Configure los puertos de red

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Configure los puertos de red

Combine puertos físicos para crear grupos de interfaces ONTAP

Un grupo de interfaces, también conocido como Grupo de Agregación de Enlaces (LAG), se crea combinando dos o más puertos físicos en el mismo nodo en un único puerto lógico. El puerto lógico proporciona una mayor resiliencia, mayor disponibilidad y uso compartido de carga.

Tipos de grupos de interfaces

El sistema de almacenamiento admite tres tipos de grupos de interfaces: Modo único, modo estático y modo múltiple dinámico. Cada grupo de interfaces proporciona diferentes niveles de tolerancia a fallos. Los grupos de interfaces multimodo proporcionan métodos de equilibrio de carga del tráfico de red.

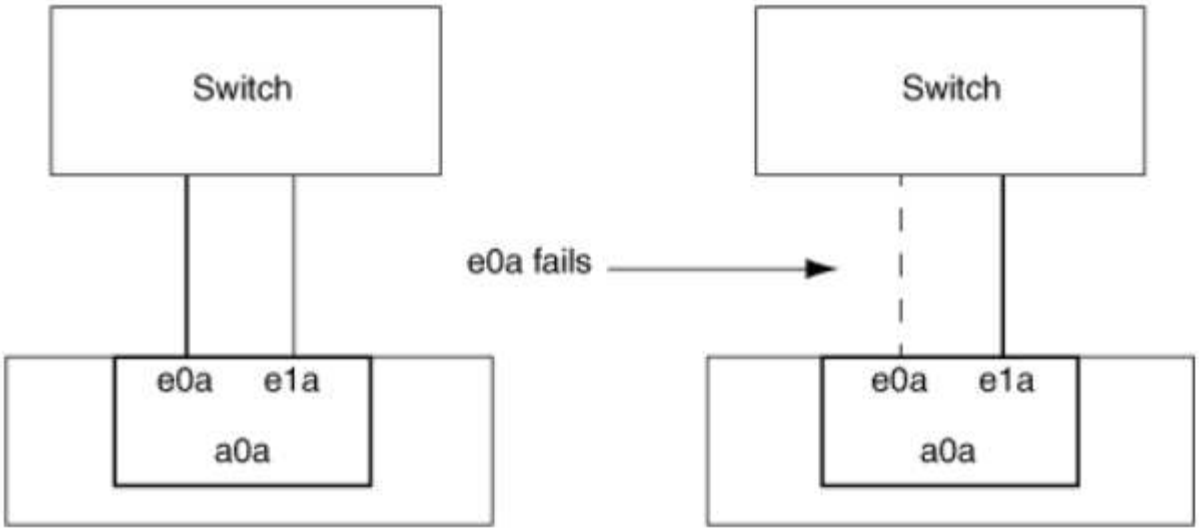
Características de los grupos de interfaces de un único modo

En un grupo de interfaces de un solo modo, solo una de las interfaces del grupo de interfaces está activa. Las otras interfaces están en espera y listas para hacerse cargo si falla la interfaz activa.

Características de los grupos de interfaces de un único modo:

- En caso de conmutación por error, el clúster supervisa el enlace activo y controla la conmutación por error. Dado que el clúster supervisa el enlace activo, no es necesario configurar el switch.
- Puede haber más de una interfaz en espera en un grupo de interfaces de un solo modo.
- Si un grupo de interfaces de un único modo abarca varios switches, debe conectar los switches con un enlace entre switches (ISL).
- Para un grupo de interfaces de un solo modo, los puertos del switch deben estar en el mismo dominio de retransmisión.
- Los paquetes ARP de supervisión de enlaces, que tienen la dirección de origen 0.0.0.0, se envían a través de los puertos para verificar que los puertos están en el mismo dominio de retransmisión.

La siguiente figura es un ejemplo de un grupo de interfaces de modo único. En la figura, e0a y e1a forman parte del grupo de interfaces de modo único a0a. Si la interfaz activa, e0a, falla, la interfaz e1a en espera toma el control y mantiene la conexión con el switch.



Para lograr la funcionalidad de modo único, el método recomendado es utilizar en su lugar grupos de conmutación por error. Al utilizar un grupo de conmutación por error, el segundo puerto puede seguir siendo utilizado para otros LIF y, por lo tanto, no tiene por qué quedar sin utilizar. Además, los grupos de conmutación por error pueden abarcar más de dos puertos y pueden abarcar puertos en varios nodos.

Características de los grupos de interfaces estáticas multimodo

La implementación del grupo de interfaces estáticas multimodo en ONTAP cumple con IEEE 802.3ad (estático). Cualquier switch compatible con agregados, pero no tiene intercambio de paquetes de control para configurar un agregado, se puede utilizar con grupos de interfaces estáticas multimodo.

Los grupos de interfaces estáticas multimodo no cumplen el estándar IEEE 802.3ad (dinámico), también conocido como Protocolo de control de agregación de enlaces (LACP). LACP equivale al Protocolo de agregación de puertos (PAgP), el protocolo de agregación de enlaces de propiedad de Cisco.

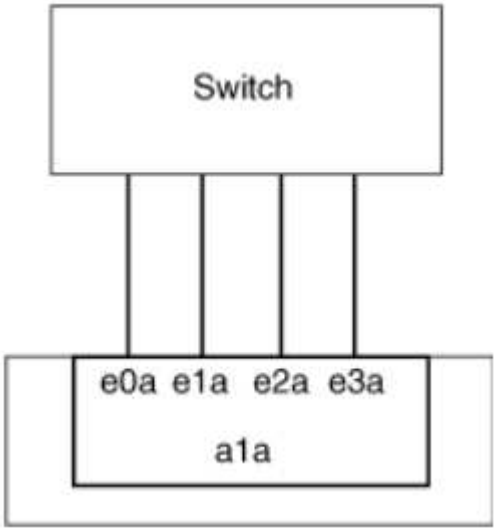
Las siguientes son características de un grupo de interfaces estáticas multimodo:

- Todas las interfaces del grupo de interfaces están activas y comparten una única dirección MAC.
  - Se distribuyen varias conexiones individuales entre las interfaces del grupo de interfaces.
  - Cada conexión o sesión utiliza una interfaz dentro del grupo de interfaces. Cuando se utiliza el esquema de equilibrio de carga secuencial, todas las sesiones se distribuyen por los enlaces disponibles de forma individual y no están vinculadas a una interfaz determinada del grupo de interfaces.
- Los grupos de interfaces estáticas multimodo pueden recuperarse de un fallo de hasta interfaces n-1, donde n es el número total de interfaces que forman el grupo de interfaces.
- Si un puerto falla o está desenchufado, el tráfico que atravesaba el vínculo fallido se redistribuye automáticamente a una de las interfaces restantes.
- Los grupos de interfaces estáticas multimodo pueden detectar una pérdida de enlaces, pero además no pierden la conectividad con las configuraciones erróneas de switches o clientes que podrían afectar a la conectividad y al rendimiento.
- Un grupo de interfaces estáticas multimodo requiere un switch que admita la agregación de enlaces en varios puertos de switch. El switch está configurado de modo que todos los puertos a los que están conectados los enlaces de un grupo de interfaces formen parte de un único puerto lógico. Es posible que algunos switches no admitan la agregación de enlaces de puertos configurados para tramas gigantes.

Para obtener más información, consulte la documentación de su proveedor de switches.

- Hay disponibles varias opciones de equilibrio de carga para distribuir el tráfico entre las interfaces de un grupo de interfaces estáticas multimodo.

La siguiente figura muestra un ejemplo de un grupo de interfaces estáticas multimodo. Las interfaces e0a, e1a, e2a y e3a forman parte del grupo de interfaces multimodo a1a. Las cuatro interfaces del grupo de interfaces multimodo a1a están activas.



Existen varias tecnologías que permiten distribuir el tráfico de un único enlace agregado por varios switches físicos. Las tecnologías utilizadas para lograr esta funcionalidad varían entre los productos de red. Los grupos de interfaces estáticas multimodo de ONTAP cumplen los estándares IEEE 802.3. Si se dice que una tecnología de agregación de enlaces de conmutación múltiple en particular interopera o se ajusta a los estándares IEEE 802.3, debe funcionar con ONTAP.

El estándar IEEE 802.3 indica que el dispositivo de transmisión de un enlace agregado determina la interfaz física para la transmisión. Por lo tanto, ONTAP sólo es responsable de distribuir el tráfico saliente y no puede controlar cómo llegan las tramas entrantes. Si desea gestionar o controlar la transmisión del tráfico entrante en un enlace agregado, dicha transmisión debe modificarse en el dispositivo de red conectado directamente.

Grupo de interfaces dinámicas multimodo

Los grupos de interfaces dinámicas multimodo implementan el protocolo de control de agregación de enlaces (LACP) para comunicar la pertenencia a grupos al switch conectado directamente. LACP permite detectar la pérdida del estado de enlace y la incapacidad del nodo para comunicarse con el puerto del switch de conexión directa.

La implementación de grupos de interfaces dinámicas multimodo en ONTAP cumple con IEEE 802.3 AD (802.1 AX). ONTAP no admite el Protocolo de agregación de puertos (PAgP), que es un protocolo de agregación de enlaces de propiedad de Cisco.

Un grupo de interfaces dinámicas multimodo requiere un switch compatible con LACP.

ONTAP implementa LACP en el modo activo no configurable que funciona bien con los switches configurados en modo activo o pasivo. ONTAP implementa los temporizadores LACP cortos y largos (para su uso con valores no configurables de 3 segundos y 90 segundos), tal y como se especifica en IEEE 802.3 AD (802.1AX).

El algoritmo de equilibrio de carga de ONTAP determina el puerto de miembro que se va a utilizar para

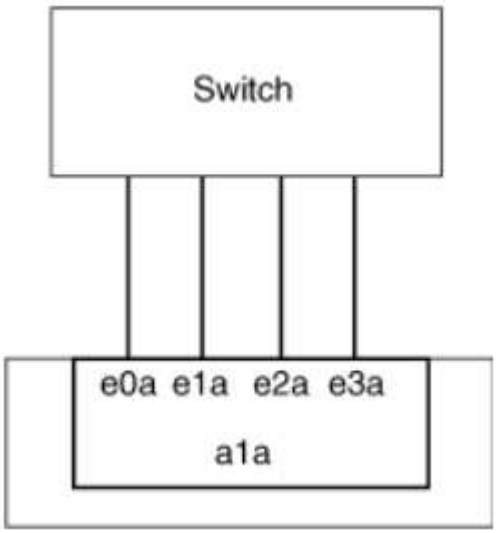
transmitir tráfico saliente y no controla cómo se reciben las tramas entrantes. El conmutador determina el miembro (puerto físico individual) de su grupo de canales de puertos que se utilizará para la transmisión, en función del algoritmo de equilibrio de carga configurado en el grupo de canales de puertos del conmutador. Por lo tanto, la configuración del switch determina el puerto miembro (puerto físico individual) del sistema de almacenamiento que recibirá tráfico. Para obtener más información sobre la configuración del switch, consulte la documentación de su proveedor de switches.

Si una interfaz individual no puede recibir paquetes de protocolo LACP sucesivos, dicha interfaz individual se Marca como "lag_inactive" en el resultado del comando "ifgrp status". El tráfico existente se redirecciona automáticamente a las interfaces activas restantes.

Las siguientes reglas se aplican cuando se utilizan grupos de interfaces dinámicas multimodo:

- Deben configurarse los grupos de interfaces dinámicas multimodo para utilizar los métodos de equilibrio de carga por turnos, basados en puertos, IP, MAC o round-robin.
- En un grupo de interfaces dinámicas multimodo, todas las interfaces deben estar activas y compartir una única dirección MAC.

La siguiente figura muestra un ejemplo de un grupo de interfaces dinámicas multimodo. Las interfaces e0a, e1a, e2a y e3a forman parte del grupo de interfaces multimodo a1a. Las cuatro interfaces del grupo de interfaces dinámicas multimodo a1a están activas.



Equilibrio de carga en grupos de interfaces multimodo

Puede asegurarse de que todas las interfaces de un grupo de interfaces multimodo se usen igual para el tráfico saliente. Para ello, utilice la dirección IP, dirección MAC, secuencial o los métodos de equilibrio de carga basados en puerto para distribuir el tráfico de red de forma equitativa por los puertos de red de un grupo de interfaces multimodo.

Solo se puede especificar el método de equilibrio de carga de un grupo de interfaces multimodo cuando se crea el grupo de interfaces.

Mejor práctica: Se recomienda el equilibrio de carga basado en puerto siempre que sea posible. Utilice el equilibrio de carga basado en puerto a menos que haya un motivo o una limitación específicos en la red que lo impida.

Equilibrio de carga basado en puertos

El equilibrio de carga basado en puerto es el método recomendado.

Puede equilibrar el tráfico en un grupo de interfaces multimodo según los puertos de la capa de transporte (TCP/UDP) usando el método de equilibrio de carga basado en puerto.

El método de equilibrio de carga basado en puertos utiliza un algoritmo de funciones hash rápidas en las direcciones IP de origen y destino junto con el número de puerto de la capa de transporte.

Dirección IP y equilibrio de carga de direcciones MAC

Las direcciones IP y el equilibrio de carga de direcciones MAC son los métodos para equilibrar el tráfico de los grupos de interfaces multimodo.

Estos métodos de equilibrio de carga utilizan un algoritmo de funciones hash rápidas en las direcciones de origen y destino (dirección IP y dirección MAC). Si el resultado del algoritmo de funciones hash se asigna a una interfaz que no está en EL estado DE enlace ACTIVO, se utiliza la siguiente interfaz activa.

> No seleccione el método de equilibrio de carga de direcciones MAC al crear grupos de interfaces en un sistema que se conecta directamente a un router. En este tipo de configuración, para cada trama IP saliente, la dirección MAC de destino es la dirección MAC del router. Como resultado, sólo se utiliza una interfaz del grupo de interfaces.

El equilibrio de carga de direcciones IP funciona del mismo modo para las direcciones IPv4 e IPv6.

Equilibrio de carga secuencial

Puede utilizar el equilibrio de carga secuencial para distribuir de forma equitativa paquetes entre varios vínculos mediante un algoritmo de operación por turnos. Puede utilizar la opción secuencial para equilibrar la carga del tráfico de una conexión única en varios enlaces con el fin de aumentar el rendimiento de la conexión.

No obstante, debido a que el equilibrio de carga secuencial puede provocar una entrega de paquetes fuera de servicio, puede resultar en un rendimiento extremadamente bajo. Por lo tanto, por lo general no se recomienda el equilibrio de carga secuencial.

Cree un grupo de interfaces o LAG

Puede crear un grupo de interfaces o LAG —de un solo modo, multimodo estático o modo múltiple dinámico (LACP)— para presentar una única interfaz a los clientes combinando las funcionalidades de los puertos de red agregados.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para crear un LAG

Pasos

1. Seleccione **Red > Puerto Ethernet > + Grupo de agregación de enlaces** para crear un LAG.
2. Seleccione el nodo de la lista desplegable.
3. Elija una de las siguientes opciones:
   a. ONTAP to **selecciona automáticamente el dominio de difusión (recomendado)**.
   b. Para seleccionar manualmente un dominio de retransmisión.
4. Seleccione los puertos que van a formar LAG.
5. Seleccione el modo:
   a. Único: Solo se utiliza un puerto a la vez.
   b. Múltiples: Todos los puertos se pueden utilizar simultáneamente.
   c. LACP: El protocolo LACP determina los puertos que se pueden utilizar.
6. Seleccione el equilibrio de carga:
   a. Basado en IP
   b. Basado en Mac
   c. Puerto
   d. Secuencial
7. Guarde los cambios.

CLI

Utilice la CLI para crear un grupo de interfaces

Al crear un grupo de interfaces multimodo, puede especificar cualquiera de los siguientes métodos de equilibrio de carga:

- `port`: El tráfico de red se distribuye en función de los puertos de la capa de transporte (TCP/UDP). Este es el método de equilibrio de carga recomendado.
- `mac`: El tráfico de red se distribuye sobre la base de direcciones MAC.
- `ip`: El tráfico de red se distribuye sobre la base de direcciones IP.
- `sequential`: El tráfico de red se distribuye a medida que se recibe.

> La dirección MAC de un grupo de interfaces se determina por el orden de los puertos subyacentes y cómo se inicializan estos puertos durante el arranque. Por lo tanto, no debe asumir que la dirección MAC de ifgrp permanece en reinicios o actualizaciones de ONTAP.

Paso

Utilice `network port ifgrp create` el comando para crear un grupo de interfaces.

Se debe asignar un nombre a los grupos de interfaces mediante la sintaxis `a<number><letter>`. Por ejemplo, a0a, a0b, a1c y a2a son nombres de grupos de interfaces válidos.

Obtenga más información sobre `network port ifgrp create` en el "Referencia de comandos del ONTAP".

El siguiente ejemplo muestra cómo crear un grupo de interfaces llamado a0a con una función de distribución de puerto y un modo de modo múltiple:

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

Agregue un puerto a un grupo de interfaces o LAG

Puede agregar hasta 16 puertos físicos a un grupo de interfaces o LAG para todas las velocidades de puerto.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para agregar un puerto a un LAG

Pasos

1. Seleccione **Red > Puerto Ethernet > LAG** para editar un LAG.
2. Seleccione puertos adicionales en el mismo nodo para agregarlos al LAG.
3. Guarde los cambios.

CLI

Utilice la CLI para agregar puertos a un grupo de interfaces

Paso

Añada puertos de red al grupo de interfaces:

```
network port ifgrp add-port
```

En el siguiente ejemplo se muestra cómo agregar el puerto e0c a un grupo de interfaces llamado a0a:

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

A partir de ONTAP 9.8, los grupos de interfaces se colocan automáticamente en un dominio de retransmisión adecuado un minuto después de agregar el primer puerto físico al grupo de interfaces. Si no desea que ONTAP haga esto y prefiere colocar manualmente el ifgrp en un dominio de retransmisión, especifique `-skip-broadcast-domain-placement` el parámetro como parte del `ifgrp add-port` comando.

Obtenga más información acerca de `network port ifgrp add-port` las restricciones de configuración que se aplican a los grupos de interfaces de puertos en "Referencia de comandos del ONTAP".

Quite un puerto de un grupo de interfaces o LAG

Puede quitar un puerto de un grupo de interfaces que aloje LIF, siempre y cuando no sea el último puerto del grupo de interfaces. No es necesario que el grupo de interfaces no deba ser LIF de host ni que el grupo de

interfaces no sea el puerto de inicio de una LIF teniendo en cuenta que no está quitando el último puerto del grupo de interfaces. Sin embargo, si va a eliminar el último puerto, primero debe migrar o mover las LIF del grupo de interfaces.

Acerca de esta tarea

Puede eliminar hasta 16 puertos (interfaces físicas) de un grupo de interfaces o LAG.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para quitar un puerto de un LAG

Pasos

1. Seleccione **Red > Puerto Ethernet > LAG** para editar un LAG.
2. Seleccione los puertos que desea eliminar del LAG.
3. Guarde los cambios.

CLI

Utilice la CLI para quitar puertos de un grupo de interfaces

Paso

Quite puertos de red de un grupo de interfaces:

```
network port ifgrp remove-port
```

Obtenga más información sobre `network port ifgrp remove-port` en el "Referencia de comandos del ONTAP".

En el ejemplo siguiente se muestra cómo quitar el puerto e0c de un grupo de interfaces llamado a0a:

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

Eliminar un grupo de interfaces o LAG

Puede eliminar grupos de interfaces o LAG si desea configurar LIF directamente en los puertos físicos subyacentes o si decide cambiar el grupo de interfaces, el modo LAG o la función de distribución.

Antes de empezar

- El grupo de interfaces o LAG no deben alojar una LIF.
- El grupo de interfaces o LAG no deben ser ni el puerto de inicio ni el destino de conmutación por error de una LIF.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice el Administrador del sistema para eliminar un LAG

Pasos

1. Seleccione **Red > Puerto Ethernet > LAG** para eliminar un LAG.
2. Seleccione el LAG que desea eliminar.
3. Elimine el LAG.

CLI

Utilice la CLI para eliminar un grupo de interfaces

Paso

Utilice `network port ifgrp delete` el comando para eliminar un grupo de interfaces.

Obtenga más información sobre `network port ifgrp delete` en el "Referencia de comandos del ONTAP".

El siguiente ejemplo muestra cómo eliminar un grupo de interfaces llamado a0b:

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

Configure LAS VLAN de ONTAP en puertos físicos

Puede utilizar VLAN en ONTAP para proporcionar segmentación lógica de redes mediante la creación de dominios de retransmisión independientes que se definen en función del puerto del switch en lugar de los dominios de retransmisión tradicionales, definidos en límites físicos.

Una VLAN puede abarcar varios segmentos de red física. Las estaciones finales que pertenecen a una VLAN están relacionadas por función o aplicación.

Por ejemplo, las estaciones finales de una VLAN podrían agruparse por departamentos, como ingeniería y contabilidad, o por proyectos, como release1 y reubicación2. Debido a que la proximidad física de las estaciones finales no es esencial en una VLAN, puede dispersar geográficamente las estaciones finales y todavía contener el dominio de difusión en una red conmutada.

En ONTAP 9.14.1 y 9.13.1, los puertos sin etiquetar que no son utilizados por ninguna interfaz lógica (LIF) y que carecen de conectividad VLAN nativa en el conmutador conectado se marcan como degradados. Esto es para ayudar a identificar puertos no utilizados y no indica una interrupción. Las VLAN nativas permiten tráfico sin etiquetar en el puerto base ifgrp, como transmisiones ONTAP CFM. Configure VLAN nativas en el conmutador para evitar el bloqueo del tráfico sin etiquetar.

Puede gestionar las VLAN si crea, elimina o muestra información acerca de ellas.

No debe crear una VLAN en una interfaz de red con el mismo identificador que la VLAN nativa del switch. Por ejemplo, si la interfaz de red e0b se encuentra en una VLAN 10 nativa, no se debe crear una VLAN e0b-10 en esa interfaz.

Cree una VLAN

Puede utilizar System Manager o `network port vlan create` el comando para crear VLAN con el fin de mantener dominios de retransmisión independientes en el mismo dominio de redes.

Antes de empezar

Confirme que se han cumplido los siguientes requisitos:

- Los switches implementados en la red deben cumplir los estándares IEEE 802.1Q o tener una implementación de VLAN específica por proveedor.
- Para admitir varias VLAN, una estación final debe estar configurada de forma estática para que pertenezca a una o varias VLAN.
- La VLAN no está conectada a un puerto que aloja una LIF de clúster.
- La VLAN no está conectada a los puertos asignados al espacio IP del clúster.
- La VLAN no se crea en un puerto del grupo de interfaces que no contiene puertos miembro.

Acerca de esta tarea

La creación de una VLAN asocia la VLAN con el puerto de red en un nodo especificado de un clúster.

Cuando se configura una VLAN por primera vez en un puerto, el puerto podría estar inactivo, lo que podría dar lugar a una desconexión temporal de la red. Las adiciones posteriores de VLAN al mismo puerto no afectan al estado del puerto.

> No debe crear una VLAN en una interfaz de red con el mismo identificador que la VLAN nativa del switch. Por ejemplo, si la interfaz de red e0b se encuentra en una VLAN 10 nativa, no se debe crear una VLAN e0b-10 en esa interfaz.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice System Manager para crear un VLAN

A partir de ONTAP 9.12.0, puede seleccionar automáticamente el dominio de difusión o seleccionar manualmente en de la lista. Antes, los dominios de retransmisión siempre se seleccionaban automáticamente en función de la conectividad de la capa 2. Si selecciona manualmente un dominio de retransmisión, aparecerá una advertencia que indica que la selección manual de un dominio de retransmisión podría provocar la pérdida de conectividad.

Pasos

1. Seleccione **Red > Puerto Ethernet > + VLAN**.
2. Seleccione el nodo de la lista desplegable.
3. Elija una de las siguientes opciones:
   a. ONTAP to **selecciona automáticamente el dominio de difusión (recomendado)**.
   b. Para seleccionar manualmente un dominio de difusión de la lista.
4. Seleccione los puertos que van a formar VLAN.
5. Especifique el ID de VLAN.
6. Guarde los cambios.

CLI

Utilice la CLI para crear un VLAN

En determinadas circunstancias, si desea crear el puerto VLAN en un puerto degradado sin corregir el problema del hardware o cualquier configuración incorrecta del software, puede establecer el `-ignore -health-status` parámetro `network port modify` del comando como `true`.

Obtenga más información sobre `network port modify` en el "Referencia de comandos del ONTAP".

Pasos

1. Utilice `network port vlan create` el comando para crear una VLAN.
2. Debe especificar `vlan-name` `port` `vlan-id` las opciones o y al crear una VLAN. El nombre de la VLAN es una combinación del nombre del puerto (o grupo de interfaces) y del identificador de VLAN del switch de red, con un guión entre. Por ejemplo, `e0c-24` y `e1c-80` son nombres de VLAN válidos.

En el ejemplo siguiente se muestra cómo crear una `e1c-80` VLAN conectada al puerto de red `e1c` en el nodo `cluster-1-01`:

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

A partir de ONTAP 9.8, las VLAN se colocan automáticamente en dominios de retransmisión adecuados un minuto después de su creación. Si no desea que ONTAP haga esto y prefiere colocar manualmente la VLAN en un dominio de retransmisión, especifique `-skip-broadcast-domain-placement` el parámetro como parte del `vlan create` comando.

Obtenga más información sobre `network port vlan create` en el "Referencia de comandos del ONTAP".

Editar un VLAN

Puede cambiar el dominio de retransmisión o deshabilitar una VLAN.

Utilice System Manager para editar una VLAN

A partir de ONTAP 9.12.0, puede seleccionar automáticamente el dominio de difusión o seleccionar manualmente en de la lista. Los dominios de retransmisión anteriores siempre se seleccionaron automáticamente en función de la conectividad de la capa 2. Si selecciona manualmente un dominio de retransmisión, aparecerá una advertencia que indica que la selección manual de un dominio de retransmisión podría provocar la pérdida de conectividad.

Pasos

1. Seleccione **Red > Puerto Ethernet > VLAN**.
2. Seleccione el icono de edición.
3. Debe realizar una de las siguientes acciones:
   - Cambie el dominio de difusión seleccionando otro de la lista.
   - Desactive la casilla de verificación **Activado**.
4. Guarde los cambios.

Eliminar un VLAN

Es posible que tenga que eliminar una VLAN antes de extraer una NIC de su ranura. Cuando se elimina una VLAN, se elimina automáticamente de todas las reglas y grupos de conmutación por error que la usan.

Antes de empezar

Asegúrese de que no hay ninguna LIF asociada con la VLAN.

Acerca de esta tarea

Si se elimina la última VLAN de un puerto, se puede producir una desconexión temporal de la red del puerto.

El procedimiento que siga depende de la interfaz que utilice: System Manager o CLI:

System Manager

Utilice el Administrador del sistema para eliminar un VLAN

Pasos

1. Seleccione **Red > Puerto Ethernet > VLAN**.
2. Seleccione el VLAN que desea eliminar.
3. Haga clic en **Eliminar**.

CLI

Utilice la CLI para eliminar una VLAN

Paso

Utilice `network port vlan delete` el comando para eliminar una VLAN.

El siguiente ejemplo muestra cómo eliminar VLAN `e1c-80` del puerto de red `e1c` en el nodo `cluster-1-01`:

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

Obtenga más información sobre `network port vlan delete` en el "Referencia de comandos del ONTAP".

Modificar los atributos de puertos de red ONTAP

Puede modificar la configuración de la autonegociación, el dúplex, el control de flujo, la velocidad y el estado de un puerto de red física.

Antes de empezar

El puerto que desea modificar no debe estar alojando ningún LIF.

Acerca de esta tarea

- No se recomienda modificar la configuración administrativa de las interfaces de red 100 GbE, 40 GbE, 10 GbE o 1 GbE.

  Los valores configurados para el modo doble y la velocidad del puerto se denominan configuración administrativa. Según las limitaciones de la red, la configuración administrativa puede diferir de la configuración operativa (es decir, el modo doble y la velocidad que utiliza realmente el puerto).

- No se recomienda modificar la configuración administrativa de los puertos físicos subyacentes en un grupo de interfaces.

  ```
  `-up-admin`El parámetro (disponible en el nivel de privilegios
  avanzados) modifica la configuración administrativa del puerto.
  ```

- No se recomienda establecer `-up-admin` la configuración administrativa en FALSE para todos los puertos

de un nodo ni para el puerto que aloja el último LIF de clúster operativo en un nodo.

- No se recomienda modificar el tamaño de MTU del puerto de gestión, `e0M`.
- El tamaño de MTU de un puerto en un dominio de retransmisión no se puede cambiar del valor MTU que se establece para el dominio de retransmisión.
- El tamaño de MTU de una VLAN no puede superar el valor del tamaño de MTU de su puerto base.

Pasos

1. Modifique los atributos de un puerto de red:

   `network port modify`

2. Puede definir `-ignore-health-status` el campo en true para especificar que el sistema pueda ignorar el estado del puerto de red de un puerto especificado.

   El estado del puerto de red cambia automáticamente del estado degradado al correcto, y este puerto ahora se puede utilizar para alojar LIF. Debe establecer el control de flujo de los puertos del cluster en `none`. De forma predeterminada, el control de flujo se establece en `full`.

El comando siguiente deshabilita el control de flujo en el puerto e0b estableciendo el control de flujo en none:

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

Obtenga más información sobre `network port modify` en el "Referencia de comandos del ONTAP".

Cree puertos 10GbE para redes ONTAP mediante la conversión de puertos NIC de 40GbE

Es posible convertir las tarjetas de interfaz de red (NIC) X1144A-R6 40 GbE y X91440A-R6 para admitir cuatro puertos 10 GbE.

Si va a conectar una plataforma de hardware que admita una de estas NIC a un clúster que admita la interconexión de clúster 10 GbE y las conexiones de datos del cliente, la NIC debe convertirse para proporcionar las conexiones 10 GbE necesarias.

Antes de empezar

Debe utilizar un cable de cable de conexión compatible.

Acerca de esta tarea

Para obtener una lista completa de las plataformas que admiten NIC, consulte la "Hardware Universe".

> En la NIC X1144A-R6, solo el puerto A puede convertirse para admitir las cuatro conexiones 10 GbE. Una vez convertido el puerto A, el puerto e no está disponible para su uso.

Pasos

1. Entre en el modo de mantenimiento.
2. Convierta el NIC del soporte de 40 GbE al soporte de 10 GbE.

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. Tras utilizar el comando convert, detenga el nodo.
4. Instale o cambie el cable.
5. Según el modelo de hardware, use el SP (Service Processor) o BMC (Baseboard Management Controller) para apagar y encender el nodo para que la conversión surta efecto.

Configure los puertos UTA X1143A-R6 para la red ONTAP

De manera predeterminada, el adaptador de destino unificado X1143A-R6 está configurado en el modo de destino FC, pero puede configurar sus puertos como puertos Ethernet de 10 Gb y FCoE (CNA), o como puertos iniciadores FC o de destino de 16 Gb. Esto requiere distintos adaptadores de SFP+.

Cuando se configura para Ethernet y FCoE, los adaptadores X1143A-R6 admiten el tráfico de destino NIC y FCoE simultáneo en el mismo puerto de 10 GBE. Cuando se configura para FC, cada par de dos puertos que comparte el mismo ASIC se puede configurar individualmente para modo iniciador FC o destino FC. Esto significa que un solo adaptador X1143A-R6 puede admitir el modo objetivo FC en un par de dos puertos y el modo iniciador de FC en otro par de dos puertos. Los pares de puertos conectados al mismo ASIC deben configurarse en el mismo modo.

En el modo FC, el adaptador X1143A-R6 se comporta como cualquier dispositivo FC existente con velocidades de hasta 16 Gbps. En el modo CNA, se puede utilizar el adaptador X1143A-R6 para el tráfico NIC y FCoE simultáneo que comparta el mismo puerto 10 GbE. El modo CNA solo admite el modo de destino FC para la función FCoE.

Para configurar el adaptador de objetivo unificado (X1143A-R6), debe configurar los dos puertos adyacentes en el mismo chip en el mismo modo Personality.

Pasos

1. Vea la configuración del puerto:

```
system hardware unified-connect show
```

2. Configure los puertos según sea necesario para Fibre Channel (FC) o adaptador de red convergente (CNA):

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. Conecte los cables adecuados para FC o Ethernet de 10 GB.
4. Compruebe que tiene instalado el SFP+ correcto:

```
network fcp adapter show -instance -node -adapter
```

Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB, a partir de la estructura de FC al que se está conectando.

Convierta el puerto UTA2 para su uso en la red ONTAP

Puede convertir el puerto UTA2 del modo de adaptador de red convergente (CNA) al modo Fibre Channel (FC), o viceversa.

Debe cambiar la personalidad de UTA2 del modo CNA al modo FC cuando necesite cambiar el soporte físico que conecta el puerto a su red o para admitir los iniciadores y el destino de FC.

Del modo CNA al modo FC

Pasos

1. Desconectar el adaptador:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. Cambie el modo de puerto:

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
```

3. Reinicie el nodo y a continuación, active el adaptador:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin up
```

4. Notifique a su administrador o VIF Manager que elimine o quite el puerto, según corresponda:
   - Si el puerto se utiliza como puerto de inicio de una LIF, es miembro de un grupo de interfaces (ifgrp) o una VLAN de host, un administrador debe hacer lo siguiente:
     - Mueva las LIF, quite el puerto del ifgrp o elimine las VLAN respectivamente.
     - Elimine manualmente el puerto ejecutando `network port delete` el comando. Si el `network port delete` comando falla, el administrador debe solucionar los errores y a continuación, volver a ejecutar el comando.
   - Si el puerto no se usa como puerto de inicio de una LIF, no es miembro de un ifgrp y no aloja VLAN, el gestor VIF debería eliminar el puerto de sus registros en el momento del reinicio. Si el administrador de VIF no elimina el puerto, el administrador debe eliminarlo manualmente después del reinicio mediante el `network port delete` comando.

     Obtenga más información sobre `network port delete` en el "Referencia de comandos del ONTAP".

5. Compruebe que tiene instalado el SFP+ correcto:

```
network fcp adapter show -instance -node -adapter
```

   Para CNA, se debe usar un SFP Ethernet de 10 GB. Para FC, se debe usar un SFP de 8 GB o un SFP de 16 GB antes de cambiar la configuración en el nodo.

Del modo FC al modo CNA

Pasos

1. Desconectar el adaptador:

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. Cambie el modo de puerto:

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. Reiniciar el nodo
4. Compruebe que tiene instalado el SFP+ correcto.

   Para CNA, se debe usar un SFP Ethernet de 10 GB.

Convierta los módulos ópticos CNA/UTA2 para la red ONTAP

Debe cambiar los módulos ópticos del adaptador de destino unificado (CNA/UTA2) para admitir el modo de personalidad seleccionado para el adaptador.

Pasos

1. Verifique el SFP+ actual utilizado en la tarjeta. A continuación, reemplace el SFP+ actual por el SFP+ adecuado para la personalidad preferida (FC o CNA).
2. Retire los módulos ópticos actuales del adaptador X1143A-R6.
3. Inserte los módulos correctos para la óptica del modo de personalidad preferido (FC o CNA).
4. Compruebe que tiene instalado el SFP+ correcto:

```
network fcp adapter show -instance -node -adapter
```

   Los módulos SFP+ admitidos y los cables de cobre (Twinax) de marca Cisco se muestran en la "NetApp Hardware Universe".

Quite las NIC de los nodos del clúster de ONTAP

Es posible que tenga que extraer una NIC defectuosa de su ranura o mover la NIC a otra ranura para realizar tareas de mantenimiento.

> El procedimiento para eliminar una NIC es diferente en ONTAP 9,7 y versiones anteriores. Si necesita quitar una NIC de un nodo de clúster de ONTAP que ejecuta ONTAP 9,7 y versiones anteriores, consulte el procedimiento "Eliminar una NIC del nodo (ONTAP 9,7 o anterior)".

Pasos

1. Apague el nodo.

2. Extraiga físicamente la NIC de su ranura.
3. Encienda el nodo.
4. Compruebe que el puerto se ha eliminado:

```
network port show
```

> ONTAP quita automáticamente el puerto de cualquier grupo de interfaces. Si el puerto era el único miembro de un grupo de interfaces, se elimina el grupo de interfaces. Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

5. Si el puerto tenía alguna VLAN configurada en él, se desplazarán. Las VLAN desplazadas se pueden ver mediante el siguiente comando:

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

> `displaced-interface show` `displaced-vlans show` `displaced-vlans restore`Los comandos , , y son únicos y no requieren el nombre de comando completo, que comienza por `cluster controller-replacement network`.

6. Estas VLAN se eliminan, pero se pueden restaurar mediante el siguiente comando:

```
displaced-vlans restore
```

7. Si el puerto tenía alguna LIF configurada en él, ONTAP elige automáticamente nuevos puertos raíz para esas LIF en otro puerto del mismo dominio de retransmisión. Si no se encuentra ningún puerto de inicio adecuado en el mismo servidor de almacenamiento, se considera que esos LIF están desplazados. Puede ver las LIF desplazadas mediante el siguiente comando:

   `displaced-interface show`

8. Cuando se agrega un nuevo puerto al dominio de retransmisión en el mismo nodo, los puertos iniciales para las LIF se restauran automáticamente. Como alternativa, puede establecer el puerto de inicio con `network interface modify -home-port -home-node or use the displaced- interface restore` el comando.

Información relacionada

- "eliminación de la interfaz desplazada de la red de sustitución de la controladora de cluster"
- "modificación de la interfaz de red"

Supervise los puertos de red

Supervise el estado de los puertos de red ONTAP

La gestión de ONTAP de los puertos de red incluye supervisión automática del estado y

un conjunto de monitores de estado para ayudarle a identificar puertos de red que podrían no ser adecuados para alojar LIF.

Acerca de esta tarea

Si un monitor de estado determina que un puerto de red no es bueno, advierte a los administradores a través de un mensaje de EMS o Marca el puerto como degradado. ONTAP evita el alojamiento de LIF en puertos de red degradados si existen destinos de conmutación al nodo de respaldo alternativos en buen estado para esa LIF. Un puerto puede degradarse debido a un evento de fallo de software, como el enlace flapping (enlaces que rebotan rápidamente entre arriba y abajo) o la partición de red:

- Los puertos de red del espacio IP del clúster se marcan como degradados cuando experimentan el enlace flopping o la pérdida de la capacidad de acceso de la capa 2 (L2) a otros puertos de red en el dominio de retransmisión.
- Los puertos de red de los espacios IP que no pertenecen al clúster se marcan como degradados cuando experimentan un enlace flapping.

Debe tener en cuenta los siguientes comportamientos de un puerto degradado:

- No se puede incluir un puerto degradado en una VLAN o en un grupo de interfaces.

  Si un puerto del miembro de un grupo de interfaces se Marca como degradado, pero el grupo de interfaces sigue marcado como correcto, las LIF se pueden alojar en ese grupo de interfaces.

- Los LIF se migran automáticamente de puertos degradados a puertos en buen estado.
- Durante un evento de conmutación por error, no se considera un puerto degradado como destino de conmutación por error. Si no hay puertos en buen estado disponibles, puertos LIF degradados del host según la política de conmutación al respaldo normal.
- No puede crear, migrar o revertir un LIF a un puerto degradado.

  Puede modificar `ignore-health-status` la configuración del puerto de red a `true`. Luego puede alojar una LIF en los puertos en buen estado.

Pasos

1. Inicie sesión en el modo de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Compruebe qué monitores de estado están habilitados para supervisar el estado del puerto de red:

   ```
   network options port-health-monitor show
   ```

   El estado de un puerto está determinado por el valor de los monitores de estado.

   Los siguientes monitores de estado están disponibles y están habilitados de manera predeterminada en ONTAP:

   - Monitor de estado de enlace: Monitores de enlace flapping

     Si un puerto tiene un enlace que flaquear más de una vez en cinco minutos, este puerto se Marca

como degradado.

- Monitor de estado de accesibilidad L2: Controla si todos los puertos configurados en el mismo dominio de difusión tienen accesibilidad L2 entre sí

  Este monitor de estado genera problemas de accesibilidad L2 en todos los espacios IP; sin embargo, solo Marca los puertos del espacio IP del clúster como degradados.

- Monitor CRC: Supervisa las estadísticas de CRC en los puertos

  Este monitor de estado no Marca un puerto como degradado, pero genera un mensaje de EMS cuando se observa una tasa de fallo de CRC muy alta.

Obtenga más información sobre `network options port-health-monitor show` en el "Referencia de comandos del ONTAP".

3. Habilite o deshabilite cualquiera de los monitores de estado para un espacio IP según lo desee con `network options port-health-monitor modify` el comando.

   Obtenga más información sobre `network options port-health-monitor modify` en el "Referencia de comandos del ONTAP".

4. Consulte el estado detallado de un puerto:

   ```
   network port show -health
   ```

El resultado del comando muestra el estado del puerto, `ignore health status` la configuración y la lista de motivos por los que el puerto se marca como degradado.

El estado del puerto puede ser `healthy` o. `degraded`

Si `ignore health status` el valor es `true`, indica que el `degraded` `healthy` administrador ha modificado el estado del puerto de a.

Si `ignore health status` el valor es `false`, el estado del puerto lo determina automáticamente el sistema.

Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

Supervise la accesibilidad de los puertos de red ONTAP

La supervisión de la accesibilidad está integrada en ONTAP 9.8 y versiones posteriores. Utilice esta supervisión para identificar cuándo la topología de red física no coincide con la configuración de ONTAP. En algunos casos, ONTAP puede reparar la accesibilidad de los puertos. En otros casos, se requieren pasos adicionales.

Acerca de esta tarea

Utilice estos comandos para verificar, diagnosticar y reparar configuraciones incorrectas de red procedentes de la configuración de ONTAP que no coinciden con el cableado físico o la configuración del switch de red.

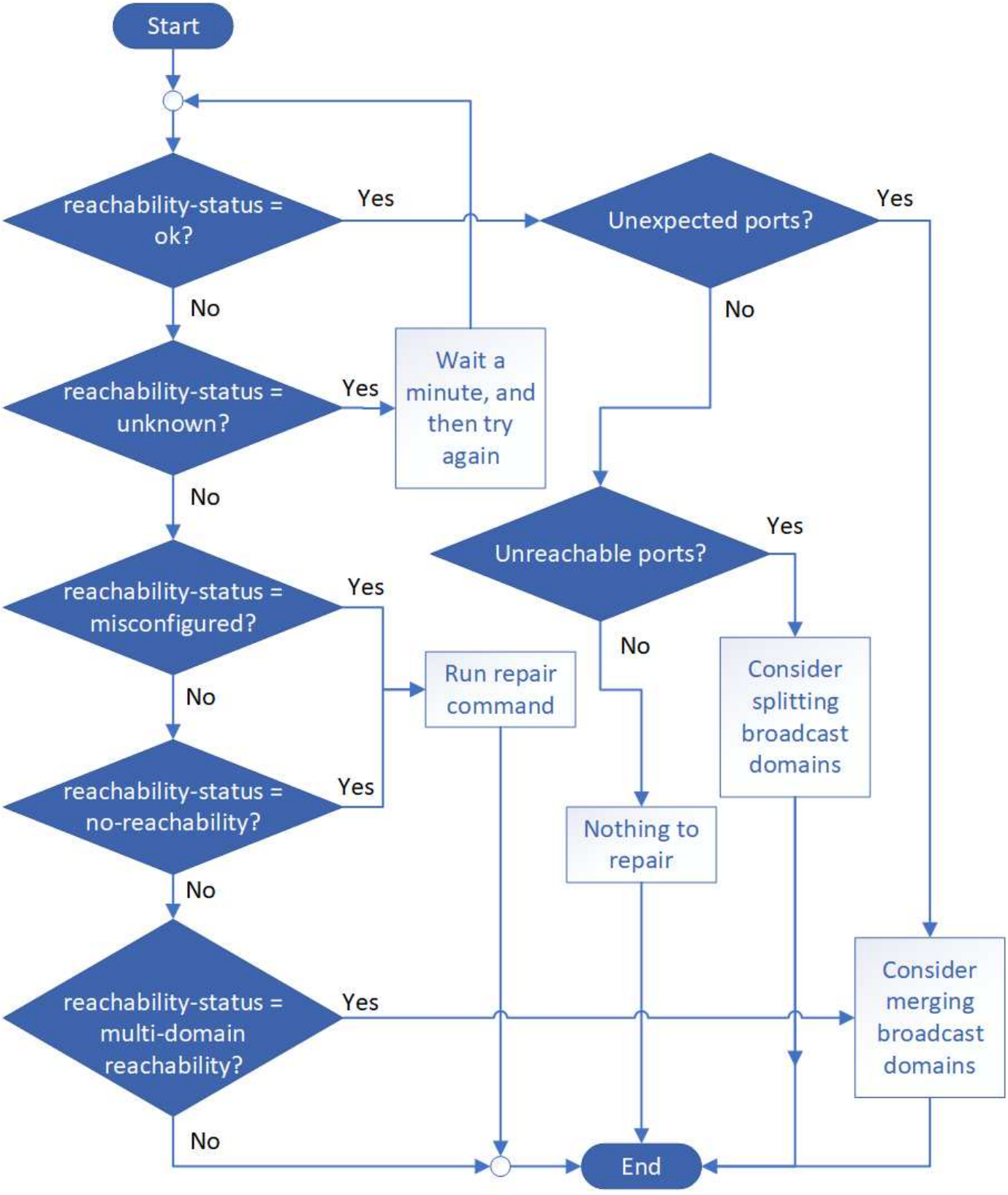
Paso

1. Ver accesibilidad de puertos:

   ```
   network port reachability show
   ```

   Obtenga más información sobre `network port reachability show` en el "Referencia de comandos del ONTAP".

2. Utilice el árbol de decisiones y la tabla siguientes para determinar el siguiente paso, si existe alguno.



Accesibilidad-estado	Descripción

de acuerdo	El puerto tiene capacidad de acceso de capa 2 a su dominio de difusión asignado. Si el reachability-status es "ok", pero hay "puertos inesperados", considere combinar uno o más dominios de difusión. Para obtener más información, consulte la siguiente fila *inesperado ports*. Si el reachability-status es "ok", pero hay "puertos inaccesibles", considere dividir uno o más dominios de difusión. Para obtener más información, consulte la siguiente fila *ports* sin acceso. Si el estado de accesibilidad es "correcto" y no hay puertos inesperados o no accesibles, la configuración es correcta.
Puertos inesperados	El puerto tiene la habilidad de la capa 2 para su dominio de broadcast asignado; sin embargo, también tiene la habilidad de la capa 2 para al menos otro dominio de broadcast. Examine la configuración física del conmutador y la conectividad para determinar si es incorrecta o si el dominio de difusión asignado al puerto necesita combinarse con uno o más dominios de difusión. Para obtener más información, consulte "Fusionar dominios de retransmisión".
Puertos inaccesibles	Si un solo dominio de difusión se ha particionado en dos conjuntos de accesibilidad diferentes, puede dividir un dominio de difusión para sincronizar la configuración de ONTAP con la topología de red física. Normalmente, la lista de puertos inaccesibles define el conjunto de puertos que se deben dividir en otro dominio de retransmisión después de verificar que la configuración física y de switch es correcta. Para obtener más información, consulte "Divida los dominios de retransmisión".
función mal configurada	El puerto no tiene posibilidad de recurrir a la capa 2 a su dominio de difusión asignado; sin embargo, el puerto tiene capacidad de acceso de capa 2 a un dominio de difusión diferente. Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto al dominio de retransmisión al que se le habrá accesibilidad: `network port reachability repair -node -port` Para obtener más información, consulte "Reparar la accesibilidad del puerto".

ausencia de accesibilidad	El puerto no tiene posibilidad de recurrir a ningún dominio de difusión existente de capa 2. Puede reparar la accesibilidad del puerto. Cuando ejecute el siguiente comando, el sistema asignará el puerto a un dominio de retransmisión creado automáticamente en el espacio IP predeterminado: `network port reachability repair -node -port` Para obtener más información, consulte "Reparar la accesibilidad del puerto". Obtenga más información sobre `network port reachability repair` en el "Referencia de comandos del ONTAP".
accesibilidad multi-dominio	El puerto tiene la habilidad de la capa 2 para su dominio de broadcast asignado; sin embargo, también tiene la habilidad de la capa 2 para al menos otro dominio de broadcast. Examine la configuración física del conmutador y la conectividad para determinar si es incorrecta o si el dominio de difusión asignado al puerto necesita combinarse con uno o más dominios de difusión. Para obtener más información, consulte "Fusionar dominios de retransmisión" o "Reparar la accesibilidad del puerto".
desconocido	Si el estado de accesibilidad es "desconocido", espere unos minutos y vuelva a intentar el comando.

Después de reparar un puerto, necesita comprobar y resolver las LIF y VLAN desplazadas. Si el puerto era parte de un grupo de interfaces, también necesita comprender lo que ha sucedido con ese grupo de interfaces. Para obtener más información, consulte "Reparar la accesibilidad del puerto".

Obtenga información acerca del uso de puertos en la red ONTAP

Varios puertos conocidos están reservados para comunicaciones ONTAP con servicios específicos. Se producen conflictos de puertos si un valor de puerto en el entorno de red de almacenamiento es el mismo que el valor de un puerto ONTAP.

Tráfico entrante

El tráfico entrante del sistema de almacenamiento de ONTAP utiliza los siguientes protocolos y puertos:

Protocolo	Puerto	Específico
Todos los ICMP	Todo	Hacer ping a la instancia
TCP	22	Acceso de shell seguro a la dirección IP de la LIF de gestión del clúster o una LIF de gestión de nodos
TCP	80	Acceso de la página web a la dirección IP de la LIF de administración del clúster
TCP/UDP	111	RPCBIND, llamada de procedimiento remoto para NFS

UDP	123	NTP, Protocolo de hora de red
TCP	135	MSRPC, llamada de procedimiento remoto de Microsoft
TCP	139	NETBIOS-SSN, sesión de servicio de NetBIOS para CIFS
TCP/UDP	161-162	SNMP, Protocolo sencillo de gestión de redes
TCP	443	Acceso seguro de la página web a la dirección IP de la LIF de administración de clúster
TCP	445	Servicios de MS Active Domain, Microsoft SMB/CIFS sobre TCP con el marco NetBIOS
TCP/UDP	635	Montaje NFS para interactuar con un sistema de archivos remoto como si fuera local
TCP	749	Kerberos
UDP	953	Daemon de nombres
TCP/UDP	2049	Daemon del servidor NFS
TCP	2050	NRV, protocolo de volumen remoto NetApp
TCP	3260	Acceso iSCSI mediante la LIF de datos iSCSI
TCP/UDP	4045	Daemon de bloqueo NFS
TCP/UDP	4046	Supervisor de estado de red para NFS
UDP	4049	RPC de NFS rquotad
UDP	4444	KRB524, Kerberos 524
UDP	5353	DNS de multidifusión
TCP	10000	Backup mediante Network Data Management Protocol (NDMP)
TCP	11104	Gestión bidireccional de sesiones de comunicación entre clústeres para SnapMirror
TCP	11105	Cluster peering y transferencia de datos SnapMirror bidireccional mediante LIF de interconexión de clústeres
SSL/TLS	30000	Acepta conexiones de control seguro NDMP entre el DMA y el servidor NDMP a través de sockets seguros (SSL/TLS). Los escáneres de seguridad pueden informar una vulnerabilidad en el puerto 30000.

Tráfico saliente

El tráfico saliente en su sistema de almacenamiento de ONTAP se puede configurar con reglas básicas o avanzadas, en función de las necesidades empresariales.

Reglas de salida básicas

Todos los puertos se pueden utilizar para todo el tráfico saliente a través de los protocolos ICMP, TCP y UDP.

Protocolo	Puerto	Específico
Todos los ICMP	Todo	Todo el tráfico saliente
Todas las TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir solo los puertos necesarios para la comunicación saliente por ONTAP.

Active Directory

Protocolo	Puerto	Origen	Destino	Específico
TCP	88	LIF de gestión de nodos, LIF de datos (NFS, CIFS, iSCSI)	Bosque de Active Directory	Autenticación Kerberos V.
UDP	137	LIF de gestión de nodos, LIF de datos (NFS, CIFS)	Bosque de Active Directory	Servicio de nombres NetBIOS
UDP	138	LIF de gestión de nodos, LIF de datos (NFS, CIFS)	Bosque de Active Directory	Servicio de datagramas NetBIOS
TCP	139	LIF de gestión de nodos, LIF de datos (NFS, CIFS)	Bosque de Active Directory	Sesión de servicio NetBIOS
TCP	389	LIF de gestión de nodos, LIF de datos (NFS, CIFS)	Bosque de Active Directory	LDAP
UDP	389	LIF de gestión de nodos, LIF de datos (NFS, CIFS)	Bosque de Active Directory	LDAP
TCP	445	LIF de gestión de nodos, LIF de datos (NFS, CIFS)	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
TCP	464	LIF de gestión de nodos, LIF de datos (NFS, CIFS)	Bosque de Active Directory	Cambiar y establecer la contraseña de Kerberos V (SET_CHANGE)
UDP	464	LIF de gestión de nodos, LIF de datos (NFS, CIFS)	Bosque de Active Directory	Administración de claves Kerberos
TCP	749	LIF de gestión de nodos, LIF de datos (NFS, CIFS)	Bosque de Active Directory	Cambiar y establecer la contraseña de Kerberos V (RPCSEC_GSS)

AutoSupport

Protocolo	Puerto	Origen	Destino	Específico
TCP	80	LIF de gestión de nodos	support.netapp.com	AutoSupport (solo si el protocolo de transporte cambia de HTTPS a HTTP)

SNMP

Protocolo	Puerto	Origen	Destino	Específico
TCP/UDP	162	LIF de gestión de nodos	Servidor de supervisión	Supervisión mediante capturas SNMP

SnapMirror

Protocolo	Puerto	Origen	Destino	Específico
TCP	11104	LIF de interconexión de clústeres	LIF de interconexión de clústeres de ONTAP	Gestión de sesiones de comunicación de interconexión de clústeres para SnapMirror

Otros servicios

Protocolo	Puerto	Origen	Destino	Específico
TCP	25	LIF de gestión de nodos	Servidor de correo	Alertas SMTP, que se pueden utilizar para AutoSupport
UDP	53	LIF de gestión de nodos y LIF de datos (NFS, CIFS)	DNS	DNS
UDP	67	LIF de gestión de nodos	DHCP	Servidor DHCP
UDP	68	LIF de gestión de nodos	DHCP	Cliente DHCP para la configuración inicial
UDP	514	LIF de gestión de nodos	Servidor de syslog	Mensajes de syslog Reenviar
TCP	5010	LIF de interconexión de clústeres	Extremo de backup o extremo de restauración	Realizar backups y restaurar operaciones para el backup en S3 función
TCP	18600 a 18699	LIF de gestión de nodos	Servidores de destino	Copia NDMP

Obtenga más información sobre los puertos internos de ONTAP

La siguiente tabla enumera los puertos que ONTAP utiliza internamente y sus funciones. ONTAP utiliza estos puertos para diversas funciones, como establecer la comunicación LIF dentro del clúster.

Esta lista no es exhaustiva y puede variar en diferentes entornos.

Puerto/protocolo	Componente/función
514	Syslog
900	RPC de clúster de NetApp

902	RPC de clúster de NetApp
904	RPC de clúster de NetApp
905	RPC de clúster de NetApp
910	RPC de clúster de NetApp
911	RPC de clúster de NetApp
913	RPC de clúster de NetApp
914	RPC de clúster de NetApp
915	RPC de clúster de NetApp
918	RPC de clúster de NetApp
920	RPC de clúster de NetApp
921	RPC de clúster de NetApp
924	RPC de clúster de NetApp
925	RPC de clúster de NetApp
927	RPC de clúster de NetApp
928	RPC de clúster de NetApp
929	RPC de clúster de NetApp
930	Servicios y funciones de gestión del kernel (KSMF)
931	RPC de clúster de NetApp
932	RPC de clúster de NetApp
933	RPC de clúster de NetApp
934	RPC de clúster de NetApp
935	RPC de clúster de NetApp
936	RPC de clúster de NetApp
937	RPC de clúster de NetApp
939	RPC de clúster de NetApp
940	RPC de clúster de NetApp
951	RPC de clúster de NetApp
954	RPC de clúster de NetApp
955	RPC de clúster de NetApp
956	RPC de clúster de NetApp
958	RPC de clúster de NetApp
961	RPC de clúster de NetApp
963	RPC de clúster de NetApp
964	RPC de clúster de NetApp

966	RPC de clúster de NetApp
967	RPC de clúster de NetApp
975	Protocolo de interoperabilidad de gestión de claves (KMIP)
982	RPC de clúster de NetApp
983	RPC de clúster de NetApp
5125	Puerto de control alternativo para el disco
5133	Puerto de control alternativo para el disco
5144	Puerto de control alternativo para el disco
65502	SSH de alcance del nodo
65503	Uso compartido de LIF
7700	Administrador de sesiones de clúster (CSM)
7810	RPC de clúster de NetApp
7811	RPC de clúster de NetApp
7812	RPC de clúster de NetApp
7813	RPC de clúster de NetApp
7814	RPC de clúster de NetApp
7815	RPC de clúster de NetApp
7816	RPC de clúster de NetApp
7817	RPC de clúster de NetApp
7818	RPC de clúster de NetApp
7819	RPC de clúster de NetApp
7820	RPC de clúster de NetApp
7821	RPC de clúster de NetApp
7822	RPC de clúster de NetApp
7823	RPC de clúster de NetApp
7824	RPC de clúster de NetApp
7835-7839 y 7845-7849	Puertos TCP para comunicación dentro del clúster
8023	Telnet de alcance de nodo
8443	Puerto NAS ONTAP S3 para Amazon FSx
8514	Alcance del nodo RSH
9877	Puerto de cliente KMIP (solo host local interno)
10006	Puerto TCP para comunicación de interconexión HA