuevos, apague el interruptor antiguo, retire los cables y retire físicamente el interruptor antiguo.

Si está reutilizando los interruptores existentes, vaya a [Paso 6](#).



No conecte el cable a los nuevos interruptores excepto a la interfaz de administración (si se utiliza).

6. Configure los conmutadores existentes.

Si ya ha configurado previamente los switches, puede omitir este paso.

Para configurar los switches existentes, siga los pasos para instalar y actualizar el firmware y los archivos RCF:

- ["Actualización del firmware en switches MetroCluster IP"](#)
- ["Actualice los archivos RCF en switches MetroCluster IP"](#)

7. Conecte los cables de los interruptores.

Puede seguir los pasos de la sección *Cableando los conmutadores IP* en ["Instalación y configuración de IP de MetroCluster"](#).

Conecte los cables de los interruptores en el siguiente orden (si es necesario):

- a. Conecte los cables ISLs al sitio remoto.
- b. Conecte el cable de las interfaces IP de MetroCluster.
- c. Cablee las interfaces del clúster local.



- Los puertos utilizados pueden ser diferentes de los del switch antiguo si el tipo de switch es diferente. Si va a actualizar o cambiar a una versión anterior de los switches, realice **NO** el cableado de los ISL locales. Solo conecte los cables de los ISL locales si va a actualizar o cambiar a una versión anterior de los switches de la segunda red, y los dos switches de un sitio son del mismo tipo y cableado.
- Si va a actualizar Switch-A1 y Switch-B1, debe realizar los pasos 1 a 6 para los switches Switch-A2 y Switch-B2.

8. Finalice el cableado del clúster local.
 - a. Si las interfaces del clúster local están conectadas a un switch:
 - i. Conecte los cables de los ISL del clúster local.
 - b. Si las interfaces del clúster local están **NOT** conectadas a un switch:
 - i. Utilice la "[Migrar a un entorno de clúster de NetApp conmutado](#)" procedimiento para convertir un clúster sin switches en un clúster con switches. Utilice los puertos indicados en "[Instalación y configuración de IP de MetroCluster](#)" O los archivos de cableado RCF para conectar la interfaz del clúster local.
9. Encienda el interruptor o los interruptores.

Si el nuevo interruptor es el mismo, encienda el nuevo interruptor. Si está actualizando o degradando los interruptores, encienda ambos interruptores. La configuración puede funcionar con dos switches diferentes en cada centro hasta que se actualice la segunda red.

10. Repita para comprobar que la configuración de MetroCluster sea correcta [Paso 1](#).

Si va a actualizar o a cambiar a una versión anterior de los switches de la primera red, es posible que haya algunas alertas relacionadas con la agrupación en clúster local.



Si actualiza o degrada las redes, repita todos los pasos para la segunda red.

11. Modifique todas las LIF de clúster para volver a habilitar la reversión automática:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -auto
-revert true
```

12. De manera opcional, mueva las bandejas NS224.

Si va a volver a configurar una configuración IP de MetroCluster que no conecta las bandejas de NS224 a los switches IP de MetroCluster, utilice el procedimiento adecuado para añadir o mover las bandejas NS224:

- "[Añadir bandejas a una IP de MetroCluster mediante switches MetroCluster de almacenamiento compartido](#)"
- "[Migre desde un clúster sin switches con almacenamiento de conexión directa](#)"
- "[Migre de una configuración sin switches con almacenamiento conectado mediante la reutilización de los switches de almacenamiento](#)"

Puertos de interfaz IP de MetroCluster en línea u fuera de línea

Cuando realiza tareas de mantenimiento, es posible que deba desconectar u conectar un puerto de interfaz IP de MetroCluster.

Acerca de esta tarea

["Active el registro de la consola"](#) antes de realizar esta tarea.

Pasos

Puede usar los siguientes pasos para conectar un puerto de interfaz IP de MetroCluster o desconectarlo.

1. Configure el nivel de privilegio en Advanced.

```
set -privilege advanced
```

Ejemplo de salida

```
Cluster A_1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when
        directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

2. Desconecte el puerto de la interfaz IP de MetroCluster.

```
system ha interconnect link off -node <node_name> -link <link_num, 0 or
1>
```

Ejemplo de salida

```
Cluster_A1::*> system ha interconnect link off -node node-a1 -link 0
```

a. Compruebe que la interfaz de IP de MetroCluster está sin conexión.

```
Cluster_A1::*> system ha interconnect port show
```

Ejemplo de salida

```

Cluster_A1::*> system ha interconnect port show
                Physical  Link
                Layer    Layer    Physical  Physical
Active
Node           Monitor  Port  State  State  Link Up  Link Down
Link
-----
node-a1        off
                0  disabled  down    4      3
false
                1  linkup   active  4      2
true
node-a2        off
                0  linkup   active  4      2
true
                1  linkup   active  4      2
true
2 entries were displayed.

```

3. Conecte el puerto de la interfaz IP de MetroCluster.

```

system ha interconnect link on -node <node_name> -link <link_num, 0 or
1>

```

Ejemplo de salida

```

Cluster_A1::*> system ha interconnect link on -node node-a1 -link 0

```

a. Compruebe que el puerto de la interfaz IP de MetroCluster está en línea.

```

Cluster_A1::*> system ha interconnect port show

```

Ejemplo de salida

```

Cluster_A1::*> system ha interconnect port show
                Physical  Link
                Layer    Layer    Physical  Physical
Active
Node           Monitor  Port   State   State   Link Up  Link Down
Link
-----
node-a1        off
                0   linkup  active   5       3
true
                1   linkup  active   4       2
true
node-a2        off
                0   linkup  active   4       2
true
                1   linkup  active   4       2
true
2 entries were displayed.

```

Actualización del firmware en switches MetroCluster IP

Es posible que deba actualizar el firmware en un switch MetroCluster IP.

Acerca de esta tarea

Debe repetir esta tarea en cada uno de los conmutadores sucesivamente.

"[Active el registro de la consola](#)" antes de realizar esta tarea.

Pasos

1. Compruebe el estado de la configuración.
 - a. Compruebe que la MetroCluster esté configurada y en modo normal de cada clúster:

```
metrocluster show
```

```

cluster_A::> metrocluster show
Cluster                Entry Name                State
-----
Local: cluster_A      Configuration state      configured
Mode                   normal
AUSO Failure Domain   auso-on-cluster-
disaster
Remote: cluster_B    Configuration state      configured
Mode                   normal
AUSO Failure Domain   auso-on-cluster-
disaster

```

b. Compruebe que el mirroring está habilitado en cada nodo:

```
metrocluster node show
```

```

cluster_A::> metrocluster node show
DR                Configuration DR
Group Cluster Node      State           Mirroring Mode
-----
-----
1      cluster_A
           node_A_1      configured      enabled      normal
           cluster_B
           node_B_1      configured      enabled      normal
2 entries were displayed.

```

c. Compruebe que los componentes de MetroCluster sean los mismos en buen estado:

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
```

```
Last Checked On: 10/1/2014 16:03:37
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok

4 entries were displayed.

Command completed. Use the "metrocluster check show -instance" command or sub-commands in "metrocluster check" directory for detailed results. To check if the nodes are ready to do a switchover or switchback operation, run "metrocluster switchover -simulate" or "metrocluster switchback -simulate", respectively.

a. Compruebe que no hay alertas de estado:

```
system health alert show
```

2. Instale el software en el primer interruptor.



Debe instalar el software del conmutador en los conmutadores en el siguiente orden: Switch_A_1, switch_B_1, Switch_A_2, switch_B_2.

Siga los pasos para instalar el software de switch en el tema correspondiente dependiendo de si el tipo de switch es Broadcom, Cisco o NVIDIA:

- ["Descargue e instale el software EFOS del conmutador Broadcom"](#)
- ["Descargue e instale el software Cisco Switch NX-OS"](#)
- ["Descargue e instale el software NVIDIA SN2100 switch Cumulus"](#)

3. Repita el paso anterior con cada uno de los conmutadores.

4. Repetición [Paso 1](#) para comprobar el estado de la configuración.

Actualice los archivos RCF en switches MetroCluster IP

Es posible que necesite actualizar un archivo RCF en un conmutador MetroCluster IP. Por ejemplo, si la versión del archivo RCF que ejecuta en los switches no es compatible con la versión de ONTAP, la versión del firmware del switch o ambos.

Compruebe que el archivo RCF es compatible

Si va a cambiar la versión de ONTAP o la versión de firmware del switch, debe comprobar que tiene un archivo RCF compatible con esa versión. Si utiliza el generador RCF, se generará el archivo RCF correcto.

Pasos

1. Utilice los siguientes comandos de los conmutadores para comprobar la versión del archivo RCF:

Desde este switch...	Emita este comando...
Switch Broadcom	(IP_switch_A_1) # show clibanner
Switch Cisco	IP_switch_A_1# show banner motd

Para cualquiera de los dos conmutadores, busque la línea en la salida que indica la versión del archivo RCF. Por ejemplo, la siguiente salida procede de un conmutador Cisco, que indica que la versión del archivo RCF es "v1.80".

```
Filename : NX3232_v1.80_Switch-A2.txt
```

2. Para comprobar qué archivos son compatibles con una versión, conmutador y plataforma ONTAP específica, utilice el RcfFileGenerator. Si puede generar el archivo RCF para la configuración que tiene o a la que desea actualizar, se admite.
3. Para verificar que el firmware del switch es compatible, consulte lo siguiente:
 - ["Hardware Universe"](#)
 - ["Matriz de interoperabilidad de NetApp"](#)

Actualice los archivos RCF

Si va a instalar un nuevo firmware de conmutador, debe instalar el firmware del conmutador antes de actualizar el archivo RCF.

Acerca de esta tarea

- Este procedimiento interrumpe el tráfico del conmutador donde se actualiza el archivo RCF. El tráfico se reanuda una vez que se aplique el nuevo archivo RCF.
- Realice los pasos en un conmutador a la vez, en el siguiente orden: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2.
- ["Active el registro de la consola"](#) antes de realizar esta tarea.

Pasos

1. Compruebe el estado de la configuración.
 - a. Compruebe que los componentes de MetroCluster están en buen estado:

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

La operación se ejecuta en segundo plano.

- b. Después del `metrocluster check run` la operación finaliza, se ejecuta `metrocluster check`

show para ver los resultados.

Después de unos cinco minutos, se muestran los siguientes resultados:

```
-----  
::*> metrocluster check show  
  
Component          Result  
-----  
nodes              ok  
lifs               ok  
config-replication ok  
aggregates        ok  
clusters          ok  
connections       not-applicable  
volumes           ok  
7 entries were displayed.
```

a. Comprobar el estado de la operación de comprobación de MetroCluster en ejecución:

```
metrocluster operation history show -job-id 38
```

b. Compruebe que no hay alertas de estado:

```
system health alert show
```

2. Prepare los switches IP para la aplicación de los nuevos archivos RCF.

Siga los pasos para su proveedor de switches:

- "Restablezca el conmutador IP Broadcom a los valores predeterminados de fábrica"
- "Restablezca el conmutador IP de Cisco a los valores predeterminados de fábrica"
- "Restablece el switch NVIDIA IP SN2100 a los valores predeterminados de fábrica"

3. Descargue e instale el archivo IP RCF, según el proveedor del switch.

- "Descargue e instale los archivos Broadcom IP RCF"
- "Descargue e instale los archivos Cisco IP RCF"
- "Descargue e instale los archivos NVIDIA IP RCF"



Si tiene una configuración de red L2 compartida o L3, es posible que deba ajustar los puertos ISL en los switches intermedio/cliente. El modo de puerto de switch puede cambiar del modo de acceso al modo de "tronco". Sólo continúe con la actualización del segundo par de conmutadores (A_2, B_2) si la conectividad de red entre los conmutadores A_1 y B_1 está totalmente operativa y la red está en buen estado.

Actualice los archivos RCF en switches IP de Cisco mediante CleanUpFiles

Es posible que necesite actualizar un archivo RCF en un conmutador IP de Cisco. Por ejemplo, una actualización de ONTAP o de firmware del switch requieren un nuevo archivo RCF.

Acerca de esta tarea

- A partir de la versión 1.4a de RcfFileGenerator, hay una nueva opción para cambiar (actualizar, degradar o reemplazar) la configuración del switch en switches IP de Cisco sin necesidad de realizar un 'borrado de escritura'.
- ["Active el registro de la consola"](#) antes de realizar esta tarea.
- El switch Cisco 9336C-FX2 tiene dos tipos de almacenamiento de switch diferentes con un nombre diferente en el RCF. Use la siguiente tabla para determinar el tipo de almacenamiento Cisco 9336C-FX2 correcto para su configuración:

Si va a conectar el siguiente almacenamiento...	Elija el tipo de almacenamiento Cisco 9336C-FX2...	Banner/MOTD del archivo RCF de ejemplo
<ul style="list-style-type: none">• Bandejas SAS conectadas directamente• Bandejas NVMe conectadas directamente• Bandejas NVMe conectadas a switches de almacenamiento dedicados	9336C-FX2: Solo almacenamiento directo	* Switch : NX9336C (direct storage, L2 Networks, direct ISL)
<ul style="list-style-type: none">• Bandejas SAS conectadas directamente• Bandejas NVMe conectadas a los switches IP de MetroCluster <div style="border: 1px solid gray; padding: 5px; margin-top: 10px;"> Se requiere al menos una bandeja NVMe conectada con Ethernet</div>	9336C-FX2: Almacenamiento SAS y Ethernet	* Switch : NX9336C (SAS and Ethernet storage, L2 Networks, direct ISL)

Antes de empezar

Puede utilizar este método si la configuración cumple los siguientes requisitos:

- Se aplica la configuración RCF estándar.
- La ["RcfFileGenerator"](#) Debe poder crear el mismo archivo RCF que se aplica, con la misma versión y configuración (plataformas, VLAN).
- NetApp no proporcionó el archivo RCF aplicado para una configuración especial.
- El archivo RCF no se modificó antes de aplicarlo.
- Antes de aplicar el archivo RCF actual, se siguieron los pasos para restablecer los valores

predeterminados de fábrica del conmutador.

- No se realizaron cambios en la configuración del conmutador (puerto) después de aplicar el RCF.

Si no cumple estos requisitos, no podrá utilizar CleanUpFiles que se crean al generar los archivos RCF. Sin embargo, puede aprovechar la función para crear CleanUpFiles genérico — la limpieza que utiliza este método se deriva de la salida de `show running-config` y es una práctica recomendada.



Debe actualizar los interruptores en el siguiente orden: Switch_A_1, Switch_B_1, Switch_A_2, Switch_B_2. O bien, puede actualizar los interruptores Switch_A_1 y Switch_B_1 al mismo tiempo, seguidos de los interruptores Switch_A_2 y Switch_B_2.

Pasos

1. Determine la versión actual del archivo RCF y qué puertos y VLAN se utilizan: `IP_switch_A_1# show banner motd`



Debe obtener esta información de los cuatro switches y completar la siguiente tabla de información.

```

* NetApp Reference Configuration File (RCF)
*
* Switch : NX9336C (SAS storage, L2 Networks, direct ISL)
* Filename : NX9336_v1.81_Switch-A1.txt
* Date : Generator version: v1.3c_2022-02-24_001, file creation time:
2021-05-11, 18:20:50
*
* Platforms : MetroCluster 1 : FAS8300, AFF-A400, FAS8700
*             MetroCluster 2 : AFF-A320, FAS9000, AFF-A700, AFF-A800
* Port Usage:
* Ports 1- 2: Intra-Cluster Node Ports, Cluster: MetroCluster 1, VLAN
111
* Ports 3- 4: Intra-Cluster Node Ports, Cluster: MetroCluster 2, VLAN
151
* Ports 5- 6: Ports not used
* Ports 7- 8: Intra-Cluster ISL Ports, local cluster, VLAN 111, 151
* Ports 9-10: MetroCluster 1, Node Ports, VLAN 119
* Ports 11-12: MetroCluster 2, Node Ports, VLAN 159
* Ports 13-14: Ports not used
* Ports 15-20: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel 10
* Ports 21-24: MetroCluster-IP ISL Ports, VLAN 119, 159, Port Channel
11, breakout mode 10gx4
* Ports 25-30: Ports not used
* Ports 31-36: Ports not used
*
#
IP_switch_A_1#

```

En este resultado, debe recopilar la información que se muestra en las dos tablas siguientes.

Información genérica	MetroCluster	SQL Server
Versión de archivo RCF		1.81
Tipo de interruptor		NX9336
Tipología de red		Redes L2, ISL directo
Tipo de almacenamiento		Almacenamiento SAS
Plataformas	1	AFF A400
	2	FAS9000

Información de VLAN	Red	Configuración de MetroCluster	Puertos de switch	Centro a	Centro B
Clúster local VLAN	Red 1	1	1, 2	111	222
		2	3, 4	151	251
	Red 2	1	1, 2	111	222
		2	3, 4	151	251
MetroCluster de VLAN	Red 1	1	9, 10	119	119
		2	11, 12	159	159
	Red 2	1	9, 10	219	219
		2	11, 12	259	259

2. cree los archivos RCF y CleanUpFiles, o cree CleanUpFiles genéricos para la configuración actual.

Si su configuración cumple los requisitos descritos en los requisitos previos, seleccione **opción 1**. Si su configuración **no** cumple los requisitos descritos en los requisitos previos, seleccione **opción 2**.

Opción 1: Cree los archivos RCF y CleanUpFiles

Utilice este procedimiento si la configuración cumple los requisitos.

Pasos

- a. Utilice el RcfFileGenerator 1.4a (o posterior) para crear los archivos RCF con la información que ha recuperado en el paso 1. La nueva versión del RcfFileGenerator crea un conjunto adicional de CleanUpFiles que puede utilizar para revertir alguna configuración y preparar el conmutador para aplicar una nueva configuración de RCF.
- b. Compare el motd del banner con los archivos RCF actualmente aplicados. Los tipos de plataforma, el tipo de switch, el uso de puertos y VLAN deben ser los mismos.



Debe utilizar CleanUpFiles desde la misma versión que el archivo RCF y para la misma configuración. El uso de CleanUpFile no funcionará y podría requerir un restablecimiento completo del conmutador.



La versión ONTAP para la que se crea el archivo RCF no es relevante. Sólo es importante la versión del archivo RCF.



El archivo RCF (incluso es la misma versión) puede enumerar menos plataformas o más. Asegúrese de que su plataforma aparece en la lista.

Opción 2: Crear CleanUpFiles genérico

Utilice este procedimiento si la configuración * no cumple todos los requisitos.

Pasos

- a. Recupere la salida de `show running-config` de cada switch.
- b. Abra la herramienta RcfFileGenerator y haga clic en 'Crear archivos genéricos de CleanUpFiles' en la parte inferior de la ventana
- c. Copie la salida que ha recuperado en el paso 1 del interruptor "uno" en la ventana superior. Puede eliminar o dejar la salida predeterminada.
- d. Haga clic en 'Crear archivos CUF'.
- e. Copie el resultado de la ventana inferior en un archivo de texto (este archivo es CleanUpFile).
- f. Repita los pasos c, d y e para todos los switches de la configuración.

Al final de este procedimiento, debería tener cuatro archivos de texto, uno para cada conmutador. Puede utilizar estos archivos de la misma forma que CleanUpFiles que puede crear utilizando la opción 1.

3. cree los archivos RCF 'new' para la nueva configuración. Cree estos archivos de la misma forma que creó los archivos en el paso anterior, excepto seleccione la versión de archivo ONTAP y RCF correspondiente.

Después de completar este paso, debe tener dos conjuntos de archivos RCF, cada conjunto que consta de doce archivos.

4. Descargue los archivos en el bootflash.

- a. Descargue los archivos CleanUpFiles que creó en [Cree los archivos RCF y CleanUpFiles](#), o cree [archivos genéricos CleanUpFiles para la configuración actual](#)



Este archivo CleanUpFile es para el archivo RCF actual que se aplica y **NO** para el nuevo RCF al que desea actualizar.

Ejemplo de CleanUpFile para Switch-A1: Cleanup_NX9336_v1.81_Switch-A1.txt

- b. Descargue los "nuevos" archivos RCF que ha creado en [Cree los archivos RCF 'nuevos' para la nueva configuración](#).

Ejemplo de archivo RCF para Switch-A1: NX9336_v1.90_Switch-A1.txt

- c. Descargue los archivos CleanUpFiles que creó en [Cree los archivos RCF 'nuevos' para la nueva configuración](#). Este paso es opcional — puede utilizar el archivo en el futuro para actualizar la configuración del switch. Coincide con la configuración aplicada actualmente.

Ejemplo de CleanUpFile para Switch-A1: Cleanup_NX9336_v1.90_Switch-A1.txt



Debe utilizar CleanUpFile para la versión RCF correcta (coincidente). Si utiliza CleanUpFile para una versión de RCF diferente o una configuración diferente, puede que la limpieza de la configuración no funcione correctamente.

El ejemplo siguiente copia los tres archivos en el bootflash:

```
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.81_MetroCluster-
IP_L2Direct_A400FAS8700_XXX_XXX_XXX_XXX/Cleanup_NX9336_v1.81_Switch-
A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_XXX_XXX_XXX_XXXNX9336_v1.90//NX9336_v
1.90_Switch-A1.txt bootflash:
IP_switch_A_1# copy sftp://user@50.50.50.50/RcfFiles/NX9336-direct-
SAS_v1.90_MetroCluster-
IP_L2Direct_A400FAS8700A900FAS9500_XXX_XXX_XXX_XXXNX9336_v1.90//Cleanup_
NX9336_v1.90_Switch-A1.txt bootflash:
```

+



Se le pedirá que especifique el enrutamiento y el reenvío virtuales (VRF).

5. Aplique CleanUpFile o CleanUpFile genérico.

Parte de la configuración se revierte y los puertos de switch se "desconectan".

- a. Confirme que no hay cambios pendientes en la configuración de inicio: `show running-config diff`

```
IP_switch_A_1# show running-config diff
IP_switch_A_1#
```

6. Si ve la salida del sistema, guarde la configuración en ejecución en la configuración de inicio: `copy running-config startup-config`



El resultado del sistema indica que la configuración de inicio y la configuración en ejecución son diferentes y los cambios pendientes. Si no guarda los cambios pendientes, no podrá retroceder utilizando una recarga del conmutador.

- a. Aplicar CleanUpFile:

```
IP_switch_A_1# copy bootflash:Cleanup_NX9336_v1.81_Switch-A1.txt
running-config
IP_switch_A_1#
```



La secuencia de comandos puede tardar un tiempo en volver al indicador del switch. No se espera ningún resultado.

7. Vea la configuración en ejecución para verificar que se borra la configuración: `show running-config`

La configuración actual debe mostrar:

- No se han configurado mapas de clases ni listas de acceso IP
- No hay ningún mapa de directivas configurado
- No hay ninguna política de servicio configurada
- No se configuró ningún perfil de puerto
- Todas las interfaces Ethernet (excepto mgmt0 que no deben mostrar ninguna configuración y sólo se debe configurar VLAN 1).

Si encuentra que alguno de los elementos anteriores está configurado, es posible que no pueda aplicar una nueva configuración de archivo RCF. Sin embargo, puede volver a la configuración anterior volviendo a cargar el conmutador **sin** guardando la configuración en ejecución en la configuración de inicio. El conmutador aparecerá con la configuración anterior.

8. Aplique el archivo RCF y compruebe que los puertos están en línea.

- a. Aplique los archivos RCF.

```
IP_switch_A_1# copy bootflash:NX9336_v1.90-X2_Switch-A1.txt running-
config
```



Aparecen algunos mensajes de advertencia mientras se aplica la configuración. Por lo general, no se esperan mensajes de error. Sin embargo, si ha iniciado sesión mediante SSH, puede recibir el siguiente error: `Error: Can't disable/re-enable ssh:Current user is logged in through ssh`

- b. Una vez aplicada la configuración, compruebe que el clúster y los puertos MetroCluster están conectados con uno de los siguientes comandos, `show interface brief`, `show cdp neighbors`, o `show lldp neighbors`



Si cambió la VLAN del clúster local y actualizó el primer switch del sitio, es posible que la supervisión del estado del clúster no informe el estado como "correcto" porque las VLAN de las configuraciones nuevas y antiguas no coinciden. Después de actualizar el segundo interruptor, el estado debe volver a correcto.

Si la configuración no se aplica correctamente o no desea conservar la configuración, puede volver a la configuración anterior volviendo a cargar el conmutador **sin** guardando la configuración en ejecución en la configuración de inicio. El conmutador aparecerá con la configuración anterior.

9. Guarde la configuración y vuelva a cargar el conmutador.

```
IP_switch_A_1# copy running-config startup-config  
  
IP_switch_A_1# reload
```

Cambiar el nombre de un switch IP de Cisco

Es posible que deba cambiar el nombre de un switch IP de Cisco a fin de proporcionar nomenclatura coherente en toda la configuración.

Acerca de esta tarea

- En los ejemplos de esta tarea, el nombre del conmutador se cambia de `myswitch` para `IP_switch_A_1`.
- ["Active el registro de la consola"](#) antes de realizar esta tarea.

Pasos

1. Entre al modo de configuración global:

```
configure terminal
```

En el ejemplo siguiente se muestra el indicador del modo de configuración. Ambas indicaciones muestran el nombre del conmutador de `myswitch`.

```
myswitch# configure terminal  
myswitch(config)#
```

2. Cambie el nombre del conmutador:

```
switchname new-switch-name
```

Si va a cambiar el nombre de ambos switches de la estructura, utilice el mismo comando de cada switch.

El símbolo del sistema de la CLI cambia para reflejar el nuevo nombre:

```
myswitch(config)# switchname IP_switch_A_1
IP_switch_A_1(config)#
```

3. Salir del modo de configuración:

exit

Se muestra el indicador del interruptor de nivel superior:

```
IP_switch_A_1(config)# exit
IP_switch_A_1#
```

4. Copie la configuración actual en ejecución en el archivo de configuración de inicio:

copy running-config startup-config

5. Compruebe que el cambio de nombre del switch sea visible en el símbolo del sistema del clúster ONTAP.

Tenga en cuenta que se muestra el nuevo nombre del conmutador y el nombre del conmutador antiguo (myswitch) no aparece.

a. Entre en el modo de privilegios avanzado, pulse **y** cuando se le solicite:

set -privilege advanced

b. Mostrar los dispositivos conectados:

network device-discovery show

c. Vuelva al modo de privilegio admin:

set -privilege admin

El siguiente ejemplo muestra que el conmutador aparece con el nuevo nombre, IP_switch_A_1:

```
cluster_A::storage show> set advanced
```

Warning: These advanced commands are potentially dangerous; use them only when directed to do so by NetApp personnel.

```
Do you want to continue? {y|n}: y
```

```
cluster_A::storage show*> network device-discovery show
```

Node/ Protocol	Local Port	Discovered Device	Interface	Platform

node_A_2/cdp				
	e0M	LF01-410J53.mycompany.com (SAL18516DZY)	Ethernet125/1/28	N9K-
C9372PX				
	e1a	IP_switch_A_1 (FOC21211RBU)	Ethernet1/2	N3K-
C3232C				
	e1b	IP_switch_A_1 (FOC21211RBU)	Ethernet1/10	N3K-
C3232C				
.				
.			Ethernet1/18	N9K-
C9372PX				
node_A_1/cdp				
	e0M	LF01-410J53.mycompany.com (SAL18516DZY)	Ethernet125/1/26	N9K-
C9372PX				
	e0a	IP_switch_A_2 (FOC21211RB5)	Ethernet1/1	N3K-
C3232C				
	e0b	IP_switch_A_2 (FOC21211RB5)	Ethernet1/9	N3K-
C3232C				
	e1a	IP_switch_A_1 (FOC21211RBU)		
.				
.				
.				

16 entries were displayed.

Añada, elimine o cambie los puertos ISL sin interrupciones en los switches IP de Cisco

Puede que deba agregar, quitar o cambiar los puertos ISL en los switches IP de Cisco. Se pueden convertir puertos ISL dedicados en puertos ISL compartidos o cambiar la velocidad de los puertos ISL en un switch IP de Cisco.

Acerca de esta tarea

Si convierte puertos ISL dedicados a puertos ISL compartidos, asegúrese de que los nuevos puertos cumplen con los ["Requisitos para los puertos ISL compartidos"](#).

Debe completar todos los pasos en ambos switches para garantizar la conectividad ISL.

En el siguiente procedimiento se supone que se reemplaza un ISL de 10 GB conectado en el puerto del switch eth1/24/1 con dos ISL de 100 GB que se conectan con los puertos del switch 17 y 18.



Si se utiliza un switch Cisco 9336C-FX2 en una configuración compartida que conecta bandejas NS224, si se cambian los ISL, es posible que se requiera un nuevo archivo RCF. No necesita un nuevo archivo RCF si su velocidad actual y nueva ISL es 40Gbps y 100Gbps. Todos los demás cambios en la velocidad ISL requieren un nuevo archivo RCF. Por ejemplo, cambiar la velocidad ISL de 40Gbps a 100Gbps no requiere un nuevo archivo RCF, pero cambiar la velocidad ISL de 10Gbps a 40Gbps requiere un nuevo archivo RCF.

Antes de empezar

Consulte la sección **Interruptores** de la ["Hardware Universe de NetApp"](#) para verificar los transceptores compatibles.

["Active el registro de la consola"](#) antes de realizar esta tarea.

Pasos

1. Deshabilite los puertos ISL de los ISL en ambos switches de la estructura que desea cambiar.



Solo tiene que deshabilitar los puertos ISL actuales si los mueve a un puerto diferente, o si la velocidad del ISL está cambiando. Si añade un puerto ISL con la misma velocidad que los ISL existentes, vaya al paso 3.

Debe introducir solo un comando de configuración para cada línea y presionar Ctrl-Z después de introducir todos los comandos, como se muestra en el siguiente ejemplo:

```

switch_A_1# conf t
switch_A_1(config)# int eth1/24/1
switch_A_1(config-if)# shut
switch_A_1(config-if)#
switch_A_1#

switch_B_1# conf t
switch_B_1(config)# int eth1/24/1
switch_B_1(config-if)# shut
switch_B_1(config-if)#
switch_B_1#

```

2. Quite los cables y transceptores existentes.
3. Cambie el puerto ISL según sea necesario.



Si utiliza switches Cisco 9336C-FX2 en una configuración compartida conectando bandejas NS224 y tiene que actualizar el archivo RCF y aplicar la nueva configuración para los puertos ISL nuevos, siga los pasos hasta ["Actualice los archivos RCF en los conmutadores IP de MetroCluster."](#)

Opción	Paso
Para cambiar la velocidad de un puerto ISL...	Conecte los nuevos ISL a los puertos designados según sus velocidades. Debe asegurarse de que estos puertos ISL para el switch aparezcan en la lista <i>MetroCluster IP Installation and Configuration</i> .
Para añadir un ISL...	Inserte QFSP en los puertos que va a agregar como puertos ISL. Asegúrese de que aparecen en la lista <i>MetroCluster IP Installation and Configuration</i> y cablearlos según corresponda.

4. Habilite todos los puertos ISL (si no está habilitado) en ambos switches en la estructura que comienzan con el siguiente comando:

```
switch_A_1# conf t
```

Debe introducir solo un comando de configuración por línea y pulsar Ctrl-Z después de introducir todos los comandos:

```
switch_A_1# conf t
switch_A_1(config)# int eth1/17
switch_A_1(config-if)# no shut
switch_A_1(config-if)# int eth1/18
switch_A_1(config-if)# no shut
switch_A_1(config-if)#
switch_A_1#
switch_A_1# copy running-config startup-config

switch_B_1# conf t
switch_B_1(config)# int eth1/17
switch_B_1(config-if)# no shut
switch_B_1(config-if)# int eth1/18
switch_B_1(config-if)# no shut
switch_B_1(config-if)#
switch_B_1#
switch_B_1# copy running-config startup-config
```

5. Compruebe que los ISL y los canales de puerto para los ISL se han establecido entre ambos switches:

```
switch_A_1# show int brief
```

Debe ver las interfaces ISL en la salida del comando, como se muestra en el ejemplo siguiente:

```

Switch_A_1# show interface brief
-----
-----
Ethernet          VLAN    Type Mode   Status Reason          Speed
Port
Interface
Ch #
-----
-----
Eth1/17           1       eth  access down  XCVR not inserted
auto(D) --
Eth1/18           1       eth  access down  XCVR not inserted
auto(D) --
-----
-----
Port-channel      VLAN    Type Mode   Status Reason
Speed  Protocol
Interface
-----
-----
Po10              1       eth  trunk  up     none
a-100G(D) lacp
Po11              1       eth  trunk  up     none
a-100G(D) lacp

```

6. Repita el procedimiento para la tela 2.

Identificar el almacenamiento en una configuración IP de MetroCluster

Si necesita sustituir un módulo de unidad o bandeja, primero tiene que identificar la ubicación.

Identificación de las bandejas locales y remotas

Cuando se muestra información de una bandeja desde un sitio MetroCluster, todas las unidades remotas están en 0 m, el adaptador de host iSCSI virtual. Esto significa que se accede a las unidades mediante las interfaces IP de MetroCluster. Las demás unidades son locales.

Después de identificar si una bandeja es remota (en 0 m), puede identificar aún más la unidad o la bandeja mediante el número de serie o, según las asignaciones de ID de bandeja de la configuración, por ID de bandeja.



En las configuraciones IP de MetroCluster que ejecutan ONTAP 9.4, no es necesario que el ID de bandeja sea único entre los sitios de MetroCluster. Esto incluye tanto bandejas internas (0) como externas. El número de serie es coherente cuando se visualiza desde cualquier nodo en cualquier sitio MetroCluster.

Los ID de bandeja deben ser únicos dentro del grupo de recuperación ante desastres (DR), excepto en la bandeja interna.

Con la unidad o el módulo de bandeja identificado, se puede sustituir el componente mediante el procedimiento correspondiente.

["Mantener bandejas de discos DS460C DS212C y DS212C"](#)

Ejemplo de salida sysconfig -a.

En el ejemplo siguiente se utiliza la `sysconfig -a` Comando para mostrar los dispositivos en un nodo de la configuración de IP de MetroCluster. Este nodo tiene las siguientes bandejas y dispositivos conectados:

- Ranura 0: Unidades internas (unidades locales)
- Ranura 3: ID de bandeja externa 75 y 76 (unidades locales)
- Ranura 0: Adaptador de host iSCSI virtual 0m (unidades remotas)

```
node_A_1> run local sysconfig -a

NetApp Release R9.4:  Sun Mar 18 04:14:58 PDT 2018
System ID: 1111111111 (node_A_1); partner ID: 2222222222 (node_A_2)
System Serial Number: serial-number (node_A_1)
.
.
.
slot 0: NVMe Disks
          0      : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500528)
          1      : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500735)
          2      : NETAPP   X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501165)
.
.
.
slot 3: SAS Host Adapter 3a (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:  Microsemi Corp. 110-03801 rev. A0
Part number:      111-03801+A0
Serial number:    7A1063AF14B
Date Code:        20170320
Firmware rev:     03.08.09.00
Base WWN:         5:0000d1:702e69e:80
```

```

Phy State:          [12] Enabled, 12.0 Gb/s
                   [13] Enabled, 12.0 Gb/s
                   [14] Enabled, 12.0 Gb/s
                   [15] Enabled, 12.0 Gb/s

Mini-SAS HD Vendor:      Molex Inc.
Mini-SAS HD Part Number: 112-00436+A0
Mini-SAS HD Type:       Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130640
                        75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                        75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                        75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)
                        75.3 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)
                        75.4 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502158)
.
.
.

Shelf 75: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220
Shelf 76: DS224-12  Firmware rev. IOM12 A: 0220  IOM12 B: 0220

slot 3: SAS Host Adapter 3c (PMC-Sierra PM8072 rev. C, SAS, <UP>)
MFG Part Number:      Microsemi Corp. 110-03801 rev. A0
Part number:         111-03801+A0
Serial number:       7A1063AF14B
Date Code:          20170320
Firmware rev:       03.08.09.00
Base WWN:           5:0000d1:702e69e:88
Phy State:          [0] Enabled, 12.0 Gb/s
                   [1] Enabled, 12.0 Gb/s
                   [2] Enabled, 12.0 Gb/s
                   [3] Enabled, 12.0 Gb/s

Mini-SAS HD Vendor:      Molex Inc.
Mini-SAS HD Part Number: 112-00436+A0
Mini-SAS HD Type:       Passive Copper (unequalized) 0.5m ID:00
Mini-SAS HD Serial Number: 614130691
                        75.0 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)
                        75.1 : NETAPP   X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)
                        75.2 : NETAPP   X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)

```

75.3 : NETAPP X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501793)

.
. .

Shelf 75: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220

Shelf 76: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220

slot 3: SAS Host Adapter 3d (PMC-Sierra PM8072 rev. C, SAS, <UP>)

MFG Part Number: Microsemi Corp. 110-03801 rev. A0

Part number: 111-03801+A0

Serial number: 7A1063AF14B

Date Code: 20170320

Firmware rev: 03.08.09.00

Base WWN: 5:0000d1:702e69e:8c

Phy State: [4] Enabled, 12.0 Gb/s

[5] Enabled, 12.0 Gb/s

[6] Enabled, 12.0 Gb/s

[7] Enabled, 12.0 Gb/s

Mini-SAS HD Vendor: Molex Inc.

Mini-SAS HD Part Number: 112-00436+A0

Mini-SAS HD Type: Passive Copper (unequalized) 0.5m ID:01

Mini-SAS HD Serial Number: 614130690

75.0 : NETAPP X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG501805)

75.1 : NETAPP X438_S1633400AMD NA04 381.3GB 520B/sect
(S20KNYAG502050)

75.2 : NETAPP X438_PHM2400MCTO NA04 381.3GB 520B/sect
(25M0A03WT2KA)

.
. .

Shelf 75: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220

Shelf 76: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220

slot 4: Quad 10 Gigabit Ethernet Controller X710 SFP+

.
. .

slot 0: Virtual iSCSI Host Adapter 0m

0.0 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500690)

0.1 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500571)

0.2 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500323)

```

0.3 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500724)
0.4 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500734)
0.5 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500598)
0.12 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J501094)
0.13 : NETAPP X4001S172A1T9NTE NA01 1831.1GB 4160B/sect
(S3NBNX0J500519)
.
.
.
Shelf 0: FS4483PSM3E Firmware rev. PSM3E A: 0103 PSM3E B: 0103
Shelf 35: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220
Shelf 36: DS224-12 Firmware rev. IOM12 A: 0220 IOM12 B: 0220

node_A_1::>

```

Adición de bandejas a una IP de MetroCluster mediante switches de MetroCluster de almacenamiento compartido

Es posible que tenga que añadir bandejas NS224 a un MetroCluster mediante switches de MetroCluster de almacenamiento compartido.

A partir de ONTAP 9.10.1, puede añadir bandejas NS224 de un MetroCluster utilizando los switches de almacenamiento compartido / MetroCluster. Es posible añadir más de una bandeja a la vez.

Antes de empezar

- Los nodos deben ejecutar ONTAP 9.9.1 o una versión posterior.
- Todas las bandejas NS224 conectadas actualmente deben estar conectadas a los mismos switches que MetroCluster (configuración de switch de almacenamiento compartido / MetroCluster).
- Este procedimiento no se puede utilizar para convertir una configuración con bandejas NS224 conectadas directamente o con bandejas NS224 conectadas a switches Ethernet dedicados a una configuración mediante switches de almacenamiento compartido/MetroCluster.
- ["Active el registro de la consola"](#) antes de realizar esta tarea.

Envío de un mensaje de AutoSupport personalizado antes del mantenimiento

Antes de realizar el mantenimiento, debe emitir un mensaje de AutoSupport para notificar al soporte técnico de NetApp que se está realizando el mantenimiento. Al informar al soporte técnico de que el mantenimiento está en marcha, se evita que abran un caso basándose en que se ha producido una interrupción.

Acerca de esta tarea

Esta tarea debe realizarse en cada sitio MetroCluster.

Pasos

1. Para evitar la generación automática de casos de soporte, envíe un mensaje de AutoSupport para indicar que la actualización está en curso.

- a. Emita el siguiente comando:

```
system node autosupport invoke -node * -type all -message "Maint=10h Adding  
or Removing NS224 shelves" _
```

En este ejemplo se especifica una ventana de mantenimiento de 10 horas. Es posible que desee permitir tiempo adicional, dependiendo de su plan.

Si el mantenimiento se completa antes de que haya transcurrido el tiempo, puede invocar un mensaje de AutoSupport que indique el final del período de mantenimiento:

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

- a. Repita el comando en el clúster de partners.

Comprobación del estado de la configuración de MetroCluster

Debe verificar el estado y la conectividad de la configuración de MetroCluster antes de llevar a cabo la transición.

Pasos

1. Compruebe el funcionamiento de la configuración de MetroCluster en ONTAP:

- a. Compruebe si el sistema es multivía:

```
node run -node node-name sysconfig -a
```

- b. Compruebe si hay alertas de estado en ambos clústeres:

```
system health alert show
```

- c. Confirme la configuración del MetroCluster y que el modo operativo es normal:

```
metrocluster show
```

- d. Realizar una comprobación de MetroCluster:

```
metrocluster check run
```

- e. Mostrar los resultados de la comprobación de MetroCluster:

```
metrocluster check show
```

- f. Ejecute Config Advisor.

["Descargas de NetApp: Config Advisor"](#)

- g. Después de ejecutar Config Advisor, revise el resultado de la herramienta y siga las recomendaciones del resultado para solucionar los problemas detectados.

2. Compruebe que el clúster esté en buen estado:

```
cluster show -vserver Cluster
```

```
cluster_A::> cluster show -vserver Cluster
Node           Health Eligibility Epsilon
-----
node_A_1      true   true      false
node_A_2      true   true      false

cluster_A::>
```

3. Compruebe que todos los puertos del clúster estén activos:

```
network port show -ipSPACE cluster
```

```
cluster_A::> network port show -ipSPACE cluster

Node: node_A_1-old

Port           IPspace      Broadcast Domain Link MTU      Speed(Mbps) Health
Admin/Oper    Status
-----
e0a            Cluster      Cluster      up   9000    auto/10000 healthy
e0b            Cluster      Cluster      up   9000    auto/10000 healthy

Node: node_A_2-old

Port           IPspace      Broadcast Domain Link MTU      Speed(Mbps) Health
Admin/Oper    Status
-----
e0a            Cluster      Cluster      up   9000    auto/10000 healthy
e0b            Cluster      Cluster      up   9000    auto/10000 healthy

4 entries were displayed.

cluster_A::>
```

4. Compruebe que todas las LIF del clúster estén en funcionamiento:

```
network interface show -vserver Cluster
```

Cada LIF de clúster debería mostrar el valor true para es Home y tener un administrador de estado/Oper de up/up

```
cluster_A::> network interface show -vserver cluster
```

Current Is	Logical	Status	Network	Current	
Vserver	Interface	Admin/Oper	Address/Mask	Node	Port
Home					
-----	-----	-----	-----	-----	-----
Cluster	node_A_1-old_clus1	up/up	169.254.209.69/16	node_A_1	e0a
true	node_A_1-old_clus2	up/up	169.254.49.125/16	node_A_1	e0b
true	node_A_2-old_clus1	up/up	169.254.47.194/16	node_A_2	e0a
true	node_A_2-old_clus2	up/up	169.254.19.183/16	node_A_2	e0b

```
4 entries were displayed.
```

```
cluster_A::>
```

5. Compruebe que la reversión automática está habilitada en todas las LIF del clúster:

```
network interface show -vserver Cluster -fields auto-revert
```

```

cluster_A::> network interface show -vserver Cluster -fields auto-revert

          Logical
Vserver  Interface      Auto-revert
-----  -
Cluster
          node_A_1-old_clus1
                        true
          node_A_1-old_clus2
                        true
          node_A_2-old_clus1
                        true
          node_A_2-old_clus2
                        true

          4 entries were displayed.

cluster_A::>

```

Aplicar el nuevo archivo RCF a los conmutadores



Si el conmutador ya está configurado correctamente, puede omitir estas secciones siguientes y pasar directamente a [Configuración del cifrado MACsec en switches Cisco 9336C](#), si corresponde o a [Conexión de la nueva bandeja NS224](#).

- Es necesario cambiar la configuración del switch para añadir bandejas.
- Debe revisar los detalles del cableado en ["Asignaciones de puertos de la plataforma"](#).
- Debe utilizar la herramienta **RcfFileGenerator** para crear el archivo RCF para su configuración. La **"RcfFileGenerator"** también ofrece información general sobre el cableado por puerto para cada switch. Asegúrese de elegir la cantidad correcta de bandejas. Existen archivos adicionales creados junto con el archivo RCF que proporcionan un diseño detallado del cableado que se ajusta a sus opciones específicas. Use esta información general sobre el cableado para verificar el cableado cuando cablee las nuevas bandejas.

Actualización de archivos RCF en switches MetroCluster IP

Si va a instalar un nuevo firmware de conmutador, debe instalar el firmware del conmutador antes de actualizar el archivo RCF.

Este procedimiento interrumpe el tráfico del conmutador donde se actualiza el archivo RCF. El tráfico se reanuda una vez que se aplique el nuevo archivo RCF.

Pasos

1. Compruebe el estado de la configuración.
 - a. Compruebe que los componentes de MetroCluster están en buen estado:

metrocluster check run

```
cluster_A::*> metrocluster check run
```

La operación se ejecuta en segundo plano.

- b. Después del `metrocluster check run` la operación finaliza, se ejecuta `metrocluster check show` para ver los resultados.

Después de unos cinco minutos, se muestran los siguientes resultados:

```
-----
::*> metrocluster check show

Component          Result
-----
nodes              ok
lifs               ok
config-replication ok
aggregates        ok
clusters           ok
connections        not-applicable
volumes           ok
7 entries were displayed.
```

- a. Para comprobar el estado de la operación de comprobación de MetroCluster en ejecución, utilice el comando:

```
metrocluster operation history show -job-id 38
```

- b. Compruebe que no hay alertas de estado:

```
system health alert show
```

2. Prepare los switches IP para la aplicación de los nuevos archivos RCF.

Restablecer los valores predeterminados de fábrica del conmutador IP de Cisco

Antes de instalar una nueva versión de software y RCF, debe borrar la configuración del conmutador Cisco y realizar la configuración básica.

Debe repetir estos pasos en cada uno de los switches IP de la configuración de IP de MetroCluster.

1. Restablezca el interruptor a los valores predeterminados de fábrica:

- a. Borrar la configuración existente: `write erase`

- b. Vuelva a cargar el software del conmutador: `reload`

El sistema se reinicia e introduce el asistente de configuración. Durante el arranque, si recibe el aviso Anular provisión automática y continuar con la configuración normal?(yes/no)[n], debe responder `yes` para continuar.

- c. En el asistente de configuración, introduzca los ajustes básicos del switch:
- Contraseña de administrador
 - Nombre del switch
 - Configuración de gestión fuera de banda
 - Pasarela predeterminada
 - Servicio SSH (RSA) después de completar el asistente de configuración, el switch se reinicia.
- d. Cuando se le solicite, introduzca el nombre de usuario y la contraseña para iniciar sesión en el conmutador.

El ejemplo siguiente muestra las indicaciones y respuestas del sistema al configurar el conmutador. Los soportes angulares (<<<) muestra dónde se introduce la información.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

Enter the password for "admin": password
Confirm the password for "admin": password
---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to
skip the remaining dialogs.
```

Debe introducir información básica en el siguiente conjunto de avisos, incluidos el nombre del switch, la dirección de administración y la puerta de enlace, y seleccionar SSH con RSA.

```

Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<
  Continue with Out-of-band (mgmt0) management configuration?
  (yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address **<<<
    Mgmt0 IPv4 netmask : management-IP-netmask **<<<
    Configure the default gateway? (yes/no) [y]: y **<<<
      IPv4 address of the default gateway : gateway-IP-address **<<<
    Configure advanced IP options? (yes/no) [n]:
    Enable the telnet service? (yes/no) [n]:
    Enable the ssh service? (yes/no) [y]: y **<<<
      Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<
      Number of rsa key bits <1024-2048> [1024]:
    Configure the ntp server? (yes/no) [n]:
    Configure default interface layer (L3/L2) [L2]:
    Configure default switchport interface state (shut/noshut) [noshut]:
shut **<<<
      Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:

```

El conjunto final de avisos completa la configuración:

The following configuration will be applied:

```
password strength-check
 switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
no feature telnet
ssh key rsa 1024 force
feature ssh
system default switchport
system default switchport shutdown
copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown
```

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:

```
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-Plane
is protected with policy copp-system-p-policy-strict.
```

```
[#####] 100%
Copy complete.
```

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Guarde la configuración:

```
IP_switch-A-1# copy running-config startup-config
```

3. Reinicie el conmutador y espere a que se vuelva a cargar:

```
IP_switch-A-1# reload
```

4. Repita los pasos anteriores en los otros tres switches de la configuración IP de MetroCluster.

Descargar e instalar el software del switch Cisco NX-OS

Debe descargar el archivo del sistema operativo del conmutador y el archivo RCF en cada switch de la configuración IP de MetroCluster.

Esta tarea requiere software de transferencia de archivos, como FTP, TFTP, SFTP o SCP para copiar los archivos en los switches.

Estos pasos deben repetirse en cada switch IP de la configuración de IP de MetroCluster.

Debe utilizar la versión de software del switch compatible.

"Hardware Universe de NetApp"

1. Descargue el archivo de software NX-OS admitido.

"Descarga de software de Cisco"

2. Copie el software del conmutador en el conmutador: `copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf management`

En este ejemplo, el archivo `nxos.7.0.3.I4.6.bin` se copia desde el servidor SFTP `10.10.99.99` en el bootflash local:

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin          100% 666MB 7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
```

3. Verifique en cada switch que los archivos NX-OS del switch estén presentes en el directorio bootflash de cada switch: `dir bootflash:`

El ejemplo siguiente muestra que los archivos están presentes en `IP_switch_A_1`:

```

IP_switch_A_1# dir bootflash:
      .
      .
      .
698629632   Jun 13 21:37:44 2017   nxos.7.0.3.I4.6.bin
      .
      .
      .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#

```

4. Instale el software del conmutador: `install all nxos bootflash:nxos.version-number.bin`

El conmutador se volverá a cargar (reiniciar) automáticamente después de instalar el software del conmutador.

En el ejemplo siguiente se muestra la instalación del software en IP_switch_A_1:

```

IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[#####] 100% -- SUCCESS

Verifying image type.
[#####] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS           [#####] 100%
-- SUCCESS

Performing module support checks.           [#####] 100%
-- SUCCESS

Notifying services about system upgrade.    [#####] 100%

```

```
-- SUCCESS
```

```
Compatibility check is done:
```

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default upgrade is not hitless

```
Images will be upgraded according to following table:
```

Module Required	Image	Running-Version(pri:alt)	New-Version	Upg-
1	nxos	7.0(3)I4(1)	7.0(3)I4(6)	yes
1	bios	v04.24(04/21/2016)	v04.24(04/21/2016)	no

```
Switch will be reloaded for disruptive upgrade.
```

```
Do you want to continue with the installation (y/n)? [n] y
```

```
Install is in progress, please wait.
```

```
Performing runtime checks. [#####] 100% --  
SUCCESS
```

```
Setting boot variables.  
[#####] 100% -- SUCCESS
```

```
Performing configuration copy.  
[#####] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.  
Warning: please do not remove or power off the module at this time.  
[#####] 100% -- SUCCESS
```

```
Finishing the upgrade, switch will reboot in 10 seconds.  
IP_switch_A_1#
```

5. Espere a que el conmutador se vuelva a cargar y, a continuación, inicie sesión en el conmutador.

Cuando el conmutador haya reiniciado, aparecerá el mensaje de inicio de sesión:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Compruebe que se ha instalado el software del conmutador: `show version`

El siguiente ejemplo muestra el resultado:

```

IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)   **<<< switch software version**
  BIOS compile time: 04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time: 3/9/2017 22:00:00 [03/10/2017 07:05:18]

Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash: 14900224 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after Mon Jun 10 21:43:52 2017

Reason: Reset due to upgrade
System version: 7.0(3)I4(1)
Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#

```

7. Repita estos pasos en los tres switches IP restantes de la configuración IP de MetroCluster.

Configuración del cifrado MACsec en switches Cisco 9336C

Si lo desea, puede configurar el cifrado MACsec en los puertos ISL WAN que se ejecutan entre los sitios. Debe configurar MACsec después de aplicar el archivo RCF correcto.



El cifrado MACsec sólo se puede aplicar a los puertos WAN ISL.

Requisitos de licencia para MACsec

MACsec requiere una licencia de seguridad. Para obtener una explicación completa del esquema de licencias de Cisco NX-OS y de cómo obtener y solicitar licencias, consulte ["Guía de licencias de Cisco NX-OS"](#)

Habilitar ISL WAN de cifrado Cisco MACsec en configuraciones IP de MetroCluster

Puede habilitar el cifrado MACsec para los switches Cisco 9336C en los ISL WAN en una configuración IP MetroCluster.

1. Entre en el modo de configuración global: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Active MACsec y MKA en el dispositivo: `feature macsec`

```
IP_switch_A_1(config)# feature macsec
```

3. Copie la configuración en ejecución en la configuración de inicio: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Desactivación del cifrado Cisco MACsec

Es posible que deba deshabilitar el cifrado MACsec para los switches Cisco 9336C en los ISL WAN en una configuración IP de MetroCluster.



Si desactiva el cifrado, también debe eliminar las claves.

1. Entre en el modo de configuración global: `configure terminal`

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Desactive la configuración de MACsec en el dispositivo: `macsec shutdown`

```
IP_switch_A_1(config)# macsec shutdown
```



Si selecciona la opción no, se restaurará la función MACsec.

3. Seleccione la interfaz que ya ha configurado con MACsec.

Puede especificar el tipo de interfaz y la identidad. En el caso de un puerto Ethernet, utilice el puerto o la ranura ethernet.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Elimine la cadena de claves, la directiva y la cadena de claves de reserva configuradas en la interfaz para eliminar la configuración de MACsec: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

5. Repita los pasos 3 y 4 en todas las interfaces en las que esté configurado MACsec.
6. Copie la configuración en ejecución en la configuración de inicio: `copy running-config startup-config`

```
IP_switch_A_1(config)# copy running-config startup-config
```

Configuración de una cadena de claves y claves MACsec

Para obtener más información sobre la configuración de una cadena de claves MACsec, consulte la documentación de Cisco del conmutador.

Conexión de la nueva bandeja NS224

Pasos

1. Instale el kit de montaje de raíl incluido con la bandeja mediante el folleto de instalación incluido en la caja del kit.
2. Utilice el folleto de instalación para instalar y proteger la bandeja en los soportes de soporte, así como en el rack o armario.
3. Conecte los cables de alimentación a la bandeja, fíjelos con el retenedor del cable de alimentación y, a continuación, conecte los cables de alimentación a distintas fuentes de alimentación para obtener flexibilidad.

Una bandeja se enciende cuando está conectada a una fuente de alimentación; no tiene interruptores de alimentación. Cuando funciona correctamente, el LED bicolor de una fuente de alimentación se ilumina en verde.

4. Establezca el ID de bandeja en un número único dentro de la pareja de alta disponibilidad y en toda la configuración.
5. Conecte los puertos de la bandeja en el siguiente orden:
 - a. Conecte NSM-A, e0a al conmutador (Switch-A1 o Switch-B1)
 - b. Conecte NSM-B, e0a al conmutador (Switch-A2 o Switch-B2)

- c. Conecte el NSM-A y el e0b al interruptor (interruptor A1 o interruptor B1)
 - d. Conecte el NSM-B, e0b al interruptor (interruptor-A2 o interruptor-B2)
6. Utilice la distribución de cableado generada con la herramienta **RcfFileGenerator** para conectar la bandeja a los puertos apropiados.

Una vez que la bandeja nueva se ha cableado correctamente, ONTAP la detecta automáticamente en la red.

Configure el cifrado integral en una configuración IP de MetroCluster

A partir de ONTAP 9.15.1, puede configurar el cifrado integral para cifrar el tráfico de back-end, como NVlog y los datos de replicación de almacenamiento, entre los sitios en una configuración de IP de MetroCluster.

Acerca de esta tarea

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Para poder configurar el cifrado integral, se debe ["Configure la gestión de claves externas"](#).
- Revise los sistemas compatibles y la versión mínima de ONTAP requerida para configurar el cifrado integral en una configuración de IP de MetroCluster:

Versión de ONTAP mínima	Sistemas compatibles
ONTAP 9.15.1	<ul style="list-style-type: none"> • AFF A400 • FAS8300 • FAS8700

Habilite el cifrado integral

Realice los siguientes pasos para habilitar el cifrado de extremo a extremo.

Pasos

1. Compruebe el estado de la configuración de MetroCluster.
 - a. Compruebe que los componentes de MetroCluster están en buen estado:

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

La operación se ejecuta en segundo plano.

- b. Después del `metrocluster check run` la operación finaliza, ejecute:

```
metrocluster check show
```

Después de unos cinco minutos, se muestran los siguientes resultados:

```
cluster_A:::*> metrocluster check show
```

Component	Result
-----	-----
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok
clusters	ok
connections	not-applicable
volumes	ok

7 entries were displayed.

a. Comprobar el estado de la operación de comprobación de MetroCluster en ejecución:

```
metrocluster operation history show -job-id <id>
```

b. Compruebe que no hay alertas de estado:

```
system health alert show
```

2. Compruebe que la gestión de claves externas está configurada en ambos clústeres:

```
security key-manager external show-status
```

3. Habilite el cifrado integral para cada grupo de recuperación ante desastres:

```
metrocluster modify -is-encryption-enabled true -dr-group-id  
<dr_group_id>
```

ejemplo

```

cluster_A::*> metrocluster modify -is-encryption-enabled true -dr-group
-id 1
Warning: Enabling encryption for a DR Group will secure NVLog and
Storage
        replication data sent between MetroCluster nodes and have an
impact on
        performance. Do you want to continue? {y|n}: y
[Job 244] Job succeeded: Modify is successful.

```

Repita este paso con cada grupo de recuperación ante desastres de la configuración.

4. Verifique que el cifrado integral está activado:

```
metrocluster node show -fields is-encryption-enabled
```

ejemplo

```

cluster_A::*> metrocluster node show -fields is-encryption-enabled

dr-group-id cluster      node          configuration-state is-encryption-
enabled
-----
1           cluster_A    node_A_1     configured         true
1           cluster_A    node_A_2     configured         true
1           cluster_B    node_B_1     configured         true
1           cluster_B    node_B_2     configured         true
4 entries were displayed.

```

Deshabilite el cifrado integral

Realice los siguientes pasos para desactivar el cifrado de extremo a extremo.

Pasos

1. Compruebe el estado de la configuración de MetroCluster.
 - a. Compruebe que los componentes de MetroCluster están en buen estado:

```
metrocluster check run
```

```
cluster_A::*> metrocluster check run
```

La operación se ejecuta en segundo plano.

b. Después del `metrocluster check` run la operación finaliza, ejecute:

```
metrocluster check show
```

Después de unos cinco minutos, se muestran los siguientes resultados:

```
cluster_A:::*> metrocluster check show
```

Component	Result
nodes	ok
lifs	ok
config-replication	ok
aggregates	ok
clusters	ok
connections	not-applicable
volumes	ok

7 entries were displayed.

a. Comprobar el estado de la operación de comprobación de MetroCluster en ejecución:

```
metrocluster operation history show -job-id <id>
```

b. Compruebe que no hay alertas de estado:

```
system health alert show
```

2. Compruebe que la gestión de claves externas está configurada en ambos clústeres:

```
security key-manager external show-status
```

3. Deshabilite el cifrado integral en cada grupo de recuperación ante desastres:

```
metrocluster modify -is-encryption-enabled false -dr-group-id  
<dr_group_id>
```

ejemplo

```
cluster_A::*> metrocluster modify -is-encryption-enabled false -dr-group
-id 1
[Job 244] Job succeeded: Modify is successful.
```

Repita este paso con cada grupo de recuperación ante desastres de la configuración.

4. Verifique que el cifrado integral está desactivado:

```
metrocluster node show -fields is-encryption-enabled
```

ejemplo

```
cluster_A::*> metrocluster node show -fields is-encryption-enabled

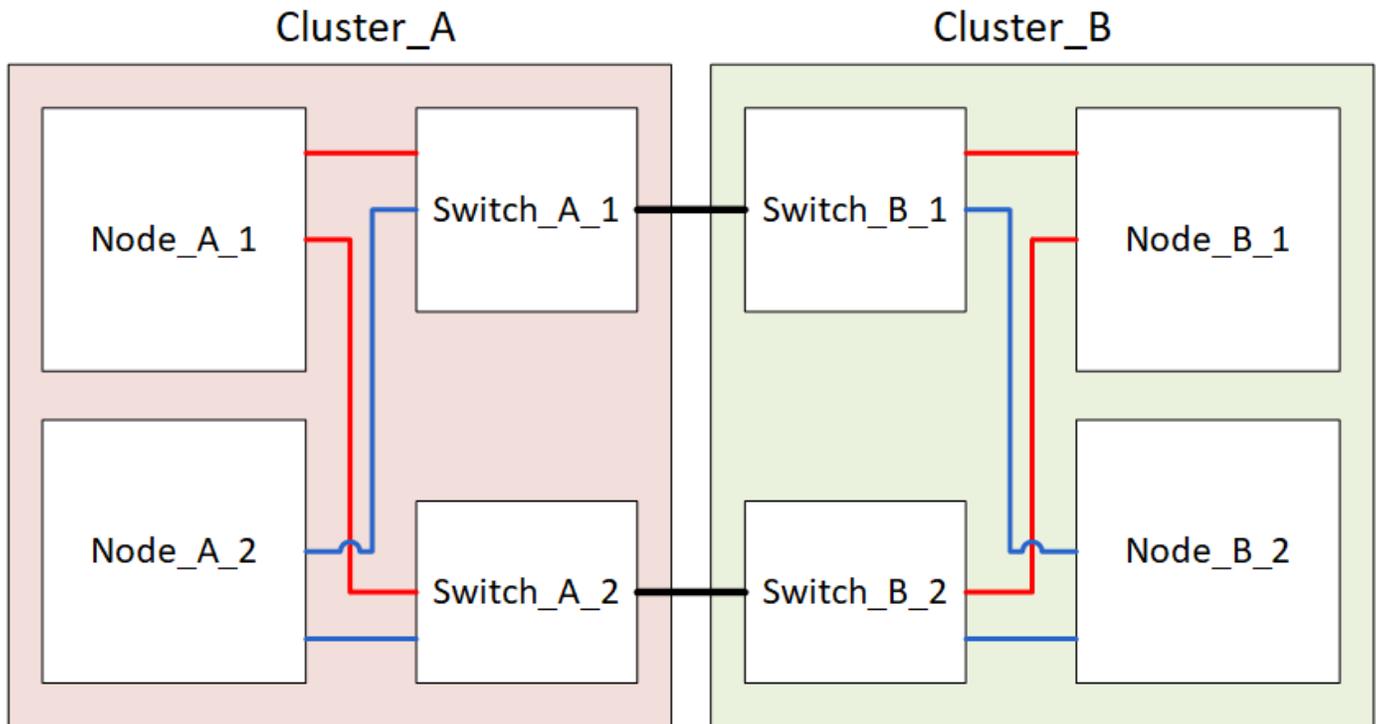
dr-group-id cluster      node      configuration-state is-encryption-
enabled
-----
1           cluster_A    node_A_1  configured         false
1           cluster_A    node_A_2  configured         false
1           cluster_B    node_B_1  configured         false
1           cluster_B    node_B_2  configured         false
4 entries were displayed.
```

Apagar y encender un sitio único en una configuración IP de MetroCluster

Si necesita realizar el mantenimiento del sitio o reubicar un solo sitio en una configuración IP de MetroCluster, debe saber cómo apagar y encender el sitio.

Si necesita reubicar y reconfigurar un sitio (por ejemplo, si necesita ampliar un clúster de cuatro nodos a uno de ocho nodos), no podrá completar estas tareas al mismo tiempo. Este procedimiento sólo cubre los pasos necesarios para realizar el mantenimiento del sitio o para reubicar un sitio sin cambiar su configuración.

El siguiente diagrama muestra una configuración de MetroCluster. El Cluster_B se apaga para realizar tareas de mantenimiento.



Apagar un sitio MetroCluster

Debe apagar un sitio y todo el equipo antes de que pueda comenzar el mantenimiento o la reubicación del sitio.

Acerca de esta tarea

Todos los comandos de los siguientes pasos se emiten desde el sitio que permanece encendido.

Pasos

1. Antes de comenzar, compruebe que los agregados no reflejados del sitio no están desconectados.
2. Compruebe el funcionamiento de la configuración de MetroCluster en ONTAP:
 - a. Compruebe si el sistema es multivía:

```
node run -node node-name sysconfig -a
```

- b. Compruebe si hay alertas de estado en ambos clústeres:

```
system health alert show
```

- c. Confirme la configuración del MetroCluster y que el modo operativo es normal:

```
metrocluster show
```

- d. Realice una comprobación de MetroCluster:

```
metrocluster check run
```

- e. Mostrar los resultados de la comprobación de MetroCluster:

```
metrocluster check show
```

- f. Compruebe si hay alertas de estado en los switches (si existen):

```
storage switch show
```

- g. Ejecute Config Advisor.

["Descargas de NetApp: Config Advisor"](#)

- h. Después de ejecutar Config Advisor, revise el resultado de la herramienta y siga las recomendaciones del resultado para solucionar los problemas detectados.

3. Desde el sitio que desea mantener activo, implemente la conmutación de sitios:

```
metrocluster switchover
```

```
cluster_A::*> metrocluster switchover
```

La operación puede tardar varios minutos en completarse.

4. Supervise y verifique que se haya completado la conmutación:

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
Operation: Switchover
Start time: 10/4/2012 19:04:13
State: in-progress
End time: -
Errors:

cluster_A::*> metrocluster operation show
Operation: Switchover
Start time: 10/4/2012 19:04:13
State: successful
End time: 10/4/2012 19:04:22
Errors: -
```

5. Si tiene una configuración IP de MetroCluster que ejecuta ONTAP 9.6 o posterior, espere a que los complejos del sitio de recuperación ante desastres se conecten y las operaciones de reparación se completen automáticamente.

En configuraciones IP de MetroCluster que ejecutan ONTAP 9,5 o una versión anterior, los nodos del sitio de recuperación ante desastres no arrancan automáticamente en ONTAP y los complejos permanecen sin conexión.

6. Mueva todos los volúmenes y LUN que pertenecen a los agregados no reflejados sin conexión.
 - a. Mueva los volúmenes sin conexión.

```
cluster_A::* volume offline <volume name>
```

b. Desconecte las LUN.

```
cluster_A::* lun offline lun_path <lun_path>
```

7. Mover agregados no reflejados sin conexión: `storage aggregate offline`

```
cluster_A*::> storage aggregate offline -aggregate <aggregate-name>
```

8. En función de su configuración y versión de ONTAP, identifique y mueva los complejos afectados sin conexión que se encuentren en la ubicación ante desastres (Cluster_B).

Debe mover los siguientes complejos sin conexión:

- Complejos no reflejados que residen en discos ubicados en el sitio de recuperación ante desastres.

Si no mueve los complejos no reflejados en el sitio de recuperación ante desastres sin conexión, se puede producir una interrupción del servicio cuando el sitio de recuperación ante desastres se apague más tarde.

- Plexes reflejados que residen en discos ubicados en el centro de recuperación ante desastres para el mirroring de agregados. Una vez que se han movido fuera de línea, no se puede acceder a los complejos.

a. Identifique los complejos afectados.

Los complejos que son propiedad de nodos en el sitio superviviente consisten en discos de la piscina 1. Los complejos que son propiedad de nodos en el sitio de desastre consisten en discos de la piscina 0.

```

Cluster_A::> storage aggregate plex show -fields aggregate,status,is-
online,Plex,pool
aggregate      plex  status          is-online pool
-----
Node_B_1_aggr0 plex0 normal,active true      0
Node_B_1_aggr0 plex1 normal,active true      1

Node_B_2_aggr0 plex0 normal,active true      0
Node_B_2_aggr0 plex5 normal,active true      1

Node_B_1_aggr1 plex0 normal,active true      0
Node_B_1_aggr1 plex3 normal,active true      1

Node_B_2_aggr1 plex0 normal,active true      0
Node_B_2_aggr1 plex1 normal,active true      1

Node_A_1_aggr0 plex0 normal,active true      0
Node_A_1_aggr0 plex4 normal,active true      1

Node_A_1_aggr1 plex0 normal,active true      0
Node_A_1_aggr1 plex1 normal,active true      1

Node_A_2_aggr0 plex0 normal,active true      0
Node_A_2_aggr0 plex4 normal,active true      1

Node_A_2_aggr1 plex0 normal,active true      0
Node_A_2_aggr1 plex1 normal,active true      1
14 entries were displayed.

Cluster_A::>

```

Los plex afectados son los que son remotos al clúster A. La siguiente tabla muestra si los discos son locales o remotos en relación con el clúster A:

Nodo	Discos en el pool	¿Los discos se deben establecer sin conexión?	Ejemplo de complejos que se van a mover fuera de línea
Nodo_A_1 y nodo_A_2	Discos en el pool 0	No Los discos son locales para el clúster A.	-

Discos en el pool 1	Sí. Los discos son remotos para el clúster A.	Node_A_1_aggr0/plex4 Node_A_1_aggr1/plex1 Node_A_2_aggr0/plex4 Node_A_2_aggr1/plex1	Nodo _B_1 y nodo _B_2
Discos en el pool 0	Sí. Los discos son remotos para el clúster A.	Node_B_1_aggr1/plex0 Node_B_1_aggr0/plex0 Node_B_2_aggr0/plex0 Node_B_2_aggr1/plex0	Discos en el pool 1

b. Mueva los complejos afectados sin conexión:

```
storage aggregate plex offline
```

```
storage aggregate plex offline -aggregate Node_B_1_aggr0 -plex plex0
```

+



Realice este paso para todos los plexes que tengan discos remotos para Cluster_A.

9. Desconecta de forma persistente los puertos del switch ISL según el tipo de switch.

10. Detenga los nodos ejecutando el siguiente comando en cada nodo:

```
node halt -inhibit-takeover true -skip-lif-migration true -node <node-name>
```

11. Apague el equipo en el sitio de desastre.

Debe apagar el siguiente equipo en el orden indicado:

- Controladoras de almacenamiento: Las controladoras de almacenamiento actualmente deben estar en LOADER aviso, debe apagarlos por completo.
- Switches IP de MetroCluster
- Bandejas de almacenamiento

Reubicación del sitio de alimentación fuera del MetroCluster

Una vez apagado el sitio, puede comenzar a realizar tareas de mantenimiento. Este procedimiento es el mismo, tanto si se reubican los componentes de MetroCluster dentro del mismo centro de datos como si se reubican a otro centro de datos.

- El hardware debe cablearse del mismo modo que el sitio anterior.
- Si la velocidad, longitud o número del enlace entre switches (ISL) ha cambiado, todos ellos deben volver a configurarse.

Pasos

1. Verifique que el cableado de todos los componentes se registre con cuidado para poder volver a conectarlo correctamente en la nueva ubicación.
2. Reubique físicamente todo el hardware, las controladoras de almacenamiento, los switches IP, FibreBridges y las bandejas de almacenamiento.
3. Configure los puertos ISL y compruebe la conectividad entre sitios.
 - a. Encienda los interruptores IP.



No encienda ningún otro equipo.

4. Utilice herramientas en los switches (según estén disponibles) para verificar la conectividad entre sitios.



Solo debe continuar si los enlaces están correctamente configurados y estables.

5. Vuelva a desactivar los vínculos si se encuentran estables.

Encienda la configuración de MetroCluster y vuelva al funcionamiento normal

Tras completar el mantenimiento o mover el sitio, debe encender el sitio y restablecer la configuración de MetroCluster.

Acerca de esta tarea

Todos los comandos de los pasos siguientes se emiten en el sitio que se enciende.

Pasos

1. Encienda los switches.

Primero debe encender los interruptores. Es posible que se hayan encendido durante el paso anterior si se reubicó el sitio.

- a. Vuelva a configurar el enlace entre switches (ISL) si es necesario o si no se ha completado como parte de la reubicación.
 - b. Habilite el ISL si se ha completado la delimitación.
 - c. Verifique el ISL.
2. Encienda las controladoras de almacenamiento y espere hasta que vea el `LOADER` prompt. Las controladoras no deben arrancarse por completo.

Si el inicio automático está activado, pulse `Ctrl+C` para detener el arranque automático de las controladoras.

3. Encienda las bandejas teniendo tiempo suficiente para que se enciendan por completo.
4. Verifique que el almacenamiento esté visible.
 - a. Compruebe que el almacenamiento está visible en el sitio superviviente. Vuelva a conectar los complejos sin conexión para reiniciar la operación de resincronización y restablecer `SyncMirror`.
 - b. Compruebe que el almacenamiento local sea visible en el nodo en modo de mantenimiento:

```
disk show -v
```

5. Restablezca la configuración de MetroCluster.

Siga las instrucciones de "[Verificación de que su sistema está listo para una conmutación de estado](#)" Para llevar a cabo operaciones de reparación y conmutación de estado de acuerdo con su configuración de MetroCluster.

Apagado de una configuración de IP de MetroCluster completa

Debe apagar toda la configuración de IP de MetroCluster y todo el equipo antes de que pueda iniciarse el mantenimiento o la reubicación.



A partir de ONTAP 9.8, el **storage switch** el comando se sustituye por **system switch**. Los siguientes pasos muestran el **storage switch** Pero si ejecuta ONTAP 9.8 o una versión posterior, el **system switch** el comando es preferido.

1. Compruebe la configuración de MetroCluster en ambos sitios de la configuración de MetroCluster.

- a. Confirmar que la configuración de MetroCluster y el modo operativo son normales.

```
metrocluster show
```

- b. Ejecute el siguiente comando:

```
metrocluster interconnect show
```

- c. Confirme la conectividad con los discos introduciendo el siguiente comando en uno de los nodos MetroCluster:

```
run local sysconfig -v
```

- d. Ejecute el siguiente comando:

```
storage port show
```

- e. Ejecute el siguiente comando:

```
storage switch show
```

- f. Ejecute el siguiente comando:

```
network interface show
```

- g. Ejecute el siguiente comando:

```
network port show
```

- h. Ejecute el siguiente comando:

```
network device-discovery show
```

- i. Realice una comprobación de MetroCluster:

```
metrocluster check run
```

- j. Mostrar los resultados del control MetroCluster:

```
metrocluster check show
```

- k. Ejecute el siguiente comando:

```
metrocluster configuration-settings interface show
```

2. Si es necesario, deshabilite AUSO modificando EL dominio de fallo DE AUSO a.

```
auso-disabled
```

```
cluster_A_site_A::*>metrocluster modify -auto-switchover-failure-domain
auso-disabled
```



En una configuración de IP de MetroCluster, el dominio de fallo DE AUSO ya está establecido en 'auso-disabled' a menos que la configuración esté configurada con Mediator de ONTAP.

3. Compruebe el cambio con el comando

metrocluster operation show

```
cluster_A_site_A::*> metrocluster operation show
Operation: modify
State: successful
Start Time: 4/25/2020 20:20:36
End Time: 4/25/2020 20:20:36
Errors: -
```

4. Detenga los nodos:

halt

```
system node halt -node node1_SiteA -inhibit-takeover true -ignore-quorum
-warnings true
```

5. Apague el siguiente equipo en el sitio:

- Controladoras de almacenamiento
- Switches IP de MetroCluster
- Bandejas de almacenamiento

6. Espere treinta minutos y, a continuación, encienda todas las bandejas de almacenamiento, los switches IP de MetroCluster y las controladoras de almacenamiento.

7. Después de encender las controladoras, compruebe la configuración de MetroCluster en ambos sitios.

Para verificar la configuración, repita el paso 1.

8. Realice comprobaciones de ciclo de encendido y apagado.

a. Compruebe que todas las SVM sincronizada en origen estén en línea:

```
vserver show
```

b. Inicie cualquier SVM sincronizada en origen que no estén en línea:

```
vserver start
```

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 INTERRUPTIÓN 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.