Configure los componentes de hardware de MetroCluster

ONTAP MetroCluster

NetApp
April 25, 2024

Tabla de contenidos

Configure los componentes de hardware de MetroCluster

Parte de una configuración de IP de MetroCluster

Al planificar la configuración IP de MetroCluster, deberá comprender los componentes de hardware y cómo se interconectan.

Elementos clave del hardware

Una configuración IP de MetroCluster incluye los siguientes elementos clave de hardware:

- Controladoras de almacenamiento

  Las controladoras de almacenamiento se configuran como clústeres de dos nodos.

- Red de IP

  Esta red IP back-end proporciona conectividad para dos usos distintos:

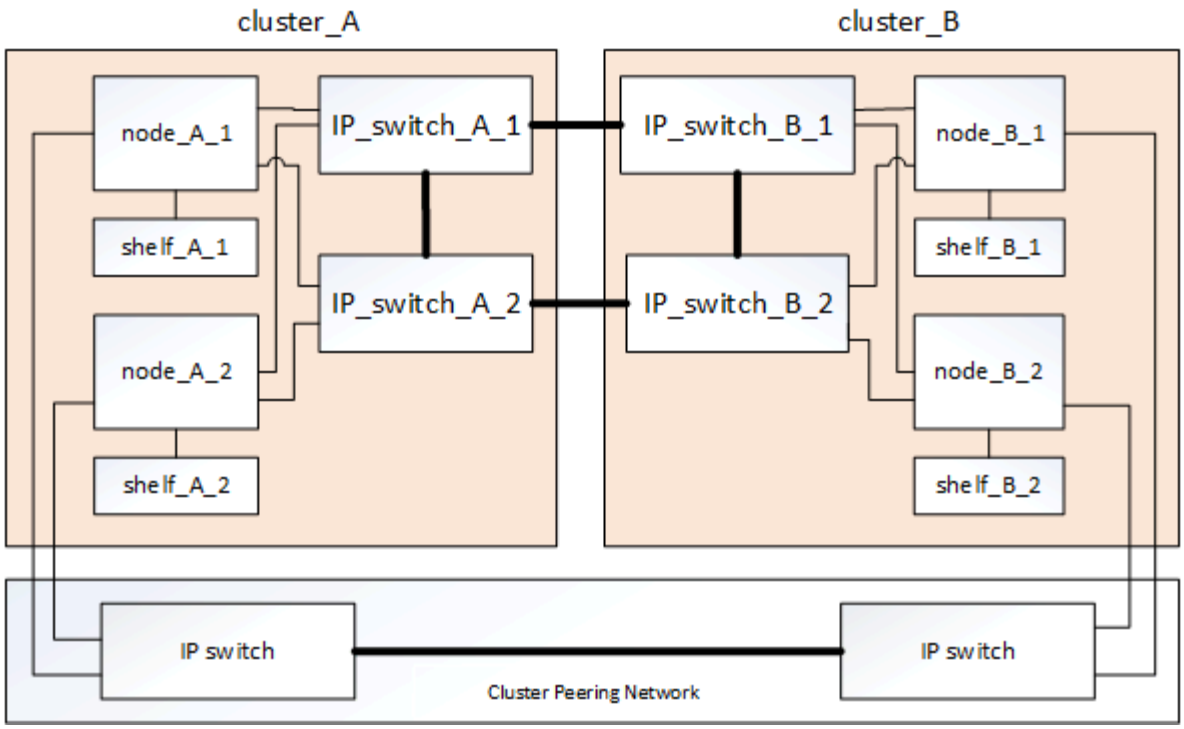
  - Conectividad de clúster estándar para las comunicaciones dentro del clúster.

    Esta es la misma funcionalidad de switch de clúster que se utiliza en clústeres de ONTAP sin switches de MetroCluster.

  - Conectividad back-end de MetroCluster para replicación de datos de almacenamiento y caché no volátil.

- Red de conexión de clústeres entre iguales

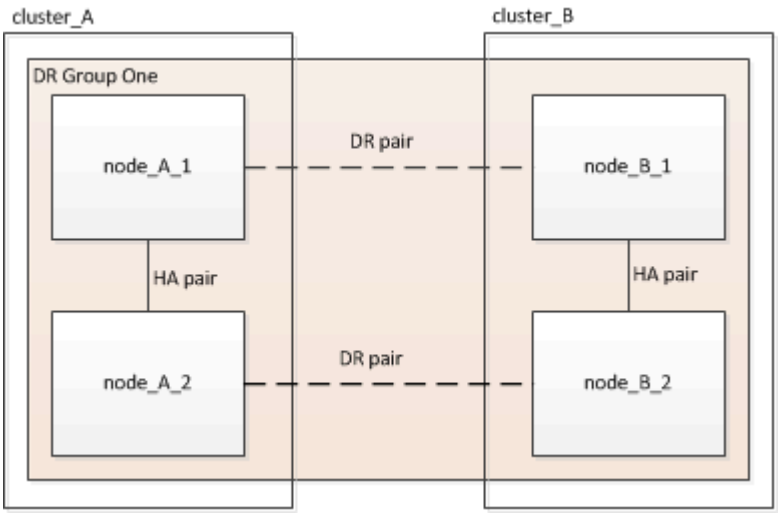
  La red de paridad de clústeres ofrece conectividad para el mirroring de la configuración de clústeres, lo que incluye la configuración de máquinas virtuales de almacenamiento (SVM). La configuración de todas las SVM de un clúster se refleja en el clúster partner.



Grupos de recuperación ante desastres

Una configuración IP de MetroCluster consta de un grupo de recuperación ante desastres de cuatro nodos.

En la siguiente ilustración, se muestra la organización de los nodos en una configuración de MetroCluster de cuatro nodos:

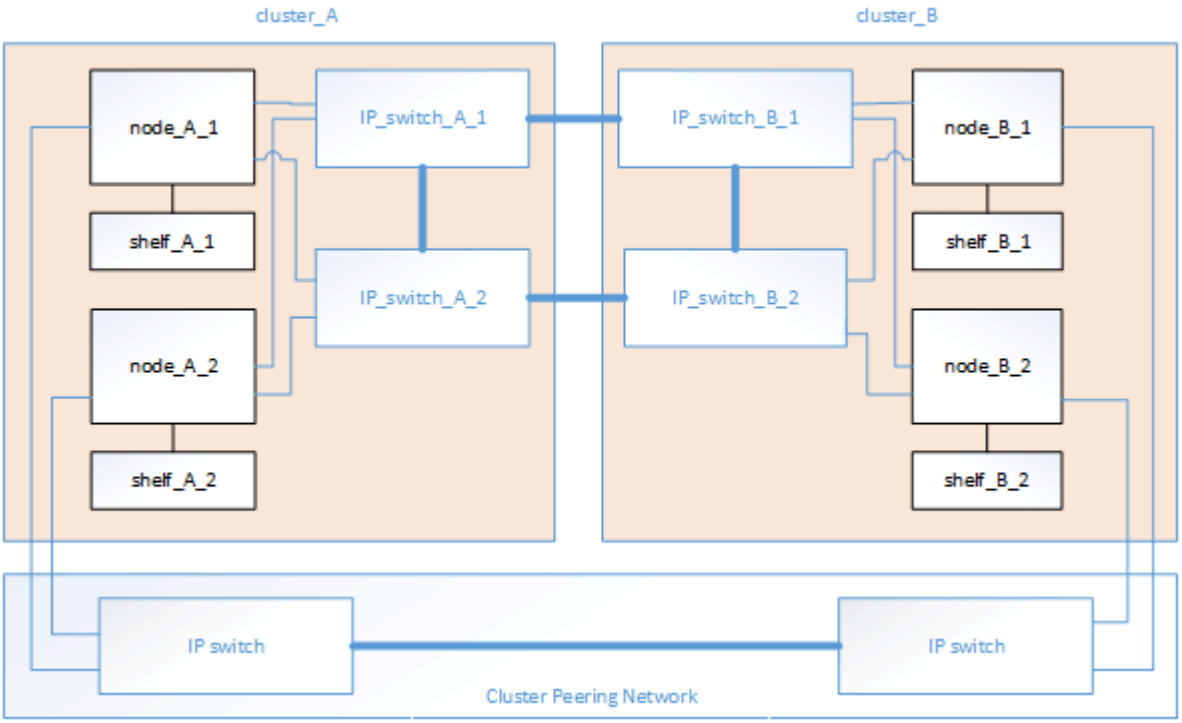


Una ilustración de los pares de alta disponibilidad locales en una configuración MetroCluster

Cada sitio de MetroCluster consta de controladoras de almacenamiento configuradas como par de alta disponibilidad. Esto permite una redundancia local de modo que si falla una controladora de almacenamiento, su partner de alta disponibilidad local puede hacer el relevo. Estos fallos pueden gestionarse sin una operación de conmutación de sitios MetroCluster.

Las operaciones locales de conmutación por error y devolución del servicio de alta disponibilidad se realizan

con los comandos de conmutación por error del almacenamiento, del mismo modo que una configuración que no sea de MetroCluster.

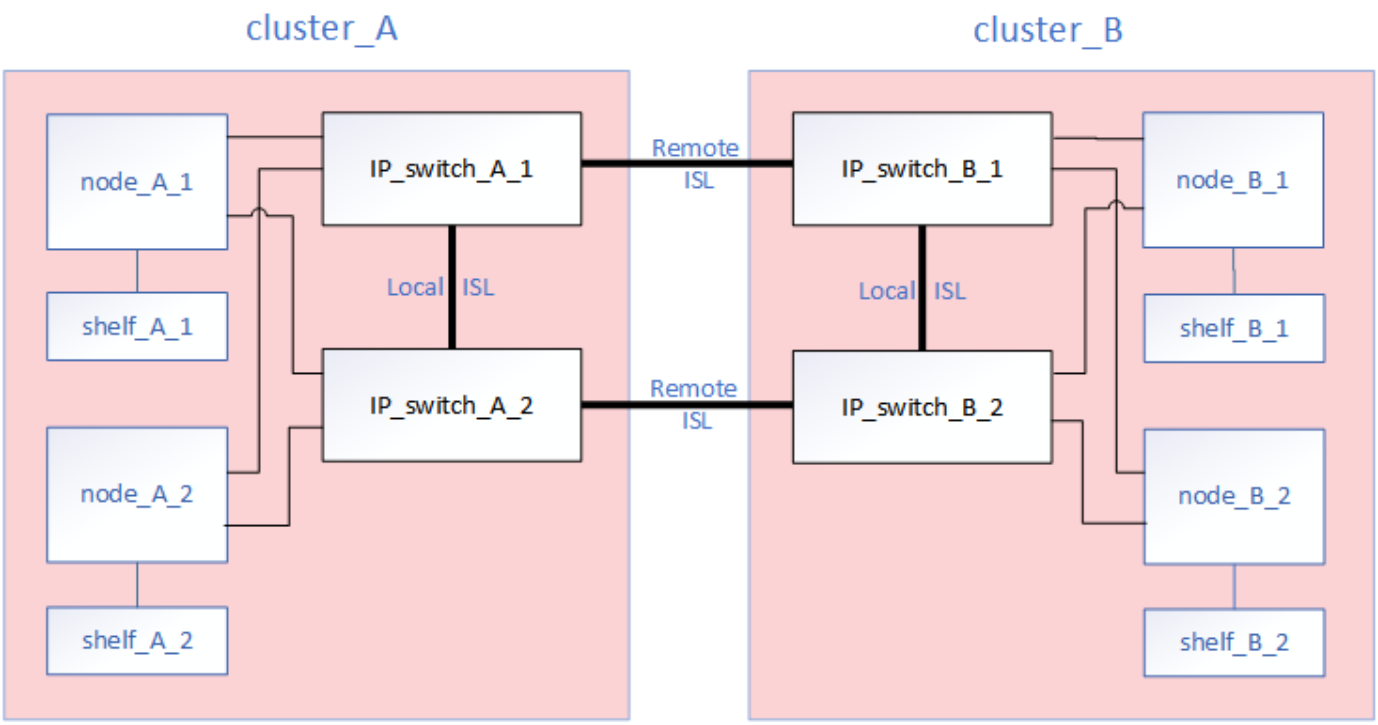


Información relacionada

"Conceptos de ONTAP"

Ilustración de la red de interconexión de clúster y la IP de MetroCluster

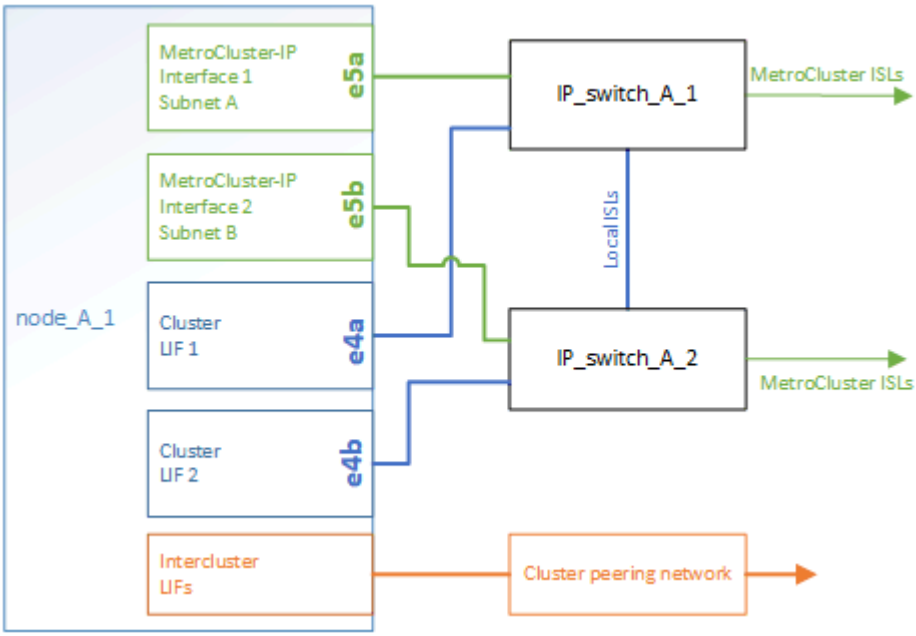
En general, los clústeres de ONTAP incluyen una red de interconexión de clúster para el tráfico entre los nodos del clúster. En configuraciones de IP de MetroCluster, esta red también se utiliza para transportar tráfico de replicación de datos entre los sitios de MetroCluster.



Cada nodo de la configuración IP de MetroCluster tiene interfaces dedicadas para la conexión con la red IP back-end:

- Dos interfaces MetroCluster IP
- Dos interfaces de clúster locales

En la siguiente ilustración se muestran estas interfaces. El uso de puertos mostrado es para un sistema A700 o FAS9000 de AFF.



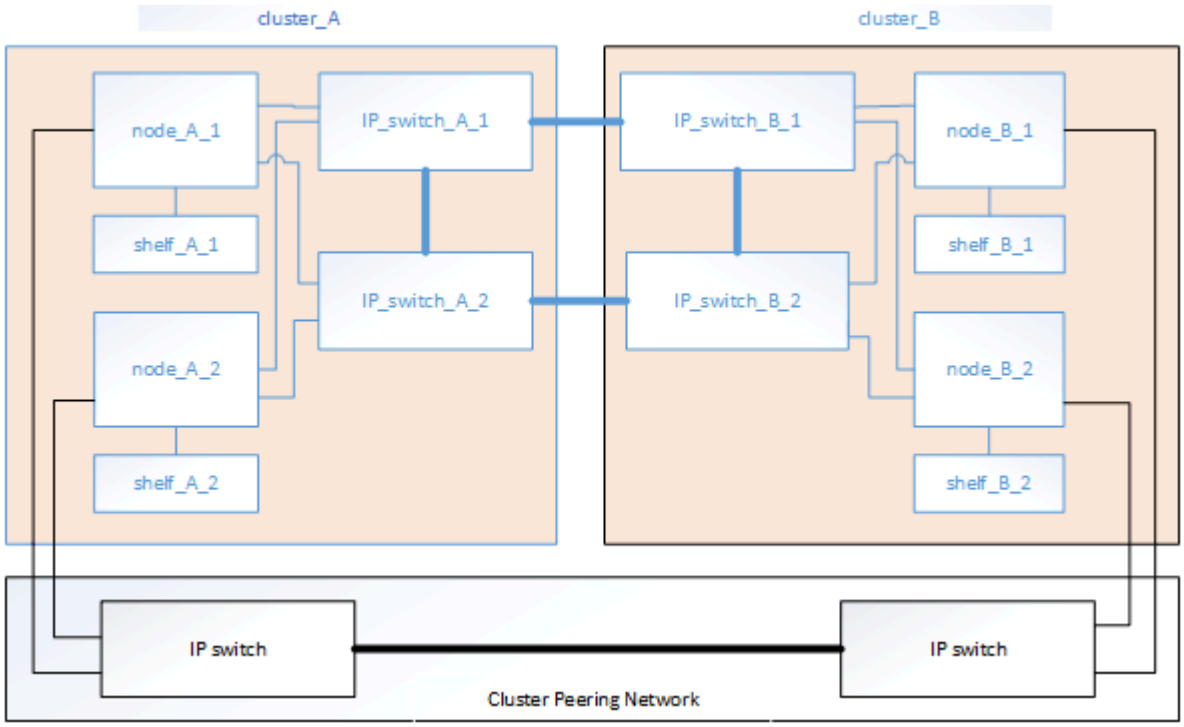
Información relacionada

"Consideraciones sobre la configuración de IP de MetroCluster"

Ilustración de la red de paridad de clústeres

Los dos clústeres de la configuración de MetroCluster tienen una relación entre iguales a través de una red de clústeres proporcionada por el cliente. Cluster peering admite el mirroring síncrono de máquinas virtuales de almacenamiento (SVM, antes denominadas Vserver) entre sitios.

Las LIF de interconexión de clústeres deben configurarse en cada nodo de la configuración de MetroCluster y los clústeres deben configurarse para paridad. Los puertos con las LIF de interconexión de clústeres están conectados a la red de paridad de clústeres proporcionada por el cliente. La replicación de la configuración de SVM se realiza en esta red a través del servicio de replicación de configuración.



Información relacionada

"Configuración exprés de relación entre iguales de clústeres y SVM"

"Consideraciones que tener en cuenta al configurar la relación de clústeres entre iguales"

"Conectar el cableado de las conexiones de los clústeres entre iguales"

"Una relación entre iguales de los clústeres"

Componentes de MetroCluster IP y convenciones de nomenclatura necesarias

Al planificar la configuración IP de MetroCluster, debe comprender los componentes de hardware y software necesarios y compatibles. Para mayor comodidad y claridad, también debe comprender las convenciones de nomenclatura que se utilizan para los componentes en ejemplos de la documentación.

Software y hardware compatibles

El hardware y el software deben ser compatibles con la configuración IP de MetroCluster.

"Hardware Universe de NetApp"

Al usar sistemas AFF, todos los módulos de controladora de la configuración MetroCluster deben configurarse como sistemas AFF.

Requisitos de redundancia de hardware en una configuración IP de MetroCluster

Debido a la redundancia del hardware en la configuración IP de MetroCluster, hay dos componentes cada sitio. Los sitios son asignados arbitrariamente las letras A y B, y los componentes individuales son asignados arbitrariamente los números 1 y 2.

Requisitos del clúster de ONTAP en una configuración de IP de MetroCluster

Las configuraciones de IP de MetroCluster requieren dos clústeres de ONTAP, uno en cada sitio de MetroCluster.

La nomenclatura debe ser única en la configuración de MetroCluster.

Nombres de ejemplo:

- Sitio A: Cluster_A
- Centro B: Cluster_B

Requisitos del switch de IP en una configuración de MetroCluster IP

Las configuraciones de IP de MetroCluster requieren cuatro switches IP. Los cuatro switches forman dos estructuras de almacenamiento de switches que proporcionan el ISL entre cada uno de los clústeres en la configuración IP de MetroCluster.

Los switches IP también proporcionan comunicación dentro del clúster entre los módulos de controladora de cada clúster.

La nomenclatura debe ser única en la configuración de MetroCluster.

Nombres de ejemplo:

- Sitio A: Cluster_A
  - IP_switch_A_1
  - IP_switch_A_2
- Centro B: Cluster_B
  - IP_switch_B_1
  - IP_switch_B_2

Requisitos del módulo de controlador en una configuración de IP de MetroCluster

Las configuraciones de IP de MetroCluster requieren cuatro o ocho módulos de controladora.

Los módulos de controladora de cada sitio forman un par de alta disponibilidad. Cada módulo de controladora tiene un partner de recuperación ante desastres en la otra ubicación.

Cada módulo de controlador debe ejecutar la misma versión de ONTAP. Los modelos de plataforma compatibles dependen de la versión de ONTAP:

- ONTAP 9.4 no admite nuevas instalaciones IP de MetroCluster en sistemas FAS.

  Las configuraciones de IP de MetroCluster existentes en sistemas FAS se pueden actualizar a ONTAP 9.4.

- A partir de ONTAP 9.5, se admiten las nuevas instalaciones IP de MetroCluster en sistemas FAS.
- A partir de ONTAP 9.4, los módulos de controladora configurados para ADP son compatibles.

Nombres de ejemplo

Los siguientes nombres de ejemplo se utilizan en la documentación:

- Sitio A: Cluster_A
  - Controller_A_1
  - Controller_A_2
- Centro B: Cluster_B
  - Controller_B_1
  - Controller_B_2

Requisitos de adaptador Gigabit Ethernet en una configuración IP de MetroCluster

Las configuraciones de IP de MetroCluster utilizan un adaptador Ethernet de 40/100 Gbps o 10/25 Gbps para las interfaces IP de los switches IP utilizados en la estructura IP de MetroCluster.

Modelo de plataforma	Adaptador Gigabit Ethernet necesario	Ranura necesaria para el adaptador	Puertos
AFF A900, ASA A900 y FAS9500	X91146A	Ranura 5, ranura 7	e5b, e7b
AFF A700 y FAS9000	X91146A-C.	Ranura 5	e5a, e5b
AFF A800, AFF C800, ASA A800 y ASA C800	Puertos X1146A/incorporados	Ranura 1	e0b. e1b
FAS8300, AFF A400, ASA A400, ASA C400 y AFF C400	X1146A	Ranura 1	e1a, e1b
AFF A300 y FAS8200	X1116A	Ranura 1	e1a, e1b
FAS2750, AFF A150, ASA A150 y AFF A220	Puertos incorporados	Ranura 0	e0a y e0b

FAS500f, AFF A250, ASA A250, ASA C250 y AFF C250	Puertos incorporados	Ranura 0	e0c, e0d
AFF A320	Puertos incorporados	Ranura 0	e0g, e0h

"Obtenga más información sobre la asignación automática de unidades y los sistemas ADP en las configuraciones IP de MetroCluster".

Requisitos de pool y unidad (compatible como mínimo)

Se recomiendan ocho bandejas de discos SAS (cuatro bandejas en cada sitio) para permitir la propiedad de los discos por bandeja.

Una configuración IP de MetroCluster de cuatro nodos requiere la configuración mínima en cada sitio:

- Cada nodo tiene al menos un pool local y un pool remoto en el sitio.
- Al menos siete unidades en cada pool.

  En una configuración MetroCluster de cuatro nodos con un único agregado de datos reflejados por nodo, la configuración mínima requiere 24 discos en el sitio.

En la configuración mínima compatible, cada pool tiene la siguiente distribución de unidades:

- Tres unidades raíz
- Tres unidades de datos
- Una unidad de repuesto

En una configuración mínima compatible, se necesita al menos una bandeja por sitio.

Las configuraciones de MetroCluster son compatibles con RAID-DP y RAID4.

Consideraciones sobre la ubicación de la unidad para bandejas parcialmente ocupadas

Para conseguir la asignación automática correcta de unidades cuando se utilizan bandejas que se han rellenado a la mitad (12 unidades en una bandeja de 24 unidades), las unidades se deben ubicar en las ranuras 0-5 y 18-23.

En una configuración con una bandeja parcialmente ocupada, las unidades deben distribuirse de forma uniforme en los cuatro cuadrantes de la bandeja.

Consideraciones sobre la ubicación de las unidades internas AFF A800

Para una correcta implementación de la función ADP, las ranuras de disco del sistema AFF A800 se deben dividir en trimestres y los discos deben ubicarse de forma simétrica en los trimestres.

Un sistema AFF A800 tiene 48 bahías de unidad. Las bahías se pueden dividir en trimestres:

- Primer trimestre:

    - Bahías 0 - 5
    - Bahías 24 - 29
- Segundo trimestre:
    - Bahías 6 - 11
    - Bahías 30 - 35
- Tercer trimestre:
    - Bahías 12 - 17
    - Bahías 36 - 41
- Cuarto trimestre:
    - Bahías 18 - 23
    - Bahías 42 - 47

Si este sistema se ocupa de 16 unidades, deben distribuirse simétricamente entre los cuatro trimestres:

- Cuatro unidades en el primer trimestre: 0, 1, 2, 3
- Cuatro unidades en el segundo trimestre: 6, 7, 8, 9
- Cuatro unidades en el tercer trimestre: 12, 13, 14, 15
- Cuatro unidades en el cuarto trimestre: 18, 19, 20, 21

Mezcla módulos IOM12 e IOM 6 en una pila

Su versión de ONTAP debe admitir la mezcla de bandejas. Consulte la "Herramienta de matriz de interoperabilidad de NetApp (IMT)" Para ver si su versión de ONTAP admite la mezcla de bandejas.

Para obtener más información sobre la mezcla de estantes, consulte "Bandejas añadidas en caliente con módulos IOM12 a una pila de bandejas con módulos IOM6"

Acumular en rack los componentes de hardware

Si no ha recibido el equipo ya instalado en armarios, debe montar los componentes en rack.

Acerca de esta tarea

Esta tarea debe realizarse en los dos sitios MetroCluster.

Pasos

1. Planifique la colocación de los componentes de MetroCluster.

   El espacio en rack depende del modelo de plataforma de los módulos de la controladora, los tipos de switch y el número de pilas de bandejas de discos que haya en la configuración.

2. Puesta a tierra apropiadamente usted mismo.
3. Instale los módulos de la controladora en el rack o armario.

   "Instrucciones de instalación y configuración de los sistemas AFF A220/FAS2700"

   "Instrucciones de instalación y configuración de sistemas AFF A250"

"Instrucciones de instalación y configuración de los sistemas AFF A300"

"Sistemas AFF A320: Instalación y configuración"

"Instrucciones de instalación y configuración de los sistemas AFF A400"

"Instrucciones de instalación y configuración del sistema AFF A700"

"Instrucciones de instalación y configuración de los sistemas AFF A800"

"Instrucciones de instalación y configuración de sistemas FAS500f"

"Instrucciones de instalación y configuración de los sistemas FAS8200"

"Instrucciones de instalación y configuración de los sistemas FAS8300 y FAS8700"

"Instrucciones de instalación y configuración de los sistemas FAS9000"

4. Instale los switches IP en el rack o armario.
5. Instale las bandejas de discos, enciúdeles a encender y, a continuación, configure los ID de bandeja.
   - Debe apagar y encender cada bandeja de discos.
   - Los ID de bandeja únicos se recomiendan en gran medida para cada bandeja de discos SAS dentro de cada grupo de recuperación ante desastres de MetroCluster, como ayuda en la solución de problemas.

> No conecte el cable de las bandejas de discos que estén destinadas a contener agregados no reflejados en este momento. Debe esperar a implementar bandejas destinadas a agregados no reflejados hasta que se complete la configuración de MetroCluster y solo implementarla después de utilizar el `metrocluster modify -enable-unmirrored -aggr-deployment true` comando.

Conecte los cables de los switches IP de MetroCluster

Utilizar las tablas de puertos con la herramienta RcfFileGenerator o varias configuraciones de MetroCluster

Debe comprender cómo utilizar la información de las tablas de puertos para generar correctamente los archivos RCF.

Antes de empezar

Revise estas consideraciones antes de utilizar las tablas:

- Las siguientes tablas muestran el uso del puerto para el sitio A. El mismo cableado se utiliza para el centro B.
- Los switches no pueden configurarse con puertos de diferentes velocidades (por ejemplo, una combinación de puertos de 100 Gbps y puertos de 40 Gbps).
- Realizar un seguimiento del grupo de puertos de MetroCluster (MetroCluster 1, MetroCluster 2, etc.). Necesitará esta información cuando utilice la herramienta RcfFileGenerator como se describe más adelante en este procedimiento de configuración.

- La "RcfFileGenerator para MetroCluster IP" también ofrece información general sobre el cableado por puerto para cada switch. Utilice esta información general sobre el cableado para verificar el cableado.

Cableado de configuraciones MetroCluster de ocho nodos

Para la configuración de MetroCluster que ejecuta ONTAP 9.8 y versiones anteriores, algunos procedimientos que se realizan para realizar la transición de una actualización requieren la adición de un segundo grupo de recuperación ante desastres de cuatro nodos a la configuración para crear una configuración temporal de ocho nodos. A partir de ONTAP 9,9.1, se admiten las configuraciones permanentes de MetroCluster de ocho nodos.

Acerca de esta tarea

Para dichas configuraciones, utilice el mismo método que se describe anteriormente. En lugar de una segunda MetroCluster, está cablear un grupo de recuperación ante desastres de cuatro nodos adicional.

Por ejemplo, la configuración incluye lo siguiente:

- Switches Cisco 3132Q-V.
- MetroCluster 1: Plataformas FAS2750
- MetroCluster 2: Plataformas AFF A700 (estas plataformas se están añadiendo como un segundo grupo de recuperación ante desastres de cuatro nodos)

Pasos

1. Para MetroCluster 1, conecte los cables de los switches Cisco 3132Q-V utilizando la tabla para la plataforma FAS2750 y las filas para las interfaces MetroCluster 1.
2. Para MetroCluster 2 (el segundo grupo de recuperación ante desastres), conecte los switches Cisco 3132Q-V utilizando la tabla para la plataforma AFF A700 y las filas para interfaces MetroCluster 2.

Asignaciones de puertos de la plataforma para los switches Cisco 3132Q-V.

El uso del puerto en una configuración IP de MetroCluster depende del modelo del switch y el tipo de plataforma.

Revise estas directrices antes de utilizar las tablas:

- Si se configura el switch para la transición de MetroCluster FC a IP, se puede utilizar el puerto 5, el puerto 6, el puerto 13 o el puerto 14 para conectar las interfaces del clúster local del nodo MetroCluster FC. Consulte la "RcfFileGenerator" y los archivos de cableado generados para obtener más detalles sobre el cableado de esta configuración. Para todas las demás conexiones, puede utilizar las asignaciones de uso de puertos que se muestran en las tablas.

Uso de puertos para los sistemas FAS2750 o AFF A220 y un switch Cisco 3132Q-V.

Cabling a FAS2750 or AFF A220 to a Cisco 3132Q-V switch			
Switch Port	Port use	FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 40G / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b
13/2-4		disabled	
14/1		e0a	e0b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Uso de puertos para sistemas FAS9000 o AFF A700 y un switch Cisco 3132Q-V.

Cabling a FAS9000 or AFF A700 to a Cisco 3132Q-V switch			
Switch Port	Port use	FAS9000 AFF A700	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e4a	e4e / e8a
2			
3	MetroCluster 2, Local Cluster interface	e4a	e4e / e8a
4			
5	MetroCluster 3, Local Cluster interface	e4a	e4e / e8a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e5a	e5b
10			
11	MetroCluster 2, MetroCluster interface	e5a	e5b
12			
13	MetroCluster 3, MetroCluster interface	e5a	e5b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Uso de puertos para sistemas AFF A800 o ASA A800 y un switch Cisco 3132Q-V.

Cabling an AFF A800 or ASA A800 to a Cisco 3132Q-V switch			
Switch Port	Port use	AFF A800 ASA A800	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e1a
2			
3	MetroCluster 2, Local Cluster interface	e0a	e1a
4			
5	MetroCluster 3, Local Cluster interface	e0a	e1a
6			
7	ISL, Local Cluster native speed 40G	ISL, Local Cluster	
8			
9	MetroCluster 1, MetroCluster interface	e0b	e1b
10			
11	MetroCluster 2, MetroCluster interface	e0b	e1b
12			
13	MetroCluster 3, MetroCluster interface	e0b	e1b
14			
15	ISL, MetroCluster native speed 40G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25 - 32	Unused	disabled	

Asignaciones de puertos de la plataforma para los switches Cisco 3232C o Cisco 9336C

El uso del puerto en una configuración IP de MetroCluster depende del modelo del switch y el tipo de plataforma.

Revise estas consideraciones antes de utilizar las tablas:

- Las siguientes tablas muestran el uso del puerto para el sitio A. El mismo cableado se utiliza para el centro B.
- Los switches no pueden configurarse con puertos de diferentes velocidades (por ejemplo, una combinación de puertos de 100 Gbps y puertos de 40 Gbps).
- Si está configurando un único MetroCluster con los conmutadores, utilice el grupo de puertos **MetroCluster 1**.

  Realice un seguimiento del grupo de puertos MetroCluster (MetroCluster 1, MetroCluster 2, MetroCluster 3

o MetroCluster 4). Lo necesitará cuando utilice la herramienta RcfFileGenerator como se describe más adelante en este procedimiento de configuración.

- El RcfFileGenerator para MetroCluster IP también proporciona una descripción general del cableado por puerto para cada switch.

  Utilice esta información general sobre el cableado para verificar el cableado.

- Se necesita la versión v2,10 o posterior del archivo RCF para el modo de desglose 25G para los ISL de MetroCluster.
- Se necesitan ONTAP 9.13.1 o posterior y la versión 2,00 del archivo RCF para utilizar una plataforma distinta de FAS8200 o AFF A300 en el grupo «MetroCluster 4».

Cableado de dos configuraciones de MetroCluster a los switches

Al cablear más de una configuración MetroCluster a un switch Cisco 3132Q-V, debe cablear cada MetroCluster según la tabla correspondiente. Por ejemplo, si se realiza el cableado de un sistema FAS2750 y un A700 de AFF al mismo switch Cisco 3132Q-V. A continuación, cablee FAS2750 como "MetroCluster 1" en la Tabla 1, y el AFF A700 según "MetroCluster 2" o "MetroCluster 3" en la Tabla 2. No puede conectar físicamente el sistema FAS2750 y el AFF A700 como "MetroCluster 1".

Cableado de un AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, sistema AFF C250, ASA C250, AFF A250 o ASA A250 a un switch Cisco 3232C o Cisco 9336-FX2C

Cabling an AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 or ASA A250 to a Cisco 3232C or Cisco 9336-FX2C switch					
Switch Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
8					
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
9/2-4		disabled		disabled	
10/1		e0a	e0b	e0c	e0d
10/2-4		disabled		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
11/2-4		disabled		disabled	
12/1		e0a	e0b	e0c	e0d
12/2-4		disabled		disabled	
13/1	MetroCluster 3, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
13/2-4		disabled		disabled	
14/1		e0a	e0b	e0c	e0d
14/2-4		disabled		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster	
16					
17					
18					
19					
20					
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
22/1-4					
23/1-4					
24/1-4					
25/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b	e0c	e0d
25/2-4		disabled		disabled	
26/1		e0a	e0b	e0c	e0d
26/2-4		disabled		disabled	
27 - 32	Unused	disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled	

Cableado de un sistema FAS8200 o AFF A300 a un switch Cisco 3232C o Cisco 9336C

Cabling a FAS8200 or AFF A300 to a Cisco 3232C or Cisco 9336C-FX2 switch			
Switch Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5/1	MetroCluster 3, MetroCluster interface	e0a	e0b
5/2-4		disabled	
6/1		e0a	e0b
6/2-4		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13/1	MetroCluster 3, MetroCluster interface	e1a	e1b
13/2-4		disabled	
14/1		e1a	e1b
14/2-4		disabled	
15	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster	
16			
17			
18			
19			
20			
21/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster	
22/1-4			
23/1-4			
24/1-4			
25/1	MetroCluster 4, MetroCluster interface	e1a	e1b
25/2-4		disabled	
26/1		e1a	e1b
26/2-4		disabled	
27 - 28	Unused	disabled	
29/1	MetroCluster 4, Local Cluster interface	e0a	e0b
29/2-4		disabled	
30/1		e0a	e0b
30/2-4		disabled	
25 - 32	Unused	disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled	

Si va a realizar una actualización desde archivos RCF anteriores, es posible que la configuración de cableado esté utilizando puertos del grupo «MetroCluster 4» (puertos 25/26 y 29/30).

Cableado de un AFF A320, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, FAS8700, FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900, o sistema ASA A900 a un switch Cisco 3232C o Cisco 9336C-FX2

Cabling a AFF A320, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 FAS8700, FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 or ASA A900 to a Cisco 3232C or Cisco 9336C-FX2 switch													
Switch Port	Port use	AFF A320		FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 2	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
3 4	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
5 6	MetroCluster 3, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
7 8	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
9 10	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
11 12	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
13 14	MetroCluster 3, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
15 16 17 18 19 20	ISL, MetroCluster native speed 40G / 100G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
21/1-4 22/1-4 23/1-4 24/1-4	ISL, MetroCluster breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
25 26	MetroCluster 4, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
27 - 28	Unused	disabled		disabled		disabled		disabled		disabled		disabled	
29 30	MetroCluster 4, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
31 - 32	Unused	disabled		disabled		disabled		disabled		disabled		disabled	
33 - 34	Unused (Cisco 9336C-FX2 only)	disabled		disabled		disabled		disabled		disabled		disabled	

Nota 1: Si utiliza un adaptador X91440A (40Gbps), utilice los puertos E4A y E4E o E4A y E8a. Si usa un adaptador de X91153A (100Gbps), utilice los puertos E4A y e4b o E4A y E8a.

El uso de puertos en el grupo «MetroCluster 4» requiere ONTAP 9.13.1 o posterior.

Asignaciones de puertos de plataforma para un switch compartido Cisco 9336C-FX2

El uso del puerto en una configuración IP de MetroCluster depende del modelo del switch y el tipo de plataforma.

Revise estas consideraciones antes de utilizar las tablas:

- Al menos un grupo de recuperación de desastres o configuración MetroCluster debe admitir bandejas NS224 conectadas a switch.
- Las plataformas que no admiten bandejas NS224 conectadas a switches solo pueden conectarse como segunda configuración de MetroCluster o como segundo grupo de recuperación ante desastres.
- RcfFileGenerator solo muestra plataformas elegibles cuando se selecciona la primera plataforma.
- Para conectar una configuración MetroCluster de ocho o dos nodos se requiere ONTAP 9.14.1 o una versión posterior.

Cableado de un AFF A320, AFF C400, ASA C400, AFF A400, ASA A400, AFF A700, AFF C800, ASA C800, AFF A800, AFF A900, o el sistema ASA A900 a un switch compartido Cisco 9336C-FX2

Cabling an AFF A320, AFF C400, ASA C400, AFF A400, ASA A400, AFF A700, AFF C800, ASA C800, AFF A800 , AFF A900, or ASA A900 to a Cisco 9336C-FX2 shared switch													
Switch Port	Port Use	AFF A320		AFF C400 ASA C400		AFF A400 ASA A400		AFF A700		AFF C800 ASA C800 AFF A800		AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2													
3	MetroCluster 2, Local Cluster interface	e0a	e0d	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4													
5	Storage shelf 1 (9)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
6		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8													
9	MetroCluster 1, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
10													
11	MetroCluster 2, MetroCluster interface	e0g	e0h	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
12													
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14													
15													
16													
17	MetroCluster 1, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2) e1a (option 3)	e3b (option 1) e10b (option 2) e11b (option 3)
18													
19	MetroCluster 2, Ethernet Storage Interface	e0c	e0f	e4a	e4b / e5b	e0c	e0d / e5b	e3a	e3b / e7b	e5a	e5b / e3b	e3a (option 1) e2a (option 2) e1a (option 3)	e3b (option 1) e10b (option 2) e11b (option 3)
20													
21	Storage shelf 2 (8)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
22		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
23	Storage shelf 3 (7)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
24		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
25	Storage shelf 4 (6)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
26		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
27	Storage shelf 5 (5)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
28		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
29	Storage shelf 6 (4)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
30		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
31	Storage shelf 7 (3)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
32		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
33	Storage shelf 8 (2)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
34		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b
35	Storage shelf 9 (1)	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b	NSM-1, e0a	NSM-1, e0b
36		NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b	NSM-2, e0a	NSM-2, e0b

Nota 1: Si utiliza un adaptador X91440A (40Gbps), utilice los puertos E4A y E4E o E4A y E8a. Si usa un adaptador de X91153A (100Gbps), utilice los puertos E4A y e4b o E4A y E8a.

Cableado de un sistema AFF A150, ASA A150, FAS2750 o AFF A220 a un switch compartido Cisco 9336C-FX2

Cabling an AFF A150, ASA A150, FAS2750 or AFF A220 to a Cisco 9336C-FX2 shared switch			
Switch Port	Port Use	AFF A150 ASA A150 FAS2750 AFF A220	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0a	e0b
9/2-4		disabled	
10/1		e0a	e0b
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0a	e0b
11/2-4		disabled	
12/1		e0a	e0b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Cableado de un sistema FAS500f, AFF C250, ASA C250, AFF A250 o ASA A250 a un switch compartido Cisco 9336C-FX2

Cabling a FAS500f, AFF C250, ASA C250, AFF A250, ASA A250 to a Cisco 9336C-FX2 shared switch			
Switch Port	Port Use	FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d
9/2-4		disabled	
10/1		e0c	e0d
10/2-4		disabled	
11/1	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d
11/2-4		disabled	
12/1		e0c	e0d
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Cableado de un sistema FAS8200 o AFF A300 a un switch compartido Cisco 9336C-FX2

Cabling a FAS8200 or AFF A300 to a Cisco 9336C-FX2 shared switch			
Switch Port	Port Use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1/1	MetroCluster 1, Local Cluster interface	e0a	e0b
1/2-4		disabled	
2/1		e0a	e0b
2/2-4		disabled	
3/1	MetroCluster 2, Local Cluster interface	e0a	e0b
3/2-4		disabled	
4/1		e0a	e0b
4/2-4		disabled	
5-6	Unused	disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
8			
9/1	MetroCluster 1, MetroCluster interface	e1a	e1b
9/2-4		disabled	
10/1		e1a	e1b
10/2-4		disabled	
11/1	MetroCluster 2, MetroCluster interface	e1a	e1b
11/2-4		disabled	
12/1		e1a	e1b
12/2-4		disabled	
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster	
14			
15			
16			
17-36	Unused	disabled	

Cableado de un sistema FAS8300, FAS8700, FAS9000 o FAS9500 a un switch compartido Cisco 9336C-FX2

Cabling a FAS8300, FAS8700, FAS9000, or FAS9500 to a Cisco 9336C-FX2 shared switch							
Switch Port	Port Use	FAS8300 FAS8700		FAS9000		FAS9500	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e4a	e4e / e8a	e4a	e4b(e) / e8a Note 1
2							
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e4a	e4e / e8a	e4a	e4b(e) / e8a Note 1
4							
5-6	Unused	disabled		disabled		disabled	
7	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
8							
9	MetroCluster 1, MetroCluster interface	e1a	e1b	e5a	e5b	e5b	e7b
10							
11	MetroCluster 2, MetroCluster interface	e1a	e1b	e5a	e5b	e5b	e7b
12							
13	ISL MetroCluster, native speed 40G / 100G breakout mode 10G / 25G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14							
15							
16							
17-36	Unused	disabled		disabled		disabled	

Nota 1: Si utiliza un adaptador X91440A (40Gbps), utilice los puertos E4A y E4E o E4A y E8a. Si usa un adaptador de X91153A (100Gbps), utilice los puertos E4A y e4b o E4A y E8a.

Asignaciones de puertos de plataforma para switches IP BES-53248 compatibles con Broadcom

El uso del puerto en una configuración IP de MetroCluster depende del modelo del switch y el tipo de plataforma.

Los switches no se pueden utilizar con puertos ISL remotos de diferentes velocidades (por ejemplo, un puerto de 25 Gbps conectado a un puerto ISL de 10 Gbps).

Revise esta información antes de utilizar las tablas:

- Si se configura la transición del switch para MetroCluster FC a IP, se usan los siguientes puertos en función de la plataforma objetivo que se elija:

Plataforma objetivo	Puerto
FAS500f, AFF C250, ASA C250, AFF A250, ASA A250, FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, o FAS8700 plataformas	Puertos 1 - 6, 10Gbps
Plataformas FAS8200 o AFF A300	Puertos 3 - 4 y 9 - 12, 10Gbps

- Es posible que los sistemas AFF A320 configurados con switches Broadcom BES-53248 no admitan todas las funciones.

  No se admite ninguna configuración o función que requiera que las conexiones de clúster local estén conectadas a un switch. Por ejemplo, no se admiten las siguientes configuraciones ni procedimientos:

  - Configuraciones MetroCluster de ocho nodos
  - Transición de las configuraciones FC de MetroCluster a IP de MetroCluster
  - Actualizar una configuración IP de MetroCluster de cuatro nodos (ONTAP 9.8 y versiones posteriores)

Notas a las que se hace referencia en las tablas:

- **Nota 1**: El uso de estos puertos requiere una licencia adicional.
- **Nota 2**: Solo se puede conectar al switch una sola MetroCluster de cuatro nodos utilizando sistemas AFF A320.

  Esta configuración no admite las funciones que requieren un clúster con switches, incluidos los procedimientos de transición de FC a IP de MetroCluster y actualización tecnológica.

- **Nota 3**: El conmutador BES-53248 requiere que todos los puertos de un grupo de cuatro puertos funcionen a la misma velocidad. Para conectar una combinación de plataformas AFF 150, ASA A150, FAS2750, AFF A220 y FAS500f, AFF C250, ASA C250, AFF A250 y ASA A250, se deben usar puertos de switch ubicados en grupos de cuatro puertos separados. Si necesita este tipo de configuración, se aplica lo siguiente:
  - En la "RcfFileGenerator para MetroCluster IP", Los campos desplegables de «MetroCluster 1» y «MetroCluster 2» solo se rellenan después de seleccionar una plataforma para MetroCluster 3 o «MetroCluster 4». Consulte "Utilizar las tablas de puertos con la herramienta RcfFileGenerator o varias configuraciones de MetroCluster" para obtener más información sobre cómo utilizar las tablas de puertos.
  - Si ambas configuraciones de MetroCluster utilizan la misma plataforma, NetApp recomienda que seleccione el grupo «MetroCluster 3» para una configuración y el grupo «MetroCluster 4» para la otra. Si las plataformas son diferentes, debe seleccionar «MetroCluster 3» o «MetroCluster 4» para la primera configuración y seleccionar «MetroCluster 1» o «MetroCluster 2» para la segunda configuración.

Cableado de un AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 o ASA A250 a un switch Broadcom BES-53248

Cabling an AFF A150, ASA A150, FAS2750, AFF A220, FAS500f, AFF C250, ASA C250, AFF A250 or ASA A250 to a Broadcom BES-53248 switch					
Physical Port	Port use	AFF A150 ASA A150 FAS2750 AFF A220		FAS500f AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 4	Unused	disabled		disabled	
5	MetroCluster 1, Shared Cluster and MetroCluster interface (note 3)	e0a	e0b	e0c	e0d
6					
7	MetroCluster 2, Shared Cluster and MetroCluster interface (note 3)	e0a	e0b	e0c	e0d
8					
9	MetroCluster 3, Shared Cluster and MetroCluster interface (note 3)	e0a	e0b	e0c	e0d
10					
11	MetroCluster 4, Shared Cluster and MetroCluster interface (note 3)	e0a	e0b	e0c	e0d
12					
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
..	Ports not licensed (17 - 54)				
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
54					
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
56					

Cableado de un sistema FAS8200, AFF A300 o AFF A320 a un switch Broadcom BES-53248

Cabling a FAS8200 or AFF A300 to a Broadcom BES-53248 switch			
Physical Port	Port use	FAS8200 AFF A300	
		IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0a	e0b
2			
3	MetroCluster 2, Local Cluster interface Not used during Transition	e0a	e0b
4			
5	MetroCluster 1, MetroCluster interface	e1a	e1b
6			
7	MetroCluster 2, MetroCluster interface	e1a	e1b
8			
9 - 12	Unused	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster	
54			
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster	
56			

Cabling an AFF A320 to a Broadcom BES-53248 switch			
		AFF A320	
Physical Port	Port use	IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (note 2)	disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster	
14			
15			
16			
..	Ports not licensed (17 - 54)		
53	ISL, MetroCluster, native speed 40G / 100G (see note 1)	ISL, MetroCluster	
54			
55	MetroCluster 1, MetroCluster interface (note 2)	e0g	e0h
56			

Cableado de un sistema FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 o FAS8700 a un switch Broadcom BES-53248

Cabling a FAS8300, AFF C400, ASA C400, AFF A400, ASA A400 or FAS8700 to a Broadcom BES-53248 switch					
Physical Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 12	Ports not used (see note 2)	disabled		disabled	
13	ISL, MetroCluster native speed 10G / 25G	ISL, MetroCluster		ISL, MetroCluster	
14					
15					
16					
..	Ports not licensed (17 - 48)				
49	MetroCluster 5, Local Cluster interface (note 1)	e0c	e0d	e3a	e3b
50					
51	MetroCluster 5, MetroCluster interface (note 1)	e1a	e1b	e1a	e1b
52					
53	ISL, MetroCluster, native speed 40G / 100G (note 1)	ISL, MetroCluster		ISL, MetroCluster	
54					
55	ISL, Local Cluster native speed / 100G	ISL, Local Cluster		ISL, Local Cluster	
56					

Asignaciones de puertos de plataforma para switches IP SN2100 compatibles con NVIDIA

El uso del puerto en una configuración IP de MetroCluster depende del modelo del switch y el tipo de plataforma.

Configuraciones admitidas

Actualmente no se admiten las siguientes configuraciones:

- Transición de FC a IP de MetroCluster

Revise estas consideraciones antes de utilizar las tablas de configuración

- Para conectar una configuración MetroCluster de ocho o dos nodos se requiere ONTAP 9.14.1 o posterior y el archivo RCF versión 2,00 o posterior.
- Si realiza cables con varias configuraciones de MetroCluster, siga la tabla correspondiente. Por ejemplo:
  - Si conecta dos configuraciones de MetroCluster de cuatro nodos del tipo AFF A700, a continuación, conecte el primer MetroCluster que se muestra como "MetroCluster 1" y el segundo MetroCluster que se muestra como "MetroCluster 2" en la tabla A700 de AFF.

> Los puertos 13 y 14 se pueden utilizar en el modo de velocidad nativa que admite 40 Gbps y 100 Gbps, o en el modo de arranque para admitir 4 × 25 Gbps o 4 × 10 Gbps. Si utilizan el modo de velocidad nativo, se representan como puertos 13 y 14. Si utilizan el modo de arranque, 4 × 25 Gbps o 4 × 10 Gbps, entonces se representan como puertos 13s0-3 y 14s0-3.

En las siguientes secciones se describe el esquema del cableado físico. También puede consultar la "RcfFileGenerator" para obtener información detallada sobre el cableado.

Cableado de un AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, el sistema AFF A250 o ASA A250 a un switch NVIDIA SN2100

Cabling a AFF A150, ASA A150, FAS500f, AFF C250, ASA C250, AFF A250 or ASA A250 to a NVIDIA SN2100 switch					
Switch Port	Port use	AFF A150 ASA A150		FAS500F AFF C250 ASA C250 AFF A250 ASA A250	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1 - 6	Unused	disabled		disabled	
7s0	MetroCluster 1, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
7s1-3		disabled		disabled	
8s0		e0c	e0d	e0c	e0d
8s1-3		disabled		disabled	
9s0	MetroCluster 2, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
9s1-3		disabled		disabled	
10s0		e0c	e0d	e0c	e0d
10s1-3		disabled		disabled	
11s0	MetroCluster 3, Shared Cluster and MetroCluster interface	e0c	e0d	e0c	e0d
11s1-3		disabled		disabled	
12s0		e0c	e0d	e0c	e0d
12s1-3		disabled		disabled	
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3					
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster	
16					

Cableado A FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, FAS8700, FAS9000, AFF A700, AFF C800, ASA C800, sistema AFF A800, ASA A800, FAS9500, AFF A900 o ASA A900 a un switch NVIDIA SN2100

Cabling a FAS8300, AFF C400, ASA C400, AFF A400, ASA A400, FAS8700, FAS9000, AFF A700, AFF C800, ASA C800, AFF A800, ASA A800, FAS9500, AFF A900 or ASA A900 to a NVIDIA SN2100 switch											
Switch Port	Port use	FAS8300 AFF C400 ASA C400 FAS8700		AFF A400 ASA A400		FAS9000 AFF A700		AFF C800 ASA C800 AFF A800 ASA A800		FAS9500 AFF A900 ASA A900	
		IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2	IP_Switch_x_1	IP_Switch_x_2
1	MetroCluster 1, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
2											
3	MetroCluster 2, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
4											
5	MetroCluster 3, Local Cluster interface	e0c	e0d	e3a	e3b	e4a	e4e / e8a	e0a	e1a	e4a	e4b(e) / e8a Note 1
6											
7	MetroCluster 1, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
8											
9	MetroCluster 2, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
10											
11	MetroCluster 3, MetroCluster interface	e1a	e1b	e1a	e1b	e5a	e5b	e0b	e1b	e5b	e7b
12											
13 / 13s0-3	MetroCluster ISL 40/100G or 4x25G or 4x10G	ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster		ISL, MetroCluster	
14 / 14s0-3											
15	ISL, Local Cluster 100G	ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster		ISL, Local Cluster	
16											

Nota 1: Si utiliza un adaptador X91440A (40Gbps), utilice los puertos E4A y E4E o E4A y E8a. Si usa un adaptador de X91153A (100Gbps), utilice los puertos E4A y e4b o E4A y E8a.

Cableado de los puertos de conexión, datos y gestión de las controladoras

Debe cablear los puertos del módulo de controladora que se utilizan para la conexión de clústeres entre iguales, la gestión y la conectividad de datos.

Esta tarea debe realizarse en cada módulo del controlador de la configuración de MetroCluster.

Se deben utilizar al menos dos puertos en cada módulo de controlador para la conexión de clústeres entre iguales.

El ancho de banda mínimo recomendado para los puertos y la conectividad de red es de 1 GbE.

1. Identifique y conecte al menos dos puertos para la conexión de clústeres entre iguales y compruebe que tengan conectividad de red con el clúster de socios.

   La relación de clústeres entre iguales puede realizarse en puertos dedicados o en puertos de datos. El uso de puertos dedicados proporciona un rendimiento mayor para el tráfico de paridad de clústeres.

   "Configuración exprés de relación entre iguales de clústeres y SVM"

2. Conecte los puertos de datos y de gestión de la controladora a las redes de datos y gestión en el sitio local.

   Utilice las instrucciones de instalación de la plataforma en "Documentación de los sistemas de hardware de ONTAP".

   > Los sistemas IP de MetroCluster no tienen puertos de alta disponibilidad dedicados. Cuando se utilice *ONTAP Hardware Systems Documentation* para instalar la plataforma, no debe seguir las instrucciones para cablear el clúster y los puertos de alta disponibilidad.

Configure los switches IP de MetroCluster

Configuración de switches IP de Broadcom

Debe configurar los switches IP de Broadcom para su uso como Cluster Interconnect y para conectividad IP de MetroCluster back-end.

> Su configuración requiere licencias adicionales (licencia de puerto de 6 x 100 GB) en las siguientes situaciones:

- Utiliza los puertos 53 y 54 como un ISL MetroCluster de 40 Gbps o 100 Gbps.
- Se utiliza una plataforma que conecta el clúster local y las interfaces MetroCluster a los puertos 49 - 52.

Restablecer los valores predeterminados de fábrica del conmutador IP de Broadcom

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

Acerca de esta tarea

- Debe repetir estos pasos en cada uno de los switches IP de la configuración de IP de MetroCluster.
- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Cambie al símbolo del sistema elevado (`#`): `enable`

```
(IP_switch_A_1)> enable
(IP_switch_A_1) #
```

2. Borre la configuración de inicio y elimine el banner

   a. Borrar la configuración de inicio:

      `erase startup-config`

      ```
      (IP_switch_A_1) #erase startup-config

      Are you sure you want to clear the configuration? (y/n) y

      (IP_switch_A_1) #
      ```

      Este comando no borra el banner.

   b. Quite el banner:

      `no set clibanner`

```
(IP_switch_A_1) #configure
(IP_switch_A_1)(Config) # no set clibanner
(IP_switch_A_1)(Config) #
```

3. Reinicie el switch:*`(IP_switch_A_1) #reload`*

```
Are you sure you would like to reset the system? (y/n) y
```

> Si el sistema pregunta si desea guardar la configuración no guardada o modificada antes de volver a cargar el conmutador, seleccione **no**.

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

   El usuario predeterminado es "'admin'" y no se establece ninguna contraseña. Se muestra un símbolo del sistema similar a lo siguiente:

```
(Routing)>
```

5. Cambie al símbolo del sistema elevado:

   `enable`

```
Routing)> enable
(Routing) #
```

6. Establezca el protocolo del puerto de servicio en `none`:

   `serviceport protocol none`

   ```
   (Routing) #serviceport protocol none
   Changing protocol mode will reset ip configuration.
   Are you sure you want to continue? (y/n) y

   (Routing) #
   ```

7. Asigne la dirección IP al puerto de servicio:

   `serviceport ip` *`ip-address netmask gateway`*

   En el ejemplo siguiente se muestra una dirección IP asignada a un puerto de servicio "10.10.10.10" con subred "255.255.255.0" y puerta de enlace "10.10.10.1":

   ```
   (Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
   ```

8. Compruebe que el puerto de servicio esté configurado correctamente:

   `show serviceport`

   En el ejemplo siguiente se muestra que el puerto está activo y que se han asignado las direcciones correctas:

```
(Routing) #show serviceport

Interface Status............................... Up
IP Address..................................... 10.10.10.10
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.10.10.1
IPv6 Administrative Mode....................... Enabled
IPv6 Prefix is ................................
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router............................ fe80::222:bdff:fef8:19ff
Configured IPv4 Protocol....................... None
Configured IPv6 Protocol....................... None
IPv6 AutoConfig Mode........................... Disabled
Burned In MAC Address.......................... D8:C4:97:56:87:D7

(Routing) #
```

9. Si lo desea, configure el servidor SSH.

> El archivo RCF desactiva el protocolo Telnet. Si no configura el servidor SSH, sólo puede acceder al puente utilizando la conexión de puerto serie.

a. Generar claves RSA.

```
(Routing) #configure
(Routing) (Config)#crypto key generate rsa
```

b. Generar claves DSA (opcional)

```
(Routing) #configure
(Routing) (Config)#crypto key generate dsa
```

c. Si está utilizando la versión compatible con FIPS de EFOS, genere las claves ECDSA. El siguiente ejemplo crea las claves con una longitud de 521. Los valores válidos son 256, 384 o 521.

```
(Routing) #configure
(Routing) (Config)#crypto key generate ecdsa 521
```

d. Habilite el servidor SSH.

Si es necesario, salga del contexto de configuración.

```
(Routing) (Config)#end
(Routing) #ip ssh server enable
```

+

> Si las claves ya existen, es posible que se le pida que las sobrescriba.

10. Si lo desea, configure el dominio y el servidor de nombres:

    `configure`

    En el siguiente ejemplo se muestra el `ip domain` y.. `ip name server` comandos:

    ```
    (Routing) # configure
    (Routing) (Config)#ip domain name lab.netapp.com
    (Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
    (Routing) (Config)#exit
    (Routing) (Config)#
    ```

11. Si lo desea, configure la zona horaria y la sincronización horaria (SNTP).

    En el siguiente ejemplo se muestra el `sntp` Comandos, que especifican la dirección IP del servidor SNTP y la zona horaria relativa.

    ```
    (Routing) #
    (Routing) (Config)#sntp client mode unicast
    (Routing) (Config)#sntp server 10.99.99.5
    (Routing) (Config)#clock timezone -7
    (Routing) (Config)#exit
    (Routing) (Config)#
    ```

    Para la versión 3.10.0.3 de EFOS y posterior, utilice el `ntp` comando, como se muestra en el siguiente ejemplo:

```
> (Config)# ntp ?

authenticate             Enables NTP authentication.
authentication-key       Configure NTP authentication key.
broadcast                Enables NTP broadcast mode.
broadcastdelay           Configure NTP broadcast delay in microseconds.
server                   Configure NTP server.
source-interface         Configure the NTP source-interface.
trusted-key              Configure NTP authentication key number for
trusted time source.
vrf                      Configure the NTP VRF.

>(Config)# ntp server ?

ip-address|ipv6-address|hostname  Enter a valid IPv4/IPv6 address or
hostname.

>(Config)# ntp server 10.99.99.5
```

12. Configure el nombre del switch:

    ```
    hostname IP_switch_A_1
    ```

    El indicador del interruptor mostrará el nuevo nombre:

    ```
    (Routing) # hostname IP_switch_A_1

    (IP_switch_A_1) #
    ```

13. Guarde la configuración:

    ```
    write memory
    ```

    Recibe mensajes y resultados similares al ejemplo siguiente:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

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

Descarga e instalación del software EFOS del conmutador Broadcom

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

Acerca de esta tarea

Esta tarea debe repetirse en cada switch de la configuración de IP de MetroCluster.

Tenga en cuenta lo siguiente:

- Al actualizar desde EFOS 3.4.x.x a EFOS 3.7.x.x o posterior, el conmutador debe ejecutar EFOS 3.4.4.6 (o posterior versión 3.4.x.x). Si está ejecutando una versión anterior a esa, actualice primero el conmutador a EFOS 3.4.4.6 (o posterior versión 3.4.x.x) y, a continuación, actualice el conmutador a EFOS 3.7.x.x o posterior.
- La configuración para EFOS 3.4.x.x y 3.7.x.x o posterior es diferente. Para cambiar la versión de EFOS de 3.4.x.x a 3.7.x.x o posterior, o viceversa, es necesario restablecer los valores predeterminados de fábrica del conmutador y aplicar los archivos RCF de la versión de EFOS correspondiente. Este procedimiento requiere acceso a través del puerto de la consola de serie.
- A partir de la versión 3.7.x.x de EFOS o posterior, está disponible una versión no compatible con FIPS y compatible con FIPS. Se aplican diferentes pasos al cambiar a desde una versión que no sea compatible con FIPS a una versión compatible con FIPS o viceversa. Si cambia EFOS de una versión no conforme a FIPS a una versión compatible con FIPS o viceversa, el cambio se restablecerá a los valores predeterminados de fábrica. Este procedimiento requiere acceso a través del puerto de la consola de serie.

Pasos

1. Compruebe si su versión de EFOS cumple con FIPS o no cumple con FIPS mediante el uso de `show fips status` comando. En los ejemplos siguientes: `IP_switch_A_1` Está utilizando EFOS y EFOS compatibles con FIPS `IP_switch_A_2` Utiliza EFOS no compatibles con FIPS.

   Ejemplo 1

```
IP_switch_A_1 #show fips status

System running in FIPS mode

IP_switch_A_1 #
```

Ejemplo 2

```
IP_switch_A_2 #show fips status
                     ^
% Invalid input detected at `^` marker.

IP_switch_A_2 #
```

2. Utilice la siguiente tabla para determinar qué método debe seguir:

Procedimiento	**Versión EFOS actual**	**Nueva versión EFOS**	* Pasos de alto nivel*
Pasos para actualizar EFOS entre dos versiones (no compatibles con FIPS) compatibles con FIPS	3.4.x.x.	3.4.x.x.	Instale la nueva imagen de EFOS utilizando el método 1) se conserva la información de configuración y licencia
3.4.4.6 (o posterior 3.4.x.x)	3.7.x.x o superior, no conforme a FIPS	Actualice el EFOS mediante el método 1. Restablezca el conmutador a los valores predeterminados de fábrica y aplique el archivo RCF para EFOS 3.7.x.x o posterior	3.7.x.x o superior, no conforme a FIPS
3.4.4.6 (o posterior 3.4.x.x)	Degradar EFOS mediante el método 1. Restablezca el interruptor a los valores predeterminados de fábrica y aplique el archivo RCF para EFOS 3.4.x.x.	3.7.x.x o superior, no conforme a FIPS	
Instale la nueva imagen del EFOS mediante el método 1. Se conserva la información de configuración y licencia	3.7.x.x o posterior, conforme a FIPS	3.7.x.x o posterior, conforme a FIPS	Instale la nueva imagen del EFOS mediante el método 1. Se conserva la información de configuración y licencia

Pasos para actualizar a/desde una versión de EFOS conforme a FIPS	No conforme a FIPS	Conforme a FIPS	Instalación de la imagen del EFOS mediante el método 2. Se perderá la información de licencia y configuración del switch.

- Método 1: Pasos para actualizar EFOS con la descarga de la imagen de software a la partición de inicio de copia de seguridad
- Método 2: Pasos para actualizar EFOS mediante LA instalación DEL SO

Pasos para actualizar EFOS con la descarga de la imagen de software a la partición de inicio de copia de seguridad

Sólo puede realizar los siguientes pasos si ambas versiones de EFOS no son compatibles con FIPS o ambas son compatibles con FIPS.

> No utilice estos pasos si una versión es compatible con FIPS y la otra no es compatible con FIPS.

Pasos

1. Copie el software del conmutador en el conmutador: `copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.4.6.stk backup`

   En este ejemplo, el archivo del sistema operativo efos-3.4.4.6.stk se copia desde el servidor SFTP en 50.50.50.50 a la partición de copia de seguridad. Debe utilizar la dirección IP del servidor TFTP/SFTP y el nombre de archivo del archivo RCF que necesita instalar.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/switchsoftware/efos-
3.4.4.6.stk backup
Remote Password:*************

Mode........................................ SFTP
Set Server IP................................ 50.50.50.50
Path......................................... /switchsoftware/
Filename..................................... efos-3.4.4.6.stk
Data Type.................................... Code
Destination Filename......................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...


File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. Ajuste el conmutador a arrancar desde la partición de copia de seguridad en el siguiente reinicio del conmutador:

   `boot system backup`

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. Compruebe que la nueva imagen de arranque estará activa en el siguiente arranque:

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.4.2    3.4.4.6      3.4.4.2        3.4.4.6

(IP_switch_A_1) #
```

4. Guarde la configuración:

   `write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

5. Reinicie el switch:

   `reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

6. Espere a que se reinicie el switch.

En raras ocasiones, es posible que el conmutador no se inicie. Siga la Pasos para actualizar EFOS mediante LA instalación DEL SO para instalar la nueva imagen.

7. Si cambia el cambio de EFOS 3.4.x.x a EFOS 3.7.x.x o viceversa, siga los dos procedimientos siguientes para aplicar la configuración correcta (RCF):
   a. Restablecer los valores predeterminados de fábrica del conmutador IP de Broadcom
   b. Descarga e instalación de los archivos Broadcom RCF
8. Repita estos pasos en los tres switches IP restantes de la configuración IP de MetroCluster.

Pasos para actualizar EFOS mediante LA instalación DEL SO

Puede realizar los siguientes pasos si una versión de EFOS es compatible con FIPS y la otra versión de EFOS no es compatible con FIPS. Estos pasos se pueden utilizar para instalar la imagen EFOS 3.7.x.x no compatible con FIPS o FIPS desde ONIE si el conmutador no arranca.

Pasos

1. Arranque el interruptor en el modo DE instalación ONIE.

   Durante el arranque, seleccione ONIE cuando aparezca la siguiente pantalla:

```
+-----------------------------------------------------------------------+
|EFOS                                                                   |
|*ONIE                                                                  |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
|                                                                       |
+-----------------------------------------------------------------------+
```

   Después de seleccionar "ONIE", el interruptor se cargará y le presentará las siguientes opciones:

```
 +-----------------------------------------------------------------+
 |*ONIE: Install OS                                                |
 | ONIE: Rescue                                                    |
 | ONIE: Uninstall OS                                              |
 | ONIE: Update ONIE                                               |
 | ONIE: Embed ONIE                                                |
 | DIAG: Diagnostic Mode                                           |
 | DIAG: Burn-In Mode                                              |
 |                                                                 |
 |                                                                 |
 |                                                                 |
 |                                                                 |
 |                                                                 |
 +-----------------------------------------------------------------+
```

El conmutador se iniciará ahora en el modo DE instalación ONIE.

2. Detenga EL descubrimiento DE ONIE y configure la interfaz ethernet

   Una vez que aparezca el siguiente mensaje, pulse <enter> para invocar LA consola ONIE:

```
 Please press Enter to activate this console. Info: eth0:  Checking
link... up.
 ONIE:/ #
```

> El descubrimiento DE ONIE continuará y los mensajes se imprimirán en la consola.

```
Stop the ONIE discovery
ONIE:/ # onie-discovery-stop
discover: installer mode detected.
Stopping: discover... done.
ONIE:/ #
```

3. Configure la interfaz ethernet y agregue la ruta mediante `ifconfig eth0 <ipAddress> netmask <netmask> up` y.. `route add default gw <gatewayAddress>`

```
ONIE:/ # ifconfig eth0 10.10.10.10 netmask 255.255.255.0 up
ONIE:/ # route add default gw 10.10.10.1
```

4. Compruebe que se puede acceder al servidor que aloja el archivo DE instalación ONIE:

```
ONIE:/ # ping 50.50.50.50
PING 50.50.50.50 (50.50.50.50): 56 data bytes
64 bytes from 50.50.50.50: seq=0 ttl=255 time=0.429 ms
64 bytes from 50.50.50.50: seq=1 ttl=255 time=0.595 ms
64 bytes from 50.50.50.50: seq=2 ttl=255 time=0.369 ms
^C
--- 50.50.50.50 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.369/0.464/0.595 ms
ONIE:/ #
```

5. Instale el nuevo software del conmutador

```
ONIE:/ # onie-nos-install http:// 50.50.50.50/Software/onie-installer-
x86_64
discover: installer mode detected.
Stopping: discover... done.
Info: Fetching http:// 50.50.50.50/Software/onie-installer-3.7.0.4 ...
Connecting to 50.50.50.50 (50.50.50.50:80)
installer            100% |*******************************| 48841k
0:00:00 ETA
ONIE: Executing installer: http:// 50.50.50.50/Software/onie-installer-
3.7.0.4
Verifying image checksum ... OK.
Preparing image archive ... OK.
```

El software instalará y reiniciará el conmutador. Deje que el interruptor se reinicie normalmente en la nueva versión de EFOS.

6. Compruebe que el nuevo software del conmutador está instalado

show bootvar

```
(Routing) #show bootvar
Image Descriptions
active :
backup :
Images currently available on Flash
----    ----------- -------- --------------- ------------
unit    active     backup   current-active  next-active
----    ----------- -------- --------------- ------------
1   3.7.0.4     3.7.0.4  3.7.0.4         3.7.0.4
(Routing) #
```

7. Complete la instalación

   El conmutador se reiniciará sin que se aplique ninguna configuración y se restablecerán los valores predeterminados de fábrica. Siga los dos procedimientos para configurar los ajustes básicos del conmutador y aplicar el archivo RCF como se describe en los dos documentos siguientes:

   a. Configure los ajustes básicos del conmutador. Siga el paso 4 y posterior: Restablecer los valores predeterminados de fábrica del conmutador IP de Broadcom
   b. Cree y aplique el archivo RCF como se indica en la Descarga e instalación de los archivos Broadcom RCF

Descarga e instalación de los archivos Broadcom RCF

Debe descargar e instalar el archivo RCF del conmutador en cada conmutador de la configuración IP de MetroCluster.

Antes de empezar

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

Acerca de esta tarea

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

Existen cuatro archivos RCF, uno para cada uno de los cuatro conmutadores de la configuración IP de MetroCluster. Debe utilizar los archivos RCF correctos para el modelo de conmutador que esté utilizando.

Conmutador	Archivo RCF
IP_switch_A_1	v1.32_Switch-A1.txt
IP_switch_A_2	v1.32_Switch-A2.txt
IP_switch_B_1	v1.32_Switch-B1.txt
IP_switch_B_2	v1.32_Switch-B2.txt

> Los archivos RCF para EFOS versión 3.4.4.6 o posterior 3.4.x.x. La versión 3.7.0.4 y la versión de EFOS son diferentes. Debe asegurarse de que ha creado los archivos RCF correctos para la versión EFOS en la que se está ejecutando el conmutador.

Versión EFOS	Versión de archivo RCF
3.4.x.x.	v1.3x, v1.4x
3.7.x.x.	v2.x

Pasos

1. Genere los archivos RCF de Broadcom para MetroCluster IP.
   a. Descargue el "RcfFileGenerator para MetroCluster IP"
   b. Genere el archivo RCF para su configuración utilizando el RcfFileGenerator para MetroCluster IP.

No se admiten las modificaciones realizadas en los archivos RCF después de la descarga.

2. Copie los archivos RCF en los conmutadores:

   a. Copie los archivos RCF en el primer conmutador: `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF/BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr`

      En este ejemplo, el archivo RCF "BES-53248_v1.32_Switch-A1.txt" se copia desde el servidor SFTP en "50.50.50.50" al bootflash local. Debe utilizar la dirección IP del servidor TFTP/SFTP y el nombre de archivo del archivo RCF que necesita instalar.

```
(IP_switch_A_1) #copy sftp://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*************

Mode............................................ SFTP
Set Server IP................................... 50.50.50.50
Path............................................ /RcfFiles/
Filename........................................ BES-
53248_v1.32_Switch-A1.txt
Data Type....................................... Config Script
Destination Filename........................... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.


Validating configuration script...

config

set clibanner
"*******************************************************************
*******

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248



...
The downloaded RCF is validated. Some output is being logged here.
...


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

b. Compruebe que el archivo RCF se guarda como una secuencia de comandos:

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name        Size(Bytes)  Date of Modification
-------------------------------  -----------  --------------------
BES-53248_v1.32_Switch-A1.scr             852   2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Aplicar el script RCF:

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y


config

set clibanner
"*********************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Guarde la configuración:

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

e. Reinicie el switch:

```
reload
```

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

a. Repita los pasos anteriores para cada uno de los otros tres conmutadores, asegurándose de copiar el archivo RCF correspondiente al conmutador correspondiente.

3. Vuelva a cargar el interruptor:

```
reload
```

```
IP_switch_A_1# reload
```

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

Deshabilite los puertos ISL y los canales de puertos no utilizados

NetApp recomienda deshabilitar los puertos ISL y los canales de puertos no utilizados para evitar alertas de estado innecesarias.

1. Identifique los puertos ISL y los canales de puerto no utilizados mediante el banner del archivo RCF:

> Si el puerto está en modo de separación, el nombre de puerto especificado en el comando puede ser diferente al nombre indicado en el banner de RCF. También puede usar los archivos de cableado RCF para buscar el nombre del puerto.

Para los detalles del puerto ISL

Ejecute el comando `show port all`.

Para obtener detalles del canal de puerto

Ejecute el comando `show port-channel all`.

2. Deshabilite los puertos ISL y los canales de puertos sin utilizar.

   Debe ejecutar los siguientes comandos para cada puerto o canal de puerto no utilizado identificado.

```
(SwtichA_1)> enable
(SwtichA_1)# configure
(SwtichA_1)(Config)# <port_name>
(SwtichA_1)(Interface 0/15)# shutdown
(SwtichA_1)(Interface 0/15)# end
(SwtichA_1)# write memory
```

Configure los switches IP de Cisco

Configuración de switches Cisco IP

Debe configurar los switches IP de Cisco para que se usen como interconexión de clúster y para la conectividad IP de MetroCluster back-end.

Acerca de esta tarea

Varios de los procedimientos de esta sección son procedimientos independientes y sólo necesita ejecutar los que se dirigen o son relevantes para su tarea.

Restablecer los valores predeterminados de fábrica del conmutador IP de Cisco

Antes de instalar cualquier archivo RCF, debe borrar la configuración del conmutador Cisco y realizar la configuración básica. Este procedimiento es necesario cuando desea volver a instalar el mismo archivo RCF después de que se haya producido un error en la instalación anterior, o si desea instalar una nueva versión de un archivo RCF.

Acerca de esta tarea

- Debe repetir estos pasos en cada uno de los switches IP de la configuración de IP de MetroCluster.
- Debe estar conectado al conmutador mediante la consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

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 mensaje "'Anular provisión automática y continuar con la configuración normal? (sí/no)", you should respond `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 conmutador 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.

Acerca de esta tarea

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"

Pasos

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       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     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.

Descarga e instalación de los archivos Cisco IP RCF

Debe descargar el archivo RCF en cada switch de la configuración IP de MetroCluster.

Acerca de esta tarea

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"

Existen cuatro archivos RCF, uno para cada uno de los cuatro conmutadores de la configuración IP de MetroCluster. Debe utilizar los archivos RCF correctos para el modelo de conmutador que esté utilizando.

Conmutador	Archivo RCF
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_switch_B_2	NX3232_v1.80_Switch-B2.txt

Pasos

1. Descargue los archivos RCF IP de MetroCluster.

   No se admiten las modificaciones realizadas en los archivos RCF después de la descarga.

2. Copie los archivos RCF en los conmutadores:

   a. Copie los archivos RCF en el primer conmutador:

   ```
   copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
   bootflash: vrf management
   ```

   En este ejemplo, el archivo NX3232_v1.80_Switch-A1.txt RCF se copia desde el servidor SFTP en 10.10.99.99 al bootflash local. Debe utilizar la dirección IP del servidor TFTP/SFTP y el nombre del archivo RCF que necesita instalar.

```
IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt bootflash:
vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get   /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141     5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#
```

a. Repita el subpaso anterior para cada uno de los otros tres conmutadores, asegurándose de copiar el archivo RCF correspondiente al conmutador correspondiente.

3. Compruebe en cada switch que el archivo RCF está presente 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:
                  .
                  .
                  .
5514    Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
                  .
                  .
                  .

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

4. Configure las regiones de TCAM en los switches Cisco 3132Q-V y Cisco 3232C.

   Evite este paso si no tiene switches Cisco 3132Q-V o Cisco 3232C.

   a. En el conmutador Cisco 3132Q-V, establezca las siguientes regiones de TCAM:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

b. En el switch Cisco 3232C, establezca las siguientes regiones de TCAM:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

c. Después de configurar las regiones de TTAM, guarde la configuración y vuelva a cargar el interruptor:

```
copy running-config startup-config
reload
```

5. Copie el archivo RCF correspondiente del bootflash local a la configuración en ejecución de cada switch:

   `copy bootflash:switch-specific-RCF.txt running-config`

6. Copie los archivos RCF de la configuración en ejecución a la configuración de inicio de cada switch:

   `copy running-config startup-config`

   Debería ver una salida similar a la siguiente:

   ```
   IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
   IP_switch-A-1# copy running-config startup-config
   ```

7. Vuelva a cargar el interruptor:

   `reload`

   ```
   IP_switch_A_1# reload
   ```

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

Configuración de la corrección de errores de reenvío para sistemas que utilizan conectividad de 25 Gbps

Si el sistema está configurado con conectividad de 25 Gbps, debe establecer manualmente el parámetro Reenviar corrección de error (Fec) en OFF después de aplicar el archivo RCF. El archivo RCF no aplica esta configuración.

Acerca de esta tarea

Los puertos de 25 Gbps se deben cablear antes de ejecutar este procedimiento.

"Asignaciones de puertos de la plataforma para los switches Cisco 3232C o Cisco 9336C"

Esta tarea sólo se aplica a plataformas que utilizan conectividad de 25 Gbps:

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

Esta tarea debe realizarse en los cuatro switches de la configuración de IP de MetroCluster.

Pasos

1. Establezca el parámetro fec en OFF en cada puerto de 25 Gbps conectado a un módulo de controlador y, a continuación, copie la configuración en ejecución a la configuración de inicio:

   a. Entrar al modo de configuración: `config t`

   b. Especifique la interfaz de 25 Gbps para configurar: `interface interface-ID`

   c. Establecer Fec como desactivado: `fec off`

   d. Repita los pasos anteriores para cada puerto de 25 Gbps del conmutador.

   e. Salir del modo de configuración: `exit`

   El siguiente ejemplo muestra los comandos para la interfaz ethernet1/25/1 en el conmutador IP_switch_A_1:

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Repita el paso anterior en los otros tres switches de la configuración IP de MetroCluster.

Deshabilite los puertos ISL y los canales de puertos no utilizados

NetApp recomienda deshabilitar los puertos ISL y los canales de puertos no utilizados para evitar alertas de estado innecesarias.

1. Identifique los puertos ISL y los canales de puertos sin utilizar:

```
show interface brief
```

2. Deshabilite los puertos ISL y los canales de puertos sin utilizar.

   Debe ejecutar los siguientes comandos para cada puerto o canal de puerto no utilizado identificado.

```
SwitchA_1# config t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA_1(config)# int Eth1/14
SwitchA_1(config-if)# shutdown
SwitchA_12(config-if)# exit
SwitchA_1(config-if)# copy running-config startup-config
[##########################################] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Configurar el cifrado MACsec en switches Cisco 9336C

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

Configurar el cifrado MACsec en switches Cisco 9336C

Solo debe configurar el cifrado MACsec en los puertos ISL WAN que se ejecuten entre los sitios. Debe configurar MACsec después de aplicar el archivo RCF correcto.

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"

Habilita 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.

Pasos

1. Entre al 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
```

Configure una cadena de claves y claves MACsec

Puede crear una cadena de claves o claves MACsec en su configuración.

Key Lifetime y Hless Key Rollover

Una cadena de claves MACsec puede tener varias claves precompartidas (PSK), cada una configurada con un ID de clave y una vida útil opcional. El período de vida de una clave especifica el momento en que se activa y caduca la clave. En ausencia de una configuración de por vida, la vida útil predeterminada es ilimitada. Cuando se configura una vida útil, MKA se desplaza hasta la siguiente clave previamente compartida configurada en la cadena de claves después de que expire la vida útil. La zona horaria de la clave puede ser local o UTC. La zona horaria predeterminada es UTC. Una tecla puede pasar a una segunda clave dentro de la misma cadena de claves si configura la segunda tecla (en la cadena de claves) y configura una vida útil para la primera tecla. Cuando caduca la vida útil de la primera clave, ésta se desplaza automáticamente a la siguiente clave de la lista. Si la misma clave está configurada en ambos lados del enlace al mismo tiempo, la sustitución de la clave es inútil (es decir, la clave se desplaza sin interrupción del tráfico).

Pasos

1. Entre en el modo de configuración global:

   `configure terminal`

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

2. Para ocultar la cadena de octeto de clave cifrada, reemplace la cadena por un carácter comodín en la salida del `show running-config` y.. `show startup-config` comandos:

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```

   > La cadena de octeto también se oculta cuando se guarda la configuración en un archivo.

   De forma predeterminada, las claves PSK se muestran en formato cifrado y se pueden descifrar fácilmente. Este comando sólo se aplica a las cadenas de teclas MACsec.

3. Cree una cadena de claves MACsec para mantener un conjunto de claves MACsec e introduzca el modo de configuración de la cadena de claves MACsec:

```
key chain name macsec
```

```
IP_switch_A_1(config)# key chain 1 macsec
IP_switch_A_1(config-macseckeychain)#
```

4. Cree una tecla MACsec e introduzca el modo de configuración de la tecla MACsec:

```
key key-id
```

El intervalo va de 1 a 32 dígitos hexadecimales de la cadena de clave y el tamaño máximo es de 64 caracteres.

```
IP_switch_A_1 switch(config-macseckeychain)# key 1000
IP_switch_A_1 (config-macseckeychain-macseckey)#
```

5. Configure la cadena de octeto para la clave:

```
key-octet-string octet-string cryptographic-algorithm AES_128_CMAC |
AES_256_CMAC
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789
cryptographic-algorithm AES_256_CMAC
```

> El argumento octeto-string puede contener hasta 64 caracteres hexadecimales. La clave de octeto se codifica internamente, por lo que la clave en texto sin cifrar no aparece en el resultado del `show running-config macsec` comando.

6. Configure una vida útil de envío para la clave (en segundos):

```
send-lifetime start-time duration duration
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00
Oct 04 2020 duration 100000
```

De forma predeterminada, el dispositivo considera la hora de inicio como UTC. El argumento de hora de inicio es la hora del día y la fecha en que la clave se activa. El argumento duración es la duración de la vida en segundos. La longitud máxima es de 2147483646 segundos (aproximadamente 68 años).

7. 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
```

8. Muestra la configuración de la cadena de teclas:

   `show key chain name`

   ```
   IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
   ```

Configure una directiva de MACsec

Pasos

1. Entre al modo de configuración global:

   `configure terminal`

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

2. Crear una directiva de MACsec:

   `macsec policy name`

   ```
   IP_switch_A_1(config)# macsec policy abc
   IP_switch_A_1(config-macsec-policy)#
   ```

3. Configure uno de los siguientes cifrados: GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 o GCM-AES-XPN-256:

   `cipher-suite name`

   ```
   IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
   ```

4. Configure la prioridad del servidor de claves para romper el vínculo entre iguales durante un intercambio de claves:

   `key-server-priority number`

   ```
   switch(config-macsec-policy)# key-server-priority 0
   ```

5. Configure la directiva de seguridad para definir el manejo de los paquetes de datos y de control:

   `security-policy security policy`

   Elija una directiva de seguridad entre las siguientes opciones:

   - Seguro obligatorio — los paquetes que no transportan encabezados MACsec se han eliminado

- Debería-Secure — los paquetes que no portan encabezados MACsec están permitidos (éste es el valor predeterminado)

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. Configure la ventana de protección de repetición de modo que la interfaz segura no acepte un paquete menor que el tamaño de ventana configurado: `window-size number`

> El tamaño de la ventana de protección de reproducción representa el máximo de tramas fuera de secuencia que MACsec acepta y no se descartan. El intervalo es de 0 a 596000000.

```
IP_switch_A_1(config-macsec-policy)# window-size 512
```

7. Configure el tiempo en segundos para forzar una reclave SAK:

   `sak-expiry-time time`

   Puede usar este comando para cambiar la clave de sesión por un intervalo de tiempo previsible. El valor predeterminado es 0.

```
IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
```

8. Configure uno de los siguientes desplazamientos de confidencialidad en la trama de capa 2 donde comienza el cifrado:

   `conf-offsetconfidentiality offset`

   Elija entre las siguientes opciones:

   - CONF-OFFSET-0.
   - CONF-OFFSET-30.
   - CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```

> Este comando puede ser necesario para que los conmutadores intermedios utilicen encabezados de paquete (dmac, smac, etype) como etiquetas MPLS.

9. 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
```

10. Mostrar la configuración de directivas de MACsec:

    `show macsec policy`

    ```
    IP_switch_A_1(config-macsec-policy)# show macsec policy
    ```

Active el cifrado Cisco MACsec en las interfaces

1. Entre al modo de configuración global:

   `configure terminal`

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

2. Seleccione la interfaz que configuró con el cifrado 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)#
   ```

3. Agregue la cadena de claves y la directiva que se van a configurar en la interfaz para agregar la configuración de MACsec:

   `macsec keychain keychain-name policy policy-name`

   ```
   IP_switch_A_1(config-if)# macsec keychain 1 policy abc
   ```

4. Repita los pasos 1 y 2 en todas las interfaces en las que se va a configurar el cifrado MACsec.
5. 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
   ```

Deshabilita los ISL de WAN de cifrado Cisco MACs en las configuraciones IP de MetroCluster

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

Pasos

1. Entre al 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
   ```

   Al seleccionar la opción '"no"' se restaura 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 y la directiva configuradas en la interfaz para eliminar la configuración de MACsec:

   `no macsec keychain keychain-name policy policy-name`

   ```
   IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
   ```

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
   ```

Verificación de la configuración de MACsec

Pasos

1. Repita **todos** de los procedimientos anteriores en el segundo interruptor de la configuración para establecer una sesión de MACsec.

2. Ejecute los siguientes comandos para verificar que ambos switches estén cifrados correctamente:

   a. Ejecución: `show macsec mka summary`

   b. Ejecución: `show macsec mka session`

   c. Ejecución: `show macsec mka statistics`

   Puede verificar la configuración de MACsec mediante los siguientes comandos:

Comando	Muestra información acerca de…
`show macsec mka session interface typeslot/port number`	La sesión MACsec MKA para una interfaz específica o para todas las interfaces
`show key chain name`	La configuración de la cadena de claves
`show macsec mka summary`	La configuración de MACsec MKA
`show macsec policy policy-name`	La configuración para una directiva específica de MACsec o para todas las directivas de MACsec

Configure el conmutador NVIDIA IP SN2100

Debe configurar los switches IP de NVIDIA SN2100 para que se utilicen como interconexión del clúster y como conectividad IP de MetroCluster back-end.

reinicie el conmutador NVIDIA IP SN2100 con los valores predeterminados de fábrica

Puede elegir entre los siguientes métodos para restablecer los ajustes predeterminados de fábrica de un conmutador.

- Restablezca el conmutador mediante la opción de archivo RCF
- Restablezca el interruptor con la opción de instalación Cumulus

reinicie el conmutador mediante la opción de archivo RCF

Antes de instalar una nueva configuración de RCF, debe revertir la configuración del conmutador NVIDIA.

Acerca de esta tarea

Para restaurar la configuración predeterminada del conmutador, ejecute el archivo RCF con el `restoreDefaults` opción. Esta opción copia los archivos de copia de seguridad originales en su ubicación original y, a continuación, reinicia el conmutador. Después del reinicio, el conmutador se conecta con la configuración original que existía cuando ejecutó por primera vez el archivo RCF para configurar el conmutador.

No se restablecen los siguientes detalles de configuración:

- Configuración de credenciales y usuarios
- Configuración del puerto de red de gestión, eth0

Todos los demás cambios de configuración que se produzcan durante la aplicación del archivo RCF se revierten a la configuración original.

Antes de empezar

- Debe configurar el conmutador de acuerdo con Descargue e instale el archivo NVIDIA RCF. Si no ha configurado de esta manera o ha configurado funciones adicionales antes de ejecutar el archivo RCF, no podrá utilizar este procedimiento.
- Debe repetir estos pasos en cada uno de los switches IP de la configuración de IP de MetroCluster.
- Debe estar conectado al conmutador mediante una conexión de consola serie.
- Esta tarea restablece la configuración de la red de gestión.

Pasos

1. Compruebe que la configuración RCF se ha aplicado correctamente con la misma versión de archivo RCF o compatible y que los archivos de copia de seguridad existen.

   La salida puede mostrar archivos de copia de seguridad, archivos conservados o ambos. Si los archivos de copia de seguridad o los archivos conservados no aparecen en la salida, no podrá utilizar este procedimiento.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_1.py
[sudo] password for cumulus:
>>> Opened RcfApplyLog
A RCF configuration has been successfully applied.
  Backup files exist.
    Preserved files exist.
    Listing completion of the steps:
        Success: Step: 1: Performing Backup and Restore
        Success: Step: 2: updating MOTD file
        Success: Step: 3: Disabling apt-get
        Success: Step: 4: Disabling cdp
        Success: Step: 5: Adding lldp config
        Success: Step: 6: Creating interfaces
        Success: Step: 7: Configuring switch basic settings: Hostname,
SNMP
        Success: Step: 8: Configuring switch basic settings: bandwidth
allocation
        Success: Step: 9: Configuring switch basic settings: ecn
        Success: Step: 10: Configuring switch basic settings: cos and
dscp remark
        Success: Step: 11: Configuring switch basic settings: generic
egress cos mappings
        Success: Step: 12: Configuring switch basic settings: traffic
classification
        Success: Step: 13: Configuring LAG load balancing policies
        Success: Step: 14: Configuring the VLAN bridge
        Success: Step: 15: Configuring local cluster ISL ports
        Success: Step: 16: Configuring MetroCluster ISL ports
        Success: Step: 17: Configuring ports for MetroCluster-1, local
cluster and MetroCluster interfaces
        Success: Step: 18: Configuring ports for MetroCluster-2, local
cluster and MetroCluster interfaces
        Success: Step: 19: Configuring ports for MetroCluster-3, local
cluster and MetroCluster interfaces
        Success: Step: 20: Configuring L2FC for MetroCluster interfaces
        Success: Step: 21: Configuring the interface to UP
        Success: Step: 22: Final commit
        Success: Step: 23: Final reboot of the switch
    Exiting ...
<<< Closing RcfApplyLog
cumulus@IP_switch_A_1:mgmt:~$
```

2. Ejecute el archivo RCF con la opción de restaurar los valores predeterminados: `restoreDefaults`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_2.py
restoreDefaults
[sudo] password for cumulus:
>>> Opened RcfApplyLog
Can restore from backup directory. Continuing.
This will reboot the switch !!!
Enter yes or no: yes
```

3. Responda "sí" al mensaje. El conmutador vuelve a la configuración original y se reinicia.
4. Espere a que se reinicie el switch.

   El switch se restablece y conserva la configuración inicial, como la configuración de red de gestión y las credenciales actuales, tal y como existían antes de aplicar el archivo RCF. Después del reinicio, puede aplicar una nueva configuración utilizando la misma versión o una versión diferente del archivo RCF.

reinicie el interruptor con la opción de instalación Cumulus

Acerca de esta tarea

Utilice estos pasos si desea reiniciar el conmutador por completo aplicando la imagen Cumulus.

Antes de empezar

- Debe estar conectado al conmutador mediante una conexión de consola serie.
- La imagen del software del conmutador Cumulus es accesible a través de HTTP.

> Para obtener más información sobre la instalación de Cumulus Linux, consulte "Descripción general de la instalación y configuración de los switches NVIDIA SN2100"

- Debe tener la contraseña raíz para `sudo` acceso a los comandos.

Pasos

1. Desde la consola Cumulus, descargue y ponga en cola la instalación del software del conmutador con el comando `onie-install -a -i` seguido de la ruta de archivo al software del switch:

   En este ejemplo, el archivo de firmware `cumulus-linux-4.4.2-mlx-amd64.bin` Se copia del servidor HTTP '50.50.50.50' al conmutador local.

```
cumulus@IP_switch_A_1:mgmt:~$ sudo onie-install -a -i
http://50.50.50.50/switchsoftware/cumulus-linux-4.4.2-mlx-amd64.bin
Fetching installer: http://50.50.50.50/switchsoftware/cumulus-linux-
4.4.2-mlx-amd64.bin
Downloading URL: http://50.50.50.50/switchsoftware/cumulus-linux-4.4.2-
mlx-amd64.bin
######################################################################
# 100.0%
Success: HTTP download complete.
tar: ./sysroot.tar: time stamp 2021-01-30 17:00:58 is 53895092.604407122
```

```
s in the future
tar: ./kernel: time stamp 2021-01-30 17:00:58 is 53895092.582826352 s in
the future
tar: ./initrd: time stamp 2021-01-30 17:00:58 is 53895092.509682557 s in
the future
tar: ./embedded-installer/bootloader/grub: time stamp 2020-12-10
15:25:16 is 49482950.509433937 s in the future
tar: ./embedded-installer/bootloader/init: time stamp 2020-12-10
15:25:16 is 49482950.509336507 s in the future
tar: ./embedded-installer/bootloader/uboot: time stamp 2020-12-10
15:25:16 is 49482950.509213637 s in the future
tar: ./embedded-installer/bootloader: time stamp 2020-12-10 15:25:16 is
49482950.509153787 s in the future
tar: ./embedded-installer/lib/init: time stamp 2020-12-10 15:25:16 is
49482950.509064547 s in the future
tar: ./embedded-installer/lib/logging: time stamp 2020-12-10 15:25:16 is
49482950.508997777 s in the future
tar: ./embedded-installer/lib/platform: time stamp 2020-12-10 15:25:16
is 49482950.508913317 s in the future
tar: ./embedded-installer/lib/utility: time stamp 2020-12-10 15:25:16 is
49482950.508847367 s in the future
tar: ./embedded-installer/lib/check-onie: time stamp 2020-12-10 15:25:16
is 49482950.508761477 s in the future
tar: ./embedded-installer/lib: time stamp 2020-12-10 15:25:47 is
49482981.508710647 s in the future
tar: ./embedded-installer/storage/blk: time stamp 2020-12-10 15:25:16 is
49482950.508631277 s in the future
tar: ./embedded-installer/storage/gpt: time stamp 2020-12-10 15:25:16 is
49482950.508523097 s in the future
tar: ./embedded-installer/storage/init: time stamp 2020-12-10 15:25:16
is 49482950.508437507 s in the future
tar: ./embedded-installer/storage/mbr: time stamp 2020-12-10 15:25:16 is
49482950.508371177 s in the future
tar: ./embedded-installer/storage/mtd: time stamp 2020-12-10 15:25:16 is
49482950.508293856 s in the future
tar: ./embedded-installer/storage: time stamp 2020-12-10 15:25:16 is
49482950.508243666 s in the future
tar: ./embedded-installer/platforms.db: time stamp 2020-12-10 15:25:16
is 49482950.508179456 s in the future
tar: ./embedded-installer/install: time stamp 2020-12-10 15:25:47 is
49482981.508094606 s in the future
tar: ./embedded-installer: time stamp 2020-12-10 15:25:47 is
49482981.508044066 s in the future
tar: ./control: time stamp 2021-01-30 17:00:58 is 53895092.507984316 s
in the future
tar: .: time stamp 2021-01-30 17:00:58 is 53895092.507920196 s in the
```

```
future
Staging installer image...done.
WARNING:
WARNING: Activating staged installer requested.
WARNING: This action will wipe out all system data.
WARNING: Make sure to back up your data.
WARNING:
Are you sure (y/N)? y
Activating staged installer...done.
Reboot required to take effect.
cumulus@IP_switch_A_1:mgmt:~$
```

2. Responda `y` al mensaje de confirmación de la instalación cuando la imagen se descarga y se verifica.
3. Reinicie el interruptor para instalar el nuevo software: `sudo reboot`

```
cumulus@IP_switch_A_1:mgmt:~$ sudo reboot
```

> El conmutador se reinicia y entra en la instalación del software del conmutador, lo que lleva algún tiempo. Una vez finalizada la instalación, el switch se reinicia y permanece en el aviso de inicio de sesión.

4. Configure los ajustes básicos del switch
   a. Cuando se inicie el conmutador y en el indicador de inicio de sesión, inicie sesión y cambie la contraseña.

      > El nombre de usuario es 'cumulus' y la contraseña predeterminada es 'cumulus'.

```
Debian GNU/Linux 10 cumulus ttyS0

cumulus login: cumulus
Password:
You are required to change your password immediately (administrator
enforced)
Changing password for cumulus.
Current password:
New password:
Retype new password:
Linux cumulus 4.19.0-cl-1-amd64 #1 SMP Cumulus 4.19.206-1+cl4.4.2u1
(2021-12-18) x86_64

Welcome to NVIDIA Cumulus (R) Linux (R)

For support and online technical documentation, visit
http://www.cumulusnetworks.com/support

The registered trademark Linux (R) is used pursuant to a sublicense from
LMI,
the exclusive licensee of Linus Torvalds, owner of the mark on a world-
wide
basis.

cumulus@cumulus:mgmt:~$
```

5. Configure la interfaz de red de gestión.

> El ejemplo siguiente muestra cómo configurar el nombre de host (IP_switch_A_1), la dirección IP (10.10.10.10), la máscara de red (255.255.255.0 (24)) y la puerta de enlace (10.10.10.1) utilizando los comandos: `net add hostname <hostname>`, `net add interface eth0 ip address <IPAddress/mask>`, y. `net add interface eth0 ip gateway <Gateway>`.

```
cumulus@cumulus:mgmt:~$ net add hostname IP_switch_A_1
cumulus@cumulus:mgmt:~$ net add interface eth0 ip address 10.0.10.10/24
cumulus@cumulus:mgmt:~$ net add interface eth0 ip gateway 10.10.10.1
cumulus@cumulus:mgmt:~$ net pending

.
.
.


cumulus@cumulus:mgmt:~$ net commit

.
.
.


net add/del commands since the last "net commit"


User Timestamp Command

cumulus 2021-05-17 22:21:57.437099 net add hostname Switch-A-1
cumulus 2021-05-17 22:21:57.538639 net add interface eth0 ip address
10.10.10.10/24
cumulus 2021-05-17 22:21:57.635729 net add interface eth0 ip gateway
10.10.10.1

cumulus@cumulus:mgmt:~$
```

6. Reinicie el conmutador con el `sudo reboot` comando.

```
cumulus@cumulus:~$ sudo reboot
```

Cuando se reinicie el conmutador, puede aplicar una nueva configuración siguiendo los pasos de Descargue e instale el archivo NVIDIA RCF.

Descargue e instale los archivos NVIDIA RCF

Debe descargar e instalar el archivo RCF del conmutador en cada conmutador de la configuración IP de MetroCluster.

Antes de empezar

- Debe tener la contraseña raíz para `sudo` acceso a los comandos.

- El software del switch está instalado y la red de administración está configurada.
- Ha seguido los pasos para instalar inicialmente el conmutador mediante el método 1 o el método 2.
- No ha aplicado ninguna configuración adicional después de la instalación inicial.

> Si lleva a cabo una configuración adicional después de restablecer el conmutador y antes de aplicar el archivo RCF, no podrá utilizar este procedimiento.

Acerca de esta tarea

Debe repetir estos pasos en cada uno de los switches IP de la configuración de IP de MetroCluster (nueva instalación) o en el conmutador de sustitución (sustitución del switch).

Pasos

1. Genere los archivos NVIDIA RCF para MetroCluster IP.
   a. Descargue el "RcfFileGenerator para MetroCluster IP".
   b. Genere el archivo RCF para su configuración utilizando el RcfFileGenerator para MetroCluster IP.
   c. Desplácese al directorio inicial. Si ha registrado como "cumulus", la ruta de acceso del archivo es `/home/cumulus`.

   ```
   cumulus@IP_switch_A_1:mgmt:~$ cd ~
   cumulus@IP_switch_A_1:mgmt:~$ pwd
   /home/cumulus
   cumulus@IP_switch_A_1:mgmt:~$
   ```

   d. Descargue el archivo RCF en este directorio. El ejemplo siguiente muestra que utiliza SCP para descargar el archivo `MSN2100_v1.0_IP_switch_A_1.txt` desde el servidor '50.50.50.50' a su directorio principal y guárdelo como `MSN2100_v1.0_IP_switch_A_1.py`:

```
cumulus@Switch-A-1:mgmt:~$ scp
username@50.50.50.50:/RcfFiles/MSN2100_v1.0_IP_switch_A_1.txt
./MSN2100_v1.0_IP_switch-A1.py
The authenticity of host '50.50.50.50 (50.50.50.50)' can't be
established.
RSA key fingerprint is
SHA256:B5gBtOmNZvdKiY+dPhh8=ZK9DaKG7g6sv+2gFlGVF8E.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '50.50.50.50' (RSA) to the list of known
hosts.
*******************************************************************
**
Banner of the SCP server
*******************************************************************
**
username@50.50.50.50's password:
MSN2100_v1.0-X2_IP_switch_A1.txt 100% 55KB 1.4MB/s 00:00
cumulus@IP_switch_A_1:mgmt:~$
```

2. Ejecute el archivo RCF. El archivo RCF requiere una opción para aplicar uno o más pasos. A menos que el soporte técnico se lo indique, ejecute el archivo RCF sin la opción de línea de comandos. Para verificar el estado de finalización de los diferentes pasos del archivo RCF, utilice la opción '-1' o 'All' para aplicar todos los pasos (pendientes).

```
cumulus@IP_switch_A_1:mgmt:~$ sudo python3 MSN2100_v1.0_IP_switch_A_1.py
all
[sudo] password for cumulus:
The switch will be rebooted after the step(s) have been run.
Enter yes or no: yes



... the steps will apply - this is generating a lot of output ...



Running Step 24: Final reboot of the switch



... The switch will reboot if all steps applied successfully ...
```

Deshabilite los puertos ISL y los canales de puertos no utilizados

NetApp recomienda deshabilitar los puertos ISL y los canales de puertos no utilizados para evitar alertas de estado innecesarias.

1. Identifique los puertos ISL y los canales de puerto no utilizados mediante el banner del archivo RCF:

> Si el puerto está en modo de separación, el nombre de puerto especificado en el comando puede ser diferente al nombre indicado en el banner de RCF. También puede usar los archivos de cableado RCF para buscar el nombre del puerto.

```
net show interface
```

2. Deshabilite los puertos ISL y los canales de puerto no utilizados con el archivo RCF.

```
cumulus@mcc1-integrity-a1:mgmt:~$ sudo python3 SN2100_v2.0_IP_Switch-
A1.py runCmd
[sudo] password for cumulus:
    Running cumulus version  : 5.4.0
    Running RCF file version : v2.0
Help for runCmd:
    To run a command execute the RCF script as follows:
    sudo python3 <script> runCmd <option-1> <option-2> <option-x>
    Depending on the command more or less options are required. Example
to 'up' port 'swp1'
        sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd swp1 up
    Available commands:
        UP / DOWN the switchport
            sudo python3 SN2100_v2.0_IP_Switch-A1.py runCmd <switchport>
state <up | down>
        Set the switch port speed
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
speed <10 | 25 | 40 | 100 | AN>
        Set the fec mode on the switch port
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
fec <default | auto | rs | baser | off>
        Set the [localISL | remoteISL] to 'UP' or 'DOWN' state
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd [localISL |
remoteISL] state [up | down]
        Set the option on the port to support DAC cables. This option
does not support port ranges.
            You must reload the switch after changing this option for
the required ports. This will disrupt traffic.
            This setting requires Cumulus 5.4 or a later 5.x release.
            sudo python3 SN2100_v2.0_Switch-A1.py runCmd <switchport>
DacOption [enable | disable]
cumulus@mcc1-integrity-a1:mgmt:~$
```

El siguiente comando de ejemplo inhabilita el puerto «swp14»:

```
sudo python3 SN2100_v2.0_Switch-A1.py runCmd swp14 state down
```

Repita este paso para cada puerto o canal de puerto no utilizado identificado.

Configure los conmutadores IP de MetroCluster para la supervisión del estado

En las configuraciones IP de MetroCluster, puede configurar SNMPv3 para supervisar el estado de los switches IP.

Paso 1: Configure el usuario SNMPv3 en los conmutadores IP de MetroCluster

Siga estos pasos para configurar el usuario SNMPv3 en los conmutadores IP de MetroCluster.

> Se deben usar los protocolos de autenticación y de privacidad en los comandos. No se admite el uso de autenticación sin privacidad.

Para switches IP Broadcom

Pasos

1. Si el grupo de usuarios 'network-admin' no existe, créelo:

   ```
   (IP_switch_1) (Config)# snmp-server group network-admin v3 auth read
   "Default"
   ```

2. Confirme que se ha creado el grupo 'network-admin':

   ```
   (IP_switch_1) (Config)# show snmp group
   ```

3. Configure el usuario SNMPv3 en los conmutadores IP de Broadcom:

   ```
   (IP_switch_1)# config
   (IP_switch_1) (Config)# snmp-server user <user_name> network-admin
   [auth-md5/auth-sha/noauth] "<auth_password>" [priv-aes128/priv-des]
   "<priv_password>"
   ```

   En el ejemplo siguiente se deben usar entre comillas para la autenticación y las contraseñas de privacidad:

   ```
   snmp-server user admin1 network-admin auth-md5 "password" priv-des
   "password"
   ```

Para switches IP Cisco

Pasos

1. Ejecute los siguientes comandos para configurar el usuario SNMPv3 en un conmutador IP de Cisco:

   ```
   IP_switch_A_1 # configure terminal
   IP_switch_A_1 (config) # snmp-server user <user_name>  auth
   [md5/sha/sha-256] <auth_password> priv (aes-128) <priv_password>
   ```

2. Compruebe que el usuario SNMPv3 está configurado en el conmutador:

   ```
   IP_switch_A_1(config) # show snmp user <user_name>
   ```

   El siguiente ejemplo muestra que el usuario `admin` Está configurado para SNMPv3:

```
IP_switch_A_1(config)# show snmp user admin
User                Auth      Priv(enforce) Groups
acl_filter

____                ____      _____________ ______
__________

admin               md5       aes-128(no)   network-admin
```

Paso 2: Configure el usuario SNMPv3 en ONTAP

Siga estos pasos para configurar el usuario SNMPv3 en ONTAP.

1. Configure el usuario SNMPv3 en ONTAP:

   ```
   security login create -user-or-group-name <user_name> -application snmp
   -authentication-method usm -remote-switch-ipaddress <ip_address>
   ```

2. Configure la supervisión del estado del switch para supervisar el switch utilizando el nuevo usuario SNMPv3:

   ```
   system switch ethernet modify -device <device_id> -snmp-version SNMPv3
   -community-or-username <user_name>
   ```

3. Compruebe que el número de serie del dispositivo que se supervisará con el usuario SNMPv3 recién creado es correcto:

   a. Muestra el periodo de tiempo de sondeo de monitorización del estado del switch:

      ```
      system switch ethernet polling-interval show
      ```

   b. Ejecute el siguiente comando una vez que haya transcurrido el tiempo de sondeo:

      ```
      system switch ethernet show-all -instance -device <device_serial_number>
      ```