Gestión de redes

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Gestión de redes

Manos a la obra

Visualizar la red de ONTAP mediante System Manager

A partir de ONTAP 9.8, puede usar System Manager para mostrar un gráfico que muestra los componentes y la configuración de la red, lo que le permite ver las rutas de conexión de red entre los hosts, los puertos, las SVM, los volúmenes, etc. A partir de ONTAP 9.12.1, puede ver la asociación de LIF y subred en la cuadrícula interfaces de red.

El gráfico se muestra cuando selecciona **Red > Descripción general** o cuando selecciona → en la sección **Red** del Panel de control.

En el gráfico se muestran las siguientes categorías de componentes:

- Hosts
- Puertos de almacenamiento
- Interfaces de red
- Máquinas virtuales de almacenamiento
- Componentes de acceso a datos

Cada sección muestra detalles adicionales que puede pasar el ratón sobre o seleccionar para realizar tareas de configuración y gestión de la red.

Si utiliza el administrador del sistema clásico (disponible sólo en ONTAP 9, 7 y anteriores), consulte "Gestión de la red".

Ejemplos

A continuación se muestran algunos ejemplos de las muchas maneras en que puede interactuar con el gráfico para ver detalles sobre cada componente o iniciar acciones para administrar su red:

- Haga clic en un host para ver su configuración: Los puertos, las interfaces de red, las máquinas virtuales de almacenamiento y los componentes de acceso a datos asociados con este.
- Pase el ratón por la cantidad de volúmenes de una máquina virtual de almacenamiento para seleccionar un volumen para ver sus detalles.
- Seleccione una interfaz de iSCSI para ver el rendimiento durante la última semana.
- Haga clic en ⋮ junto a un componente para iniciar acciones para modificar ese componente.
- Determine rápidamente dónde pueden ocurrir los problemas en la red, indicado por una "X" junto a componentes que no son sanos.

Vídeo sobre visualización de red de System Manager

Obtenga información sobre los componentes de red de un clúster de ONTAP

Antes de configurar el clúster, debe familiarizarse con los componentes de red de un clúster. La configuración de los componentes físicos de redes de un clúster en componentes lógicos proporciona la flexibilidad y la funcionalidad multi-tenancy en ONTAP.

Los diferentes componentes de red de un clúster son los siguientes:

- Puertos físicos

  Las tarjetas de interfaz de red (NIC) y los adaptadores de bus host (HBA) proporcionan conexiones físicas (Ethernet y Fibre Channel) desde cada nodo a las redes físicas (redes de gestión y datos).

  Para conocer los requisitos del sitio, la información sobre switches, el cableado de puertos y el cableado de puertos integrados de la controladora, consulte el Hardware Universe en "hwu.netapp.com".

- Puertos lógicos

  Las redes de área local virtual (VLAN) y los grupos de interfaces constituyen los puertos lógicos. Los grupos de interfaces tratan varios puertos físicos como un único puerto, mientras que las VLAN subdividen un puerto físico en varios puertos separados.

- Espacios IP

  Puede usar un espacio IP para crear un espacio de direcciones IP distinto para cada SVM de un clúster. Esto permite a los clientes en dominios de red separados administrativamente acceder a los datos del clúster mientras utilizan direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

- Dominios de retransmisión

Un dominio de retransmisión reside en un espacio IP y contiene un grupo de puertos de red, potencialmente de varios nodos del clúster, que pertenecen a la misma red de capa 2. Los puertos del grupo se usan en una SVM para el tráfico de datos.

- Subredes

  Una subred se crea dentro de un dominio de difusión y contiene un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Este pool de direcciones IP simplifica la asignación de direcciones IP durante la creación de la LIF.

- Interfaces lógicas

  Una interfaz lógica (LIF) es una dirección IP o un nombre de puerto WWPN asociado a un puerto. Está asociado con atributos como grupos de conmutación por error, reglas de conmutación por error y reglas de firewall. Un LIF se comunica a través de la red a través del puerto (físico o lógico) al que está enlazado actualmente.

  Los diferentes tipos de LIF de un clúster son las LIF de datos, las LIF de gestión de ámbito de clúster, las LIF de gestión de ámbito de nodo, las LIF de interconexión de clústeres y las LIF de clúster. La propiedad de las LIF depende de la SVM en la que reside el LIF. Las LIF de datos son propiedad de las SVM de datos, las LIF de gestión de ámbito de nodo, la gestión de ámbito del clúster y las LIF de interconexión de clústeres son propiedad de las SVM de administrador y las LIF de clúster son propiedad de la SVM del clúster.

- Zonas DNS

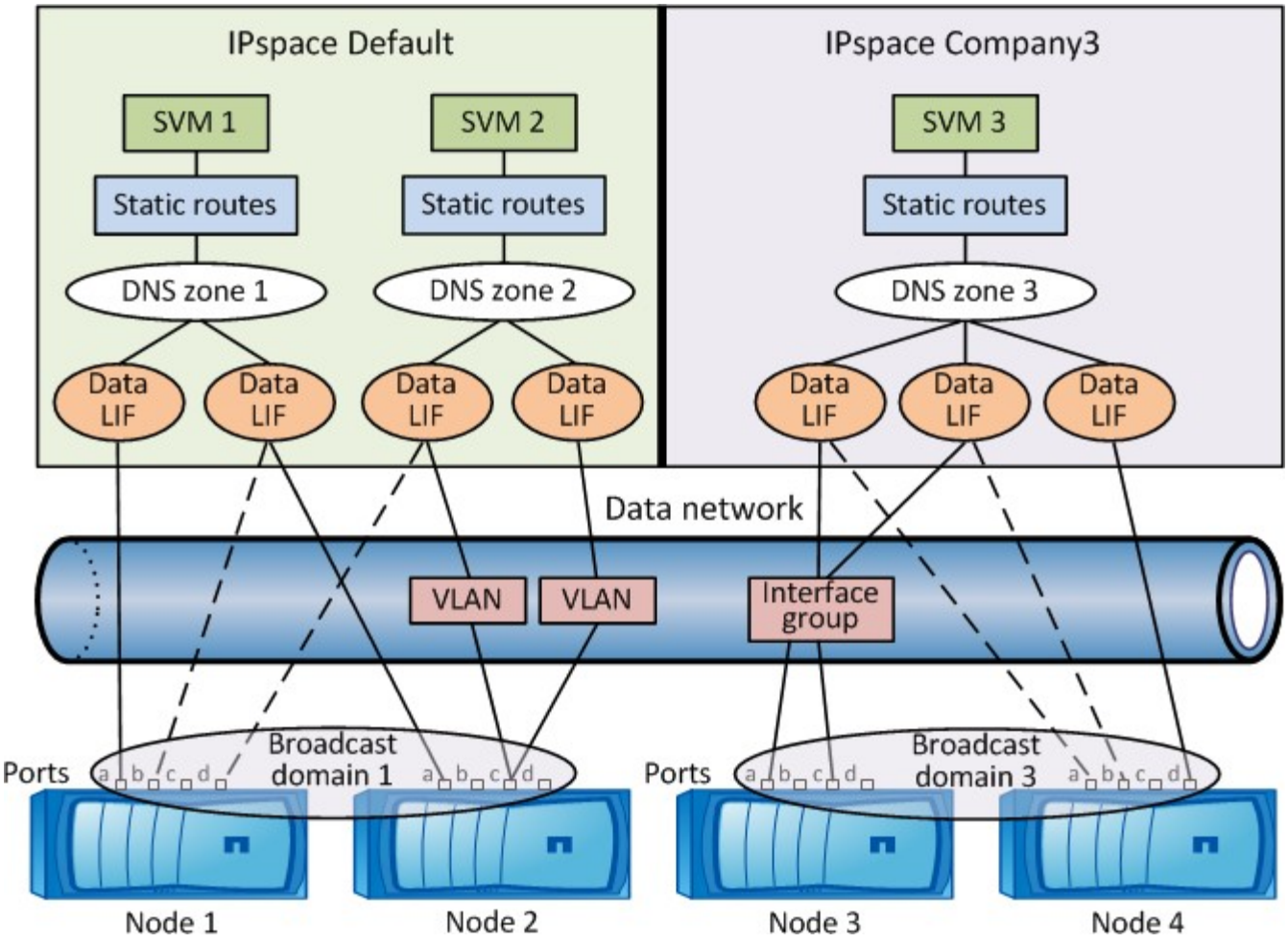
  Puede especificarse la zona DNS durante la creación de LIF, con un nombre para la LIF que se va a exportar a través del servidor DNS del clúster. Varias LIF pueden compartir el mismo nombre, lo que permite que la característica de equilibrio de carga de DNS distribuya direcciones IP para el nombre según la carga.

  Las instancias de SVM pueden tener varias zonas DNS.

- Enrutamiento

  Cada SVM es autosuficiente con respecto a las redes. Una SVM es propietaria de LIF y rutas que pueden llegar a cada uno de los servidores externos configurados.

  En la siguiente figura, se muestra cómo están asociados los diferentes componentes de red en un clúster de cuatro nodos:

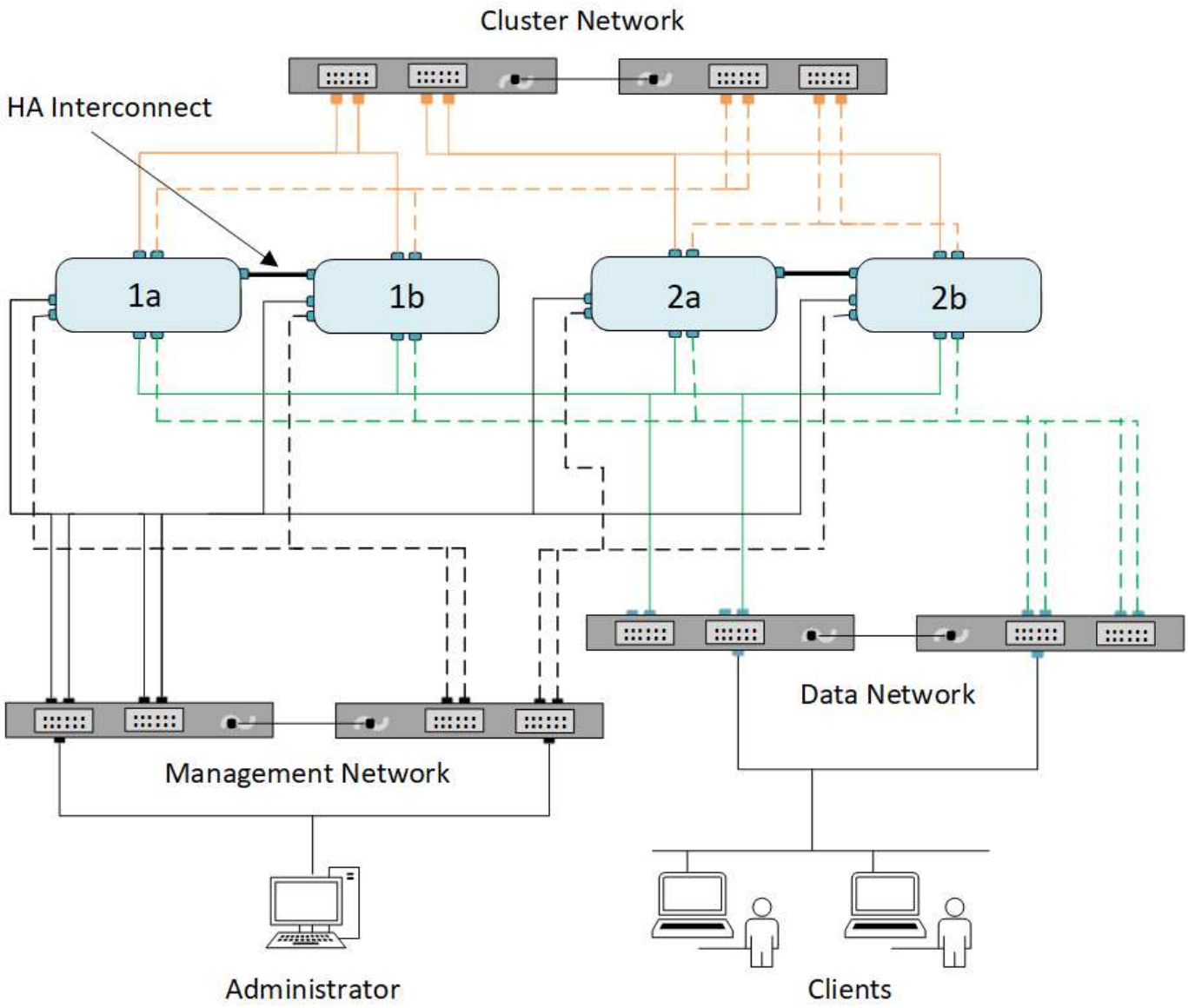


Prácticas recomendadas para el cableado de red de ONTAP

Las prácticas recomendadas para el cableado de red separan el tráfico en las siguientes redes: Clústeres, gestión y datos.

Debe cablear un clúster de modo que el tráfico del clúster esté en una red separada de todo el resto del tráfico. Se trata de una práctica opcional, pero recomendada. Mantener el tráfico de gestión de redes separado del tráfico dentro del clúster y de los datos. Al mantener redes independientes, puede mejorar el rendimiento, la facilidad de administración y mejorar el acceso a los nodos de seguridad y gestión.

En el siguiente diagrama se muestra el cableado de red de un clúster de alta disponibilidad de cuatro nodos que incluye tres redes independientes:



Debe seguir ciertas directrices al cablear las conexiones de red:

- Cada nodo debe estar conectado a tres redes distintas.

  Una red es para la gestión, otra para el acceso a los datos y otra para la comunicación dentro del clúster. Las redes de datos y gestión se pueden separar de forma lógica.

- Puede tener más de una conexión de red de datos a cada nodo para mejorar el flujo de tráfico de cliente (datos).
- Se puede crear un clúster sin conexiones de red de datos, pero debe incluir una conexión de interconexión de clúster.
- Siempre debe haber dos o más conexiones de clúster a cada nodo.

Para obtener más información sobre el cableado de red, consulte "Centro de documentación de los sistemas AFF y FAS" y la "Hardware Universe".

Determine qué política de recuperación tras fallos de LIF se debe utilizar en una red de ONTAP

Los dominios de retransmisión, los grupos de conmutación por error y las políticas de conmutación por error trabajan en conjunto para determinar qué puerto tomará el relevo cuando se produzca un error en el nodo o puerto en el que se ha configurado un LIF.

Un dominio de retransmisión enumera todos los puertos a los que se puede acceder en la misma red Ethernet de capa 2. Todos los demás puertos del dominio de retransmisión ven un paquete de retransmisión Ethernet enviado desde uno de los puertos. Esta característica de accesibilidad común de un dominio de retransmisión es importante para los LIF, ya que si una LIF se conmute a otro puerto del dominio de retransmisión, todavía podría llegar a todos los hosts locales y remotos a los que se pudiera acceder desde el puerto original.

Los grupos de conmutación por error definen los puertos dentro de un dominio de retransmisión que proporcionan cobertura de conmutación por error de LIF entre sí. Cada dominio de retransmisión tiene un grupo de conmutación al nodo de respaldo que incluye todos sus puertos. Este grupo de conmutación por error que contiene todos los puertos del dominio de retransmisión es el grupo de conmutación por error predeterminado y recomendado para la LIF. Puede crear grupos de conmutación por error con subconjuntos más pequeños que defina, como un grupo de conmutación por error de puertos que tengan la misma velocidad de enlace dentro de un dominio de difusión.

Una política de conmutación por error dicta cómo un LIF utiliza los puertos de un grupo de recuperación tras fallos cuando un nodo o puerto está inactivo. Considere la política de conmutación por error como un tipo de filtro que se aplica a un grupo de conmutación por error. Los destinos de conmutación por error de una LIF (el conjunto de puertos en los que se puede conmutar un LIF) están determinados por medio de la aplicación de la política de conmutación por error de la LIF al grupo de conmutación por error de la LIF en el dominio de retransmisión.

Puede ver los destinos de conmutación por error de una LIF con el siguiente comando CLI:

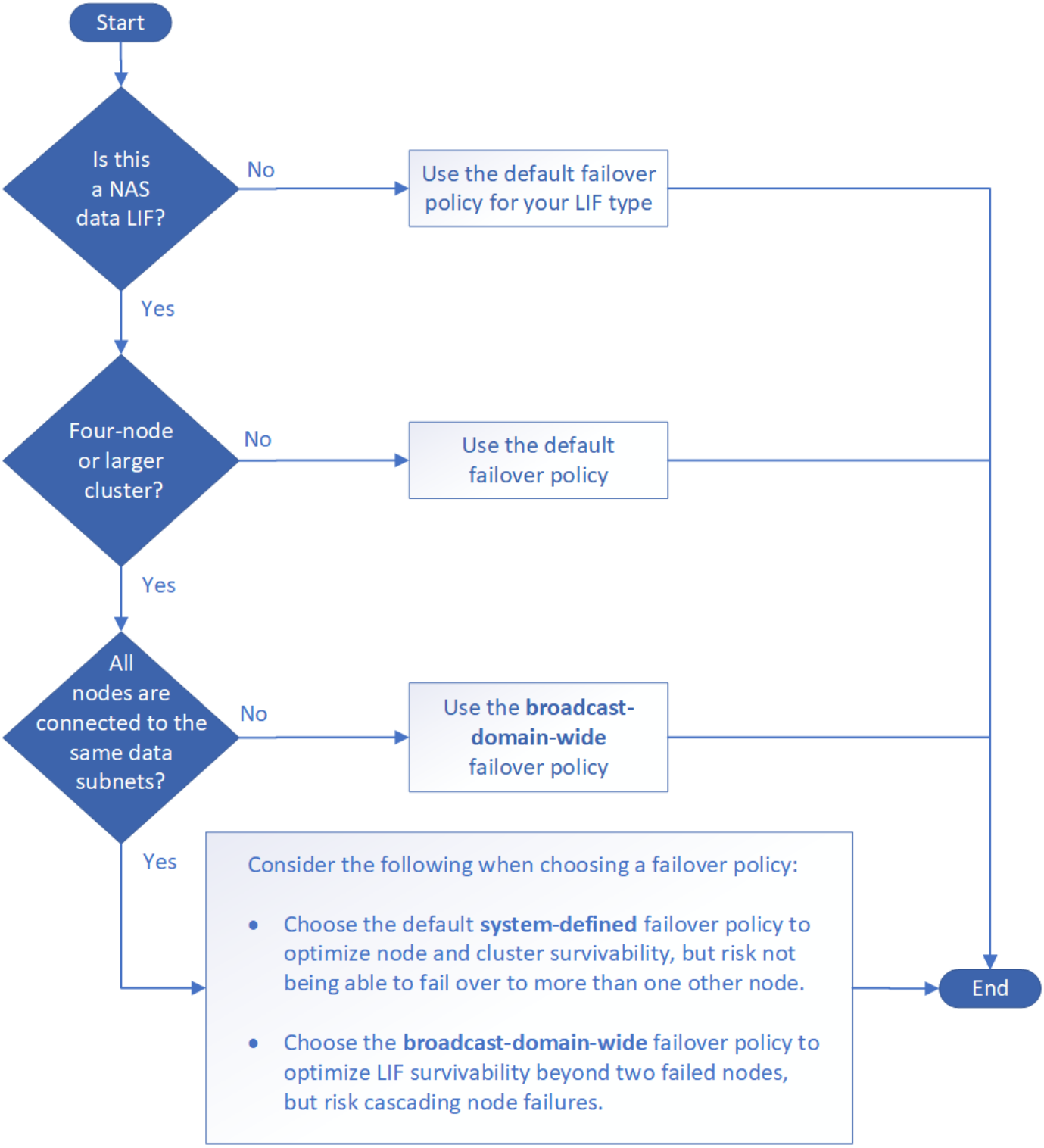
```
network interface show -failover
```

NetApp recomienda utilizar la política de conmutación por error predeterminada para el tipo de LIF.

Decidir qué política de conmutación por error de LIF se utilizará

Decidir si se utilizará la política de conmutación por error predeterminada recomendada o si se va a cambiar según el tipo y el entorno de LIF.

Árbol de decisión de directiva de conmutación por error



Políticas de conmutación por error predeterminadas por tipo de LIF

Tipo de LIF	Política de conmutación por error predeterminada	Descripción
LIF de BGP	deshabilitado	LIF no conmuta al nodo de respaldo a otro puerto.
LIF del clúster	solo local	LIF conmuta por error a los puertos del mismo nodo únicamente.

LIF de gestión del clúster	ámbito de difusión	LIF conmuta por error a los puertos del mismo dominio de retransmisión, en todos los nodos del clúster.
LIF de interconexión de clústeres	solo local	LIF conmuta por error a los puertos del mismo nodo únicamente.
LIF de datos NAS	definido por el sistema	LIF conmuta por error a otro nodo que no es el partner de alta disponibilidad.
LIF de gestión de nodos	solo local	LIF conmuta por error a los puertos del mismo nodo únicamente.
LIF de datos SAN	deshabilitado	LIF no conmuta al nodo de respaldo a otro puerto.

La política de recuperación tras fallos "solo para sfo" no es un valor predeterminado, pero se puede usar cuando desee que la LIF realice la conmutación al nodo de respaldo en un puerto del nodo de inicio o del partner SFO únicamente.

Información relacionada

- "se muestra la interfaz de red"

Flujo de trabajo de recuperación tras fallos de ruta NAS

Configurar la recuperación tras fallos de la ruta NAS en la red ONTAP

Si ya está familiarizado con los conceptos básicos de red, es posible que pueda ahorrar tiempo en la configuración de la red revisando este flujo de trabajo práctico para la configuración de conmutación por error de ruta NAS.

> El flujo de trabajo de configuración de conmutación por error de ruta de NAS es diferente en ONTAP 9,7 y versiones anteriores. Si necesita configurar la conmutación por error del NAS en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte el flujo de trabajo "Flujo de trabajo de conmutación al nodo de respaldo de ruta NAS (ONTAP 9,7 y versiones anteriores)".

Un LIF NAS migra automáticamente a un puerto de red superviviente tras un error de enlace en su puerto actual. Puede confiar en los valores predeterminados de ONTAP para gestionar la recuperación tras fallos de rutas.

> Un LIF SAN no migra (a menos que lo mueva manualmente después del fallo del enlace). En su lugar, la tecnología multivía en el host desvía el tráfico a otra LIF. Para obtener más información, consulte "Administración de SAN".

1 **"Rellene la hoja de trabajo"**

Utilice la hoja de trabajo para planificar la conmutación por error de ruta NAS.

2 **"Cree espacios IP"**

Cree un espacio de dirección IP distinto para cada SVM en un clúster.

3 **"Mueva los dominios de retransmisión a los espacios IP"**

Mover dominios de difusión a espacios IP.

4 **"Cree SVM"**

Cree SVM para servir datos a los clientes.

5 **"Cree LIF"**

Cree LIF en los puertos que desee utilizar para acceder a los datos.

6 **"Configure los servicios DNS para la SVM"**

Configure los servicios DNS para la SVM antes de crear un servidor NFS o SMB.

Hoja de trabajo para la conmutación por error de ruta NAS en la red ONTAP

Debe completar todas las secciones de la hoja de trabajo antes de configurar la conmutación por error de la ruta NAS.

> La información para la conmutación por error de NAS en la red ONTAP es diferente en ONTAP 9,7 y versiones anteriores. Si necesita configurar la conmutación por error del NAS en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte "Hoja de datos para la configuración de conmutación al nodo de respaldo de ruta NAS (ONTAP 9,7 y versiones anteriores)".

Configuración del espacio IP

Puede usar un espacio IP para crear un espacio de direcciones IP distinto para cada SVM de un clúster. Esto permite a los clientes en dominios de red separados administrativamente acceder a los datos del clúster mientras utilizan direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

Información	Necesario	Sus valores
Nombre del espacio IP el identificador único del espacio IP.	Sí	

Configuración de dominio de retransmisión

Un dominio de retransmisión agrupa puertos que pertenecen a la misma red de capa 2 y establece la MTU para los puertos de dominio de retransmisión.

Los dominios de retransmisión se asignan a un espacio IP. Un espacio IP puede contener uno o varios dominios de retransmisión.

> El puerto al que se conmuta por error un LIF debe ser miembro del grupo de conmutación por error de la LIF. Para cada dominio de retransmisión creado por ONTAP, también se crea un grupo a prueba de fallos con el mismo nombre que contiene todos los puertos del dominio de retransmisión.

Información	Necesario	Sus valores
Nombre del espacio IP el espacio IP al que se asigna el dominio de retransmisión. Este espacio IP debe existir.	Sí	
Nombre de dominio de retransmisión el nombre del dominio de retransmisión. Este nombre debe ser único en el espacio IP.	Sí	
MTU el valor máximo de la unidad de transmisión para el dominio de difusión, normalmente establecido en **1500** o **9000**. El valor MTU se aplica a todos los puertos del dominio de retransmisión y a los puertos que se añadan posteriormente al dominio de retransmisión. El valor MTU debe coincidir con todos los dispositivos conectados a esa red. Tenga en cuenta que el tráfico de gestión de puertos e0M y del procesador de servicios debe tener la MTU establecida en no más de 1500 bytes.	Sí	
Los puertos se asignan a dominios de retransmisión en función de la accesibilidad. Una vez finalizada la asignación de puerto, compruebe la accesibilidad ejecutando `network port reachability show` el comando. Estos puertos pueden ser puertos físicos, VLAN o grupos de interfaces. Obtenga más información sobre `network port reachability show` en el "Referencia de comandos del ONTAP".	Sí	

Configuración de subred

Una subred contiene pools de direcciones IP y una puerta de enlace predeterminada que se pueden asignar a las LIF utilizadas por las SVM que residen en el espacio IP.

- Al crear una LIF en una SVM, puede especificar el nombre de la subred en lugar de suministrar una dirección IP y una subred.
- Dado que puede configurarse una subred con una puerta de enlace predeterminada, no tiene que crear la puerta de enlace predeterminada en un paso independiente al crear una SVM.
- Un dominio de retransmisión puede contener una o varias subredes.

- Puede configurar las LIF de SVM que están en diferentes subredes mediante la asociación de más de una subred al dominio de retransmisión del espacio IP.
- Cada subred debe contener direcciones IP que no se superpongan con direcciones IP asignadas a otras subredes en el mismo espacio IP.
- Puede asignar direcciones IP específicas a LIF de datos de SVM y crear una puerta de enlace predeterminada para la SVM en lugar de usar una subred.

Información	Necesario	Sus valores
Nombre del espacio IP el espacio IP al que se asignará la subred. Este espacio IP debe existir.	Sí	
Nombre de subred el nombre de la subred. Este nombre debe ser único en el espacio IP.	Sí	
Nombre de dominio de difusión el dominio de difusión al que se asignará la subred. Este dominio de retransmisión debe residir en el espacio IP especificado.	Sí	
Nombre de subred y máscara la subred y la máscara en la que residen las direcciones IP.	Sí	
Puerta de enlace puede especificar una puerta de enlace predeterminada para la subred. Si no asigna una puerta de enlace al crear la subred, puede asignarla otra más adelante.	No	
Los rangos de direcciones IP pueden especificar un rango de direcciones IP o direcciones IP específicas. Por ejemplo, puede especificar un rango como: `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` Si no especifica un rango de direcciones IP, el rango completo de direcciones IP de la subred especificada está disponible para asignarse a las LIF.	No	

Forzar actualización de asociaciones de LIF especifica si se debe forzar la actualización de las asociaciones de LIF existentes. De forma predeterminada, se produce un error en la creación de subredes si alguna interfaz de procesador de servicio o interfaces de red está utilizando las direcciones IP de los rangos proporcionados. El uso de este parámetro asocia cualquier interfaz tratada manualmente con la subred y permite que el comando se lleve a cabo correctamente.	No	

Configuración de SVM

Utiliza SVM para servir datos a los clientes y hosts.

Los valores registrados sirven para crear una SVM de datos predeterminada. Si va a crear una SVM de origen de MetroCluster, consulte "Guía de instalación y configuración de MetroCluster estructural"o la "Guía de instalación y configuración de MetroCluster con ampliación".

Información	Necesario	Sus valores
Nombre de SVM el nombre de dominio completo (FQDN) de la SVM. Este nombre debe ser único en las ligas de clústeres.	Sí	
Nombre del volumen raíz: El nombre del volumen raíz de la SVM.	Sí	
Nombre de agregado: El nombre del agregado que contiene el volumen raíz de la SVM. Debe existir este agregado.	Sí	
Estilo de seguridad el estilo de seguridad para el volumen raíz de SVM. Los valores posibles son **ntfs**, **unix** y **mezclado**.	Sí	
Nombre IP el espacio IP al que se asigna la SVM. Este espacio IP debe existir.	No	
El idioma de la SVM establece el idioma predeterminado que se utilizará para la SVM y sus volúmenes. Si no especifica un idioma predeterminado, el idioma de SVM predeterminado se establece en **C.UTF-8**. La configuración de idioma de SVM determina el conjunto de caracteres utilizado para mostrar los nombres de archivos y los datos de todos los volúmenes NAS de la SVM. Puede modificar el idioma después de crear la SVM.	No	

Configuración de LIF

Una SVM proporciona datos a clientes y hosts a través de una o varias interfaces lógicas de red (LIF).

Información	Necesario	Sus valores
Nombre de SVM el nombre de la SVM para el LIF.	Sí	
Nombre de LIF el nombre del LIF. Puede asignar varios LIF de datos por nodo y puede asignar LIF a cualquier nodo del clúster, siempre y cuando el nodo tenga puertos de datos disponibles. Para proporcionar redundancia, debe crear al menos dos LIF de datos para cada subred de datos, y las LIF asignadas a una subred en particular deben asignarse puertos principales en nodos diferentes. **Importante:** Si está configurando un servidor SMB para que aloje Hyper-V o SQL Server a través de SMB para soluciones de operaciones no disruptivas, la SVM debe tener al menos una LIF de datos en cada nodo del clúster.	Sí	
Política de servicio para la LIF. La política de servicio define qué servicios de red pueden utilizar la LIF. Hay disponibles políticas de servicio y servicios incorporados para gestionar el tráfico de datos y gestión de las SVM de los datos y del sistema.	Sí	
Los protocolos permitidos LIF basadas en IP no requieren protocolos permitidos; utilice la fila de política de servicio en su lugar. Especifique los protocolos permitidos para LIF SAN en puertos FibreChannel. Estos son los protocolos que pueden utilizar esa LIF. Los protocolos que usan la LIF no se pueden modificar una vez creada la LIF. Debe especificar todos los protocolos al configurar la LIF.	No	
Nodo principal: El nodo al que se devuelve el LIF cuando el LIF se revierte a su puerto principal. Debería registrar un nodo de inicio para cada LIF de datos.	Sí	
Puerto de inicio o dominio de difusión eligió uno de los siguientes: **Puerto**: Especifique el puerto al que devuelve la interfaz lógica cuando el LIF vuelve a su puerto de origen. Esto solo se realiza para la primera LIF de la subred de un espacio IP, si no es necesario. **Dominio de difusión**: Especifique el dominio de difusión, y el sistema seleccionará el puerto apropiado al que la interfaz lógica devuelve cuando el LIF vuelve a su puerto de origen.	Sí	

Nombre de subred que se asignará a la SVM. Todos los LIF de datos utilizados para crear conexiones SMB disponibles de forma continua para servidores de aplicaciones deben estar en la misma subred.	Sí (si se utiliza una subred)	

Configuración de DNS

Debe configurar DNS en la SVM antes de crear un servidor NFS o SMB.

Información	Necesario	Sus valores
Nombre de SVM el nombre de la SVM en la que desea crear un servidor NFS o SMB.	Sí	
Nombre de dominio DNS Lista de nombres de dominio que se deben anexar a un nombre de host al realizar la resolución de nombres de host a IP. Enumere primero el dominio local, seguido de los nombres de dominio para los que se realizan más a menudo las consultas DNS.	Sí	
Direcciones IP de los servidores DNS Lista de direcciones IP para los servidores DNS que proporcionan resolución de nombres para el servidor NFS o SMB. Los servidores DNS enumerados deben contener los registros de ubicación de servicio (SRV) necesarios para localizar los servidores LDAP de Active Directory y los controladores de dominio para el dominio al que se unirá el servidor SMB. El registro SRV se utiliza para asignar el nombre de un servicio al nombre de equipo DNS de un servidor que ofrece ese servicio. Se produce un error en la creación del servidor SMB si ONTAP no puede obtener los registros de ubicación del servicio mediante consultas DNS locales. La forma más sencilla de garantizar que ONTAP pueda localizar los registros SRV de Active Directory es configurar los servidores DNS integrados de Active Directory como servidores DNS de SVM. Puede utilizar servidores DNS no integrados en Active Directory siempre que el administrador DNS haya agregado manualmente los registros SRV a la zona DNS que contenga información acerca de los controladores de dominio de Active Directory. Para obtener información sobre los registros SRV integrados en Active Directory, consulte el tema "Cómo funciona la compatibilidad con DNS para Active Directory en Microsoft TechNet".	Sí	

Configuración de DNS dinámica

Antes de poder utilizar DNS dinámico para agregar automáticamente entradas DNS a los servidores DNS integrados en Active Directory, debe configurar DNS dinámico (DDNS) en la SVM.

Se crean registros de DNS para cada LIF de datos de la SVM. Si crea varias LIF de datos en la SVM, puede equilibrar las conexiones de clientes con las direcciones IP de datos asignadas. La carga DNS equilibra las conexiones que se realizan utilizando el nombre de host a las direcciones IP asignadas en un turno rotatorio.

Información	Necesario	Sus valores
Nombre de SVM a la SVM en la que desea crear un servidor NFS o SMB.	Sí	
Si se utiliza DDNS especifica si se debe usar DDNS. Los servidores DNS configurados en la SVM deben ser compatibles con DDNS. De forma predeterminada, DDNS está desactivado.	Sí	
Si se utiliza DDNS seguro sólo se admite con DNS integrado en Active Directory. Si el DNS integrado en Active Directory sólo permite actualizaciones DDNS seguras, el valor de este parámetro debe ser TRUE. De forma predeterminada, la DDNS segura está desactivada. La DDNS segura solo se puede habilitar después de que se haya creado un servidor SMB o una cuenta de Active Directory para la SVM.	No	
FQDN del dominio DNS el FQDN del dominio DNS. Debe usar el mismo nombre de dominio configurado para los servicios de nombre DNS en la SVM.	No	

Puertos de red

Obtenga información sobre la configuración de puertos de red ONTAP

Los puertos son puertos físicos (NIC) o puertos virtualizados, como grupos de interfaces o VLAN.

Las redes de área local virtual (VLAN) y los grupos de interfaces constituyen los puertos virtuales. Los grupos de interfaces tratan varios puertos físicos como un único puerto, mientras que las VLAN subdividen un puerto físico en varios puertos lógicos distintos.

- Puertos físicos: Las LIF se pueden configurar directamente en puertos físicos.
- Grupo de interfaces: Agregado de puertos que contiene dos o más puertos físicos que actúan como un único puerto de enlace. Un grupo de interfaces puede ser de modo único, multimodo o multimodo dinámico.
- VLAN: Puerto lógico que recibe y envía tráfico etiquetado mediante VLAN (estándar IEEE 802.1Q). Las características del puerto VLAN incluyen el identificador de VLAN del puerto. Los puertos de puerto físico o de grupo de interfaces subyacentes se consideran puertos troncales VLAN y los puertos del switch conectados se deben configurar para que los identificadores de VLAN se queden troncales.

Los puertos de puerto físico o grupo de interfaces subyacentes de un puerto VLAN pueden seguir aumentando los LIF del host, que transmiten y reciben tráfico sin etiquetas.

- Puerto IP virtual (VIP): Puerto lógico que se utiliza como puerto raíz de un LIF VIP. El sistema crea los puertos VIP automáticamente y solo admite un número limitado de operaciones. Los puertos VIP son compatibles a partir de ONTAP 9.5.

La convención de nomenclatura de puertos es *enumeración*:

- El primer carácter describe el tipo de puerto. "e" representa Ethernet.
- El segundo carácter indica la ranura numerada en la que se encuentra el adaptador de puerto.
- El tercer carácter indica la posición del puerto en un adaptador multipuerto. "a" indica el primer puerto, "b" indica el segundo puerto, etc.

Por ejemplo, `e0b` indica que un puerto Ethernet es el segundo puerto en la placa base del nodo.

Las VLAN deben ser nombradas mediante la sintaxis `port_name-vlan-id`.

`port_name` especifica el puerto físico o grupo de interfaces.

`vlan-id` Especifica la identificación de VLAN en la red. Por ejemplo, `e1c-80` es un nombre de VLAN válido.

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

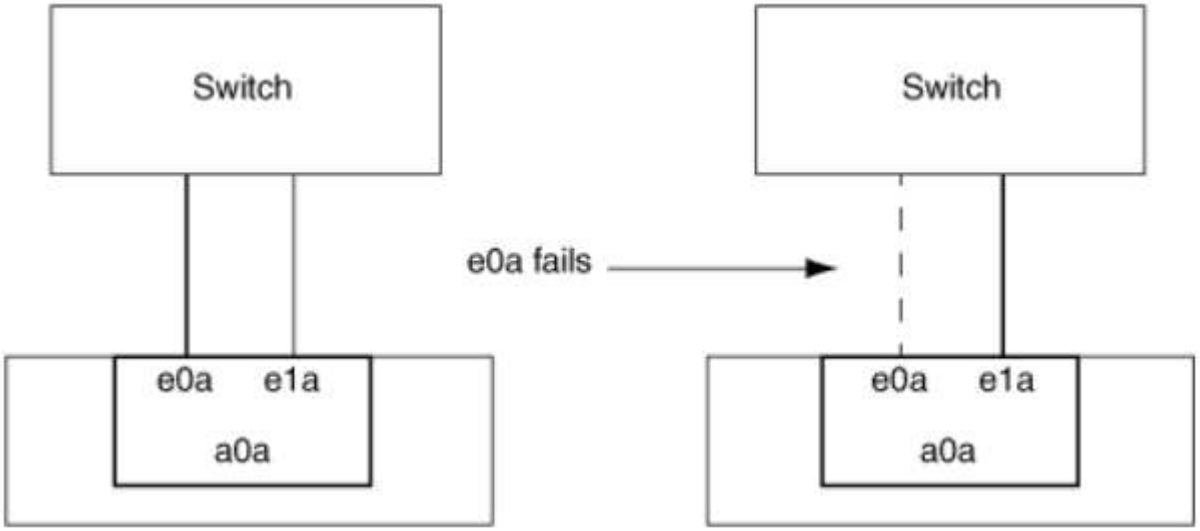
En un grupo de interfaces de un solo modo, solo una de las interfaces del grupo de interfaces está activa. Las otras interfaces están en espera y listas para hacerse cargo si falla la interfaz activa.

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.

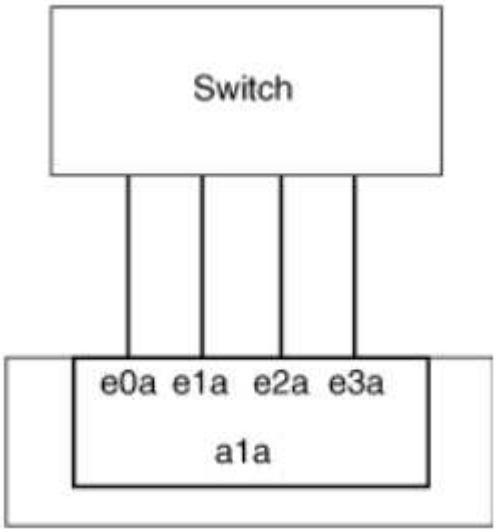
Los grupos de interfaces estáticas multimodo no cumplen el estándar IEEE 802.3ad (dinámico), también conocido como Protocolo de control de agregación de enlaces (LACP). LACP equivale al Protocolo de agregación de puertos (PAgP), el protocolo de agregación de enlaces de propiedad de Cisco.

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).

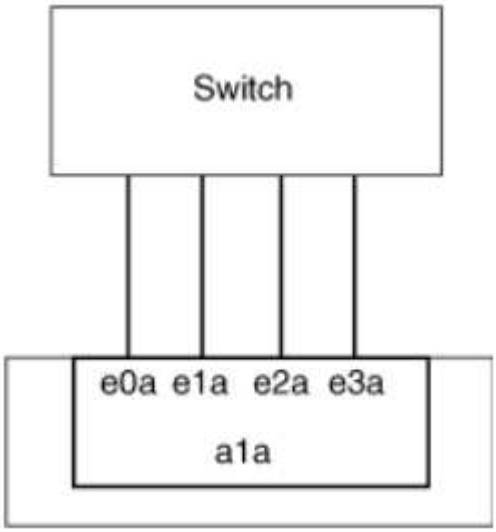
El algoritmo de equilibrio de carga de ONTAP determina el puerto de miembro que se va a utilizar para transmitir tráfico saliente y no controla cómo se reciben las tramas entrantes. El conmutador determina el miembro (puerto físico individual) de su grupo de canales de puertos que se utilizará para la 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.

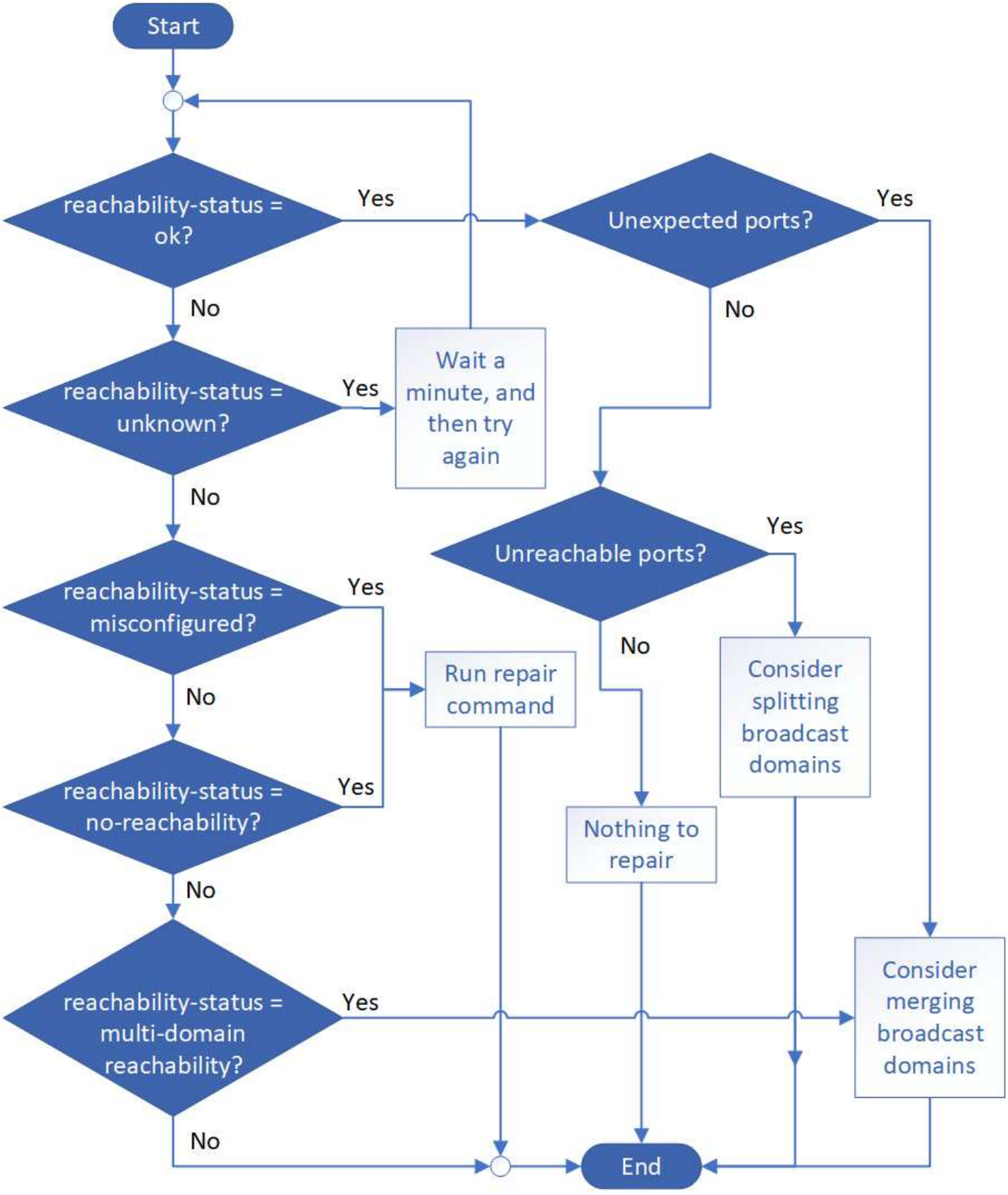
Paso

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

Espacios IP

Obtenga más información sobre la configuración del espacio IP de ONTAP

Los espacios IP permiten configurar un único clúster ONTAP para que los clientes puedan acceder a él desde más de un dominio de red separado por administración, incluso si esos clientes utilizan el mismo rango de subred de direcciones IP. Esto permite la separación del tráfico de clientes para privacidad y seguridad.

Un espacio IP define un espacio de dirección IP diferente en el que residen las máquinas virtuales de almacenamiento (SVM). Los puertos y las direcciones IP definidos para un espacio IP solo se aplican dentro de ese espacio IP. Se mantiene una tabla de enrutamiento distinta para cada SVM dentro de un espacio IP; por lo tanto, no se produce ninguna ruta de tráfico entre SVM o entre espacio IP.

Los espacios IP admiten direcciones IPv4 e IPv6 en sus dominios de enrutamiento.

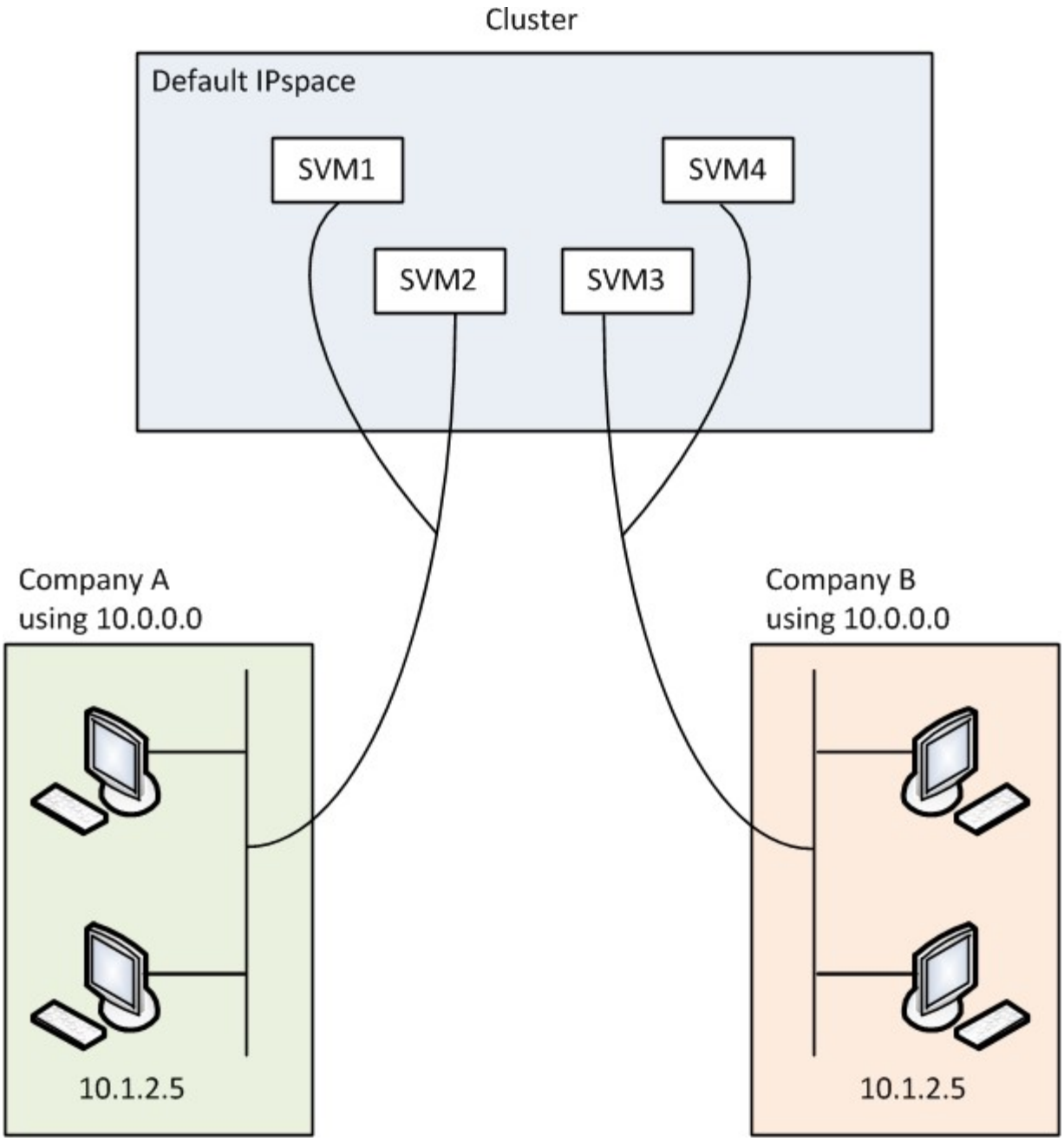
Si gestiona almacenamiento para una única organización, no necesitará configurar espacios IP. Si va a gestionar almacenamiento para varias empresas en un único clúster de ONTAP y tiene la seguridad de que ninguno de sus clientes tiene configuraciones de red en conflicto, tampoco necesitará utilizar espacios IP. En muchos casos, el uso de máquinas virtuales de almacenamiento (SVM), con sus propias tablas de enrutamiento IP distintas, puede utilizarse para segregar configuraciones de red únicas en lugar de usar espacios IP.

Ejemplo de uso de espacios IP

Una aplicación común para el uso de espacios IP es cuando un proveedor de servicios de almacenamiento (SSP) necesita conectar a los clientes de las empresas A y B a un clúster ONTAP en las instalaciones del SSP y ambas empresas utilizan los mismos rangos de direcciones IP privadas.

El SSP crea SVM en el clúster para cada cliente y proporciona una ruta de red dedicada de dos SVM a la red de la empresa A y de las otras dos SVM a la red de la empresa B.

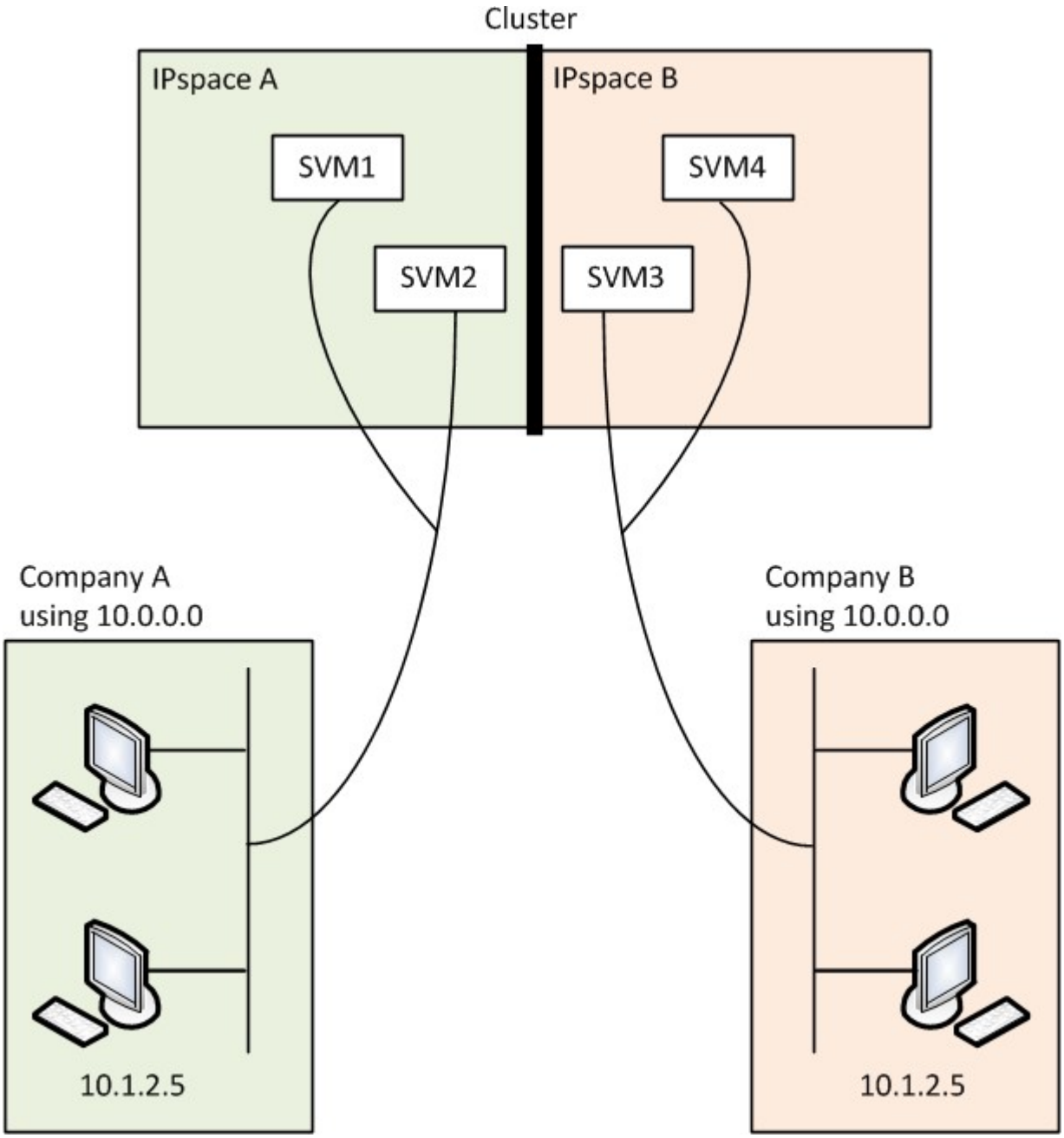
Este tipo de implementación se muestra en la siguiente ilustración y funciona si ambas empresas utilizan rangos de direcciones IP no privados. Sin embargo, la ilustración muestra a ambas empresas que utilizan los mismos rangos de direcciones IP privadas, lo que causa problemas.



Ambas empresas utilizan la subred de direcciones IP privadas 10.0.0.0, causando los siguientes problemas:

- Las SVM del clúster en la ubicación del SSP tienen direcciones IP contradictorias si ambas compañías deciden utilizar la misma dirección IP para sus SVM correspondientes.
- Incluso si las dos empresas acuerdan usar diferentes direcciones IP para sus SVM, pueden surgir problemas.
- Por ejemplo, si un cliente en la red de A tiene la misma dirección IP que un cliente en la red de B, los paquetes destinados a un cliente en el espacio de direcciones De A pueden enrutarse a un cliente en el espacio de direcciones de B, y viceversa.
- Si las dos empresas deciden utilizar espacios de direcciones mutuamente excluyentes (Por ejemplo, A utiliza 10.0.0.0 con una máscara de red de 255.128.0.0 y B utiliza 10.128.0.0 con una máscara de red de 255.128.0.0), El SSP debe configurar las rutas estáticas en el clúster para enrutar el tráfico correctamente a las redes De A y B.

- Esta solución no es escalable (debido a rutas estáticas) ni segura (el tráfico de difusión se envía a todas las interfaces del clúster).para superar estos problemas, el SSP define dos espacios IP en el clúster, uno para cada empresa. Como no se enrutará ningún tráfico de entre espacios IP, los datos de cada empresa se dirigen de forma segura a su red respectiva aunque todas las SVM se hayan configurado en el espacio de direcciones 10.0.0.0, como se muestra en la siguiente ilustración:



Además, las direcciones IP a las que hacen referencia los distintos archivos de configuración, como el `/etc/hosts` archivo, el `/etc/hosts.equiv` archivo y `the /etc/rc` el archivo, son relativas a ese espacio IP. Por lo tanto, los espacios IP permiten que el SSP configure la misma dirección IP para los datos de configuración y autenticación de varias SVM, sin conflictos.

Propiedades estándar de los espacios IP

Los espacios IP especiales se crean de forma predeterminada cuando se crea por primera vez el clúster. Además, se crean máquinas virtuales de almacenamiento (SVM) especiales para cada espacio IP.

Cuando se inicializa el clúster, se crean dos espacios IP automáticamente:

- Espacio IP «predeterminado»

  Este espacio IP es un contenedor de puertos, subredes y SVM que proporcionan datos. Si su configuración no necesita espacios IP separados para los clientes, todas las SVM se pueden crear en este espacio IP. Este espacio IP también contiene los puertos de gestión del clúster y de gestión de nodos.

- Espacio IP de «cluster»

  Este espacio IP contiene todos los puertos del clúster de todos los nodos del clúster. Se crea automáticamente cuando se crea el clúster. Proporciona conectividad a la red de clústeres privada interna. A medida que más nodos se unen al clúster, los puertos del clúster de esos nodos se añaden al espacio IP «Cluster».

Hay una SVM del sistema para cada espacio IP. Cuando crea un espacio IP, se crea una SVM del sistema predeterminada del mismo nombre:

- La SVM del sistema para el espacio IP de «clúster» transporta tráfico de clústeres entre nodos de un clúster en la red de clúster privada interna.

  Lo gestiona el administrador del clúster y tiene el nombre «Cluster».

- La SVM del sistema para el espacio IP «predeterminado» transporta el tráfico de gestión del clúster y los nodos, incluido el tráfico de interconexión de clústeres entre clústeres.

  Lo gestiona el administrador del clúster y utiliza el mismo nombre que el clúster.

- La SVM del sistema para un espacio IP personalizado que crea transporta el tráfico de gestión de esa SVM.

  El administrador del clúster lo gestiona y utiliza el mismo nombre que el espacio IP.

Puede haber una o varias SVM para los clientes en un espacio IP. Cada SVM del cliente tiene sus propios volúmenes de datos y configuraciones, y se administra independientemente de las otras SVM.

Cree espacios IP para la red ONTAP

Los espacios IP son espacios de direcciones IP distintos en los que residen las máquinas virtuales de almacenamiento (SVM). Puede crear espacios IP cuando necesite que sus SVM tengan su propia capacidad de almacenamiento, administración y enrutamiento seguros. Puede usar un espacio IP para crear un espacio de direcciones IP distinto para cada SVM de un clúster. Esto permite a los clientes en dominios de red separados administrativamente acceder a los datos del clúster mientras utilizan direcciones IP superpuestas del mismo rango de subredes de direcciones IP.

Acerca de esta tarea

Existe un límite para todo el clúster de 512 espacios IP. El límite para todo el clúster se reduce a 256 espacios IP para clústeres que contienen nodos con 6 GB de RAM. Consulte la Hardware Universe para determinar si se aplican límites adicionales a su plataforma.

"NetApp Hardware Universe"

El nombre del espacio IP no puede ser "todos" porque "todos" es un nombre reservado del sistema.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Paso

1. Cree un espacio IP:

```
network ipspace create -ipspace ipspace_name
```

`ipspace_name` Es el nombre del espacio IP que desea crear. El siguiente comando crea el espacio IP ipspace1 en un clúster:

```
network ipspace create -ipspace ipspace1
```

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

2. Visualice los espacios IP:

`network ipspace show`

```
IPspace             Vserver List          Broadcast Domains
------------------- --------------------- ----------------------------
Cluster             Cluster               Cluster
Default             Cluster1              Default
ipspace1            ipspace1              -
```

Se crea el espacio IP, junto con la SVM del sistema para el espacio IP. La SVM del sistema transporta el tráfico de gestión.

Después de terminar

Si crea un espacio IP en un clúster de en una configuración de MetroCluster, los objetos IPspace se deben replicar manualmente en los clústeres de partners. Las SVM que se crean y se asignan a un espacio IP antes de que se replique el espacio IP no se replicarán en los clústeres asociados.

Los dominios de retransmisión se crean automáticamente en el espacio IP «predeterminado» y se pueden mover entre espacios IP mediante el siguiente comando:

```
network port broadcast-domain move
```

Por ejemplo, si desea mover un dominio de difusión de "default" a "ips1", utilizando el siguiente comando:

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

Vea los espacios IP en la red ONTAP

Puede mostrar la lista de espacios IP que hay en un clúster y puede ver las máquinas virtuales de almacenamiento (SVM), los dominios de retransmisión y los puertos asignados a cada espacio IP.

Paso

Muestre los espacios IP y las SVM en un clúster:

```
network ipspace show [-ipspace ipspace_name]
```

El siguiente comando muestra todos los espacios IP, las SVM y los dominios de retransmisión del clúster:

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  -----------------------  -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

El siguiente comando muestra los nodos y puertos que forman parte del espacio IP ipspace1:

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

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

Elimine espacios IP de la red ONTAP

Si ya no necesita un espacio IP, puede eliminarlo.

Antes de empezar

No debe haber dominios de retransmisión, interfaces de red ni SVM asociados al espacio IP que desea

eliminar.

Los espacios IP definidos por el sistema «predeterminados» y «clúster» no se pueden eliminar.

Paso

Eliminar un espacio IP:

```
network ipspace delete -ipspace ipspace_name
```

El siguiente comando elimina el espacio IP ipspace1 del clúster:

```
network ipspace delete -ipspace ipspace1
```

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

Dominios de retransmisión

Obtenga más información sobre los dominios de retransmisión de ONTAP

Los dominios de difusión están destinados a agrupar puertos de red que pertenecen a la misma red de capa 2. Los puertos del grupo pueden usarse en una máquina virtual de almacenamiento (SVM) para el tráfico de datos o gestión.

> La gestión de dominios de difusión es diferente en ONTAP 9,7 y versiones anteriores. Si necesita administrar dominios de difusión en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte "Información general sobre el dominio de retransmisión (ONTAP 9,7 y anteriores)".

Un dominio de retransmisión reside en un espacio IP. Durante la inicialización del clúster, el sistema crea dos dominios de retransmisión predeterminados:

- El dominio de retransmisión "predeterminado" contiene puertos que se encuentran en el espacio IP "predeterminado".

  Estos puertos se utilizan principalmente para servir datos. Los puertos de gestión de clústeres y gestión de nodos también están en este dominio de retransmisión.

- El dominio de retransmisión "Cluster" contiene puertos que están en el espacio IP de "Cluster".

  Estos puertos se utilizan para la comunicación del clúster e incluyen todos los puertos de clúster de todos los nodos del clúster.

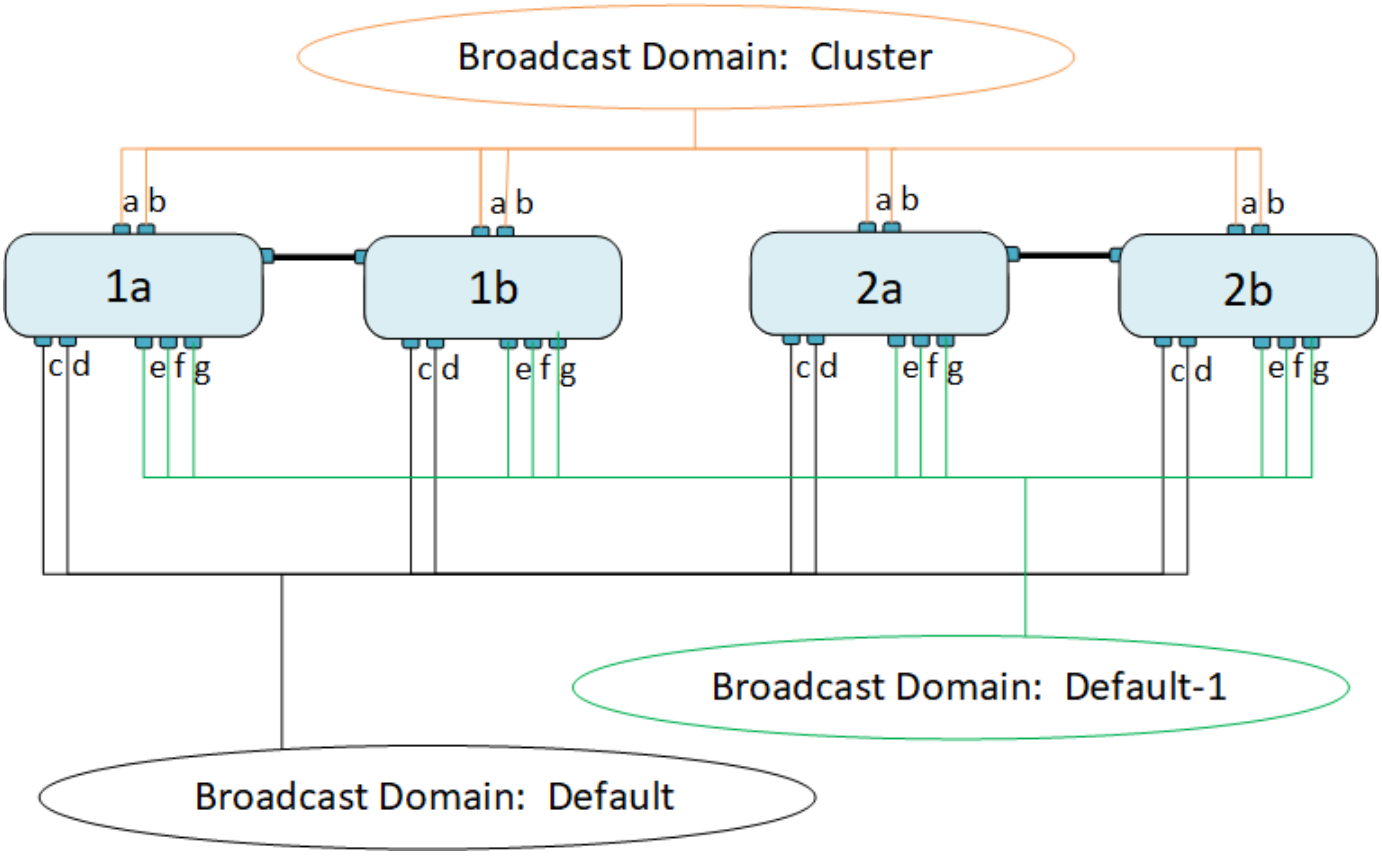
  El sistema crea dominios de retransmisión adicionales en el espacio IP predeterminado cuando sea necesario. El dominio de retransmisión "predeterminado" contiene el puerto raíz de la LIF de gestión, además de cualquier otro puerto que tenga acceso a ese puerto desde una nueva capa 2. Los dominios de retransmisión adicionales se denominan "default-1", "default-2", etc.

Ejemplo de uso de dominios de retransmisión

Un dominio de retransmisión es un conjunto de puertos de red en el mismo espacio IP que también tiene capacidad para el uno al otro de la capa 2, lo que suele incluir puertos de muchos nodos del clúster.

En la ilustración, se muestran los puertos asignados a tres dominios de retransmisión en un clúster de cuatro nodos:

- El dominio de retransmisión "Cluster" se crea automáticamente durante la inicialización del clúster. Contiene los puertos a y b de cada nodo del clúster.
- El dominio de retransmisión "predeterminado" también se crea automáticamente durante la inicialización del clúster y contiene los puertos c y d de cada nodo del clúster.
- El sistema crea automáticamente todos los dominios de retransmisión adicionales durante la inicialización del clúster en función de la accesibilidad de red de la capa 2. Estos dominios de retransmisión adicionales se denominan default-1, default-2, etc.



Un grupo de conmutación por error con el mismo nombre y los mismos puertos de red que cada dominio de retransmisión se crea automáticamente. El sistema administra automáticamente este grupo de conmutación por error, lo que significa que, a medida que se agregan o quitan puertos del dominio de retransmisión, se agregan o se quitan automáticamente de este grupo de conmutación por error.

Cree dominios de retransmisión de ONTAP

Los dominios de retransmisión agrupan los puertos de red del clúster que pertenecen a la misma red de capa 2. Los puertos pueden entonces ser utilizados por las SVM.

Los dominios de retransmisión se crean automáticamente durante la operación de creación o unión del clúster. A partir de ONTAP 9.12.0, además de los dominios de retransmisión creados automáticamente, puede añadir

manualmente un dominio de retransmisión en System Manager.

> El procedimiento para crear dominios de difusión es diferente en ONTAP 9,7 y versiones anteriores. Si necesita crear dominios de difusión en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte "Crear un dominio de retransmisión (ONTAP 9,7 y versiones anteriores)".

Antes de empezar

Los puertos que desea añadir al dominio de retransmisión no deben pertenecer a otro dominio de retransmisión. Si los puertos que desea utilizar pertenecen a otro dominio de retransmisión, pero no se utilizan, quite esos puertos del dominio de retransmisión original.

Acerca de esta tarea

- Todos los nombres de dominio de retransmisión deben ser únicos en un espacio IP.
- Los puertos agregados a un dominio de difusión pueden ser puertos de red físicos, VLAN o grupos de agregación de enlaces/grupos de interfaces (LAG/ifgrps).
- Si los puertos que desea usar pertenecen a otro dominio de retransmisión, pero no se utilizan, elimínelos del dominio de retransmisión existente antes de agregarlos al nuevo.
- La unidad de transmisión máxima (MTU) de los puertos agregados a un dominio de retransmisión se actualiza al valor MTU establecido en el dominio de retransmisión.
- El valor de MTU debe coincidir con todos los dispositivos conectados a esa red de capa 2, excepto en el caso del puerto e0M que gestiona el tráfico de gestión.
- Si no especifica un nombre de espacio IP, el dominio de retransmisión se crea en el espacio IP «predeterminado».

Para facilitar la configuración del sistema, se crea automáticamente un grupo de conmutación por error con el mismo nombre que contiene los mismos puertos.

System Manager

Pasos

1. Seleccione **Red > Descripción general > dominio de difusión**.
2. Haga clic en + Add
3. Asigne un nombre al dominio de retransmisión.
4. Establezca la MTU.
5. Seleccione el espacio IP.
6. Guarde el dominio de retransmisión.

Puede editar o eliminar un dominio de retransmisión después de que se haya agregado.

CLI

Si utiliza ONTAP 9,8 y versiones posteriores, los dominios de difusión se crean automáticamente en función de la accesibilidad de capa 2. Para obtener más información, consulte "Reparar la accesibilidad del puerto".

También puede crear manualmente un dominio de retransmisión.

Pasos

1. Vea los puertos que no están asignados actualmente a un dominio de retransmisión:

   `network port show`

   Si la pantalla es grande, utilice `network port show -broadcast-domain` el comando para ver sólo los puertos no asignados.

2. Cree un dominio de retransmisión:

   `network port broadcast-domain create -broadcast-domain` *`broadcast_domain_name`* `-mtu` *`mtu_value`* `[-ipspace` *`ipspace_name`*`] [-ports` *`ports_list`*`]`

   a. `broadcast_domain_name` es el nombre del dominio de retransmisión que desea crear.

   b. `mtu_value` Es el tamaño de MTU para los paquetes IP; 1500 y 9000 son valores típicos.

      Este valor se aplica a todos los puertos que se agregan a este dominio de difusión.

   c. `ipspace_name` Es el nombre del espacio IP al que se agregará este dominio de retransmisión.

      El espacio IP «predeterminado» se utiliza a menos que especifique un valor para este parámetro.

   d. `ports_list` es la lista de puertos que se agregarán al dominio de retransmisión.

      Los puertos se agregan en el formato `node_name:port_number`, por ejemplo, `node1:e0c`.

3. Compruebe que el dominio de retransmisión se ha creado como desee:

   `network port show -instance -broadcast-domain new_domain`

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

Ejemplo

El siguiente comando crea el dominio de broadcast bcast1 en el espacio IP predeterminado, establece la MTU en 1500 y agrega cuatro puertos:

`network port broadcast-domain create -broadcast-domain` *`bcast1`* `-mtu` *`1500`* `-ports` *`cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f`*

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

Después de terminar

Puede definir el pool de direcciones IP disponibles en el dominio de retransmisión mediante la creación de una subred, o puede asignar SVM e interfaces al espacio IP en este momento. Para obtener más información, consulte "Relaciones entre iguales de clústeres y SVM".

Si necesita cambiar el nombre de un dominio de retransmisión existente, utilice `network port broadcast-domain rename` el comando.

Obtenga más información sobre `network port broadcast-domain rename` en el "Referencia de comandos del ONTAP".

Añada o quite puertos de un dominio de retransmisión de ONTAP

Los dominios de retransmisión se crean automáticamente durante la operación de creación o unión del clúster. No es necesario quitar los puertos de los dominios de retransmisión manualmente.

Si la posibilidad de recurrir a un puerto de red ha cambiado, ya sea mediante la conectividad física de red o la configuración de un switch, y un puerto de red pertenece a un dominio de difusión diferente, consulte el siguiente tema:

"Reparar la accesibilidad del puerto"

El procedimiento para agregar o eliminar puertos para dominios de retransmisión es diferente en ONTAP 9,7 y versiones anteriores. Si necesita agregar o eliminar puertos de dominios de difusión en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte "Agregar o quitar puertos de un dominio de retransmisión (ONTAP 9,7 y versiones anteriores)".

System Manager

A partir de ONTAP 9.14.1, puede usar System Manager para reasignar los puertos Ethernet en los dominios de retransmisión. Es recomendable asignar cada puerto Ethernet a un dominio de retransmisión. Por lo tanto, si anula la asignación de un puerto Ethernet de un dominio de retransmisión, debe reasignarlo a un dominio de retransmisión diferente.

Pasos

Para reasignar puertos Ethernet, realice los siguientes pasos:

1. Selecciona **Red > Descripción general**.
2. En la sección **Dominios de difusión**, seleccione ⋮ junto al nombre de dominio.
3. En el menú desplegable, seleccione **Editar**.
4. En la página **Editar dominio de difusión**, deseleccione los puertos Ethernet que desea reasignar a otro dominio.
5. Para cada puerto no seleccionado, se muestra la ventana **Reasignar puerto Ethernet**. Seleccione el dominio de difusión al que desea reasignar el puerto y, a continuación, seleccione **Reasignar**.
6. Seleccione todos los puertos que desea asignar al dominio de difusión actual y guarde los cambios.

CLI

Si la posibilidad de recurrir a un puerto de red ha cambiado, ya sea mediante la conectividad física de red o la configuración de un switch, y un puerto de red pertenece a un dominio de difusión diferente, consulte el siguiente tema:

"Reparar la accesibilidad del puerto"

Como alternativa, puede agregar o quitar puertos manualmente de los dominios de retransmisión mediante el `network port broadcast-domain add-ports` `network port broadcast-domain remove-ports` comando o.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Los puertos que desea agregar a un dominio de difusión no deben pertenecer a otro dominio de difusión.
- Los puertos que ya pertenecen a un grupo de interfaces no se pueden agregar individualmente a un dominio de retransmisión.

Acerca de esta tarea

Las siguientes reglas se aplican al agregar y quitar puertos de red:

Al agregar puertos…	Al quitar puertos…
Los puertos pueden ser puertos de red, VLAN o grupos de interfaces (ifgrps).	N / A
Los puertos se añaden al grupo de conmutación al nodo de respaldo definido por el sistema del dominio de retransmisión.	Los puertos se quitan de todos los grupos de conmutación al nodo de respaldo en el dominio de retransmisión.
El MTU de los puertos se actualiza con el valor de MTU establecido en el dominio de retransmisión.	El MTU de los puertos no cambia.

El espacio IP de los puertos se actualiza al valor IPspace del dominio de retransmisión.	Los puertos se mueven al espacio IP "predeterminado" sin ningún atributo de dominio de difusión.

Si quita el último puerto miembro de un grupo de interfaces mediante `network port ifgrp remove-port` el comando, hace que el puerto del grupo de interfaces se elimine del dominio de retransmisión porque no se permite un puerto de grupo de interfaces vacío en un dominio de retransmisión. Obtenga más información sobre `network port ifgrp remove-port` en el "Referencia de comandos del ONTAP".

Pasos

1. Muestra los puertos que están actualmente asignados o sin asignar a un dominio de retransmisión mediante `network port show` el comando.
2. Añada o quite puertos de red del dominio de retransmisión:

Si desea…	Usar…
Añada puertos a un dominio de retransmisión	`network port broadcast-domain add-ports`
Quite puertos de un dominio de retransmisión	`network port broadcast-domain remove-ports`

3. Compruebe que los puertos se han agregado o eliminado del dominio de retransmisión:

   `network port show`

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

Ejemplos de cómo agregar y quitar puertos

El siguiente comando agrega el puerto e0g en el nodo cluster-1-01 y el puerto e0g en el nodo cluster-1-02 al dominio de retransmisión bcast1 en el espacio IP predeterminado:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

El siguiente comando añade dos puertos de clúster al clúster de retransmisión en el espacio IP del clúster:

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

El siguiente comando elimina el puerto e0e en el cluster no1-01 del dominio de broadcast bcast1 en el espacio IP predeterminado:

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

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

Información relacionada

- "Referencia de comandos del ONTAP"

Reparar la accesibilidad del puerto ONTAP

Los dominios de retransmisión se crean automáticamente. Sin embargo, si un puerto se vuelve a transferir o si cambia la configuración del switch, es posible que sea necesario reparar un puerto en un dominio de difusión diferente (nuevo o existente).

ONTAP puede detectar y recomendar automáticamente soluciones para problemas de cableado de red en función de la accesibilidad de la capa 2 de un componente de dominio de difusión (puertos ethernet).

El cableado incorrecto durante puede provocar una asignación inesperada del puerto de dominio de retransmisión. A partir de ONTAP 9.10.1, el clúster comprueba automáticamente si hay problemas de cableado de red mediante la verificación de la accesibilidad del puerto después de la configuración del clúster o cuando un nuevo nodo se une a un clúster existente.

System Manager

Si se detecta un problema de accesibilidad del puerto, System Manager recomienda una operación de reparación para resolver el problema.

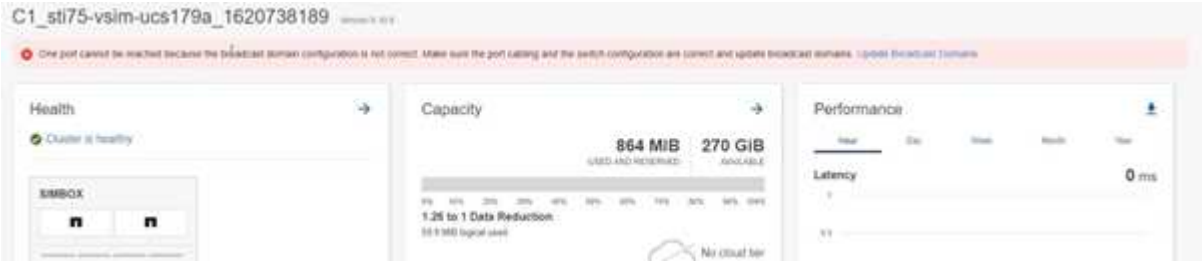
Después de configurar el clúster, se informan los problemas de cableado de red en la consola.

Después de unir un nodo nuevo a un clúster, aparecen los problemas de cableado de red en la página Nodes.

También puede ver el estado del cableado de red en el diagrama de red. Los problemas de accesibilidad del puerto se indican en el diagrama de red mediante un icono de error rojo.

Tras la configuración del clúster

Después de configurar el clúster, si el sistema detecta un problema de cableado de red, aparece un mensaje en la consola.



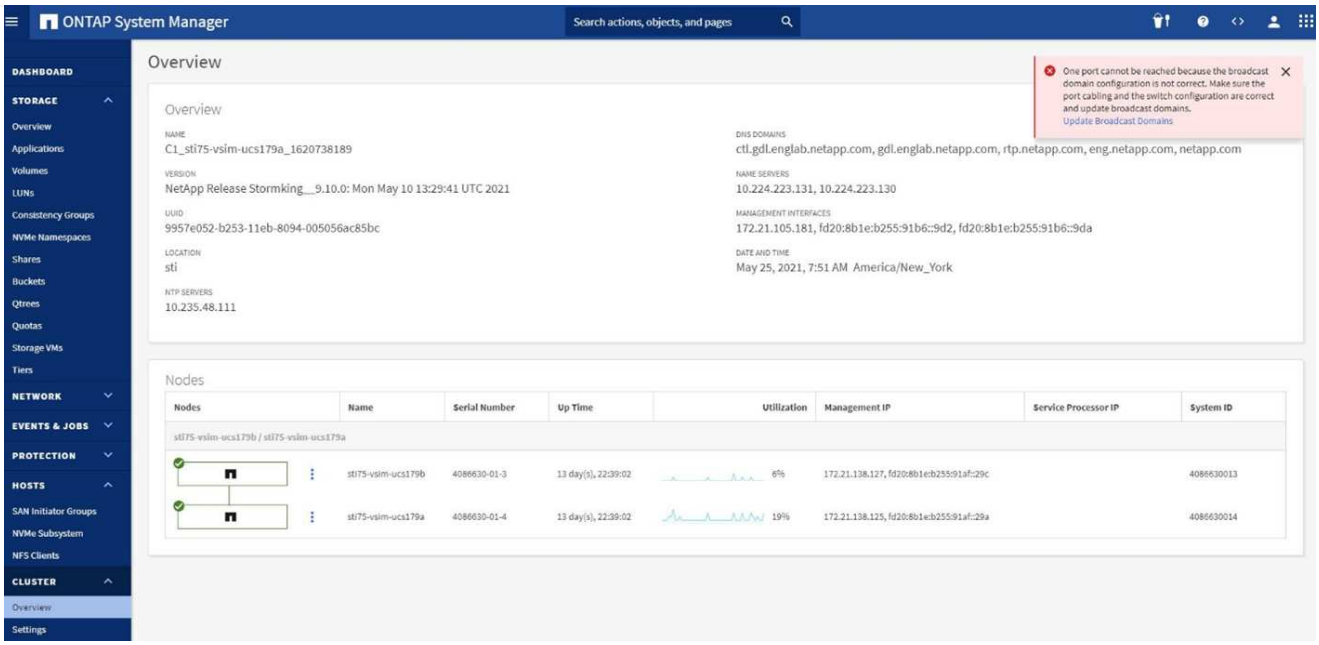
Pasos

1. Corrija el cableado como se indica en el mensaje.
2. Haga clic en el vínculo para abrir el cuadro de diálogo Actualizar dominios de difusión. Se abre el cuadro de diálogo Actualizar dominios de difusión.

3. Revise la información sobre el puerto, incluido el nodo, los problemas, el dominio de retransmisión actual y el dominio de retransmisión esperado.
4. Seleccione los puertos que desea reparar y haga clic en **solucionar**. El sistema moverá los puertos del dominio de retransmisión actual al dominio de retransmisión esperado.

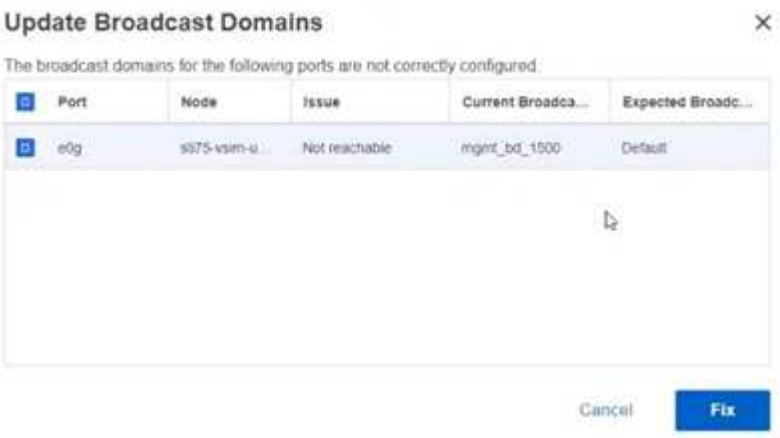
Unión del nodo posterior

Tras unir un nodo nuevo a un clúster, si el sistema detecta un problema de cableado de red, aparece un mensaje en la página Nodes.



Pasos

1. Corrija el cableado como se indica en el mensaje.
2. Haga clic en el vínculo para abrir el cuadro de diálogo Actualizar dominios de difusión. Se abre el cuadro de diálogo Actualizar dominios de difusión.



3. Revise la información sobre el puerto, incluido el nodo, los problemas, el dominio de retransmisión actual y el dominio de retransmisión esperado.
4. Seleccione los puertos que desea reparar y haga clic en **solucionar**. El sistema moverá los puertos del dominio de retransmisión actual al dominio de retransmisión esperado.

CLI

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

Acerca de esta tarea

Hay un comando disponible para reparar automáticamente la configuración del dominio de difusión para un puerto según la accesibilidad de la capa 2 detectada por ONTAP.

Pasos

1. Compruebe la configuración y el cableado del switch.

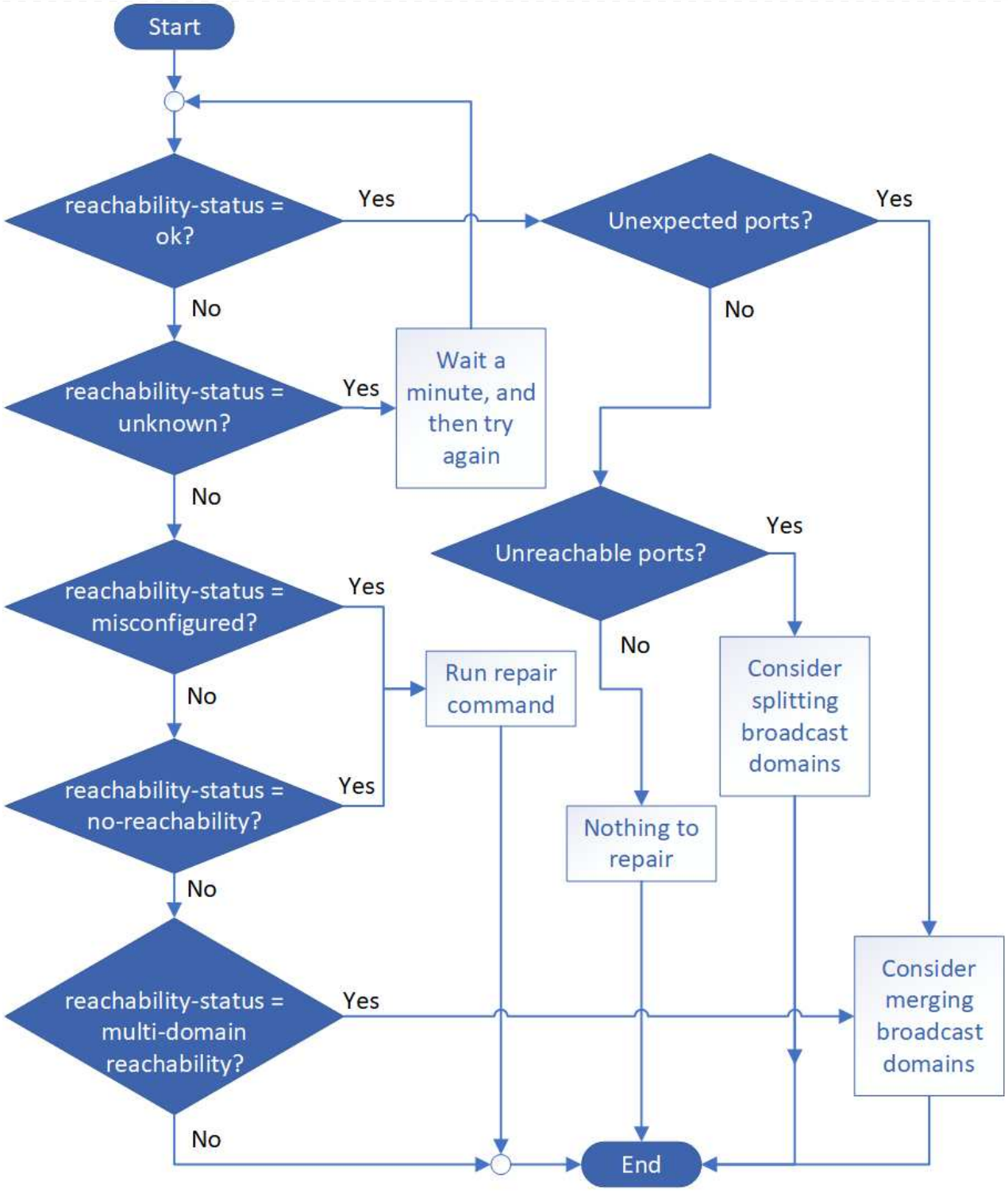
2. Compruebe la accesibilidad del puerto:

   `network port reachability show -detail -node -port`

   El resultado del comando contiene resultados de accesibilidad.

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

3. Use el árbol de decisión y la tabla siguientes para comprender los resultados de la accesibilidad y determinar qué hacer, si es que hay algo, a continuación.



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 de la conectividad física y del switch para determinar si es incorrecta o si el dominio de difusión asignado al puerto debe fusionarse 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`

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` **Nota:** Si todos los puertos miembros del grupo de interfaz (ifgrp) informan `no-reachability`, la ejecución del `network port reachability repair` comando en cada puerto miembro haría que cada uno se eliminara del ifgrp y se colocara en un nuevo dominio de difusión, causando finalmente que el ifgrp mismo sea eliminado. Antes de ejecutar `network port reachability repair` el comando, compruebe que el dominio de retransmisión accesible del puerto sea el que espera en función de la topología de red física. 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 de la conectividad física y del switch para determinar si es incorrecta o si el dominio de difusión asignado al puerto debe fusionarse con uno o más dominios de difusión. Para obtener más información, consulte "Fusionar dominios de retransmisión".
desconocido	Si el estado de accesibilidad es "desconocido", espere unos minutos y vuelva a intentar el comando.

Después de reparar un puerto, compruebe si hay VLAN y LIF desplazadas. Si el puerto era parte de un grupo de interfaces, también necesita comprender lo que ha sucedido con ese grupo de interfaces.

LIF

Cuando se repara un puerto y se mueve a otro dominio de difusión, los LIF configurados en el puerto reparado se asignarán automáticamente a un nuevo puerto doméstico. Si es posible, ese puerto de inicio se selecciona del mismo dominio de difusión en el mismo nodo. Como alternativa, se selecciona un puerto de inicio de otro nodo o, si no existen puertos de inicio adecuados, se borrará el puerto de inicio.

Si se mueve el puerto principal de una LIF a otro nodo, o se borra, se considera que esta ha sido «desplazada». Puede ver estas LIF desplazadas con el siguiente comando:

```
displaced-interface show
```

Si hay alguna LIF desplazada, debe:

- Restaurar el hogar de la LIF desplazada:

  ```
  displaced-interface restore
  ```

- Establezca la casa de la LIF manualmente:

  ```
  network interface modify -home-port -home-node
  ```

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

- Quite la entrada de la tabla de "interfaces desplazadas" si está satisfecho con el hogar configurado actualmente de la LIF:

  ```
  displaced-interface delete
  ```

VLAN

Si el puerto reparado tenía VLAN, esas VLAN se eliminan automáticamente, pero también se registran como "desplazadas". Puede ver estas VLAN desplazadas:

```
displaced-vlans show
```

Si hay alguna VLAN desplazada, debe:

- Restaure las VLAN a otro puerto:

  ```
  displaced-vlans restore
  ```

- Quite la entrada de la tabla "desplazados-vlan":

  ```
  displaced-vlans delete
  ```

Grupos de interfaces

Si el puerto reparado formaba parte de un grupo de interfaces, se elimina de ese grupo de interfaces. Si era el único puerto miembro asignado al grupo de interfaces, se elimina el propio grupo de interfaces.

Información relacionada

- "Compruebe la configuración de red después de actualizar"
- "Supervise la accesibilidad de los puertos de red"
- "Referencia de comandos del ONTAP"

Mueva los dominios de retransmisión de ONTAP a espacios IP

A partir de ONTAP 9,8, puede mover los dominios de retransmisión que el sistema creó en función de la accesibilidad de la capa 2 a los espacios IP que creó.

Antes de mover el dominio de retransmisión, debe comprobar la accesibilidad de los puertos en los dominios de retransmisión.

El análisis automático de puertos puede determinar qué puertos pueden llegar entre sí y colocarlos en el mismo dominio de difusión, pero este análisis no puede determinar el espacio IP adecuado. Si el dominio de retransmisión pertenece a un espacio IP no predeterminado, deberá moverlo manualmente siguiendo los pasos de esta sección.

Antes de empezar

Los dominios de retransmisión se configuran automáticamente como parte de las operaciones de creación y unión de clústeres. ONTAP define el dominio de retransmisión "predeterminado" como el conjunto de puertos que tienen conectividad de capa 2 con el puerto de inicio de la interfaz de gestión en el primer nodo creado en el clúster. Si es necesario, se crean otros dominios de difusión y se denominan **default-1**, **default-2**, etc.

Cuando un nodo se une a un clúster existente, sus puertos de red unen automáticamente los dominios de retransmisión existentes en función de su accesibilidad de la capa 2. Si no tienen la posibilidad de recurrir a un dominio de retransmisión existente, los puertos se colocan en uno o varios dominios de retransmisión nuevos.

Acerca de esta tarea

- Los puertos de las LIF del clúster se colocan automáticamente en el espacio IP «clúster».
- Los puertos con accesibilidad al puerto inicial de la LIF de gestión de nodos se colocan en el dominio de retransmisión "predeterminado".
- ONTAP crea automáticamente otros dominios de retransmisión como parte de la operación de creación o unión del clúster.
- A medida que se añaden las VLAN y los grupos de interfaces, se colocan automáticamente en el dominio de retransmisión adecuado un minuto después de crearlo.

Pasos

1. Compruebe la accesibilidad de los puertos en los dominios de retransmisión. ONTAP supervisa automáticamente la accesibilidad de la capa 2. Utilice el siguiente comando para comprobar que cada puerto se ha agregado a un dominio de difusión y que tiene la posibilidad de recurrir a "ok".

   ```
   network port reachability show -detail
   ```

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

2. Si es necesario, mueva los dominios de retransmisión a otros espacios IP:

   ```
   network port broadcast-domain move
   ```

   Por ejemplo, si desea mover un dominio de difusión de "default" a "ips1":

   ```
   network port broadcast-domain move -ipspace Default -broadcast-domain Default
   -to-ipspace ips1
   ```

Información relacionada

- "movimiento de dominio de difusión de puerto de red"

Dividir los dominios de retransmisión de ONTAP

Si la posibilidad de recurrir a un puerto de red ha cambiado, ya sea mediante la conectividad de red física o la configuración del switch. Además, un grupo de puertos de red previamente configurados en un único dominio de difusión se ha particionado en dos conjuntos diferentes de accesibilidad, puede dividir un dominio de difusión para sincronizar la configuración de ONTAP con la topología de red física.

El procedimiento para dividir dominios de retransmisión es diferente en ONTAP 9,7 y versiones anteriores. Si necesita dividir dominios de difusión en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte "Dividir dominios de retransmisión (ONTAP 9,7 o anterior)".

Para determinar si un dominio de difusión de puerto de red está particionado en más de un conjunto de accesibilidad, utilice el `network port reachability show -details` comando y preste atención a qué puertos no tienen conectividad entre sí («Puertos inaccesibles»). 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. Obtenga más información sobre `network port reachability show` en el "Referencia de comandos del ONTAP".

Paso

Divida un dominio de retransmisión en dos dominios de retransmisión:

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` es el nombre del ipspace donde reside el dominio de difusión.
- `-broadcast-domain` es el nombre del dominio de retransmisión que se dividirá.
- `-new-broadcast-domain` es el nombre del nuevo dominio de retransmisión que se creará.
- `-ports` es el nombre del nodo y el puerto que se van a agregar al nuevo dominio de retransmisión.

Información relacionada

- "división de dominio de retransmisión de puerto de red"

Combine dominios de retransmisión de ONTAP

Si se ha cambiado la posibilidad de recurrir a puertos de red, ya sea mediante una conectividad de red física o mediante una configuración de switch, y dos grupos de puertos de red previamente configurados en varios dominios de retransmisión ahora pueden volver a compartir, la fusión de dos dominios de difusión se puede utilizar para sincronizar la configuración de ONTAP con la topología de red física.

El procedimiento para fusionar dominios de difusión es diferente en ONTAP 9,7 y versiones anteriores. Si necesita fusionar dominios de difusión en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte "Fusionar dominios de retransmisión (ONTAP 9,7 o anterior)".

Para determinar si varios dominios de difusión pertenecen a un conjunto de accesibilidad, utilice el `network port reachability show -details` comando y preste atención a qué puertos que están configurados en otro dominio de difusión realmente tienen conectividad entre sí ("Puertos inesperados"). Generalmente, la lista de puertos inesperados define el conjunto de puertos que se deben combinar en el dominio de retransmisión después de verificar que la configuración física y de switch es precisa.

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

Paso

Fusionar los puertos de un dominio de difusión en un dominio de difusión existente:

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` es el nombre del ipspace donde residen los dominios de difusión.
- `-broadcast-domain` es el nombre del dominio de retransmisión que se fusionará.
- `-into-broadcast-domain` es el nombre del dominio de retransmisión que recibirá puertos adicionales.

Información relacionada

- "puerto de red broadcast-domain-merge"

Cambie el valor de MTU para los puertos de un dominio de retransmisión de ONTAP

Puede modificar el valor MTU para un dominio de retransmisión para cambiar el valor de MTU para todos los puertos en ese dominio de retransmisión. Esto se puede hacer para admitir cambios de topología que se han realizado en la red.

El procedimiento para cambiar el valor de MTU para puertos de dominio de retransmisión es diferente en ONTAP 9,7 y versiones anteriores. Si necesita cambiar el valor de MTU para puertos de dominio de retransmisión en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte "Cambiar el valor de MTU para los puertos en un dominio de retransmisión (ONTAP 9,7 y anteriores)".

System Manager

A partir de ONTAP 9.12.1, puedes usar System Manager para modificar el valor de MTU de un dominio de difusión y así cambiar el valor de MTU de todos los puertos en ese dominio de difusión.

Pasos

1. Selecciona **Network > Broadcast Domains**.
2. En la sección **Dominios de difusión**, selecciona el nombre del dominio de difusión para el que quieres cambiar el valor de MTU.
3. Aparece un mensaje para confirmar que quieres cambiar el valor de MTU para todos los puertos en el dominio de difusión. Haz clic en **Yes** para continuar con el cambio.
4. Modifica el valor de MTU según sea necesario y guarda los cambios.

   El sistema aplica el nuevo valor de MTU a todos los puertos del dominio de difusión, lo que provoca una breve interrupción en el tráfico sobre esos puertos.

CLI

Antes de empezar

El valor de MTU debe coincidir con todos los dispositivos conectados a esa red de capa 2, excepto en el caso del puerto e0M que gestiona el tráfico de gestión.

Acerca de esta tarea

Cambiar el valor de MTU provoca una breve interrupción del tráfico en los puertos afectados. El sistema muestra un mensaje al que debes responder con **y** para hacer el cambio de MTU.

Paso

Cambie el valor de MTU para todos los puertos de un dominio de retransmisión:

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

Dónde:

- `broadcast_domain` es el nombre del dominio de retransmisión.
- `mtu` Es el tamaño de MTU para los paquetes IP; 1500 y 9000 son valores típicos.
- `ipspace` es el nombre del IPspace en el que reside este dominio de difusión. El IPspace "Default" se usa a menos que especifiques un valor para esta opción.

  El siguiente comando cambia la MTU a 9000 para todos los puertos en el dominio de difusión bcast1:

  ```
  network port broadcast-domain modify -broadcast-domain <Default-1>
  -mtu < 9000 >
  Warning: Changing broadcast domain settings will cause a momentary
  data-serving interruption.
  Do you want to continue? {y|n}: <y>
  ```

Información relacionada

- "modificación del dominio de difusión del puerto de red"

Ver los dominios de retransmisión de ONTAP

Puede mostrar la lista de dominios de retransmisión dentro de cada espacio IP de un clúster. El resultado también muestra la lista de puertos y el valor MTU para cada dominio de retransmisión.

> El procedimiento para mostrar dominios de difusión es diferente en ONTAP 9,7 y versiones anteriores. Si necesita mostrar dominios de difusión en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte "Mostrar dominios de retransmisión (ONTAP 9,7 o anterior)".

Paso

Muestre los dominios de retransmisión y los puertos asociados en el clúster:

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

El siguiente comando muestra todos los dominios de retransmisión y los puertos asociados en el clúster:

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        Default-1    1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

El siguiente comando muestra los puertos del dominio de retransmisión predeterminado-1 que tienen un estado de actualización de error, lo que indica que el puerto no se ha podido actualizar correctamente:

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ------------ -----  ---------------------- --------------
Default Default-1    1500
                            cluster-1-02:e0g       error
```

Información relacionada

- "broadcast-domain de puerto de red"

Elimine dominios de retransmisión ONTAP

Si ya no necesita un dominio de retransmisión, puede eliminarlo. Esto mueve los puertos asociados a ese dominio de retransmisión al espacio IP "predeterminado".

Antes de empezar

No debe haber subredes, interfaces de red ni SVM asociadas al dominio de retransmisión que desee eliminar.

Acerca de esta tarea

- El dominio de retransmisión "Cluster" creado por el sistema no se puede eliminar.
- Cuando se elimina el dominio de retransmisión, se quitan todos los grupos de conmutación por error relacionados con el dominio de retransmisión.

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

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para eliminar un dominio de difusión

La opción delete no se muestra cuando el dominio de retransmisión contiene puertos o está asociado a una subred.

Pasos

1. Seleccione **Red > Descripción general > dominio de difusión**.
2. Seleccione ⋮ **> Eliminar** junto al dominio de difusión que desea eliminar.

CLI

Utilice la CLI para eliminar un dominio de difusión

Paso

Eliminar un dominio de retransmisión:

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

El siguiente comando elimina el dominio de difusión predeterminado-1 en IPspace1:

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

Información relacionada

- "eliminación de dominio de difusión de puerto de red"

Grupos y políticas de conmutación por error

Obtenga información sobre la conmutación al respaldo de LIF en redes ONTAP

La conmutación por error de LIF hace referencia a la migración automática de una LIF a un puerto de red diferente en respuesta a un error de enlace en el puerto actual de la LIF. Este es un componente clave para proporcionar alta disponibilidad para las conexiones a SVM. Configurar la conmutación por error de LIF implica crear un grupo de conmutación por error, modificar la LIF para utilizar el grupo de conmutación por error y especificar una política de conmutación por error.

Un grupo de conmutación al nodo de respaldo contiene un conjunto de puertos de red (puertos físicos, VLAN y grupos de interfaces) desde uno o más nodos de un clúster. Los puertos de red presentes en el grupo de conmutación por error definen los destinos de conmutación por error disponibles para la LIF. Un grupo de recuperación tras fallos puede tener asignadas LIF de datos NAS, gestión de clústeres y nodos, interconexión de clústeres.

Cuando se configura una LIF sin un destino de conmutación por error válido, se produce una interrupción cuando la LIF intenta conmutar por error. Puede utilizar `network interface show -failover` el comando para verificar la configuración de conmutación por error. Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

Cuando se crea un dominio de retransmisión, se crea automáticamente un grupo de conmutación por error con el mismo nombre que contiene los mismos puertos de red. El sistema administra automáticamente este grupo de conmutación por error, lo que significa que, a medida que se agregan o quitan puertos del dominio de retransmisión, se agregan o se quitan automáticamente de este grupo de conmutación por error. Este enfoque se proporciona como una eficiencia para los administradores que no quieren gestionar sus propios grupos de conmutación al nodo de respaldo.

Crear grupos de recuperación tras fallos ONTAP

Puede crear un grupo de recuperación tras fallos de puertos de red para que un LIF pueda migrar automáticamente a otro puerto si se produce un fallo de enlace en el puerto actual de la LIF. Esto permite al sistema redirigir el tráfico de red a otros puertos disponibles en el clúster.

Acerca de esta tarea

Utilice el `network interface failover-groups create` comando para crear el grupo y para agregar puertos al grupo.

- Los puertos que se añaden a un grupo de conmutación por error pueden ser puertos de red, VLAN o grupos de interfaces (ifgrps).
- Todos los puertos agregados al grupo de conmutación por error deben pertenecer al mismo dominio de retransmisión.
- Un único puerto puede residir en varios grupos de conmutación por error.
- Si tiene LIF en diferentes VLAN o dominios de retransmisión, debe configurar grupos de conmutación al nodo de respaldo para cada VLAN o dominio de retransmisión.
- Los grupos de recuperación tras fallos no se aplican en entornos SAN iSCSI o FC.

Paso

Crear un grupo de recuperación tras fallos:

`network interface failover-groups create -vserver` *`vserver_name`* `-failover-group` *`failover_group_name`* `-targets` *`ports_list`*

- *`vserver_name`* Es el nombre de la máquina virtual de almacenamiento que puede usar el grupo de conmutación por error.
- *`failover_group_name`* es el nombre del grupo de failover que desea crear.
- *`ports_list`* es la lista de puertos que se agregarán al grupo de failover. Los puertos se añaden con el formato *node_name>:<port_number>*, por ejemplo, 1:e0c.

El siguiente comando crea un grupo de conmutación por error fg3 para SVM vs3 y añade dos puertos:

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

Después de terminar

- Debería aplicar el grupo de recuperación tras fallos a una LIF ahora que se ha creado el grupo de recuperación tras fallos.
- La aplicación de un grupo de conmutación por error que no proporcione un destino de conmutación por error válido para una LIF da lugar a un mensaje de advertencia.

  Si una LIF que no tiene un destino de conmutación por error válido intenta conmutar al respaldo, se podría producir una interrupción del servicio.

- Obtenga más información sobre `network interface failover-groups create` en el "Referencia de comandos del ONTAP".

Configurar los ajustes de recuperación tras fallos de ONTAP en un LIF

Puede configurar una LIF para que conmute por error a un grupo específico de puertos de red aplicando una política de conmutación por error y un grupo de conmutación por error a la LIF. También puede deshabilitar un LIF para no conmutar por error a otro puerto.

Acerca de esta tarea

- Cuando se crea una LIF, la conmutación por error de LIF se habilita de forma predeterminada y la lista de puertos de destino disponibles está determinada por el grupo de conmutación por error y la política de recuperación tras fallos predeterminados según el tipo de LIF y la política de servicio.

  A partir de 9.5, puede especificar una política de servicio para la LIF que define qué servicios de red pueden utilizar la LIF. Algunos servicios de red imponen restricciones de conmutación por error en una LIF.

  > Si se cambia la política de servicio de un LIF de una forma que restringe aún más la conmutación por error, el sistema actualiza automáticamente la política de conmutación por error de LIF.

- Puede modificar el comportamiento de la conmutación por error de las LIF especificando valores para los parámetros -failover-group y -failover-policy en el comando network interface modify.
- La modificación de una LIF que hace que la LIF no tenga ningún destino de conmutación por error válido da como resultado un mensaje de advertencia.

  Si una LIF que no tiene un destino de conmutación por error válido intenta conmutar al respaldo, se podría producir una interrupción del servicio.

- A partir de ONTAP 9.11.1, en plataformas de cabina SAN all-flash (ASA), la conmutación por error de LIF iSCSI se activa automáticamente en LIF iSCSI recién creados en los equipos virtuales de almacenamiento recién creados.

  Además, puede "Habilite manualmente la recuperación tras fallos de LIF iSCSI en LIF iSCSI preexistentes", lo que significa que se crearon antes de actualizar a ONTAP 9.11,1 o una versión posterior.

- En la lista siguiente se describe cómo la configuración -failover-policy afecta a los puertos de destino seleccionados del grupo de conmutación por error:

> Para la conmutación por error en LIF iSCSI, sólo `local-only` `sfo-partner-only` `disabled` se admiten las políticas de conmutación por error y.

- `broadcast-domain-wide` se aplica a todos los puertos de todos los nodos del grupo de conmutación por error.
- `system-defined` Se aplica solo a los puertos del nodo principal de la LIF y otro nodo del clúster, normalmente un partner no SFO, si existe.
- `local-only` Se aplica solo a los puertos del nodo raíz de LIF.
- `sfo-partner-only` Se aplica solo a los puertos del nodo principal de la LIF y su partner SFO.
- `disabled` Indica que el LIF no está configurado para conmutación al respaldo.

Pasos

Configurar la conmutación por error para una interfaz existente:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

Ejemplos de configuración de la conmutación por error y desactivación de la conmutación por error

El siguiente comando establece la política de conmutación por error en todo el dominio de difusión y utiliza los puertos del grupo de conmutación por error fg3 como destinos de conmutación por error para los datos de LIF 1 en SVM vs3:

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

El siguiente comando deshabilita la recuperación tras fallos para los datos LIF 1 en SVM vs3:

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

Información relacionada

- "interfaz de red"

Comandos de ONTAP para gestionar políticas y grupos de conmutación al nodo de respaldo

Puede utilizar `network interface failover-groups` los comandos para gestionar grupos de conmutación al nodo de respaldo. Utiliza `network interface modify` el comando para gestionar los grupos de conmutación al respaldo y las políticas de conmutación al respaldo que se aplican a una LIF.

Si desea…	Se usa este comando…
Agregar puertos de red a un grupo de recuperación tras fallos	`network interface failover-groups add-targets`
Quitar puertos de red de un grupo de recuperación tras fallos	`network interface failover-groups remove-targets`
Modifique los puertos de red de un grupo de conmutación por error	`network interface failover-groups modify`
Mostrar los grupos de conmutación por error actuales	`network interface failover-groups show`
Configurar la conmutación por error en una LIF	`network interface modify -failover -group -failover-policy`
Mostrar el grupo de conmutación por error y la política de conmutación por error que usa cada LIF	`network interface show -fields failover-group, failover-policy`
Cambiar el nombre de un grupo de conmutación por error	`network interface failover-groups rename`
Eliminar un grupo de recuperación tras fallos	`network interface failover-groups delete`

Modificar un grupo de conmutación por error de forma que no proporcione un destino de conmutación por error válido para cualquier LIF del clúster puede provocar una interrupción del servicio cuando un LIF intenta conmutar por error.

Información relacionada

- "interfaz de red"

Subredes (solo administradores de clúster)

Obtenga información acerca de las subredes de la red ONTAP

Las subredes permiten asignar bloques o pools específicos de direcciones IP para la configuración de red ONTAP. Esto permite crear LIF con mayor facilidad ya que

especifica un nombre de subred en lugar de tener que especificar la dirección IP y los valores de máscara de red.

Una subred se crea dentro de un dominio de difusión y contiene un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Las direcciones IP de una subred se asignan a los puertos en el dominio de retransmisión cuando se crean las LIF. Una vez eliminadas las LIF, se devolverán las direcciones IP al pool de subredes y estarán disponibles para futuras LIF.

Se recomienda utilizar subredes porque hacen que la gestión de direcciones IP sea mucho más sencilla y hacen que la creación de las LIF sea un proceso más sencillo. Además, si especifica una puerta de enlace al definir una subred, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.

Cree subredes para la red ONTAP

Puede crear una subred para asignar bloques específicos de direcciones IPv4 o IPv6 que se usarán más adelante al crear LIF para la SVM.

Esto permite crear LIF con mayor facilidad ya que especifica un nombre de subred en lugar de tener que especificar la dirección IP y los valores de máscara de red para cada LIF.

Antes de empezar

Para realizar esta tarea, debe ser un administrador de clústeres.

El dominio de retransmisión y el espacio IP en el que va a agregar la subred ya deben existir.

Acerca de esta tarea

- Todos los nombres de subred deben ser únicos en un espacio IP.
- Al añadir rangos de direcciones IP a una subred, debe asegurarse de que no haya direcciones IP superpuestas en la red para que distintas subredes, o hosts, no intenten utilizar la misma dirección IP.
- Si especifica una puerta de enlace al definir una subred, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred. Si no utiliza subredes, o si no especifica una puerta de enlace al definir una subred, deberá utilizar `route create` el comando para añadir una ruta a la SVM manualmente.
- NetApp recomienda crear objetos de subred para todas las LIF en SVM de datos. Esto es especialmente importante en las configuraciones de MetroCluster, donde el objeto de subred permite a ONTAP determinar los destinos de conmutación por error en el clúster de destino porque cada objeto de subred tiene un dominio de retransmisión asociado.

Pasos

Puede crear una subred con ONTAP System Manager o la interfaz de línea de comandos de ONTAP.

System Manager

A partir de ONTAP 9.12.0, puede usar System Manager para crear una subred.

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Haga clic + Add en para crear una subred.
3. Asigne un nombre a la subred.
4. Especifique la dirección IP de la subred.
5. Defina la máscara de subred.
6. Defina el rango de direcciones IP que componen la subred.
7. Si es útil, especifique una puerta de enlace.
8. Seleccione el dominio de retransmisión al que pertenece la subred.
9. Guarde los cambios.
   a. Si una interfaz ya utiliza la dirección IP o el rango introducidos, se muestra el siguiente mensaje: `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Al hacer clic en **Aceptar**, la LIF existente se asociará a la subred.

CLI

Use la CLI para crear una subred.

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` es el nombre de la subred de capa 3 que desea crear.

  El nombre puede ser una cadena de texto como "Mgmt" o puede ser un valor IP de subred específico como 192.0.2.0/24.

- `broadcast_domain_name` es el nombre del dominio de retransmisión en el que residirá la subred.
- `ipspace_name` Es el nombre del espacio IP del que forma parte el dominio de retransmisión.

  El espacio IP «predeterminado» se utiliza a menos que especifique un valor para esta opción.

- `subnet_address` Es la dirección IP y la máscara de la subred; por ejemplo, 192,0.2,0/24.
- `gateway_address` es la puerta de enlace de la ruta predeterminada de la subred, por ejemplo, 192,0.2,1.
- `ip_address_list` Es la lista o rango de direcciones IP que se asignarán a la subred.

  Las direcciones IP pueden ser direcciones individuales, un rango de direcciones IP o una combinación de ellas en una lista separada por comas.

- El valor `true` se puede establecer para `-force-update-lif-associations` la opción.

  Este comando falla si cualquier procesador de servicios o interfaz de red están utilizando actualmente las direcciones IP del rango especificado. Si se establece este valor en true, se asocia cualquier interfaz dirigida manualmente a la subred actual y se permite que el comando se realice correctamente.

El siguiente comando crea una subred sub1 en el dominio de difusión predeterminado-1 en el espacio IP predeterminado. Añade una máscara y una dirección IP de subred IPv4, la puerta de enlace y un rango de direcciones IP:

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

El siguiente comando crea una subred sub2 en los valores predeterminados de dominio de difusión en el espacio IP "predeterminado". Añade un rango de direcciones IPv6:

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

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

Después de terminar

Puede asignar SVM e interfaces a un espacio IP en las direcciones de la subred.

Si necesita cambiar el nombre de una subred existente, utilice `network subnet rename` el comando.

Obtenga más información sobre `network subnet rename` en el "Referencia de comandos del ONTAP".

Añada o quite direcciones IP de una subred de la red ONTAP

Puede añadir direcciones IP al crear inicialmente una subred, o bien añadir direcciones IP a una subred que ya exista. También es posible quitar direcciones IP de una subred existente. Esto le permite asignar solo las direcciones IP necesarias para las SVM.

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

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para agregar o quitar direcciones IP a o desde una subred

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Seleccione ⋮ **> Editar** junto a la subred que desea cambiar.
3. Añadir o quitar direcciones IP.
4. Guarde los cambios.
   a. Si una interfaz ya utiliza la dirección IP o el rango introducidos, se muestra el siguiente mensaje: `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Al hacer clic en **Aceptar**, la LIF existente se asociará a la subred.

CLI

Utilice la CLI para agregar o quitar direcciones IP a o desde una subred

Acerca de esta tarea

Al añadir direcciones IP, recibirá un error si alguna interfaz de red o procesador de servicios utiliza las direcciones IP del rango que se va a añadir. Si desea asociar cualquier interfaz direccionada manualmente a la subred actual, puede establecer la `-force-update-lif-associations` opción en `true`.

Al quitar direcciones IP, recibirá un error si alguna interfaz de red o procesador de servicios utiliza las direcciones IP que se están quitando. Si desea que las interfaces sigan utilizando las direcciones IP después de que se hayan eliminado de la subred, puede establecer `-force-update-lif -associations` la opción en `true`.

Paso

Añada o quite direcciones IP de una subred:

Si desea…	Se usa este comando…
Añada direcciones IP a una subred	intervalos adicionales de subred de red
Quite las direcciones IP de una subred	intervalos de eliminación de subred de red

El siguiente comando agrega las direcciones IP 192.0.2.82 a 192.0.2.85 a la subred sub1:

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-
192.0.2.85>
```

El siguiente comando elimina la dirección IP 198.51.100.9 de la subred sub3:

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

Si el rango actual incluye de 1 a 10 y de 20 a 40, y desea agregar de 11 a 19 y de 41 a 50 (básicamente permitiendo de 1 a 50), puede superponer el rango existente de direcciones utilizando el comando siguiente. Este comando añade solo las direcciones nuevas y no afecta a las direcciones existentes:

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

Obtenga más información sobre `network subnet add-ranges` y `network subnet remove-ranges` en el "Referencia de comandos del ONTAP".

Cambie las propiedades de la subred de la red ONTAP

Es posible cambiar la dirección de subred y el valor de la máscara, la dirección de la puerta de enlace o el rango de direcciones IP en una subred existente.

Acerca de esta tarea

- Al modificar direcciones IP, debe asegurarse de que no haya direcciones IP superpuestas en la red, de modo que distintas subredes, o hosts, no intente utilizar la misma dirección IP.
- Si añade o cambia la dirección IP de puerta de enlace, la puerta de enlace modificada se aplica a las nuevas SVM cuando se crea una LIF en ellas mediante la subred. Se crea una ruta predeterminada a la puerta de enlace para la SVM si aún no existe la ruta. Puede que deba añadir manualmente una nueva ruta a la SVM cuando cambie la dirección IP de puerta de enlace.

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

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para cambiar las propiedades de subred

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Seleccione **> Editar** junto a la subred que desea cambiar.
3. Realice cambios.
4. Guarde los cambios.
   a. Si una interfaz ya utiliza la dirección IP o el rango introducidos, se muestra el siguiente mensaje: `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. Al hacer clic en **Aceptar**, la LIF existente se asociará a la subred.

CLI

Utilice la CLI para cambiar las propiedades de subred

Paso

Modificar propiedades de subred:

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` es el nombre de la subred que desea modificar.
- `ipspace` Es el nombre del espacio IP en el que reside la subred.
- `subnet` es la nueva dirección y máscara de la subred, si corresponde; por ejemplo, 192,0.2,0/24.
- `gateway` es la nueva puerta de enlace de la subred, si corresponde; por ejemplo, 192,0.2,1. Al introducir **''** se elimina la entrada de la puerta de enlace.
- `ip_ranges` Es la nueva lista o rango de direcciones IP que se asignarán a la subred, si corresponde. Las direcciones IP pueden ser direcciones individuales, un rango o direcciones IP, o una combinación de ambas. El intervalo especificado aquí sustituye a las direcciones IP existentes.
- `force-update-lif-associations` Se requiere al cambiar el rango de direcciones IP. Puede establecer el valor en **verdadero** para esta opción al modificar el rango de direcciones IP. Este comando falla si cualquier procesador de servicios o interfaz de red están usando las direcciones IP del rango especificado. Al establecer este valor en **true**, se asocia cualquier interfaz de dirección manual con la subred actual y se permite que el comando tenga éxito.

El siguiente comando modifica la dirección IP de la puerta de enlace de la subred sub3:

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

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

Ver subredes de la red ONTAP

Puede mostrar la lista de direcciones IP asignadas a cada subred dentro de un espacio IP. El resultado también muestra el número total de direcciones IP disponibles en cada subred y el número de direcciones que se están utilizando actualmente.

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

System Manager

A partir de ONTAP 9.12.0, puede utilizar el Administrador del sistema para mostrar subredes

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Consulte la lista de subredes.

CLI

Utilice la CLI para mostrar subredes

Paso

Mostrar la lista de subredes y los intervalos de direcciones IP asociados que se utilizan en esas subredes:

```
network subnet show
```

El siguiente comando muestra las subredes y las propiedades de subred:

```
network subnet show

IPspace: Default
Subnet                  Broadcast               Avail/
Name   Subnet           Domain    Gateway       Total   Ranges
-----  ---------------  --------- ------------ --------
-----------------------
sub1   192.0.2.0/24     bcast1   192.0.2.1     5/9     192.0.2.92-
192.0.2.100
sub3   198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

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

Elimine las subredes de la red ONTAP

Si ya no necesita una subred y desea desasignar las direcciones IP que han sido asignadas a la subred, puede eliminarla.

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

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para eliminar una subred

Pasos

1. Seleccione **Red > Descripción general > subredes**.
2. Seleccione ⋮ **> Eliminar** junto a la subred que desea eliminar.
3. Guarde los cambios.

CLI

Utilice la CLI para eliminar una subred

Acerca de esta tarea

Recibirá un error si alguna interfaz de red o procesador de servicios está utilizando actualmente direcciones IP en los rangos especificados. Si desea que las interfaces sigan usando las direcciones IP incluso después de eliminar la subred, puede establecer la opción -force-update-lif-associes TRUE para eliminar la asociación de la subred con las LIF.

Paso

Eliminar una subred:

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

El siguiente comando elimina la subred sub1 en IPspace 1:

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

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

Cree SVM para la red ONTAP

Debe crear una SVM para servir datos a los clientes.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- Se debe saber qué estilo de seguridad tendrá el volumen raíz de la SVM.

  Si piensa implementar una solución Hyper-V o SQL Server sobre SMB en esta SVM, debe utilizar el estilo de seguridad NTFS para el volumen raíz. Los volúmenes que contienen archivos de Hyper-V o archivos de base de datos de SQL se deben establecer en seguridad NTFS en el momento en el que se crean. Al establecer el estilo de seguridad del volumen raíz en NTFS, se asegura de que no se creen volúmenes de datos de estilo de seguridad mixtos o UNIX de forma accidental.

- A partir de ONTAP 9.13.1, puede establecer una capacidad máxima para una máquina virtual de almacenamiento. También puede configurar alertas cuando la SVM se acerca a un nivel de umbral de capacidad. Para obtener más información, consulte Gestionar la capacidad de SVM.

System Manager

Puede usar System Manager para crear una máquina virtual de almacenamiento.

Pasos

1. Seleccione **Storage VMs**.
2. Haga clic en + Add para crear una máquina virtual de almacenamiento.
3. Asigne un nombre a la máquina virtual de almacenamiento.
4. Seleccione el protocolo de acceso:
   - SMB/CIFS Y NFS
   - iSCSI
   - FC
   - NVMe
     i. Si selecciona **Activar SMB/CIFS**, complete la siguiente configuración:

Campo o casilla de verificación	Descripción
Nombre del administrador	Especifique el nombre de usuario del administrador para la máquina virtual de almacenamiento SMB/CIFS.
Contraseña	Especifique la contraseña de administrador para la máquina virtual de almacenamiento SMB/CIFS.
Nombre del servidor	Especifique el nombre del servidor para la máquina virtual de almacenamiento SMB/CIFS.
Dominio de Active Directory	Especifique el dominio de Active Directory para proporcionar autenticación de usuarios para la máquina virtual de almacenamiento SMB/CIFS.
Unidad organizacional	Especifique la unidad organizativa en el dominio de Active Directory asociado con el servidor SMB/CIFS. "CN=Computers" es el valor predeterminado, que se puede modificar.
Cifra datos al acceder a los recursos compartidos de la máquina virtual de almacenamiento	Seleccione esta casilla de comprobación para cifrar datos mediante SMB 3.0 para evitar el acceso no autorizado a archivos en los recursos compartidos de la máquina virtual de almacenamiento SMB/CIFS.
Dominios	Añada, elimine o reordene los dominios enumerados para la máquina virtual de almacenamiento de SMB/CIFS.

Servidores de nombres	Añada, elimine o reordene los servidores de nombres para la máquina virtual de almacenamiento SMB/CIFS.
Idioma predeterminado	Especifica la configuración de codificación de idioma predeterminada para la máquina virtual de almacenamiento y sus volúmenes. Use la interfaz de línea de comandos para cambiar la configuración de cada volumen dentro de una máquina virtual de almacenamiento.
Interfaz de red	Para cada interfaz de red que configure para el equipo virtual de almacenamiento, seleccione una subred existente (si existe al menos una) o especifique **sin subred** y complete los campos **Dirección IP** y **Máscara de subred**. Si resulta útil, active la casilla de verificación **usar la misma máscara de subred y puerta de enlace para todas las siguientes interfaces** . Puede permitir que el sistema seleccione automáticamente el puerto de inicio o seleccionar manualmente el que desea utilizar en la lista.
Administrar cuenta de administrador	Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento.

1. Si selecciona **Habilitar NFS**, complete la siguiente configuración:

Campo o casilla de verificación	Descripción
Casilla de verificación permitir el acceso de cliente NFS	Seleccione esta casilla de comprobación cuando todos los volúmenes creados en el equipo virtual de almacenamiento NFS deban usar la ruta de volumen raíz "/" para montar y recorrer. Añada reglas a la directiva de exportación "default" para permitir una transversal de montaje ininterrumpida.

Bases de datos	Haga clic + Add para crear reglas. • Especificación del cliente: Especifique los nombres de host, direcciones IP, grupos de red o dominios. • Protocolos de acceso: Seleccione una combinación de las siguientes opciones: ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • Detalles de acceso: Para cada tipo de usuario, especifique el nivel de acceso, ya sea de sólo lectura, de lectura/escritura o de superusuario. Los tipos de usuario incluyen: ◦ Todo ◦ All (como usuario anónimo) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM Guarde la regla.
Idioma predeterminado	Especifica la configuración de codificación de idioma predeterminada para la máquina virtual de almacenamiento y sus volúmenes. Use la interfaz de línea de comandos para cambiar la configuración de cada volumen dentro de una máquina virtual de almacenamiento.
Interfaz de red	Para cada interfaz de red que configure para el equipo virtual de almacenamiento, seleccione una subred existente (si existe al menos una) o especifique **sin subred** y complete los campos **Dirección IP** y **Máscara de subred**. Si resulta útil, active la casilla de verificación **usar la misma máscara de subred y puerta de enlace para todas las siguientes interfaces** . Puede permitir que el sistema seleccione automáticamente el puerto de inicio o seleccionar manualmente el que desea utilizar en la lista.

Administrar cuenta de administrador	Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento.

1. Si selecciona **Activar iSCSI**, complete la siguiente configuración:

Campo o casilla de verificación	Descripción
Interfaz de red	Para cada interfaz de red que configure para el equipo virtual de almacenamiento, seleccione una subred existente (si existe al menos una) o especifique **sin subred** y complete los campos **Dirección IP** y **Máscara de subred**. Si resulta útil, active la casilla de verificación **usar la misma máscara de subred y puerta de enlace para todas las siguientes interfaces** . Puede permitir que el sistema seleccione automáticamente el puerto de inicio o seleccionar manualmente el que desea utilizar en la lista.
Administrar cuenta de administrador	Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento.

1. Si selecciona **Habilitar FC**, complete la siguiente configuración:

Campo o casilla de verificación	Descripción
Configure los puertos FC	Seleccione las interfaces de red en los nodos que desea incluir en la máquina virtual de almacenamiento. Se recomiendan dos interfaces de red por nodo.
Administrar cuenta de administrador	Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento.

1. Si selecciona **Habilitar NVMe/FC**, complete la siguiente configuración:

Campo o casilla de verificación	Descripción
Configure los puertos FC	Seleccione las interfaces de red en los nodos que desea incluir en la máquina virtual de almacenamiento. Se recomiendan dos interfaces de red por nodo.
Administrar cuenta de administrador	Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento.

1. Si selecciona **Habilitar NVMe/TCP**, complete la siguiente configuración:

Campo o casilla de verificación	Descripción
Interfaz de red	Para cada interfaz de red que configure para el equipo virtual de almacenamiento, seleccione una subred existente (si existe al menos una) o especifique **sin subred** y complete los campos **Dirección IP** y **Máscara de subred**. Si resulta útil, active la casilla de verificación **usar la misma máscara de subred y puerta de enlace para todas las siguientes interfaces** . Puede permitir que el sistema seleccione automáticamente el puerto de inicio o seleccionar manualmente el que desea utilizar en la lista.
Administrar cuenta de administrador	Seleccione esta casilla de comprobación si desea gestionar la cuenta de administrador de máquina virtual de almacenamiento. Cuando se selecciona, especifique el nombre de usuario, la contraseña, confirme la contraseña e indique si desea añadir una interfaz de red para la gestión de máquinas virtuales de almacenamiento.

1. Guarde los cambios.

CLI

Use la interfaz de línea de comandos de ONTAP para crear una subred.

Pasos

1. Determine qué agregados son candidatos para contener el volumen raíz de la SVM.

   ```
   storage aggregate show -has-mroot false
   ```

   Debe elegir un agregado que tenga al menos 1 GB de espacio libre para contener el volumen raíz. Si piensa configurar la auditoría NAS en el SVM, debe tener como mínimo 3 GB de espacio libre

adicional en el agregado raíz, y el espacio adicional se utilizará para crear el volumen de almacenamiento provisional de auditoría cuando la auditoría esté habilitada.

> Si la auditoría de NAS ya está habilitada en una SVM existente, el volumen provisional del agregado se crea inmediatamente después de que la creación de un agregado se haya completado correctamente.

2. Registre el nombre del agregado en el que desea crear el volumen raíz de la SVM.
3. Si piensa especificar un idioma cuando crea la SVM y no conoce el valor que desea usar, identifique y registre el valor del idioma que desea especificar:

   ```
   vserver create -language ?
   ```

4. Si piensa especificar una política de Snapshot al crear la SVM y no conoce el nombre de la política, enumere las políticas disponibles e identifique y registre el nombre de la política de Snapshot que desea utilizar:

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. Si piensa especificar una política de cuota cuando crea la SVM y no conoce el nombre de la política, enumere las políticas disponibles, identifique y registre el nombre de la política de cuota que desea utilizar:

   ```
   volume quota policy show -vserver vserver_name
   ```

6. Cree una SVM:

   ```
   vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
   root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
   IPspace_name] [-language <language>] [-snapshot-policy
   snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
   ```

   ```
   vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
   -rootvolume-security-style ntfs -ipspace ipspace1 -language
   en_US.UTF-8
   ```

   ```
   [Job 72] Job succeeded: Vserver creation completed
   ```

7. Compruebe que la configuración de SVM sea correcta.

   ```
   vserver show -vserver vs1
   ```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

En este ejemplo, el comando crea la SVM llamada "vs1" en el espacio IP "ipspace1". El volumen raíz se denomina "vs1_root" y se crea en aggr3 con estilo de seguridad NTFS.

A partir de ONTAP 9.13.1, puede establecer una plantilla de grupo de políticas de calidad de servicio adaptativa, aplicando un límite máximo y mínimo de rendimiento a los volúmenes en la SVM. Solo puede aplicar esta política después de crear la SVM. Para obtener más información sobre este proceso, consulte Defina una plantilla de grupo de políticas adaptativas.

Interfaces lógicas (LIF)

Descripción general de LIF

Obtener información sobre la configuración de LIF para un clúster de ONTAP

Una LIF (interfaz lógica) representa un punto de acceso de red a un nodo del clúster. Puede configurar las LIF en los puertos a través de los que el clúster envía y recibe comunicaciones a través de la red.

Un administrador de clúster puede crear, ver, modificar, migrar, revertir, O elimine las LIF. Un administrador de SVM solo puede ver las LIF asociadas con la SVM.

Una LIF es una dirección IP o un WWPN con características asociadas, como una política de servicio, un puerto raíz, un nodo raíz, una lista de puertos a los que se debe conmutar y una política de firewall. Puede configurar las LIF en los puertos a través de los que el clúster envía y recibe comunicaciones a través de la red.

> A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "Configurar políticas de firewall para LIF".

Los LIF pueden alojarse en los siguientes puertos:

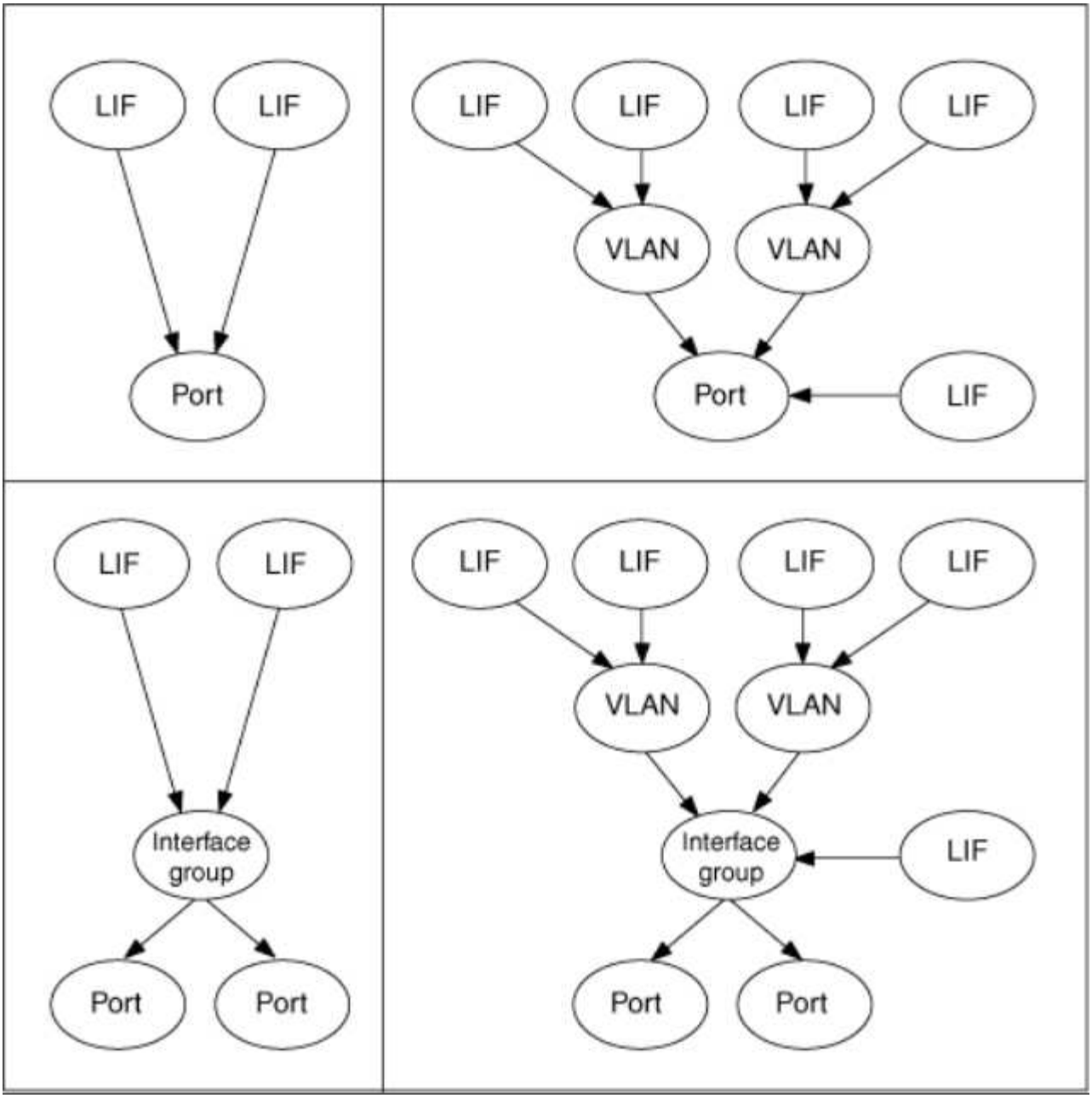
- Puertos físicos que no forman parte de los grupos de interfaces
- Grupos de interfaces
- VLAN
- Puertos físicos o grupos de interfaces que alojan VLAN
- Puertos IP virtual (VIP)

  A partir de ONTAP 9.5, los LIF VIP son compatibles y están alojados en los puertos VIP.

Mientras configura los protocolos SAN como FC en una LIF, estará asociado con un WWPN.

"Administración de SAN"

En la siguiente figura se muestra la jerarquía de puertos en un sistema ONTAP:



Conmutación al nodo primario y al nodo primario DE LIF

Una recuperación tras fallos de LIF se produce cuando un LIF se mueve de su nodo o puerto principal a su nodo o puerto asociados de alta disponibilidad. ONTAP puede activar de forma automática una recuperación tras fallos de LIF o manualmente un administrador de clústeres para determinados eventos, como un enlace de Ethernet físico inactivo o un nodo que borra el quórum de la base de datos replicada (RDB). Cuando se produce una recuperación tras fallos en LIF, ONTAP sigue funcionando con normalidad en el nodo asociado hasta que se resuelva el motivo de la conmutación al nodo de respaldo. Cuando el nodo principal o el puerto recuperan el estado, el LIF se revierte del partner de alta disponibilidad de nuevo a su puerto o nodo principal. Esta reversión se denomina retorno al nodo primario.

Para la conmutación por error y la devolución de LIF, los puertos de cada nodo deben pertenecer al mismo dominio de retransmisión. Para comprobar que los puertos relevantes de cada nodo pertenecen al mismo dominio de retransmisión, consulte lo siguiente:

- ONTAP 9.8 y posteriores: "Reparar la accesibilidad del puerto"

- ONTAP 9,7 y anteriores: "Añada o quite puertos de un dominio de retransmisión"

En el caso de los LIF con recuperación tras fallos de LIF habilitada (automática o manual), se aplica lo siguiente:

- En el caso de los LIF con una política de servicio de datos, puede comprobar las restricciones de la política de conmutación al respaldo:
  - ONTAP 9.6 y posteriores: "LIF y políticas de servicio en ONTAP 9.6 y posteriores"
  - ONTAP 9,5 y anteriores: "Roles de LIF en ONTAP 9.5 y versiones anteriores"
- La reversión automática de LIF ocurre cuando la reversión automática está configurada en `true` y cuando el puerto base del LIF esté en buen estado y sea capaz de albergar al LIF.
- En una toma de control de nodo, planificada o sin planificar, la LIF del nodo que se toma el control y conmuta al partner de alta disponibilidad. El puerto en el que se produce un fallo en el LIF viene determinado por VIF Manager.
- Una vez finalizada la conmutación al respaldo, el LIF funciona normalmente.
- Cuando se inicia una devolución, el LIF vuelve a su nodo y puerto de origen, si la reversión automática está configurada en `true` .
- Cuando un enlace ethernet deja de funcionar en un puerto que aloja uno o varios LIF, el VIF Manager migra las LIF del puerto inactivo a un puerto distinto del mismo dominio de retransmisión. El nuevo puerto podría estar en el mismo nodo o en su compañero de alta disponibilidad. Una vez que se restablezca el enlace y si la reversión automática está configurada en `true` , el administrador de VIF revierte los LIF a su nodo y puerto de origen.
- Cuando un nodo interrumpe el quórum de base de datos replicada (RDB), el gestor VIF migra las LIF del nodo de quórum a su compañero de alta disponibilidad. Una vez que el nodo vuelve al quórum y si la reversión automática está configurada en `true` , el administrador de VIF revierte los LIF a su nodo y puerto de origen.

Obtenga más información sobre la compatibilidad de LIF de ONTAP con los tipos de puerto

Los LIF pueden tener características diferentes para admitir diferentes tipos de puertos.

> Cuando se configuran las LIF de interconexión de clústeres y gestión en la misma subred, es posible que el tráfico de gestión esté bloqueado por un firewall externo y que se produzca un error en las conexiones de AutoSupport y NTP. Puede recuperar el sistema ejecutando `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` el comando para alternar la LIF de interconexión de clústeres. Sin embargo, debe configurar la LIF entre clústeres y la LIF de gestión en subredes diferentes para evitar este problema.

LUN	Descripción
LIF de datos	Una LIF asociada con una máquina virtual de almacenamiento (SVM) y se utiliza para comunicarse con los clientes. Puede tener varios LIF de datos en un puerto. Estas interfaces pueden migrar o realizar una conmutación al nodo de respaldo en todo el clúster. Puede modificar una LIF de datos para que sirva como LIF de gestión de SVM modificando su política de firewall en la gestión. Las sesiones establecidas en servidores NIS, LDAP, Active Directory, WINS y DNS utilizan LIF de datos.

LIF del clúster	Una LIF que se utiliza para transportar tráfico dentro del clúster entre nodos de un clúster. Las LIF del clúster siempre se deben crear en los puertos del clúster. Los LIF de clúster pueden conmutar por error entre los puertos de clúster del mismo nodo, pero no se pueden migrar ni realizar una conmutación por error a un nodo remoto. Cuando un nuevo nodo se une a un clúster, las direcciones IP se generan automáticamente. Sin embargo, si desea asignar direcciones IP manualmente a las LIF del clúster, debe asegurarse de que las nuevas direcciones IP se encuentren en el mismo rango de subred que las LIF del clúster existentes.
LIF de gestión de clústeres	LIF que proporciona una interfaz de gestión única para todo el clúster. Un LIF de gestión de clústeres puede conmutar al respaldo a cualquier nodo del clúster. No puede conmutar al respaldo en los puertos de clústeres o de interconexión de clústeres
LIF de interconexión de clústeres	Un LIF que se utiliza para comunicación entre clústeres, backup y replicación. Antes de que se pueda establecer una relación de paridad de clústeres, debe crear una LIF de interconexión de clústeres en cada nodo del clúster. Estos LIF solo pueden conmutar por error a los puertos del mismo nodo. No se pueden migrar ni realizar una conmutación por error a otro nodo del clúster.
LIF de gestión de nodos	Una LIF que proporciona una dirección IP dedicada para gestionar un nodo en particular en un clúster. Las LIF de gestión de nodos se crean en el momento de crear o unirse al clúster. Estas LIF se utilizan para el mantenimiento del sistema, por ejemplo, cuando un nodo se vuelve inaccesible desde el clúster.
LIF VIP	Una LIF VIP es cualquier LIF de datos creada en un puerto VIP. Para obtener más información, consulte "Configurar las LIF de IP virtual (VIP)".

Información relacionada

- "modificación de la interfaz de red"

Políticas y roles de servicio de LIF admitidos para la versión de ONTAP

Con el tiempo, ha cambiado la forma en que ONTAP gestiona el tipo de tráfico admitido en las LIF.

- ONTAP 9, el 5 y las versiones anteriores utilizan las funciones de LIF y los servicios de firewall.
- ONTAP 9.6 y versiones posteriores utilizan políticas de servicio de LIF:
  - ONTAP 9, la versión 5, introdujo las políticas de servicio de LIF.
  - ONTAP 9.6 sustituyó los roles de LIF por políticas de servicio de LIF.
  - ONTAP 9.10,1 reemplazó los servicios de firewall por políticas de servicio de LIF.

El método que configure dependerá de la versión de ONTAP que utilice.

Más información sobre:

- Políticas de firewall, consulte "Comando: Firewall-policy-show".
- Los roles de LIF, consulte "Roles de LIF (ONTAP 9,5 y anteriores)".
- Políticas de servicio de LIF, consulte "LIF y políticas de servicio (ONTAP 9,6 y posteriores)".

Obtenga más información sobre los LIF de ONTAP y las políticas de servicio

Puede asignar políticas de servicio (en lugar de roles de LIF o políticas de firewall) a las LIF que determinan el tipo de tráfico que se admiten para las LIF. Las políticas de servicio definen una colección de servicios de red compatibles con una LIF. ONTAP proporciona un conjunto de políticas de servicio integradas que se pueden asociar con una LIF.

El método de gestionar el tráfico de red es diferente en ONTAP 9,7 y versiones anteriores. Si necesita administrar el tráfico en una red que ejecute ONTAP 9,7 y versiones anteriores, consulte "Roles de LIF (ONTAP 9,5 y anteriores)".

Los protocolos FCP y NVMe/FCP no requieren actualmente una service-policy.

Puede mostrar las políticas de servicio y sus detalles mediante el siguiente comando:
`network interface service-policy show`

Obtenga más información sobre `network interface service-policy show` en el "Referencia de comandos del ONTAP".

Las funciones que no están vinculadas a un servicio específico utilizarán un comportamiento definido por el sistema para seleccionar LIF para conexiones salientes.

Las aplicaciones en una LIF con una política de servicio vacía podrían comportarse inesperadamente.

Políticas de servicio para SVM del sistema

La SVM de administrador y cualquier SVM del sistema contienen políticas de servicio que se pueden usar para las LIF de esa SVM, incluidas las LIF de gestión y interconexión de clústeres. Estas políticas se crean automáticamente en el sistema cuando se crea un espacio IP.

La siguiente tabla enumera las políticas incorporadas para los LIF en las SVM del sistema que empiezan por ONTAP 9.12.1. Para otras versiones, muestre las políticas de servicio y sus detalles usando el siguiente comando:

```
network interface service-policy show
```

Política	Servicios incluidos	Función equivalente	Descripción
interconexión de clústeres predeterminada	interconexión de clústeres núcleo, gestión https	interconexión de clústeres	Lo usan las LIF que transportan el tráfico de interconexión de clústeres. Nota: ONTAP 9.5 dispone de interconexión de clústeres-core con el nombre net-interinterconexión de clústeres.
ruta predeterminada-anuncio	gestión: bgp	-	Utilizado por LIF que portan conexiones de pares BGP Nota: Disponible en ONTAP 9.5 con el nombre net-route-announce política de servicio.

gestión predeterminada	núcleo de gestión, https de gestión, http de gestión, management-ssh, management-autosupport, management-ems, management-dns-client, management-ad-client, management-ldap-client, management-nis-client management-ntp-client, management-log-reenvio	gestión de nodos o gestión de clústeres	Utilice esta política de gestión de ámbito del sistema para crear LIF de gestión de ámbito de nodos y clústeres propiedad de una SVM del sistema. Estas LIF se pueden utilizar para conexiones salientes a servidores DNS, AD, LDAP o NIS, así como algunas conexiones adicionales para admitir aplicaciones que se ejecuten en nombre de todo el sistema. A partir de ONTAP 9.12.1, puede utilizar el `management-log-forwarding` servicio para controlar qué LIF se usan para reenviar los registros de auditoría a un servidor syslog remoto.

La tabla siguiente enumera los servicios que pueden utilizar las LIF en una SVM del sistema que empiece por ONTAP 9.11.1:

Servicio	Limitaciones de conmutación por error	Descripción
interconexión de clústeres principal	solo nodo principal	Servicios principales de interconexión de clústeres
núcleo de gestión	-	Servicios centrales de gestión
gestión-ssh	-	Servicios para el acceso de gestión SSH
gestión-http	-	Servicios para el acceso de gestión HTTP
gestión de https	-	Servicios para el acceso de gestión HTTPS
management-autosupport	-	Servicios relacionados con el envío de cargas útiles AutoSupport
gestión: bgp	solo puerto de inicio	Servicios relacionados con las interacciones entre colegas de BGP
backup-ndmp-control	-	Servicios para controles de backup NDMP
management-ems	-	Servicios de acceso a mensajería de gestión
management-ntp-client	-	Se introdujo en ONTAP 9.10.1. De servicios para el acceso de clientes NTP.

management-ntp-server	-	Se introdujo en ONTAP 9.10.1. Servicios para el acceso de gestión de servidores NTP
gestión-portmap	-	Servicios para la gestión de portmap
management-rsh-server	-	Servicios para la administración de servidores rsh
servidor-snmp-de-gestión	-	Servicios para la gestión de servidores SNMP
management-telnet-server	-	Servicios para la gestión de servidores telnet
gestión-registro-reenvío	-	Se introdujo en ONTAP 9.12.1. Servicios para el reenvío de registros de auditoría

Políticas de servicio para SVM de datos

Todos los SVM de datos contienen políticas de servicio que pueden usar los LIF en esa SVM.

La tabla siguiente enumera las políticas incorporadas para los LIF en SVM de datos que empiezan por ONTAP 9.11.1. Para otras versiones, muestre las políticas de servicio y sus detalles usando el siguiente comando:

```
network interface service-policy show
```

Política	Servicios incluidos	Protocolo de datos equivalente	Descripción
gestión predeterminada	data-core, management-https, management-http, management-ssh, management-dns-client, management-ad-client, management-ldap-client, management-nis-client	ninguno	Utilice esta política de gestión de ámbito de la SVM para crear LIF de gestión de SVM propiedad de una SVM de datos. Estos LIF se pueden usar para proporcionar acceso SSH o HTTPS a los administradores de SVM. Cuando sea necesario, estas LIF se pueden utilizar para conexiones salientes con servidores DNS, AD, LDAP o NIS externos.
bloques de datos predeterminados	núcleo de datos, iscsi de datos	iscsi	Lo utilizan las LIF para transportar tráfico de datos SAN orientado a bloques. A partir de ONTAP 9.10.1, la política «bloques de datos predeterminados» queda obsoleta. En su lugar, utilice la política de servicio "Default-data-iscsi".

archivos de datos predeterminados	data-core, data-fpolicy-client, data-dns-server, data-FlexCache, data-cifs, data-nfs, gestión-dns-client, gestión-ad-client, gestión-ldap-client, gestión-nis-client	nfs, cifs, fcache	Utilice la política predeterminada para archivos de datos para crear LIF NAS que admitan protocolos de datos basados en archivos. A veces solo hay una LIF en la SVM, por lo tanto esta política permite utilizar la LIF para conexiones salientes con un servidor DNS, AD, LDAP o NIS externo. Puede quitar estos servicios a de esta política si prefiere que estas conexiones utilicen solo LIF de gestión.
datos-iscsi predeterminados	núcleo de datos, iscsi de datos	iscsi	Lo utilizan los LIF que transportan tráfico de datos iSCSI.
default-data-nvme-tcp	núcleo de datos, nvme-tcp de datos	nvme-tcp	Lo usan las LIF que transportan el tráfico de datos NVMe/TCP.

La siguiente tabla enumera los servicios que se pueden usar en una SVM de datos junto con las restricciones que cada servicio impone a la política de conmutación por error de una LIF que empieza por ONTAP 9.11.1:

Servicio	Restricciones de conmutación por error	Descripción
gestión-ssh	-	Servicios para el acceso de gestión SSH
gestión-http	-	Se introdujo en ONTAP 9.10.1 Services para el acceso de gestión HTTP
gestión de https	-	Servicios para el acceso de gestión HTTPS
gestión-portmap	-	Servicios para el acceso de gestión de portmap
servidor-snmp-de-gestión	-	Se introdujo en ONTAP 9.10.1 Services para el acceso de gestión de servidores SNMP
núcleo de datos	-	Servicios de datos centrales
nfs de datos	-	Servicio de datos NFS
cifs de datos	-	Servicio de datos CIFS
flexcache para datos	-	Servicio de datos FlexCache
data iscsi	Puerto inicial solo para AFF/FAS; solo partner sfo para ASA	Servicio de datos iSCSI

backup-ndmp-control	-	Se presenta en ONTAP 9.10.1 Backup NDMP, que controla el servicio de datos
servidor dns de datos	-	Se introdujo en el servicio de datos del servidor DNS de ONTAP 9.10.1
cliente-fpolicy-data	-	Servicio de datos de políticas de selección de archivos
data-nvme-tcp	solo puerto de inicio	Introducido en el servicio de datos TCP de NVMe de ONTAP 9.10.1
servidor de datos s3	-	Servicio de datos del servidor simple Storage Service (S3)

Debe tener en cuenta cómo se asignan las políticas de servicio a las LIF en las SVM de datos:

- Si se crea una SVM de datos con una lista de servicios de datos, las políticas de servicio "default-data-files" y "default-data-Blocks" incorporadas en esa SVM se crean con los servicios especificados.
- Si se crea una SVM de datos sin especificar una lista de servicios de datos, las políticas de servicio "default-data-files" y "default-data-Blocks" incorporadas en esa SVM se crean utilizando una lista predeterminada de servicios de datos.

  La lista de servicios de datos predeterminada incluye los servicios iSCSI, NFS, NVMe, SMB y FlexCache.
- Cuando se crea una LIF con una lista de protocolos de datos, se asigna a la LIF una política de servicio equivalente a los protocolos de datos especificados.
- Si no existe una política de servicio equivalente, se crea una política de servicio personalizada.
- Cuando se crea una LIF sin una política de servicio o lista de protocolos de datos, la política de servicio de archivos de datos predeterminados se asigna a la LIF de forma predeterminada.

Servicio básico de datos

El servicio de núcleo de datos permite a los componentes que previamente usaban los LIF con el rol de datos para trabajar como se esperaba en los clústeres que se habían actualizado para gestionar LIF mediante políticas de servicio en lugar de roles de LIF (que quedaron obsoletos en ONTAP 9.6).

La especificación del núcleo de datos como servicio no abre ningún puerto en el firewall, pero el servicio debe incluirse en cualquier política de servicio de una SVM de datos. Por ejemplo, la política de servicio archivos de datos predeterminados contiene los siguientes servicios de forma predeterminada:

- núcleo de datos
- nfs de datos
- cifs de datos
- flexcache para datos

El servicio de núcleo de datos se debería incluir en la política para garantizar que todas las aplicaciones que utilizan el LIF funcionan como se espera, pero los otros tres servicios se pueden eliminar, si se desea.

Servicio LIF en el cliente

A partir de ONTAP 9.10.1, ONTAP proporciona servicios LIF en el cliente para varias aplicaciones. Estos servicios proporcionan control sobre qué LIF se utilizan para conexiones salientes en nombre de cada aplicación.

Los siguientes servicios nuevos dan a los administradores control sobre los LIF que se usan como direcciones de origen para ciertas aplicaciones.

Servicio	Restricciones de SVM	Descripción
cliente ad-administración	-	A partir de ONTAP 9.11.1, ONTAP proporciona servicio de cliente de Active Directory para conexiones salientes con un servidor AD externo.
management-dns-client	-	A partir de ONTAP 9.11.1, ONTAP proporciona servicio de cliente DNS para conexiones salientes a un servidor DNS externo.
management-ldap-client	-	A partir de ONTAP 9.11.1, ONTAP proporciona servicio de cliente LDAP para conexiones salientes a un servidor LDAP externo.
management-nis-client	-	A partir de ONTAP 9.11.1, ONTAP proporciona servicio de cliente NIS para conexiones salientes a un servidor NIS externo.
management-ntp-client	solo sistemas	A partir de ONTAP 9.10.1, ONTAP proporciona servicio de cliente NTP para conexiones salientes a un servidor NTP externo.
cliente-fpolicy-data	solo datos	A partir de ONTAP 9.8, ONTAP proporciona un servicio de cliente para conexiones de FPolicy de salida.

Cada uno de los nuevos servicios se incluye automáticamente en algunas de las políticas de servicio integradas, pero los administradores pueden eliminarlos de las directivas integradas o agregarlos a políticas personalizadas para controlar qué LIF se utilizan para las conexiones salientes en nombre de cada aplicación.

Información relacionada

- "interfaz de red service-policy show"

Administre las LIF

Configure políticas de servicio de LIF para un clúster de ONTAP

Puede configurar políticas de servicio de LIF para identificar un único servicio o una lista de servicios que utilizarán una LIF.

Crear una política de servicio para LIF

Puede crear una política de servicio para las LIF. Puede asignar una política de servicio a uno o más LIF y, por lo tanto, permitir que la LIF lleve tráfico para un único servicio o una lista de servicios.

Necesita una Privileges avanzada para ejecutar `network interface service-policy create` el comando.

Acerca de esta tarea

Hay disponibles políticas de servicio y servicios incorporados para gestionar el tráfico de datos y gestión de las SVM de los datos y del sistema. La mayoría de los casos de uso se resuelven con una política de servicio integrada, en lugar de crear una política de servicio personalizada.

Puede modificar estas políticas de servicio integradas, si es necesario.

Pasos

1. Vea los servicios que están disponibles en el clúster:

   ```
   network interface service show
   ```

   Los servicios representan las aplicaciones a las que accede una LIF, así como las aplicaciones que presta servicio el clúster. Cada servicio incluye cero o más puertos TCP y UDP en los que la aplicación está escuchando.

   Están disponibles los siguientes servicios adicionales de datos y gestión:

   ```
   cluster1::> network interface service show

   Service                     Protocol:Ports
   -------                     --------------
   cluster-core                -
   data-cifs                   -
   data-core                   -
   data-flexcache              -
   data-iscsi                  -
   data-nfs                    -
   intercluster-core           tcp:11104-11105
   management-autosupport      -
   management-bgp              tcp:179
   management-core             -
   management-https            tcp:443
   management-ssh              tcp:22
   12 entries were displayed.
   ```

2. Vea las políticas de servicio que hay en el clúster:

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. Cree una política de servicio:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- "service_name" especifica una lista de servicios que deben incluirse en la política.
- "IP_address/mask" especifica la lista de máscaras de subred para las direcciones que pueden tener acceso a los servicios en la directiva de servicio. De forma predeterminada, todos los servicios especificados se agregan con una lista de direcciones permitida predeterminada de 0.0.0.0/0, que permite el tráfico de todas las subredes. Cuando se proporciona una lista de direcciones permitidas de forma no predeterminada, las LIF que usan la directiva se configuran para bloquear todas las solicitudes con una dirección de origen que no coincide con ninguna de las máscaras especificadas.

  El siguiente ejemplo muestra cómo crear una política de servicio de datos, *svm1_data_policy*, para una SVM que incluye los servicios *NFS* y *SMB*:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

  El ejemplo siguiente muestra cómo crear una política de servicio de interconexión de clústeres:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. Comprobar que se ha creado la política de servicio.

```
cluster1::> network interface service-policy show
```

   El siguiente resultado muestra las políticas de servicio disponibles:

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
--------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

Después de terminar

Asigne la política de servicio a una LIF en el momento de la creación o al modificar una LIF existente.

Asigne una política de servicio a una LIF

Puede asignar una política de servicio a una LIF en el momento de crear la LIF o al modificarla. Una política de servicio define la lista de servicios que se pueden utilizar con la LIF.

Acerca de esta tarea

Puede asignar políticas de servicio para las LIF en las SVM de administrador y de datos.

Paso

Según cuándo desee asignar la política de servicio a una LIF, realice una de las siguientes acciones:

Si está…	Asignar la política de servicio…
Creación de una LIF	Interfaz de red create -vserver svm_name -lif <lif_name> -home-node <node_name> -home-Port <port_name> {(-address <IP_address> -netmask <IP_address>) -subnet-name <subnet_name>} -service-policy <service_policy_name>
Modificar una LIF	modificación de la interfaz de red -vserver <svm_name> -lif <lif_name> -service -policy <service_policy_name>

Al especificar una política de servicio para una LIF, no es necesario especificar el protocolo de datos y el rol para la LIF. También se admite la creación de LIF especificando el rol y protocolos de datos.

> Una política de servicio solo puede ser utilizada por las LIF en la misma SVM que especificó al crear la política de servicio.

Ejemplos

En el ejemplo siguiente se muestra cómo modificar la política de servicio de una LIF para utilizar la política de servicio de gestión predeterminada:

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

Comandos para gestionar las políticas de servicio de LIF

Utilice `network interface service-policy` los comandos para gestionar las políticas de servicio de LIF.

Obtenga más información sobre `network interface service-policy` en el "Referencia de comandos del ONTAP".

Antes de empezar

Modificar la política de servicio de una LIF en una relación de SnapMirror activa interrumpe la programación de replicación. Si convierte una LIF de interconexión de clústeres a que no se interconexión entre clústeres (o viceversa), esos cambios no se replican en el clúster con conexión entre iguales. Para actualizar el clúster de iguales después de modificar la política de servicio LIF, realice primero la `snapmirror abort` operación, luego resincronice la relación de replicación.

Si desea…	Se usa este comando…
Crear una política de servicio (se requieren privilegios avanzados)	`network interface service-policy create`
Agregar una entrada de servicio adicional a una política de servicio existente (se requieren privilegios avanzados)	`network interface service-policy add-service`
Clonar una política de servicio existente (se requieren privilegios avanzados)	`network interface service-policy clone`
Modificar una entrada de servicio en una política de servicio existente (se requieren privilegios avanzados)	`network interface service-policy modify-service`
Quitar una entrada de servicio de una política de servicio existente (se requieren privilegios avanzados)	`network interface service-policy remove-service`
Cambiar el nombre de una política de servicio existente (se requieren privilegios avanzados)	`network interface service-policy rename`
Eliminar una política de servicio existente (se requieren privilegios avanzados)	`network interface service-policy delete`
Restaurar una política de servicio integrada a su estado original (se requieren privilegios avanzados)	`network interface service-policy restore-defaults`
Mostrar las políticas de servicio existentes	`network interface service-policy show`

Información relacionada

- "se muestra el servicio de la interfaz de red"
- "política de servicio de la interfaz de red"
- "aborto de snapmirror"

Cree LIF ONTAP

Una SVM sirve datos a los clientes a través de una o varias interfaces lógicas de red (LIF). Debe crear LIF en los puertos que desee utilizar para acceder a datos. Una LIF (interfaz de red) es una dirección IP asociada a un puerto físico o lógico. Si hay un fallo de un componente, un LIF puede conmutar al respaldo o migrarse a un puerto físico diferente, lo que continúa comunicándose con la red.

Mejor práctica

Los puertos de switch conectados a ONTAP se deben configurar como puertos periféricos de árbol de expansión para reducir los retrasos durante la migración de LIF.

Antes de empezar

- Para realizar esta tarea, debe ser un administrador de clústeres.
- El puerto de red físico o lógico subyacente debe haber sido configurado con el estado administrativo activo.
- Si tiene pensado utilizar un nombre de subred para asignar la dirección IP y el valor de máscara de red para una LIF, la subred ya debe existir.

  Las subredes contienen un grupo de direcciones IP que pertenecen a la misma subred de capa 3. Se crean mediante System Manager o `network subnet create` el comando.

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

- El mecanismo para especificar el tipo de tráfico que maneja una LIF ha cambiado. Para ONTAP 9.5 y versiones anteriores, LIF usaba funciones para especificar el tipo de tráfico que gestionaría. A partir de ONTAP 9.6, los LIF utilizan políticas de servicio para especificar el tipo de tráfico que manejaría.

Acerca de esta tarea

- No puede asignar protocolos NAS y SAN a la misma LIF.

  Los protocolos admitidos son SMB, NFS, FlexCache, iSCSI y FC. ISCSI y FC no se pueden combinar con otros protocolos. Sin embargo, puede haber protocolos SAN basados en NAS y Ethernet en el mismo puerto físico.

  - No debe configurar los LIF que lleven tráfico SMB para revertir automáticamente a sus nodos de inicio. Esta recomendación es obligatoria si el servidor SMB va a alojar una solución para las operaciones no disruptivas con Hyper-V o SQL Server sobre SMB.
- Puede crear tanto LIF IPv4 como IPv6 en el mismo puerto de red.
- Todos los servicios de asignación de nombres y resolución de nombres de host que utiliza una SVM, como DNS, NIS, LDAP y Active Directory, Debe ser accesible desde al menos un LIF que gestiona el tráfico de datos de la SVM.
- Una LIF que gestiona tráfico dentro del clúster entre nodos no debe estar en la misma subred que una LIF que gestiona el tráfico de gestión o una LIF que gestiona el tráfico de datos.
- Crear una LIF que no tiene un destino de conmutación por error válido da lugar a un mensaje de advertencia.
- Si tiene un gran número de LIF en su clúster, puede verificar la capacidad de LIF admitida en el clúster:
  - System Manager: A partir de ONTAP 9.12.0, vea el rendimiento en la cuadrícula de interfaz de red.
  - CLI: Utilice `network interface capacity show` el comando y la capacidad de LIF admitidas en cada nodo utilizando `network interface capacity details show` el comando (en el nivel de privilegio avanzado).

    Obtenga más información sobre `network interface capacity show` y `network interface capacity details show` en el "Referencia de comandos del ONTAP".

- A partir de ONTAP 9.7, si ya existen otras LIF para la SVM en la misma subred, no es necesario especificar el puerto de inicio de la LIF. ONTAP elige automáticamente un puerto aleatorio en el nodo raíz especificado en el mismo dominio de retransmisión que las otras LIF ya configuradas en la misma subred.

  A partir de la versión 9.4 de ONTAP, se admite FC-NVMe. Si crea una LIF FC-NVMe, debe tener en cuenta lo siguiente:

    - El protocolo NVMe debe ser compatible con el adaptador de FC en el que se crea la LIF.
    - FC-NVMe puede ser el único protocolo de datos en las LIF de datos.
- Debe configurarse un LIF que gestiona el tráfico de gestión para cada máquina virtual de almacenamiento (SVM) compatible con SAN.
- Las LIF y los espacios de nombres de NVMe deben alojarse en el mismo nodo.
- Un máximo de dos LIF NVMe que gestionan el tráfico de datos se puede configurar por SVM y por nodo.
- Cuando se crea una interfaz de red con una subred, ONTAP selecciona automáticamente una dirección IP disponible desde la subred seleccionada y la asigna a la interfaz de red. Puede cambiar la subred si hay más de una subred, pero no puede cambiar la dirección IP.
- Cuando crea (añade) una SVM, para una interfaz de red, no puede especificar una dirección IP que esté en el rango de una subred existente. Recibirá un error de conflicto de subred. Este problema se produce en otros flujos de trabajo de una interfaz de red, como crear o modificar interfaces de red entre clústeres en configuraciones de SVM o configuración de clústeres.
- A partir de ONTAP 9.10,1, `network interface` los comandos de la CLI incluyen un `-rdma -protocols` parámetro para configuraciones NFS over RDMA. La creación de interfaces de red para las configuraciones de NFS over RDMA es compatible en System Manager a partir de ONTAP 9.12.1. Para obtener más información, consulte Configure LIF para NFS sobre RDMA.
- A partir de ONTAP 9.11.1, la conmutación automática por error en LIF iSCSI está disponible en las plataformas de cabinas SAN all-flash (ASA).

  La conmutación por error de LIF iSCSI se habilita automáticamente (la política de conmutación por error se establece en `sfo-partner-only` y el valor de reversión automática se establece en `true`) en los LIF iSCSI recién creados si no hay ningún LIF iSCSI en el SVM especificado o si todas las LIF iSCSI existentes del SVM especificado ya se encuentran habilitadas en la conmutación por error de LIF de iSCSI.

  Si después de actualizar a ONTAP 9.11,1 o posterior, tiene LIF iSCSI en un SVM que no se han habilitado con la función de conmutación por error de LIF iSCSI y crea nuevos LIF iSCSI en el mismo SVM, los nuevos LIF iSCSI asumen la misma política de conmutación por error (`disabled`) de los LIF iSCSI existentes en el SVM.

  "Conmutación por error de LIF de iSCSI para plataformas ASA"

A partir de ONTAP 9.7, ONTAP elige automáticamente el puerto inicial de una LIF, siempre que al menos una LIF ya exista en la misma subred en ese espacio IP. ONTAP elige un puerto principal en el mismo dominio de retransmisión que otras LIF de esa subred. Puede seguir especificando un puerto de inicio, pero ya no será necesario (a menos que aún no haya ninguna LIF en esa subred en el espacio IP especificado).

A partir de ONTAP 9.12.0, el procedimiento que siga depende de la interfaz que utilice—System Manager o la CLI:

System Manager

Utilice System Manager para agregar una interfaz de red

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione + Add .
3. Seleccione uno de los siguientes roles de interfaz:
   a. SQL Server
   b. Interconexión de clústeres
   c. Gestión de SVM
4. Seleccione el protocolo:
   a. SMB/CIFS Y NFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. Asigne un nombre a la LIF o acepte el nombre generado a partir de sus selecciones anteriores.
6. Acepte el nodo de inicio o use el menú desplegable para seleccionar uno.
7. Si al menos una subred está configurada en el espacio IP de la SVM seleccionada, se muestra la lista desplegable de subred.
   a. Si selecciona una subred, selecciónela en el menú desplegable.
   b. Si continúa sin una subred, se mostrará el menú desplegable dominio de retransmisión:
      i. Especifique la dirección IP. Si la dirección IP está en uso, aparecerá un mensaje de advertencia.
      ii. Especifique una máscara de subred.
8. Seleccione el puerto de inicio en el dominio de difusión, automáticamente (recomendado) o seleccionando uno en el menú desplegable. El control de puerto de inicio se muestra en función del dominio de difusión o de la selección de subred.
9. Guarde la interfaz de red.

CLI

Utilice la CLI para crear un LIF

Pasos

1. Determine los puertos de dominio de retransmisión que desea usar para la LIF.

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

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

2. Compruebe que la subred que desea utilizar para las LIF contiene suficientes direcciones IP sin usar.

   `network subnet show -ipspace` *`ipspace1`*

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

3. Cree uno o varios LIF en los puertos que desee utilizar para acceder a los datos.

   > NetApp recomienda crear objetos de subred para todas las LIF en SVM de datos. Esto es especialmente importante en las configuraciones de MetroCluster, donde el objeto de subred permite a ONTAP determinar los destinos de conmutación por error en el clúster de destino porque cada objeto de subred tiene un dominio de retransmisión asociado. Para obtener instrucciones, consulte "Cree una subred".

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - `-home-node` Es el nodo al que devuelve la LIF cuando `network interface revert` se ejecuta el comando en la LIF.

     También puede especificar si el LIF debe volver automáticamente al nodo raíz y al puerto raíz con la opción -auto-revert.

   Obtenga más información sobre `network interface revert` en el "Referencia de comandos del ONTAP".

   - `-home-port` Es el puerto físico o lógico al que devuelve la LIF cuando `network interface revert` el comando se ejecuta en la LIF.
   - Puede especificar una dirección IP con las `-address -netmask` opciones y, o bien habilitar la asignación desde una subred con `-subnet_name` la opción.
   - Al usar una subred para suministrar la dirección IP y la máscara de red, si la subred se definió

con una puerta de enlace, se añadirá automáticamente a la SVM una ruta predeterminada a esa puerta de enlace cuando se cree una LIF con dicha subred.

- Si asigna direcciones IP manualmente (sin una subred), es posible que deba configurar una ruta predeterminada para una puerta de enlace si hay clientes o controladores de dominio en una subred IP diferente. Obtenga más información sobre `network route create` en el "Referencia de comandos del ONTAP".
- `-auto-revert` Permite especificar si una LIF de datos se revierte automáticamente a su nodo de inicio en circunstancias como el inicio, los cambios en el estado de la base de datos de gestión o cuando se establece la conexión de red. El valor por defecto es `false`, pero puede definirlo en `true` función de las políticas de gestión de red del entorno.
- `-service-policy` A partir de ONTAP 9.5, puede asignar una política de servicio para la LIF con `-service-policy` la opción. Cuando se especifica una política de servicio para una LIF, la política se usa para construir un rol predeterminado, una política de conmutación por error y una lista de protocolos de datos para la LIF. En ONTAP 9.5, las políticas de servicio solo se admiten para los servicios entre iguales de BGP y interconexión de clústeres. En ONTAP 9.6, puede crear políticas de servicio para varios servicios de datos y gestión.
- `-data-protocol` Le permite crear una LIF que sea compatible con los protocolos FCP o NVMe/FC. Esta opción no es necesaria al crear una LIF de IP.

4. **Opcional**: Asigne una dirección IPv6 en la opción -address:

   a. Utilice el `network ndp prefix show` comando para ver la lista de prefijos RA aprendidos en varias interfaces.

   ```
   `network ndp prefix show`El comando está disponible en el nivel de privilegios avanzado.
   ```

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

   b. Utilice el formato `prefix::id` para construir la dirección IPv6 manualmente.

   `prefix` es el prefijo aprendido en diversas interfaces.

   Para derivar el `id`, seleccione un número hexadecimal aleatorio de 64 bits.

5. Compruebe que la configuración de la interfaz LIF es correcta.

   ```
   network interface show -vserver vs1
   ```

```
          Logical    Status     Network          Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask     Node      Port
Home
--------- ---------- ---------- --------------- --------- -------
----
vs1
           lif1       up/up      10.0.0.128/24   node1     e0d
true
```

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

6. Confirmar que la configuración del grupo de recuperación tras fallos es la deseada.

   `network interface show -failover -vserver vs1`

```
         Logical    Home       Failover        Failover
Vserver  interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
         lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. Compruebe que se pueda acceder a la dirección IP configurada:

Para verificar una…	Usar…
Dirección IPv4	ping de red
Dirección IPv6	red ping6

Ejemplos

El siguiente comando crea una LIF y especifica la dirección IP y los valores de la máscara de red mediante `-address -netmask` los parámetros y:

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

El siguiente comando crea una LIF y asigna valores de dirección IP y máscara de red a partir de la subred especificada (denominada cliente1_sub):

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

El siguiente comando crea una LIF NVMe/FC y especifica `nvme-fc` el protocolo de datos:

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

Modifique los LIF de ONTAP

Puede modificar una LIF cambiando los atributos, como el nodo inicial o el nodo actual, el estado administrativo, la dirección IP, la máscara de red, la política de conmutación por error política de firewall y política de servicio. También puede cambiar la familia de direcciones de un LIF de IPv4 a IPv6.

Acerca de esta tarea

- Cuando se modifica el estado administrativo de una LIF a inactivo, se retienen todos los bloqueos de NFSv4 extraordinarios hasta que se devuelva el estado administrativo de la LIF a.

  Para evitar conflictos de bloqueos que se pueden producir cuando otros LIF intentan acceder a los archivos bloqueados, debe mover los clientes de NFSv4 a una LIF diferente antes de establecer el estado administrativo como inactivo.

- No puede modificar los protocolos de datos que utiliza una LIF FC. Sin embargo, puede modificar los servicios asignados a una política de servicio o cambiar la política de servicio asignada a una LIF de IP.

  Para modificar los protocolos de datos que utiliza una LIF FC, debe eliminar y volver a crear la LIF. Para realizar cambios en la política de servicio en una LIF de IP, hay una breve interrupción mientras se realizan las actualizaciones.

- No puede modificar el nodo de inicio ni el nodo actual de una LIF de gestión de ámbito de nodo.
- Cuando se usa una subred para cambiar la dirección IP y el valor de máscara de red de una LIF, se asigna una dirección IP desde la subred especificada; si la dirección IP anterior de la LIF procede de una subred diferente, la dirección IP se devuelve a esa subred.
- Para modificar la familia de direcciones de una LIF de IPv4 a IPv6, debe usar la notación de dos puntos de la dirección IPv6 y añadir un nuevo valor para `-netmask-length` el parámetro.
- No puede modificar las direcciones IPv6 locales de enlace configuradas automáticamente.
- La modificación de una LIF que hace que la LIF no tenga ningún destino de conmutación por error válido da como resultado un mensaje de advertencia.

  Si una LIF que no tiene un destino de conmutación por error válido intenta conmutar al respaldo, se podría producir una interrupción del servicio.

- A partir de ONTAP 9.5, puede modificar la política de servicio asociada con una LIF.

En ONTAP 9.5, las políticas de servicio solo se admiten para los servicios entre iguales de BGP y interconexión de clústeres. En ONTAP 9.6, puede crear políticas de servicio para varios servicios de datos y gestión.

- A partir de ONTAP 9.11.1, la conmutación por error automática de LIF iSCSI está disponible en las plataformas de cabinas SAN all-flash (ASA).

  Para LIF iSCSI preexistentes, lo que significa LIF creadas antes de actualizar a la versión 9.11.1 o posterior, puede modificar la política de conmutación por error a "Activar recuperación tras fallos automática de LIF iSCSI".

- ONTAP utiliza el Protocolo de tiempo de red (NTP) para sincronizar la hora en todo el clúster. Después de cambiar las direcciones IP de LIF, es posible que deba actualizar la configuración de NTP para evitar fallas de sincronización. Para obtener más información, consulte la"Base de conocimientos de NetApp : La sincronización NTP falla después del cambio de IP de LIF" .

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

System Manager

A partir de ONTAP 9.12.0, puede utilizar System Manager para editar una interfaz de red

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione ⋮ **> Editar** junto a la interfaz de red que desea cambiar.
3. Cambie una o varias de las opciones de configuración de la interfaz de red. Para obtener más información, consulte "Cree una LIF".
4. Guarde los cambios.

CLI

Utilice la CLI para modificar un LIF

Pasos

1. Modifique los atributos de una LIF mediante `network interface modify` el comando.

   En el ejemplo siguiente se muestra cómo modificar la dirección IP y la máscara de red de los datos de LIF 2 mediante una dirección IP y el valor de máscara de red de la subred cliente1_sub:

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   En el ejemplo siguiente se muestra cómo modificar la política de servicio de una LIF.

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

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

2. Compruebe que sea posible acceder a las direcciones IP.

Si está usando…	Utilice…
Direcciones IPv4	`network ping`
Direcciones IPv6	`network ping6`

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

Migre LIF de ONTAP

Puede que tenga que migrar un LIF a un puerto diferente en el mismo nodo o a un nodo distinto dentro del clúster, si el puerto está defectuoso o requiere mantenimiento. Migrar

una LIF es similar a la conmutación por error de LIF, pero la migración de LIF es una operación manual, mientras que la conmutación por error de LIF es la migración automática de una LIF en respuesta a un fallo de enlace en el puerto de red actual de la LIF.

Antes de empezar

- Debe haber configurado un grupo de conmutación por error para las LIF.
- Los puertos y el nodo de destino deben estar operativos y deben poder acceder a la misma red que el puerto de origen.

Acerca de esta tarea

- Los LIF BGP residen en el puerto principal y no se pueden migrar a ningún otro nodo o puerto.
- Antes de quitar el NIC del nodo, debe migrar las LIF alojadas en los puertos que pertenecen a un NIC a otros puertos del clúster.
- Debe ejecutar el comando para migrar una LIF de clúster desde el nodo donde se aloja la LIF del clúster.
- Un LIF de ámbito de nodo, como un LIF de gestión de ámbito de nodo, LIF de clúster, LIF de interconexión de clústeres, no se puede migrar a un nodo remoto.
- Cuando se migra un LIF de NFSv4 entre nodos, se produce un retraso de hasta 45 segundos antes de que el LIF esté disponible en un puerto nuevo.

  Para solucionar este problema, utilice NFSv4.1 donde no se encuentra ninguna demora.

- Puede migrar LIF iSCSI en plataformas de cabinas all-flash SAN (ASA) que ejecuten ONTAP 9.11.1 o versiones posteriores.

  La migración de LIF iSCSI se limita a los puertos del nodo principal o del compañero de alta disponibilidad.

- Si la plataforma no es una plataforma de cabina SAN All-Flash (ASA) que ejecute ONTAP versión 9.11.1 o posterior, no se pueden migrar LIF iSCSI de un nodo a otro nodo.

  Para solucionar esta restricción, debe crear una LIF iSCSI en el nodo de destino. Obtenga más información "Creación de LIF iSCSI"sobre .

- Si desea migrar una LIF (interfaz de red) para NFS over RDMA, debe asegurarse de que el puerto de destino sea compatible con roce. Debe ejecutar ONTAP 9.10.1 o posterior para migrar un LIF con la CLI, o ONTAP 9.12.1 para realizar la migración mediante System Manager. En System Manager, una vez seleccionado el puerto de destino para roce, debe seleccionar la casilla junto a **utilizar puertos para roce** para completar la migración correctamente. Más información sobre "Configurar LIF para NFS a través de RDMA".
- Se produce un error en las operaciones de descarga de la copia VAAI de VMware cuando se migra la LIF de origen o destino. Obtenga información acerca de la descarga de copias:
  - "Entornos NFS"
  - "Entornos SAN"

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

System Manager

Utilice System Manager para migrar una interfaz de red

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione ⋮ **> Migrar** junto a la interfaz de red que desea cambiar.

   Para una LIF iSCSI, en el cuadro de diálogo **Migrate Interface**, seleccione el nodo de destino y el puerto del socio HA.

   Si desea migrar la LIF iSCSI de forma permanente, marque la casilla. La LIF de iSCSI debe estar desconectada para poder migrarla de forma permanente. Además, una vez que se migra permanentemente un LIF iSCSI, no se puede revertir. No hay ninguna opción de reversión.

3. Haga clic en **migrar**.
4. Guarde los cambios.

CLI

Utilice la CLI para migrar un LIF

Paso

En función de si desea migrar una LIF específica o todas las LIF, realice la acción correspondiente:

Si desea migrar…	Introduzca el siguiente comando…
Una LIF específica	`network interface migrate`
Todas las LIF de gestión de datos y clústeres en un nodo	`network interface migrate-all`
Todas las LIF están fuera de un puerto	`network interface migrate-all -node <node> -port <port>`

El ejemplo siguiente muestra cómo migrar una LIF llamada `datalif1` en la SVM `vs0` al puerto `e0d` en `node0b`:

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

En el ejemplo siguiente se muestra cómo migrar todas las LIF de datos y de gestión del clúster desde el nodo (local) actual:

```
network interface migrate-all -node local
```

Información relacionada

- "migración de interfaz de red"

Revierta un LIF a su puerto raíz después de una recuperación tras fallos en el nodo ONTAP o una migración de puerto

Puede revertir un LIF a su puerto raíz después de producirse un fallo o una migración a otro puerto, ya sea de forma manual o automática. Si el puerto de inicio de un LIF determinado no está disponible, el LIF se mantiene en su puerto actual y no se revierte.

Acerca de esta tarea

- Si lleva administrativamente el puerto de inicio de un LIF al estado activo antes de configurar la opción de reversión automática, la LIF no vuelve al puerto de inicio.
- LIF no revierte automáticamente a menos que el valor de la opción de "reversión automática" se configure en TRUE.
- Debe asegurarse de que esté habilitada la opción de "reversión automática" para que las LIF puedan revertir a sus puertos de inicio.

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

System Manager

Utilice System Manager para revertir una interfaz de red a su puerto doméstico

Pasos

1. Seleccione **Red > Descripción general > interfaces de red**.
2. Seleccione ⋮ **> Revertir** junto a la interfaz de red que desea cambiar.
3. Seleccione **Revert** para revertir una interfaz de red a su puerto de inicio.

CLI

Utilice la CLI para revertir una LIF a su puerto doméstico

Paso

Revierte una LIF a su puerto de inicio de forma manual o automática:

Si desea revertir una LIF a su puerto raíz…	Después, introduzca el siguiente comando…
Manualmente	`network interface revert -vserver vserver_name -lif lif_name`
Automáticamente	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

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

Recuperar un LIF de ONTAP configurado incorrectamente

No se puede crear un clúster cuando la red del clúster se cableado a un switch, pero no todos los puertos configurados en el espacio IP del clúster pueden llegar a los otros puertos configurados en el espacio IP del clúster.

Acerca de esta tarea

En un clúster con switches, si está configurada una interfaz de red de clúster (LIF) en el puerto incorrecto o si hay un puerto de clúster conectado a la red incorrecta, `cluster create` el comando puede fallar con el siguiente error:

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

Obtenga más información sobre `cluster create` en el "Referencia de comandos del ONTAP".

Los resultados `network port show` del comando podrían mostrar que se han agregado varios puertos al espacio IP del clúster porque están conectados a un puerto que está configurado con una LIF de clúster. Sin embargo, los resultados de la `network port reachability show -detail` El comando revela qué puertos no tienen conectividad entre sí.

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

Para recuperar desde un LIF de clúster configurado en un puerto que no sea accesible a los otros puertos configurados con LIF del clúster, realice los pasos siguientes:

Pasos

1. Restablezca el puerto de inicio de la LIF del clúster en el puerto correcto:

   ```
   network port modify -home-port
   ```

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

2. Quite los puertos que no tienen LIF del clúster configuradas en ellos desde el dominio de retransmisión del clúster:

   ```
   network port broadcast-domain remove-ports
   ```

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

3. Cree el clúster:

   ```
   cluster create
   ```

Resultado

Una vez finalizada la creación del clúster, el sistema detecta la configuración correcta y coloca los puertos en los dominios de retransmisión correctos.

Información relacionada

- "Mostrar la accesibilidad del puerto de red"

Elimine las LIF ONTAP

Puede eliminar una interfaz de red (LIF) que ya no sea necesaria.

Antes de empezar

Las LIF que deben eliminarse no deben estar en uso.

Pasos

1. Marque las LIF que desea eliminar como administrativas usando el siguiente comando:

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. Use `network interface delete` el comando para eliminar una o todas las LIF:

Si desea eliminar…	Introduzca el comando …
Una LIF específica	`network interface delete -vserver vserver_name -lif lif_name`
Todas las LIF	`network interface delete -vserver vserver_name -lif *`

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

   El siguiente comando elimina la LIF mgmtlif2:

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. Utilice `network interface show` el comando para confirmar que la LIF se ha eliminado.

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

Configuración de LIF de IP virtual (VIP) de ONTAP

Algunos centros de datos de última generación utilizan mecanismos de red de capa 3 (IP) que requieren que las LIF se conmuten en las subredes. ONTAP admite los LIF de datos de IP virtual (VIP) y el protocolo de enrutamiento asociado, protocolo de puerta de enlace de borde (BGP), para cumplir los requisitos de recuperación tras fallos de las redes de última generación.

Acerca de esta tarea

Una LIF de datos VIP es una LIF que no forma parte de ninguna subred y se puede acceder a ella desde todos los puertos que alojan una LIF BGP en el mismo espacio IP. Una LIF de datos VIP elimina la dependencia de un host en interfaces de red individuales. Debido a que varios adaptadores físicos transportan

el tráfico de datos, la carga completa no se concentra en un solo adaptador y en la subred asociada. La existencia de una LIF de datos VIP se anuncia para encaminadores de conexión a través del protocolo de enrutamiento Border Gateway Protocol (BGP).

Los LIF de datos VIP ofrecen las siguientes ventajas:

- Portabilidad de LIF más allá de un dominio o subred: Los LIF de datos VIP pueden conmutar por error a cualquier subred de la red al anunciar la ubicación actual de cada LIF de datos VIP a enrutadores a través de BGP.
- Rendimiento del agregado: Las LIF de datos VIP pueden admitir un rendimiento agregado que supera el ancho de banda de cualquier puerto individual, ya que las LIF VIP pueden enviar o recibir datos desde varias subredes o puertos simultáneamente.

Configuración del protocolo de puerta de enlace de borde (BGP)

Antes de crear LIF VIP, debe configurar BGP, que es el protocolo de enrutamiento utilizado para anunciar la existencia de una LIF VIP a routers de igual nivel.

A partir de ONTAP 9.9,1, VIP proporciona automatización de rutas predeterminada opcional mediante grupos de pares BGP para simplificar la configuración.

ONTAP tiene una forma sencilla de aprender rutas predeterminadas utilizando los interlocutores BGP como enrutadores de salto siguiente cuando el par BGP se encuentra en la misma subred. Para utilizar la característica, establezca el `-use-peer-as-next-hop` atributo en `true`. Por defecto, este atributo es `false`.

Si ha configurado rutas estáticas, éstas seguirán siendo preferidas en estas rutas predeterminadas automatizadas.

Antes de empezar

El router del par debe estar configurado para aceptar una conexión BGP de la LIF BGP para el número de sistema autónomo configurado (ASN).

> ONTAP no procesa ningún aviso de ruta entrante desde el enrutador; por lo tanto, debe configurar el enrutador de paridad para no enviar actualizaciones de ruta al clúster. Esto reduce el tiempo necesario para que la comunicación con el par sea completamente funcional y reduce el uso de memoria interna dentro de ONTAP.

Acerca de esta tarea

La configuración de BGP implica la creación opcional de una configuración BGP, la creación de una LIF BGP y la creación de un grupo de pares BGP. ONTAP crea automáticamente una configuración BGP predeterminada con valores predeterminados cuando se crea el primer grupo de pares BGP en un nodo determinado.

Se utiliza una LIF BGP para establecer sesiones TCP BGP con routers de pares. Para un router de par, una LIF BGP es el siguiente salto para llegar a una LIF VIP. La conmutación por error está deshabilitada para el LIF de BGP. Un grupo de pares BGP anuncia las rutas VIP para todas las SVM en el espacio IP utilizado por el grupo de pares. El espacio IP utilizado por el grupo de iguales se hereda de la LIF BGP.

A partir de ONTAP 9.16,1, la autenticación MD5 se admite en los grupos de pares BGP para proteger las sesiones BGP. Cuando MD5 está habilitado, las sesiones BGP solo se pueden establecer y procesar entre pares autorizados, evitando posibles interrupciones de la sesión por parte de un actor no autorizado.

Se han agregado los siguientes campos a los `network bgp peer-group create` comandos y. `network`

`bgp peer-group modify`

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

Estos parámetros permiten configurar un grupo de pares BGP con una firma MD5 para mejorar la seguridad. Los siguientes requisitos se aplican al uso de la autenticación MD5:

- Solo puede especificar el `-md5-secret` parámetro cuando el `-md5-enabled` parámetro está definido en `true`.
- IPSec debe estar activado globalmente para poder habilitar la autenticación BGP MD5. No es necesario que la LIF BGP tenga una configuración de IPsec activa. Consulte "Configurar la seguridad IP (IPsec) a través del cifrado de cable".
- NetApp recomienda configurar MD5 en el enrutador antes de configurarlo en la controladora ONTAP.

A partir de ONTAP 9.9.1, se han añadido estos campos:

- `-asn` O `-peer-asn` (valor de 4 bytes) el atributo en sí no es nuevo, pero ahora utiliza un entero de 4 bytes.
- `-med`
- `-use-peer-as-next-hop`

Puede realizar selecciones avanzadas de rutas con compatibilidad con el discriminador de salida múltiple (MED) para la priorización de rutas. MED es un atributo opcional en el mensaje de actualización de BGP que indica a los enrutadores que seleccionen la mejor ruta para el tráfico. MED es un entero de 32 bits sin firmar (0 - 4294967295); se prefieren valores inferiores.

A partir de ONTAP 9.8, estos campos se han agregado al `network bgp peer-group` comando:

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

Estos atributos BGP le permiten configurar los atributos AS Path y Community para el grupo de pares BGP.

> Aunque ONTAP admite los atributos BGP anteriores, los routers no necesitan respetarlos. NetApp recomienda confirmar qué atributos son compatibles con el router y configurar los grupos de pares BGP en consecuencia. Para obtener más información, consulte la documentación de BGP proporcionada por el router.

Pasos

1. Inicie sesión en el nivel de privilegio avanzado:

   `set -privilege advanced`

2. Opcional: Cree una configuración BGP o modifique la configuración BGP predeterminada del clúster realizando una de las acciones siguientes:

   a. Crear una configuración BGP:

```
network bgp config create -node {node_name | local} -asn <asn_number>
-holdtime
<hold_time> -routerid <router_id>
```

- El `-routerid` parámetro acepta un valor decimal de 32 bits que solo necesita ser único dentro de un dominio AS. NetApp recomienda utilizar la dirección IP de gestión de nodos (v4) para `<router_id>` lo cual garantiza la singularidad.
- Aunque ONTAP BGP admite números ASN de 32 bits, sólo se admite la notación decimal estándar. No se admite la notación ASN punteada, como 65000,1 en lugar de 4259840001 para un ASN privado.

Muestra con un ASN de 2 bytes:

```
network bgp config create -node node1 -asn 65502 -holdtime 180
-routerid 1.1.1.1
```

Muestra con un ASN de 4 bytes:

```
network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
1.1.1.1
```

a. Modifique la configuración predeterminada de BGP:

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>` Especifica el número ASN. A partir de ONTAP 9.8, ASN para BGP admite un entero no negativo de 2 bytes. Se trata de un número de 16 bits (de 1 a 65534 valores disponibles). A partir de ONTAP 9.9,1, ASN para BGP admite un entero no negativo de 4 bytes (1 a 4294967295). El ASN predeterminado es 65501. ASN 23456 está reservado para el establecimiento de sesiones de ONTAP con compañeros que no anuncian la funcionalidad ASN de 4 bytes.
- `<hold_time>` especifica el tiempo de espera en segundos. El valor predeterminado es 180s.

ONTAP sólo soporta un global `<asn_number>`, `<hold_time>` y `<router_id>`, incluso si configura BGP para varios espacios IP. El BGP y toda la información de enrutamiento IP está completamente aislada dentro de un espacio IP. Un espacio IP equivale a una instancia de enrutamiento y reenvío virtual (VRF).

3. Cree un LIF de BGP para la SVM del sistema:

Para el espacio IP predeterminado, el nombre de la SVM es el nombre del clúster. Para espacios IP adicionales, el nombre de la SVM es idéntico al nombre del espacio IP.

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

Puede utilizar `default-route-announce` la política de servicio para la LIF BGP o cualquier política de servicio personalizada que contenga el servicio «management-bgp».

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. Cree un grupo de pares BGP que se utilice para establecer sesiones BGP con los routers de pares remotos y configurar la información de ruta VIP que se anuncia a los routers de pares:

   Ejemplo 1: Cree un grupo de pares sin una ruta predeterminada automática

   En este caso, el administrador necesita crear una ruta estática para el par BGP.

   ```
   network bgp peer-group create -peer-group <group_name> -ipspace
   <ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
   -peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
   type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
   {-community BGP community list <0-65535>:<0-65535>}
   ```

   ```
   network bgp peer-group create -peer-group group1 -ipspace Default -bgp
   -lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
   -asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
   9000:900,8000:800
   ```

   Ejemplo 2: Cree un grupo de pares con una ruta predeterminada automática

   ```
   network bgp peer-group create -peer-group <group_name> -ipspace
   <ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
   -peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
   preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
   prepend-count <integer>} {-med <integer>} {-community BGP community list
   <0-65535>:<0-65535>}
   ```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

Ejemplo 3: Cree un grupo de pares con MD5 habilitado

a. Habilitar IPsec:

```
security ipsec config modify -is-enabled true
```

b. Cree el grupo de pares BGP con MD5 activado:

```
network bgp peer-group create -ipspace Default -peer-group
<group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
{-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
```

Ejemplo con una clave hexadecimal:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
0x746573742073656372657400
```

Ejemplo usando una cadena:

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

Después de crear el grupo de pares BGP, aparece un puerto ethernet virtual (a partir de v0a..v0z,V1A…) cuando ejecuta `network port show` el comando. La MTU de esta interfaz siempre se informa en 1500. La MTU real utilizada para el tráfico se deriva del puerto físico (LIF BGP), que se determina cuando se envía el tráfico. Obtenga más información sobre `network port show` en el "Referencia de comandos del ONTAP".

Cree una LIF de datos de IP virtual (VIP)

La existencia de una LIF de datos VIP se anuncia para encaminadores de conexión a través del protocolo de enrutamiento Border Gateway Protocol (BGP).

Antes de empezar

- Debe configurarse el grupo de pares BGP y la sesión BGP para la SVM en la que se va a crear el LIF debe estar activa.
- Se debe crear una ruta estática al enrutador BGP o cualquier otro enrutador en la subred de la LIF BGP

para cualquier tráfico VIP saliente para la SVM.

- Debe activar el enrutamiento multivía para que el tráfico VIP saliente pueda utilizar todas las rutas disponibles.

  Si el enrutamiento multivía no está habilitado, todo el tráfico VIP saliente va desde una única interfaz.

Pasos

1. Cree una LIF de datos VIP:

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

   Un puerto VIP se selecciona automáticamente si no especifica el puerto de inicio con el `network interface create` comando.

   De forma predeterminada, la LIF de datos VIP pertenece al dominio de retransmisión creado por el sistema denominado "VIP", por cada espacio IP. No se puede modificar el dominio de retransmisión VIP.

   Se puede acceder a una LIF de datos VIP en todos los puertos que alojan una LIF BGP de un espacio IP. Si no hay ninguna sesión BGP activa para la SVM de VIP en el nodo local, el LIF de datos VIP se conmuta por error al siguiente puerto VIP del nodo que tiene una sesión BGP establecida para esa SVM.

2. Compruebe que la sesión BGP está en estado activo de la SVM de la LIF de datos VIP:

```
network bgp vserver-status show

Node        Vserver  bgp status
        ----------  -------- ---------
        node1       vs1      up
```

   Si el estado de BGP es `down` para la SVM en un nodo, la LIF de datos VIP conmuta por error a un nodo diferente en el que el estado de BGP sea activo para la SVM. Si el estado BGP está `down` en todos los nodos, el LIF de datos VIP no se puede alojar en ninguna parte y tiene el estado LIF como inactivo.

Comandos para administrar el BGP

A partir de ONTAP 9.5, se utilizan `network bgp` los comandos para gestionar las sesiones BGP en ONTAP.

Administrar la configuración de BGP

Si desea…	Se usa este comando…
Crear una configuración BGP	`network bgp config create`
Modifique la configuración de BGP	`network bgp config modify`
Eliminar configuración BGP	`network bgp config delete`

Mostrar la configuración de BGP	`network bgp config show`
Muestra el estado de BGP para la SVM del LIF VIP	`network bgp vserver-status show`

Administrar valores predeterminados de BGP

Si desea…	Se usa este comando…
Modificar los valores predeterminados de BGP	`network bgp defaults modify`
Mostrar valores predeterminados de BGP	`network bgp defaults show`

Administrar grupos de pares BGP

Si desea…	Se usa este comando…
Cree un grupo de pares BGP	`network bgp peer-group create`
Modificar un grupo de pares BGP	`network bgp peer-group modify`
Eliminar un grupo de pares BGP	`network bgp peer-group delete`
Mostrar la información de grupos de pares BGP	`network bgp peer-group show`
Cambie el nombre de un grupo de pares BGP	`network bgp peer-group rename`

Gestione grupos de pares BGP con MD5

A partir de ONTAP 9.16,1, puede habilitar o deshabilitar la autenticación MD5 en un grupo de pares BGP existente.

> Si habilita o deshabilita MD5 en un grupo de pares BGP existente, la conexión BGP finaliza y se vuelve a crear para aplicar los cambios de configuración de MD5.

Si desea…	Se usa este comando…
Habilite MD5 en un grupo de pares BGP existente	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
Desactive MD5 en un grupo de pares BGP existente	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

Información relacionada

- "Referencia de comandos del ONTAP"
- "red bgp"
- "interfaz de red"
- "modificar configuración de seguridad ipsec"

Equilibre las cargas de red

Optimice el tráfico de red de ONTAP usando el equilibrio de carga de DNS

Puede configurar su clúster para que sirva las solicitudes de cliente desde LIF cargadas correctamente. Esto da como resultado un uso más equilibrado de LIF y puertos, lo que a su vez permite un mejor rendimiento del clúster.

El equilibrio de carga de DNS ayuda a seleccionar una LIF de datos cargada correctamente y a equilibrar el tráfico de red de usuario en todos los puertos disponibles (físicos, grupos de interfaces y VLAN).

Con el equilibrio de carga de DNS, las LIF se asocian a la zona de equilibrio de carga de una SVM. Un servidor DNS de todo el sitio está configurado para reenviar todas las solicitudes de DNS y devolver el LIF menos cargado en función del tráfico de red y la disponibilidad de los recursos de puertos (uso de CPU, rendimiento, conexiones abiertas, etc.). El equilibrio de carga de DNS ofrece las siguientes ventajas:

- Las nuevas conexiones de clientes se equilibran entre los recursos disponibles.
- No es necesaria ninguna intervención manual para decidir qué LIF se usarán en el montaje de una SVM en particular.
- El equilibrio de carga de DNS admite NFSv3, NFSv4, NFSv4,1, SMB 2,0, SMB 2,1, SMB 3,0 y S3.

Obtenga información sobre el equilibrio de carga de DNS para la red de ONTAP

Los clientes montan una SVM especificando una dirección IP (asociada a una LIF) o un nombre de host (asociado a varias direcciones IP). De forma predeterminada, el servidor DNS de todo el sitio selecciona los LIF por turnos, lo que equilibra la carga de trabajo entre todos los LIF.

El equilibrio de carga por turnos puede sobrecargar algunos LIF, por lo que tiene la opción de utilizar una zona de equilibrio de carga DNS que gestiona la resolución de nombres de host en una SVM. Con una zona de equilibrio de carga DNS, se garantiza un mejor equilibrio de las conexiones de los nuevos clientes en los recursos disponibles, lo que mejora el rendimiento del clúster.

Una zona de equilibrio de carga DNS es un servidor DNS dentro del clúster que evalúa de forma dinámica la carga de todas las LIF y devuelve un LIF cargado correctamente. En una zona de equilibrio de carga, DNS asigna un peso (métrica), basado en la carga, a cada LIF.

A cada LIF se le asigna un peso en función de la carga de puertos y el uso de CPU de su nodo raíz. Las LIF que están en puertos menos cargados tienen una probabilidad mayor de ser devueltas en una consulta DNS. Los pesos también se pueden asignar manualmente.

Cree zonas de equilibrio de carga DNS para la red de ONTAP

Puede crear una zona de equilibrio de carga de DNS para facilitar la selección dinámica de una LIF en función de la carga, es decir, el número de clientes montados en una LIF. Puede crear una zona de equilibrio de carga mientras crea una LIF de datos.

Antes de empezar

El transportista DNS del servidor DNS del sitio debe estar configurado para reenviar todas las solicitudes de la zona de equilibrio de carga a las LIF configuradas.

El"Base de conocimientos de NetApp : Cómo configurar el equilibrio de carga de DNS en modo clúster" Contiene más información sobre cómo configurar el equilibrio de carga de DNS mediante reenvío condicional.

Acerca de esta tarea

- Cualquier LIF de datos puede responder a consultas DNS para un nombre de zona de equilibrio de carga DNS.
- Una zona de equilibrio de carga DNS debe tener un nombre único en el clúster y el nombre de la zona debe cumplir los siguientes requisitos:
  - No debe superar los 256 caracteres.
  - Debe incluir al menos un período.
  - El primer carácter y el último no deben ser un punto ni ningún otro carácter especial.
  - No puede incluir espacios entre caracteres.
  - Cada etiqueta del nombre DNS no debe superar los 63 caracteres.

    Una etiqueta es el texto que aparece antes o después del período. Por ejemplo, la zona DNS llamada storage.company.com tiene tres etiquetas.

Paso

Utilice `network interface create` el comando con `dns-zone` la opción para crear una zona de equilibrio de carga DNS. Obtenga más información sobre `network interface create` en el "Referencia de comandos del ONTAP".

Si ya existe la zona de equilibrio de carga, se agrega el LIF.

En el siguiente ejemplo se muestra cómo crear una zona de equilibrio de carga DNS llamada storage.company.com while create the LIF `lif1`:

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

Agregue o quite un LIF de ONTAP de una zona de equilibrio de carga

Puede agregar o quitar una LIF de la zona de equilibrio de carga DNS de una máquina virtual (SVM). También puede quitar todas las LIF al mismo tiempo de una zona de equilibrio de carga.

Antes de empezar

- Todas las LIF de una zona de equilibrio de carga deben pertenecer a la misma SVM.
- Un LIF puede ser parte de solo una zona de equilibrio de carga de DNS.
- Debe haber configurado los grupos de conmutación por error de cada subred si las LIF pertenecen a subredes diferentes.

Acerca de esta tarea

Una LIF en estado administrativo inactivo se quita temporalmente de la zona de equilibrio de carga de DNS. Cuando la LIF vuelve al estado administrativo up, la LIF se agrega automáticamente a la zona de balanceo de

carga de DNS.

Paso

Añada una LIF a o quite una LIF de una zona de equilibrio de carga:

Si desea…	Introduzca…
Agregar una LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone` *`zone_name`* Ejemplo: `network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`
Quite una única LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone none` Ejemplo: `network interface modify -vserver vs1 -lif data1 -dns-zone none`
Quite todas las LIF	`network interface modify -vserver` *`vserver_name`* `-lif * -dns-zone none` Ejemplo: `network interface modify -vserver vs0 -lif * -dns-zone none` Puede eliminar una SVM de una zona de equilibrio de carga eliminando todas las LIF de la SVM de esa zona.

Información relacionada

- "modificación de la interfaz de red"

Configure los servicios DNS para la red ONTAP

Debe configurar los servicios DNS para la SVM antes de crear un servidor NFS o SMB. Generalmente, los servidores de nombres DNS son los servidores DNS integrados de Active Directory para el dominio al que se unirá el servidor NFS o SMB.

Acerca de esta tarea

Los servidores DNS integrados en Active Directory contienen los registros de ubicación de servicio (SRV) para los servidores LDAP de dominio y controlador de dominio. Si la SVM no puede encontrar los servidores LDAP de Active Directory y las controladoras de dominio, se produce un error en la configuración del servidor NFS o SMB.

Las SVM utilizan la base de datos ns-switch de servicios de nombres de hosts para determinar qué servicios de nombres utilizar y en qué orden se debe buscar información sobre los hosts. Los dos servicios de nombre admitidos para la base de datos de hosts son archivos y dns.

Debe asegurarse de que dns sea uno de los orígenes antes de crear el servidor SMB.

Para ver las estadísticas de los servicios de nombre DNS para el proceso mgwd y el proceso SECD, use la interfaz de usuario de Statistics.

Pasos

1. Determine cuál es la configuración actual para la base de datos de servicios de nombre de host. En este ejemplo, la base de datos del servicio de nombres de host utiliza la configuración predeterminada.

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Si es necesario, realice las siguientes acciones.

   a. Agregue el servicio de nombres DNS a la base de datos del servicio de nombres de host en el orden deseado o reordene los orígenes.

      En este ejemplo, la base de datos hosts está configurada para utilizar DNS y archivos locales en ese orden.

      ```
      vserver services name-service ns-switch modify -vserver vs1 -database hosts
      -sources dns,files
      ```

   b. Compruebe que la configuración del servicio de nombres es correcta.

      ```
      vserver services name-service ns-switch show -vserver vs1 -database hosts
      ```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. Configure los servicios DNS.

   ```
   vserver services name-service dns create -vserver vs1 -domains
   example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
   ```

   > El comando vserver Services NAME-service dns create realiza una validación de configuración automática e informa de un mensaje de error si ONTAP no puede contactar con el servidor de nombres.

4. Verifique que la configuración de DNS sea correcta y que el servicio esté habilitado.

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. Validar el estado de los servidores de nombres.

   ```
   vserver services name-service dns check -vserver vs1
   ```

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Configure el DNS dinámico en la SVM

Si desea que el servidor DNS integrado en Active Directory registre de forma dinámica los registros DNS de un servidor NFS o SMB en DNS, debe configurar el DNS dinámico (DDNS) en la SVM.

Antes de empezar

Los servicios de nombres DNS deben configurarse en la SVM. Si utiliza DDNS seguro, debe usar servidores de nombres DNS integrados en Active Directory y debe haber creado un servidor NFS o SMB o una cuenta de Active Directory para la SVM.

Acerca de esta tarea

El nombre de dominio completo (FQDN) especificado debe ser único:

El nombre de dominio completo (FQDN) especificado debe ser único:

- Para NFS, el valor especificado en `-vserver-fqdn` como parte del `vserver services name-service dns dynamic-update` comando se convierte en el FQDN registrado para las LIF.
- Para SMB, los valores especificados como el nombre de NetBIOS del servidor CIFS y el nombre de dominio completo del servidor CIFS se convierten en el FQDN registrado de los LIF. No se puede configurar en ONTAP. En la siguiente situación, el nombre de dominio completo del LIF es «CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                                Authentication Style: domain
                  CIFS Server Administrative Status: up
                             CIFS Server Description:
                             List of NetBIOS Aliases: -
```

Para evitar un error de configuración de un FQDN de SVM que no es compatible con las reglas RFC para las actualizaciones de DDNS, utilice un nombre FQDN que es compatible con RFC. Para obtener más información, consulte "RFC 1123".

Pasos

1. Configure DDNS en la SVM:

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Los asteriscos no se pueden utilizar como parte del FQDN personalizado. Por ejemplo, `*.netapp.com` no es válido.

2. Compruebe que la configuración DDNS es correcta:

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

Configurar servicios DNS dinámicos para la red ONTAP

Si desea que el servidor DNS integrado en Active Directory registre de forma dinámica los registros DNS de un servidor NFS o SMB en DNS, debe configurar el DNS dinámico (DDNS) en la SVM.

Antes de empezar

Los servicios de nombres DNS deben configurarse en la SVM. Si utiliza DDNS seguro, debe usar servidores de nombres DNS integrados en Active Directory y debe haber creado un servidor NFS o SMB o una cuenta de Active Directory para la SVM.

Acerca de esta tarea

El FQDN especificado debe ser único.

> Para evitar un error de configuración de un FQDN de SVM que no es compatible con las reglas RFC para las actualizaciones de DDNS, utilice un nombre FQDN que es compatible con RFC.

Pasos

1. Configure DDNS en la SVM:

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Los asteriscos no se pueden utilizar como parte del FQDN personalizado. Por ejemplo, `*.netapp.com` no es válido.

2. Compruebe que la configuración DDNS es correcta:

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

Resolución del nombre de host

Obtenga información acerca de la resolución de nombres de host para la red ONTAP

ONTAP debe poder traducir los nombres de host a direcciones IP numéricas para proporcionar acceso a los clientes y acceder a los servicios. Debe configurar máquinas virtuales de almacenamiento (SVM) para que utilicen servicios de nombres locales o externos para resolver la información del host. ONTAP admite la configuración de un servidor DNS externo o la configuración del archivo de hosts locales para la resolución del nombre de host.

Cuando utiliza un servidor DNS externo, puede configurar el DNS dinámico (DDNS), que envía automáticamente información DNS nueva o modificada del sistema de almacenamiento al servidor DNS. Sin las actualizaciones dinámicas de DNS, debe agregar manualmente la información DNS (nombre DNS y dirección IP) a los servidores DNS identificados cuando se conecta un sistema nuevo o cuando cambie la información de DNS existente. Este proceso es lento y propenso a errores. Durante la recuperación ante desastres, la configuración manual puede provocar tiempos de inactividad prolongados.

Configure el DNS para la resolución de nombre de host para la red ONTAP

Se usa DNS para acceder a orígenes locales o remotos para obtener información del host. Debe configurar DNS para acceder a uno o ambos orígenes.

ONTAP debe ser capaz de buscar la información del host para proporcionar un acceso adecuado a los clientes. Es necesario configurar los servicios de nombre para permitir que ONTAP acceda a los servicios DNS locales o externos para obtener la información del host.

ONTAP almacena la información de configuración del servicio de nombres en una tabla que es el equivalente al `/etc/nsswitch.conf` archivo en sistemas UNIX.

Configurar una SVM y LIF de datos para la resolución de nombres de host mediante un servidor DNS externo

Puede usar `vserver services name-service dns` el comando para habilitar DNS en una SVM y configurarlo para que utilice DNS para la resolución de nombre de host. Los nombres de host se resuelven mediante servidores DNS externos.

Antes de empezar

Un servidor DNS para todo el sitio debe estar disponible para las búsquedas de nombre de host.

Debe configurar más de un servidor DNS para evitar un único punto de error. El `vserver services name-service dns create` comando emite una advertencia si se introduce solo un nombre de servidor DNS.

Acerca de esta tarea

Consulte Configure los servicios DNS dinámicos para obtener más información sobre la configuración del DNS dinámico en la máquina virtual de almacenamiento (SVM).

Pasos

1. Habilite DNS en la SVM:

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

El siguiente comando habilita los servidores DNS externos en la SVM vs1:

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> El `vserver services name-service dns create` comando realiza una validación automática de la configuración y informa un mensaje de error si ONTAP no puede contactar con el servidor de nombres.

2. Valide el estado de los servidores de nombres mediante `vserver services name-service dns check` el comando.

```
vserver services name-service dns check -vserver vs1.example.com
                                    Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
-------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

Para obtener información sobre las políticas de servicio relacionadas con DNS, consulte "LIF y políticas de servicio en ONTAP 9.6 y posteriores".

Configure la tabla de switches de servicio de nombres para la resolución de nombres de host

Debe configurar correctamente la tabla del conmutador de servicio de nombres para permitir que ONTAP consulte el servicio de nombres local o externo a fin de recuperar la información del host.

Antes de empezar

Debe haber decidido qué servicio de nombres debe utilizar para la asignación de hosts en el entorno.

Pasos

1. Agregue las entradas necesarias a la tabla de cambio de servicio de nombres:

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. Compruebe que la tabla de cambio de servicio de nombres contiene las entradas esperadas en el orden deseado:

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

Ejemplo

En el siguiente ejemplo se modifica una entrada en la tabla del conmutador de servicio de nombres para SVM VS1 a fin de utilizar primero el archivo de hosts locales y, a continuación, un servidor DNS externo para resolver los nombres de host:

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

Comandos de la ONTAP para gestionar la tabla ONTAP Hosts

Un administrador de clúster puede añadir, modificar, eliminar y ver las entradas del nombre de host en la tabla hosts de la máquina virtual de almacenamiento (SVM) de administrador. Un administrador de SVM solo puede configurar las entradas del nombre de host para la SVM asignada.

Comandos para gestionar entradas de nombre de host local

Se puede usar el `vserver services name-service dns hosts` comando para crear, modificar o eliminar entradas de la tabla de host DNS.

Cuando va a crear o modificar las entradas de nombre de host DNS, puede especificar varias direcciones de alias separadas por comas.

Si desea…	Se usa este comando…
Cree una entrada DNS host-name	`vserver services name-service dns hosts create`
Modifique una entrada de nombre de host DNS	`vserver services name-service dns hosts modify`
Eliminar una entrada de nombre de host DNS	`vserver services name-service dns hosts delete`

Para obtener más información acerca de los `vserver services name-service dns hosts` comandos,

consulte la "Referencia de comandos del ONTAP".

Proteja su red

Configure la seguridad de red ONTAP mediante FIPS para todas las conexiones SSL

ONTAP cumple con los Estándares Federales de Procesamiento de Información (FIPS) 140-2 para todas las conexiones SSL. Puede activar y desactivar el modo SSL FIPS, configurar los protocolos SSL globalmente y desactivar cualquier cifrado débil dentro de ONTAP.

De forma predeterminada, SSL en ONTAP se establece con la conformidad FIPS desactivada y con los siguientes protocolos TLS activados:

- TLSv1,3 (a partir de ONTAP 9.11.1)
- TLSv1.2

Las versiones anteriores de ONTAP tenían activados de forma predeterminada los siguientes protocolos TLS:

- TLSv1,1 (deshabilitado de forma predeterminada a partir de ONTAP 9.12.1)
- TLSv1 (deshabilitado de forma predeterminada a partir de ONTAP 9,8)

Cuando el modo SSL FIPS está activado, la comunicación SSL desde ONTAP a componentes de cliente o servidor externos a ONTAP utilizará cifrado compatible con FIPS para SSL.

Si desea que las cuentas de administrador accedan a SVM con una clave pública SSH, debe asegurarse de que el algoritmo de clave de host sea compatible antes de habilitar el modo SSL FIPS.

Nota: la compatibilidad con el algoritmo de clave de host ha cambiado en ONTAP 9.11.1 y versiones posteriores.

Versión de ONTAP	Tipos de clave admitidos	Tipos de claves no compatibles
9.11.1 y posterior	ecdsa-sha2-nistp256	rsa-sha2-512 + rsa-sha2-256 + ssh-ed25519 + ssh-dss + ssh-rsa
9.10.1 y anteriores	ecdsa-sha2-nistp256 + ssh-ed25519	ssh-dss + ssh-rsa

Las cuentas de clave pública SSH existentes sin los algoritmos de clave admitidos deben volver a configurarse con un tipo de clave compatible antes de habilitar FIPS o la autenticación del administrador fallará.

Para obtener más información, consulte "Habilite cuentas de clave pública de SSH".

ONTAP 9.18.1 introduce soporte para los algoritmos criptográficos post-cuánticos ML-KEM, ML-DSA y SLH-DSA para SSL, proporcionando una capa adicional de seguridad contra posibles ataques futuros de computadoras cuánticas. Estos algoritmos solo están disponibles cuandoFIPS está desactivado . Los algoritmos criptográficos post-cuánticos se negocian cuando FIPS está deshabilitado y el par los admite.

Active FIPS

Se recomienda que todos los usuarios seguros ajusten su configuración de seguridad inmediatamente después de instalar o actualizar el sistema. Cuando el modo SSL FIPS está activado, la comunicación SSL desde ONTAP a componentes de cliente o servidor externos a ONTAP utilizará cifrado compatible con FIPS para SSL.

> Cuando FIPS está habilitada, no se puede instalar ni crear un certificado con una longitud de clave RSA de 4096.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Habilitar FIPS:

   ```
   security config modify * -is-fips-enabled true
   ```

3. Cuando se le solicite continuar, introduzca `y`
4. A partir de ONTAP 9.9.1, no es necesario reiniciar. Si está ejecutando ONTAP 9.8 o una versión anterior, reinicie manualmente cada nodo del clúster uno por uno.

Ejemplo

Si está ejecutando ONTAP 9.9.1 o posterior, no verá el mensaje de advertencia.

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Obtenga más información sobre `security config modify` la configuración del modo FIPS SSL en el "Referencia de comandos del ONTAP".

Desactive FIPS

A partir de ONTAP 9.18.1, SSL en ONTAP admite los algoritmos criptográficos de computación post-cuántica ML-KEM, ML-DSA y SLH-DSA. Estos algoritmos solo están disponibles cuando FIPS está deshabilitado y el par los admite.

Pasos

1. Cambie al nivel de privilegio avanzado:

   ```
   set -privilege advanced
   ```

2. Para deshabilitar FIPS, escriba:

   ```
   security config modify -is-fips-enabled false
   ```

3. Cuando se le solicite continuar, introduzca `y`.
4. A partir de ONTAP 9.9.1, no es necesario reiniciar. Si está ejecutando ONTAP 9.8 o una versión anterior, reinicie manualmente cada nodo del clúster.

Si necesita utilizar el protocolo SSLv3, debe deshabilitar FIPS siguiendo el procedimiento anterior. SSLv3 solo se puede habilitar cuando FIPS está deshabilitado.

Puedes habilitar SSLv3 con el siguiente comando. Si está ejecutando ONTAP 9.9.1 o posterior, no verá el mensaje de advertencia.

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

Ver el estado de cumplimiento de normativas FIPS

Puede ver si el clúster completo está ejecutando las opciones de configuración de seguridad actuales.

Pasos

1. Si está ejecutando ONTAP 9.8 o una versión anterior, reinicie manualmente cada nodo del clúster uno por uno.
2. Ver el estado de cumplimiento actual:

   ```
   security config show
   ```

```
cluster1::> security config show
Cluster    Supported
FIPS Mode  Protocols Supported Cipher Suites
---------- ---------
-----------------------------------------------------------
false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
TLS_RSA_WITH_AES_128_CCM_8,
           TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                     TLS_RSA_WITH_AES_128_CBC_SHA,
                     TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_256_CCM,
                     TLS_RSA_WITH_AES_256_CCM_8,
                     ...
```

Obtenga más información sobre `security config show` en el "Referencia de comandos del ONTAP".

Información relacionada

- "FIPS 203: Estándar de mecanismo de encapsulación de claves basado en retícula modular (ML-KEM)"
- "FIPS 204: Estándar de firma digital basado en retícula modular (ML-DSA)"
- "FIPS 205: Estándar de firma digital sin estado basada en hash (SLH-DSA)"

Configurar el cifrado en tiempo real de IPsec

Prepárese para usar la seguridad IP en la red ONTAP

A partir de ONTAP 9.8, tiene la opción de usar la seguridad IP (IPsec) para proteger el tráfico de red. IPSec es una de las diversas opciones de cifrado de datos en movimiento o en tránsito disponibles con ONTAP. Debe prepararse para configurar IPsec antes de utilizarlo en un entorno de producción.

Implementación de seguridad IP en ONTAP

IPSec es un estándar de Internet mantenido por el IETF. Proporciona cifrado e integridad de datos, así como autenticación para el tráfico que fluye entre los extremos de red a nivel de IP.

Con ONTAP, IPsec protege todo el tráfico IP entre ONTAP y los distintos clientes, incluidos los protocolos NFS, SMB e iSCSI. Además de la privacidad y la integridad de los datos, el tráfico de red está protegido contra varios ataques, como los ataques de repetición y de intermediario. ONTAP utiliza la implantación del modo de transporte IPsec. Aprovecha la versión 2 del protocolo de intercambio de claves de Internet (IKE) para negociar el material clave entre ONTAP y los clientes utilizando IPv4 o IPv6.

Cuando la funcionalidad IPsec está habilitada en un cluster, la red necesita una o más entradas en la base de datos de políticas de seguridad de ONTAP (SPD) que coincidan con las distintas características del tráfico. Estas entradas se asignan a los detalles de protección específicos necesarios para procesar y enviar los datos (por ejemplo, conjunto de cifrado y método de autenticación). También es necesario introducir el SPD correspondiente en cada cliente.

Para ciertos tipos de tráfico, es preferible otra opción de cifrado de datos en movimiento. Por ejemplo, para el

cifrado del tráfico de interconexión de clústeres y NetApp SnapMirror, por lo general se recomienda el protocolo de seguridad de la capa de transporte (TLS) en lugar de IPsec. Esto se debe a que TLS ofrece un mejor rendimiento en la mayoría de las situaciones.

Información relacionada

- "Grupo de trabajo de ingeniería de Internet (IETF)"
- "RFC 4301: Arquitectura de seguridad para el protocolo de Internet"

Evolución de la implementación de ONTAP IPsec

IPsec se introdujo por primera vez en ONTAP 9.8. Su implementación ha seguido evolucionando en versiones posteriores de ONTAP , como se describe a continuación.

ONTAP 9.18.1

La compatibilidad con la descarga de hardware de IPsec se extiende al tráfico IPv6.

ONTAP 9.17.1

El soporte para la descarga de hardware IPsec se extiende a "grupos de agregación de enlaces" . "Claves precompartidas poscuánticas (PPK)" Son compatibles con la autenticación de claves precompartidas (PSK) de IPsec.

ONTAP 9.16.1

Varias de las operaciones criptográficas, como el cifrado y las comprobaciones de integridad, se pueden descargar en una tarjeta NIC admitida. Consulte Función de descarga de hardware IPSec para obtener más información.

ONTAP 9.12.1

La compatibilidad con el protocolo de host de interfaz IPSec está disponible en configuraciones FAS MetroCluster y MetroCluster IP. La compatibilidad de IPsec que se proporciona con los clústeres de MetroCluster se limita al tráfico del host de interfaz de usuario y no es compatible con las LIF de interconexión de clústeres de MetroCluster.

ONTAP 9.10.1

Se pueden usar certificados para la autenticación IPsec, además de las claves de acceso predefinido (PSK). Antes de ONTAP 9.10.1, solo se admitían las PSK para la autenticación.

ONTAP 9.9.1

Los algoritmos de cifrado utilizados por IPsec son validados por FIPS 140-2. Estos algoritmos son procesados por el módulo criptográfico de NetApp en ONTAP, que lleva la validación FIPS 140-2.

ONTAP 9,8

La compatibilidad con IPsec está disponible inicialmente en función de la implementación del modo de transporte.

Función de descarga de hardware IPSec

Si utiliza ONTAP 9.16,1 o posterior, tiene la opción de descargar ciertas operaciones de uso intensivo computacional, como el cifrado y las comprobaciones de integridad, a una tarjeta de controladora de interfaz de red (NIC) instalada en el nodo de almacenamiento. El rendimiento de las operaciones descargadas en la tarjeta NIC es aproximadamente del 5% o menos. Esto puede mejorar significativamente el rendimiento y el rendimiento del tráfico de red protegido por IPsec.

Requisitos y recomendaciones

Hay varios requisitos que debe tener en cuenta antes de utilizar la función de descarga de hardware IPsec.

Tarjetas Ethernet compatibles

Debe instalar y usar únicamente tarjetas Ethernet compatibles. Las siguientes tarjetas Ethernet son compatibles a partir de ONTAP 9.16.1:

- X50131A (controladora Ethernet 2P, 40G/100g/200g/400G)
- X60132A (controlador Ethernet 4p, 10G/25G)

ONTAP 9.17.1 agrega soporte para las siguientes tarjetas Ethernet:

- X50135A (controlador Ethernet 2p, 40G/100G)
- X60135A (controlador Ethernet 2p, 40G/100G)

Las tarjetas X50131A y X50135A son compatibles con las siguientes plataformas:

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

Las tarjetas X60132A y X60135A son compatibles con las siguientes plataformas:

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

Ver el "NetApp Hardware Universe" para obtener más información sobre las plataformas y tarjetas compatibles.

Ámbito del clúster

La función de descarga de hardware IPsec se configura globalmente para el cluster. Así que, por ejemplo, el comando `security ipsec config` se aplica a todos los nodos del clúster.

Configuración consistente

Las tarjetas NIC admitidas deben instalarse en todos los nodos del clúster. Si solo hay disponible una tarjeta NIC compatible en algunos de los nodos, puede ver una degradación del rendimiento significativa tras una conmutación al nodo de respaldo si algunas de las LIF no están alojadas en una NIC compatible con la descarga.

Desactive la reproducción anti-repetición

Debe desactivar la protección antireproducción IPsec en ONTAP (configuración predeterminada) y los clientes

IPsec. Si no está desactivada, la fragmentación y la multiruta (ruta redundante) no serán compatibles.

Si la configuración de IPsec de ONTAP se ha cambiado de la predeterminada para activar la protección contra la reproducción, utilice este comando para desactivarla:

```
security ipsec config modify -replay-window 0
```

Debe asegurarse de que la protección contra la reproducción IPsec está desactivada en el cliente. Consulte la documentación IPsec de su cliente para desactivar la protección contra la reproducción.

Limitaciones

Hay varias limitaciones que debe considerar antes de usar la función de descarga de hardware IPsec.

IPv6

A partir de ONTAP 9.18.1, se admite IPv6 para la función de descarga de hardware IPsec. Antes de ONTAP 9.18.1, la descarga de hardware de IPsec no admite IPv6.

Núm.s de secuencia ampliados

Los números de secuencia extendida IPsec no son compatibles con la función de descarga de hardware. Solo se utilizan los números de secuencia normales de 32 bits.

Agregación de enlaces

A partir de ONTAP 9.17.1, puede utilizar la función de descarga de hardware de IPsec con un "grupo de agregación de enlaces" .

Antes de la versión 9.17.1, la función de descarga de hardware de IPsec no admitía la agregación de enlaces. No se puede utilizar con una interfaz o un grupo de agregación de enlaces administrados a través de `network port ifgrp` comandos en la CLI de ONTAP .

Compatibilidad con la configuración de la interfaz de línea de comandos de ONTAP

Tres comandos CLI existentes se actualizan en ONTAP 9.16,1 para admitir la función de descarga de hardware IPsec como se describe a continuación. Consulte también "Configure la seguridad IP en ONTAP"para obtener más información.

Comando ONTAP	Actualizar
`security ipsec config show`	El parámetro booleano `Offload Enabled` muestra el estado actual de descarga de NIC.
`security ipsec config modify`	El parámetro `is-offload-enabled` se puede utilizar para activar o desactivar la función de descarga de NIC.
`security ipsec config show-ipsecsa`	Se han agregado cuatro contadores nuevos para mostrar el tráfico entrante y saliente en bytes y paquetes.

Soporte de configuración en la API de REST DE ONTAP

Dos extremos de API REST existentes se actualizan en ONTAP 9.16,1 para admitir la función de descarga de hardware IPsec como se describe a continuación.

Extremo de REST	Actualizar
`/api/security/ipsec`	El parámetro `offload_enabled` se ha agregado y está disponible con el método de PARCHE.
`/api/security/ipsec/security_association`	Se han agregado dos nuevos valores de contador para realizar un seguimiento del total de bytes y paquetes procesados por la función de descarga.

Obtenga más información sobre la API de REST DE ONTAP, incluida "Novedades de la API de REST DE ONTAP", en la documentación de automatización de ONTAP. También debe revisar la documentación de automatización de ONTAP para obtener detalles sobre "Puntos finales IPSec".

Información relacionada

- "seguridad ipsec"

Configure la seguridad IP para la red ONTAP

Hay varias tareas que debe realizar para configurar y activar el cifrado en tiempo real de IPsec en el clúster de ONTAP.

> Asegúrese de revisar "Prepárese para usar la seguridad IP" antes de configurar IPsec. Por ejemplo, es posible que deba decidir si desea utilizar la función de descarga de hardware IPsec disponible a partir de ONTAP 9.16,1.

Habilite IPsec en el clúster

Puede habilitar IPsec en el clúster para garantizar que los datos se cifran continuamente y estén seguros mientras están en tránsito.

Pasos

1. Detectar si IPsec está activada:

   ```
   security ipsec config show
   ```

   Si el resultado incluye `IPsec Enabled: false`, continúe con el siguiente paso.

2. Habilitar IPsec:

   ```
   security ipsec config modify -is-enabled true
   ```

   Puede activar la función de descarga de hardware IPsec mediante el parámetro booleano `is-offload-enabled`.

3. Vuelva a ejecutar el comando Discovery:

   ```
   security ipsec config show
   ```

   El resultado ahora incluye `IPsec Enabled: true`.

Prepárese para la creación de directivas IPsec con autenticación de certificados

Puede omitir este paso si solo utiliza claves precompartidas (PSKs) para la autenticación y no utilizará la autenticación de certificados.

Antes de crear una política IPsec que utilice certificados para la autenticación, debe verificar que se cumplan los siguientes requisitos previos:

- Tanto ONTAP como el cliente deben tener instalado el certificado CA de la otra parte para que los certificados de la entidad final (ya sea ONTAP o el cliente) sean verificables por ambas partes
- Se instala un certificado para el LIF de ONTAP que participa en la política

> Las LIF de ONTAP pueden compartir certificados. No es necesario realizar una asignación de uno a uno entre certificados y LIF.

Pasos

1. Instale todos los certificados de CA utilizados durante la autenticación mutua, incluidas las CA de ONTAP y del lado del cliente, en la gestión de certificados de ONTAP a menos que ya esté instalado (como es el caso de una CA raíz autofirmado de ONTAP).

   Comando de muestra
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. Para asegurarse de que la CA instalada se encuentra dentro de la ruta de búsqueda de la CA IPsec durante la autenticación, agregue las CA de gestión de certificados ONTAP al módulo IPsec mediante el `security ipsec ca-certificate add` comando.

   Comando de muestra
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. Cree e instale un certificado para que lo utilice la LIF de ONTAP. La entidad emisora de certificados de este certificado ya debe estar instalada en ONTAP y agregada a IPsec.

   Comando de muestra
   ```
   cluster::> security certificate install -vserver svm_name -type server -cert
   -name my_nfs_server_cert
   ```

Para obtener más información acerca de los certificados en ONTAP, consulte los comandos de certificado de seguridad en la documentación de ONTAP 9.

Definir la base de datos de directivas de seguridad (SPD)

IPSec requiere una entrada SPD antes de permitir que el tráfico fluya por la red. Esto es cierto tanto si está utilizando un PSK como un certificado para la autenticación.

Pasos

1. Utilice `security ipsec policy create` el comando para:
   a. Seleccione la dirección IP de ONTAP o la subred de direcciones IP para participar en el transporte IPsec.

b. Seleccione las direcciones IP del cliente que se conectarán a las direcciones IP de ONTAP.

> El cliente debe admitir la versión 2 de Exchange de claves de Internet (IKEv2) con una clave compartida previamente (PSK).

c. Opcionalmente, seleccione los parámetros de tráfico detallados, como los protocolos de capa superior (UDP, TCP, ICMP, etc.), los números de puerto local y los números de puerto remoto para proteger el tráfico. Los parámetros correspondientes son `protocols` , `local-ports` y `remote-ports` respectivamente.

   Omita este paso para proteger todo el tráfico entre la dirección IP de ONTAP y la dirección IP del cliente. La protección de todo el tráfico es la opción predeterminada.

d. Introduzca PSK o la infraestructura de clave pública (PKI) para el `auth-method` parámetro del método de autenticación deseado.

   i. Si introduce un PSK, incluya los parámetros y, a continuación, pulse <enter> para que el mensaje introduzca y verifique la clave precompartida.

   > Los `local-identity` parámetros y `remote-identity` son opcionales si tanto el host como el cliente utilizan strongSwan y no se ha seleccionado ninguna política de comodín para el host o el cliente.

   ii. Si introduce un PKI, también debe introducir los `cert-name` `local-identity` `remote-identity` parámetros , ,. Si la identidad del certificado del lado remoto es desconocida o si se esperan varias identidades de cliente, introduzca la identidad especial `ANYTHING` .

e. A partir de ONTAP 9.17.1, ingrese opcionalmente una identidad de clave precompartida (PPK) postcuántica con la `ppk-identity` Parámetro. Las PPK ofrecen una capa adicional de seguridad contra posibles ataques futuros de computadoras cuánticas. Al ingresar una identidad PPK, se le solicitará que ingrese el secreto PPK. Las PPK solo son compatibles con la autenticación PSK.

Obtenga más información sobre `security ipsec policy create` en el "Referencia de comandos del ONTAP" .

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

El tráfico IP no puede fluir entre el cliente y el servidor hasta que ONTAP y el cliente hayan configurado las directivas IPsec coincidentes y las credenciales de autenticación (PSK o certificado) estén en su lugar en ambos lados.

Usar identidades IPsec

Para el método de autenticación de clave precompartida, las identidades locales y remotas son opcionales si tanto el host como el cliente utilizan strongSwan y no se selecciona ninguna política de comodín para el host o el cliente.

Para el método de autenticación PKI/certificado, las identidades locales y remotas son obligatorias. Las identidades especifican qué identidad está certificada dentro del certificado de cada lado y se utilizan en el proceso de verificación. Si la identidad remota es desconocida o si podría ser muchas identidades diferentes, utilice la identidad especial `ANYTHING` .

Acerca de esta tarea

En ONTAP, las identidades se especifican modificando la entrada SPD o durante la creación de la política SPD. El SPD puede ser una dirección IP o un nombre de identidad con formato de cadena.

Pasos

1. Utilice el siguiente comando para modificar una configuración de identidad SPD existente:

```
security ipsec policy modify
```

Comando de ejemplo

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

Configuración de varios clientes IPSec

Cuando un pequeño número de clientes necesitan aprovechar IPsec, es suficiente utilizar una sola entrada SPD para cada cliente. Sin embargo, cuando cientos o incluso miles de clientes necesitan aprovechar IPsec, NetApp recomienda el uso de una configuración de varios clientes IPsec.

Acerca de esta tarea

ONTAP admite la conexión de varios clientes a través de varias redes a una única dirección IP de SVM con IPsec habilitada. Para ello, utilice uno de los siguientes métodos:

- **Configuración de subred**

  Para permitir que todos los clientes de una subred determinada (por ejemplo, 192.168.134.0/24) se conecten a una única dirección IP de SVM mediante una única entrada de política SPD, debe especificar el `remote-ip-subnets` formato de subred. Además, debe especificar el `remote-identity` campo con la identidad del lado del cliente correcta.

  > Al utilizar una sola entrada de directiva en una configuración de subred, los clientes IPsec de esa subred comparten la identidad IPsec y la clave precompartida (PSK). Sin embargo, esto no es cierto con la autenticación de certificado. Cuando se utilizan certificados, cada cliente puede utilizar su propio certificado único o un certificado compartido para autenticarse. IPsec de ONTAP comprueba la validez del certificado en función de las CA instaladas en el almacén de confianza local. ONTAP también admite la comprobación de la lista de revocación de certificados (CRL).

- **Permitir la configuración de todos los clientes**

  Para permitir que cualquier cliente, independientemente de su dirección IP de origen, se conecte a la dirección IP habilitada para IPsec de SVM, utilice el `0.0.0.0/0` comodín al especificar el `remote-ip-`

`subnets` campo.

Además, debe especificar el `remote-identity` campo con la identidad del lado del cliente correcta. Para la autenticación del certificado, puede introducir `ANYTHING`.

Además, cuando `0.0.0.0/0` se utiliza el comodín, debe configurar un número de puerto local o remoto específico para utilizarlo. Por ejemplo, `NFS port 2049`.

Pasos

a. Utilice uno de los siguientes comandos para configurar IPsec para varios clientes.

   i. Si está utilizando **configuración de subred** para admitir varios clientes IPsec:

   ```
   security ipsec policy create -vserver vserver_name -name policy_name
   -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
   IP_address/subnet -local-identity local_id -remote-identity remote_id
   ```

Comando de ejemplo

```
security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
ontap_side_identity -remote-identity client_side_identity
```

   i. Si está utilizando **Permitir que todos los clientes configuren** para admitir múltiples clientes IPsec:

   ```
   security ipsec policy create -vserver vserver_name -name policy_name
   -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
   -ports port_number -local-identity local_id -remote-identity remote_id
   ```

Comando de ejemplo

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

Mostrar estadísticas de IPsec

A través de la negociación, se puede establecer un canal de seguridad denominado Asociación de seguridad IKE (SA) entre la dirección IP de la SVM de ONTAP y la dirección IP del cliente. Las unidades SAS IPSec se instalan en ambos extremos para que funcionen el cifrado y descifrado de datos. Puede utilizar comandos de estadísticas para comprobar el estado de las unidades SAS IPsec y SAS IKE.

> Si está utilizando la función de descarga de hardware IPsec, se muestran varios contadores nuevos con el comando `security ipsec config show-ipsecsa`.

Comandos de ejemplo

Comando de ejemplo IKE SA:

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

Ejemplo de comando SA IPSec y salida:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

Ejemplo de comando SA IPSec y salida:

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

Información relacionada

- "instalación del certificado de seguridad"
- "seguridad ipsec"

Configurar el cifrado de red del clúster backend de ONTAP

A partir de ONTAP 9.18.1, puede configurar el cifrado de seguridad de la capa de transporte (TLS) para los datos en tránsito en la red del clúster de backend. Este cifrado protege los datos de los clientes almacenados en ONTAP cuando se transmiten entre nodos ONTAP en la red del clúster de backend.

Acerca de esta tarea

- El cifrado de red del clúster de backend está desactivado por defecto.
- Cuando el cifrado de la red del clúster de backend está habilitado, todos los datos del cliente almacenados en ONTAP se cifran cuando se transmiten entre los nodos ONTAP en la red del clúster de backend. Parte del tráfico de red del clúster, como los datos de la ruta de control, no está cifrado.
- Por defecto, el cifrado de la red del clúster de backend utilizará certificados autogenerados para cada nodo del clúster. PuedeGestionar certificados de cifrado de red de clúster en cada nodo se utilizará un certificado instalado personalizado.

Antes de empezar

- Debes ser administrador de ONTAP en el `admin` Nivel de privilegios para realizar las siguientes tareas.
- Todos los nodos del clúster deben estar ejecutando ONTAP 9.18.1 o posterior para habilitar el cifrado de red del clúster de backend.

Habilitar o deshabilitar el cifrado para la comunicación de red del clúster

Pasos

1. Consulte el estado actual del cifrado de la red del clúster:

   ```
   security cluster-network show
   ```

   Este comando muestra el estado actual del cifrado de la red del clúster:

   ```
   Cluster-1::*> security cluster-network show

   Enabled: true

   Mode: tls

   Status: READY
   ```

2. Habilitar o deshabilitar el cifrado de red del clúster de backend TLS:

   ```
   security cluster-network modify -enabled <true|false>
   ```

   Este comando habilita o deshabilita la comunicación cifrada para los datos de clientes en tránsito en la red del clúster de backend.

Gestionar certificados de cifrado de red de clúster

1. Consulte la información actual del certificado de cifrado de la red del clúster:

   ```
   security cluster-network certificate show
   ```

   Este comando muestra la información actual del certificado de cifrado de la red del clúster:

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

Se muestran el certificado y el nombre de la autoridad certificadora (CA) para cada nodo del clúster.

2. Modificar el certificado de cifrado de red del clúster para un nodo:

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

Este comando modifica el certificado de cifrado de red del clúster para un nodo específico. El certificado debe estar instalado y firmado por una CA instalada antes de ejecutar este comando. Para obtener más información sobre la gestión de certificados, consulte"Gestione certificados de ONTAP con System Manager" . Si `-name` Si no se especifica, se utiliza el certificado predeterminado generado automáticamente.

Configure políticas del firewall para las LIF en la red de ONTAP

La configuración de un firewall mejora la seguridad del clúster y ayuda a evitar el acceso no autorizado al sistema de almacenamiento. De forma predeterminada, el firewall incorporado está configurado para permitir el acceso remoto a un conjunto específico de servicios IP para LIF de datos, gestión e interconexión de clústeres.

A partir de ONTAP 9,10.1:

- Las políticas de firewall quedan obsoletas y se reemplazan por las políticas de servicio de LIF. Anteriormente, el firewall incorporado se gestionaba mediante directivas de firewall. Esta funcionalidad ahora se logra usando una política de servicio de LIF.
- Todas las políticas de firewall están vacías y no abren ningún puerto en el firewall subyacente. En su lugar, se deben abrir todos los puertos con una política de servicio de LIF.
- No es necesario realizar ninguna acción después de una actualización a la versión 9.10.1 o posterior para pasar de políticas de firewall a políticas de servicio de LIF. El sistema crea automáticamente políticas de servicio de LIF coherentes con las políticas de firewall que se están usando en la versión anterior de ONTAP. Si utiliza scripts u otras herramientas que crean y gestionan políticas de firewall personalizadas, es posible que deba actualizar dichas secuencias de comandos para crear políticas de servicio personalizadas en su lugar.

Para obtener más información, consulte "LIF y políticas de servicio en ONTAP 9.6 y posteriores".

Las políticas de firewall se pueden utilizar para controlar el acceso a protocolos de servicio de gestión como SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS O SNMP. No se pueden establecer políticas de firewall para protocolos de datos como NFS o SMB.

Puede administrar el servicio y las políticas de firewall de las siguientes maneras:

- Activación o desactivación del servicio de firewall
- Mostrar la configuración actual del servicio de firewall
- Creación de una nueva directiva de firewall con el nombre de directiva y los servicios de red especificados
- Aplicar una política de firewall a una interfaz lógica
- Crear una nueva directiva de firewall que sea una copia exacta de una directiva existente

  Puede usar esto para realizar una política con características similares dentro de la misma SVM o para copiar la política en una SVM diferente.

- Mostrar información acerca de las directivas de firewall
- Modificar las direcciones IP y las máscaras de red que utiliza una directiva de firewall
- Eliminar una política de firewall que no esté en uso en una LIF

Políticas de firewall y LIF

Las políticas de firewall de LIF se utilizan para restringir el acceso al clúster en cada LIF. Debe entender cómo afecta la política de firewall predeterminada al acceso del sistema sobre cada tipo de LIF y cómo puede personalizar una política de firewall para aumentar o reducir la seguridad de una LIF.

Cuando se configura una LIF mediante `network interface create` `network interface modify` el comando o, el valor especificado para `-firewall-policy` el parámetro determina los protocolos de servicio y las direcciones IP que permiten acceder a la LIF. Obtenga más información sobre `network interface` en el "Referencia de comandos del ONTAP".

En muchos casos puede aceptar el valor predeterminado de la política de firewall. En otros casos, es posible que deba restringir el acceso a determinadas direcciones IP y ciertos protocolos de servicio de gestión. Los protocolos de servicio de gestión disponibles incluyen SSH, HTTP, HTTPS, Telnet, NTP, NDMP, NDMPS, RSH, DNS Y SNMP.

La política de firewall para todas las LIF de clúster se establece de forma predeterminada en `""` y no se puede modificar.

En la siguiente tabla se describen las políticas de firewall predeterminadas que se asignan a cada LIF, en función de su rol (ONTAP 9.5 y versiones anteriores) o política de servicio (ONTAP 9.6 y versiones posteriores), al crear la LIF:

Política de firewall	Protocolos de servicio predeterminados	Acceso predeterminado	LIF aplicadas a.
gestión	dns, http, https, ndmp, ndmps, ntp, snmp, ssh	Cualquier dirección (0.0.0.0/0)	Gestión de clústeres, gestión de SVM y LIF de gestión de nodos

gestión de nfs	dns, http, https, ndmp, ndmps, ntp, portmap, snmp, ssh	Cualquier dirección (0.0.0.0/0)	LIF de datos que también admiten el acceso a la gestión de la SVM
interconexión de clústeres	https, ndmp, ndmps	Cualquier dirección (0.0.0.0/0)	Todas las LIF de interconexión de clústeres
los datos	dns, ndmp, ndmps, portmap	Cualquier dirección (0.0.0.0/0)	Todos los LIF de datos

Configuración del servicio portmap

El servicio portmap asigna los servicios RPC a los puertos en los que escuchan.

El servicio portmap siempre se pudo acceder en ONTAP 9.3 y versiones anteriores, se pasó a configurar en ONTAP 9.4 a través de ONTAP 9.6 y se gestiona automáticamente empezando por ONTAP 9.7.

- En ONTAP 9.3 y anteriores, siempre se pudo acceder al servicio portmap (rpcbind) en el puerto 111 en configuraciones de red que dependían del firewall integrado de ONTAP en lugar de un firewall de terceros.
- Desde ONTAP 9.4 a ONTAP 9.6, puede modificar las políticas de firewall para controlar si el servicio portmap es accesible en determinadas LIF.
- A partir de ONTAP 9.7, se elimina el servicio de firewall de portmap. En su lugar, el puerto portmap se abre automáticamente para todos los LIF que admiten el servicio NFS.

El servicio Portmap se puede configurar en el firewall de ONTAP 9.4 a ONTAP 9.6.

En el resto de este tema se describe cómo configurar el servicio de firewall de portmap para versiones de ONTAP 9.4 a ONTAP 9.6.

En función de la configuración, es posible que no permita el acceso al servicio en tipos específicos de LIF, que suelen ser de gestión y LIF entre clústeres. En algunas circunstancias, puede que incluso no permita el acceso en las LIF de datos.

Qué comportamiento se puede esperar

El comportamiento de ONTAP 9.4 a ONTAP 9.6 está diseñado para proporcionar una transición fluida durante la actualización. Si ya se está accediendo al servicio portmap a través de tipos específicos de LIF, continuará siendo accesible mediante estos tipos de LIF. Al igual que en ONTAP 9,3 y versiones anteriores, puede especificar los servicios a los que se puede acceder dentro del firewall en la política de firewall para el tipo de LIF.

Para que el comportamiento surta efecto, todos los nodos del clúster deben ejecutar de ONTAP 9.4 a ONTAP 9.6. Sólo se ve afectado el tráfico entrante.

Las nuevas reglas son las siguientes:

- Tras la actualización al lanzamiento del 9.4 al 9.6, ONTAP agrega el servicio portmap a todas las políticas de firewall existentes, predeterminadas o personalizadas.
- Cuando crea un nuevo clúster o un nuevo espacio IP, ONTAP agrega el servicio portmap solo a la política de datos predeterminada, no a las políticas de gestión o interconexión de clústeres predeterminadas.
- Puede agregar el servicio portmap a las políticas predeterminadas o personalizadas según sea necesario y eliminar el servicio según sea necesario.

Cómo agregar o quitar el servicio portmap

Para agregar el servicio portmap a una política de firewall de SVM o clúster (hacer que sea accesible dentro del firewall), introduzca:

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Para quitar el servicio portmap de una política de firewall de SVM o clúster (hacer que sea inaccesible dentro del firewall), introduzca:

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

Puede usar el comando network interface modify para aplicar la política del firewall a una LIF existente. Obtenga más información sobre los comandos descritos en este procedimiento en el "Referencia de comandos del ONTAP".

Cree una política de firewall y asígnela a una LIF

Las políticas de firewall predeterminadas se asignan a cada LIF al crear la LIF. En muchos casos, la configuración predeterminada del firewall funciona bien y no es necesario modificarla. Si desea cambiar los servicios de red o las direcciones IP que pueden acceder a una LIF, puede crear una política de firewall personalizada y asignarla a la LIF.

Acerca de esta tarea

- No puede crear una política de firewall con el `policy` nombre `data`, , `intercluster`, , `cluster`o `mgmt`.

  Estos valores se reservan para las políticas de firewall definidas por el sistema.

- No puede establecer ni modificar una política de firewall para las LIF del clúster.

  La política de firewall para las LIF del clúster se establece en 0.0.0.0/0 para todos los tipos de servicios.

- Si necesita quitar un servicio de una política, debe eliminar la política de firewall existente y crear una nueva.
- Si IPv6 está habilitado en el clúster, puede crear políticas de firewall con direcciones IPv6.

  Después de activar IPv6, `data`, `intercluster` y `mgmt` las políticas de firewall incluyen ::/0, el comodín IPv6, en su lista de direcciones aceptadas.

- Cuando se usa System Manager para configurar la funcionalidad de protección de datos en todos los clústeres, se debe asegurarse de que las direcciones IP de LIF entre clústeres estén incluidas en la lista permitida y que el servicio HTTPS esté en las LIF entre clústeres y en los firewalls de propiedad de la empresa.

  De forma predeterminada, la `intercluster` política de firewall permite el acceso desde todas las direcciones IP (0,0.0,0/0, o ::/0 para IPv6) y habilita los servicios HTTPS, NDMP y NDMPS. Si modifica esta política predeterminada o crea su propia política de firewall para las LIF de interconexión de clústeres, debe añadir cada dirección IP de la LIF entre clústeres a la lista permitida y habilitar el servicio HTTPS.

- A partir de ONTAP 9.6, los servicios de firewall HTTPS y SSH no son compatibles.

En ONTAP 9.6, los `management-https` `management-ssh` servicios LIF y están disponibles para el acceso de gestión HTTPS y SSH.

Pasos

1. Cree una política de firewall que estará disponible para las LIF en una SVM específica:

   `system services firewall policy create -vserver` *`vserver_name`* `-policy` *`policy_name`* `-service` *`network_service`* `-allow-list` *`ip_address/mask`*

   Puede usar este comando varias veces para agregar más de un servicio de red y una lista de direcciones IP permitidas para cada servicio de la directiva de firewall.

2. Compruebe que la política se ha agregado correctamente mediante `system services firewall policy show` el comando.
3. Aplique la política de firewall a una LIF:

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. Compruebe que la política se ha agregado correctamente a la LIF mediante `network interface show -fields firewall-policy` el comando.

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

Ejemplo de creación de una política de firewall y asignación de ella a una LIF

El siguiente comando crea una política de firewall llamada data_http que permite el acceso al protocolo HTTP y HTTPS desde direcciones IP de la subred 10.10, aplica esa política a la LIF llamada data1 en la SVM vs1 y, a continuación, muestra todas las políticas de firewall del clúster:

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

Comandos de ONTAP para gestionar el servicio y las políticas del firewall

Puede utilizar `system services firewall` los comandos para gestionar el servicio de firewall, los `system services firewall policy` comandos para administrar las políticas de firewall y `network interface modify` el comando para gestionar la configuración del firewall para las LIF.

A partir de ONTAP 9,10.1:

- Las políticas de firewall quedan obsoletas y se reemplazan por las políticas de servicio de LIF. Anteriormente, el firewall incorporado se gestionaba mediante directivas de firewall. Esta funcionalidad ahora se logra usando una política de servicio de LIF.
- Todas las políticas de firewall están vacías y no abren ningún puerto en el firewall subyacente. En su lugar, se deben abrir todos los puertos con una política de servicio de LIF.
- No es necesario realizar ninguna acción después de una actualización a la versión 9.10.1 o posterior para pasar de políticas de firewall a políticas de servicio de LIF. El sistema crea automáticamente políticas de servicio de LIF coherentes con las políticas de firewall que se están usando en la versión anterior de ONTAP. Si utiliza scripts u otras herramientas que crean y gestionan políticas de firewall personalizadas, es posible que deba actualizar dichas secuencias de comandos para crear políticas de servicio personalizadas en su lugar.

Para obtener más información, consulte "LIF y políticas de servicio en ONTAP 9.6 y posteriores".

Si desea…	Se usa este comando…
Active o desactive el servicio de firewall	`system services firewall modify`
Muestra la configuración actual del servicio de firewall	`system services firewall show`
Cree una política de firewall o agregue un servicio a una política de firewall existente	`system services firewall policy create`
Aplique una política de firewall a una LIF	`network interface modify -lif lifname -firewall-policy`
Modifique las direcciones IP y las máscaras de red asociadas a una directiva de firewall	`system services firewall policy modify`
Mostrar información acerca de las políticas de firewall	`system services firewall policy show`
Cree una nueva directiva de firewall que sea una copia exacta de una directiva existente	`system services firewall policy clone`
Eliminar una política de firewall que no esté usando una LIF	`system services firewall policy delete`

Información relacionada

- "firewall de servicios de sistema"

- "modificación de la interfaz de red"

Marcado de QoS (solo para administradores de clústeres)

Obtenga información sobre la calidad de servicio (QoS) de la red ONTAP

La marca de calidad de servicio (QoS) de la red le ayuda a priorizar diferentes tipos de tráfico en función de las condiciones de la red para utilizar eficazmente los recursos de la red. Puede establecer el valor de punto de código de servicios diferenciados (DSCP) de los paquetes IP salientes para los tipos de tráfico admitidos por espacio IP.

Marcado DSCP para cumplimiento de UC

Puede habilitar el marcado de punto de código de servicios diferenciados (DSCP) en el tráfico de paquetes IP saliente (de salida) para un protocolo determinado con un código DSCP predeterminado o proporcionado por el usuario. El marcado DSCP es un mecanismo para clasificar y gestionar el tráfico de red y es un componente de la conformidad de Unified Capability (UC).

El marcado DSCP (también conocido como *QoS marking* o *quality of service marking*) se habilita al proporcionar un valor de espacio IP, protocolo y DSCP. Los protocolos en los que se puede aplicar la Marca DSCP son NFS, SMB, iSCSI, SnapMirror, NDMP, FTP, HTTP/HTTPS, SSH, Telnet y SNMP.

Si no se proporciona un valor DSCP al habilitar el marcado DSCP para un protocolo determinado, se utiliza un valor predeterminado:

- El valor predeterminado para el tráfico y los protocolos de datos es 0x0A (10).
- El valor predeterminado para el tráfico y los protocolos de control es 0x30 (48).

Modificar los valores de marca de QoS de la red ONTAP

Puede modificar los valores de marcado de calidad de servicio (QoS) de diferentes protocolos en cada espacio IP.

Antes de empezar

Todos los nodos del clúster deben ejecutar la misma versión de ONTAP.

Paso

Modifique los valores de marca de QoS con `network qos-marking modify` el comando.

- `–ipspace`El parámetro especifica el espacio IP para el que se va a modificar la entrada de marca QoS.
- `–protocol`El parámetro especifica el protocolo para el que se va a modificar la entrada de marca QoS.
- El `-dscp` parámetro especifica el valor de Punto de Código de Servicios Diferenciados (DSCP). Los valores posibles van de 0 a 63.
- `-is-enabled`El parámetro se utiliza para habilitar o deshabilitar la marca QoS para el protocolo especificado en el espacio IP proporcionado por `-ipspace` el parámetro.

El siguiente comando habilita el marcado de calidad de servicio del protocolo NFS en el espacio IP predeterminado:

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

El siguiente comando establece el valor de DSCP en 20 para el protocolo NFS en el espacio IP predeterminado:

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

Obtenga más información sobre `network qos-marking modify` los posibles valores del protocolo en el "Referencia de comandos del ONTAP".

Ver los valores de marca de QoS de la red ONTAP

Puede mostrar los valores de marcado de la calidad de servicio de los diferentes protocolos, en cada espacio IP.

Paso

Muestra los valores de marca de QoS con `network qos-marking show` el comando.

El siguiente comando muestra el marcado de calidad de servicio de todos los protocolos en el espacio IP predeterminado:

```
network qos-marking show -ipspace Default
IPspace              Protocol           DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                 10  false
                     FTP                  48  false
                     HTTP-admin           48  false
                     HTTP-filesrv         10  false
                     NDMP                 10  false
                     NFS                  10  true
                     SNMP                 48  false
                     SSH                  48  false
                     SnapMirror           10  false
                     Telnet               48  false
                     iSCSI                10  false
11 entries were displayed.
```

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

Gestionar SNMP (solo administradores de clústeres)

Obtenga información acerca de SNMP en la red ONTAP

Puede configurar SNMP para supervisar las SVM del clúster a fin de evitar los problemas antes de que se produzcan y responder a los problemas si se producen. La gestión de SNMP implica configurar usuarios SNMP y destinos de host de capturas de SNMP (estaciones de trabajo de gestión) para todos los eventos SNMP. SNMP está deshabilitado de forma predeterminada en las LIF de datos.

En la SVM de datos, se pueden crear y gestionar usuarios SNMP solo de lectura. Los LIF de datos deben configurarse para recibir solicitudes SNMP en la SVM.

Las estaciones de trabajo de gestión de redes SNMP, o los administradores, pueden consultar al agente SNMP de SVM para obtener información. El agente SNMP recopila información y la reenvía a los administradores SNMP. El agente SNMP también genera notificaciones de capturas siempre que se produzcan eventos específicos. El agente SNMP de la SVM tiene privilegios de solo lectura; no se puede utilizar para ninguna operación definida ni para realizar una acción correctiva en respuesta a una captura. ONTAP proporciona un agente SNMP compatible con las versiones v1, v2c y v3 de SNMP. SNMPv3 ofrece seguridad avanzada mediante passphrases y cifrado.

Para obtener más información sobre el soporte de SNMP en sistemas ONTAP, consulte "TR-4220: Compatibilidad con SNMP en Data ONTAP".

Descripción general de MIB

Un MIB (base de datos de información de gestión) es un archivo de texto que describe los objetos y las capturas SNMP.

Los MIB describen la estructura de los datos de gestión del sistema de almacenamiento y utilizan un espacio de nombres jerárquico que contiene identificadores de objeto (OIDs). Cada OID identifica una variable que se puede leer mediante SNMP.

Dado que los MIB no son archivos de configuración y ONTAP no lee estos archivos, la función SNMP no se ve afectada por los MIB. ONTAP proporciona el siguiente archivo MIB:

- Una MIB personalizada de NetApp (`netapp.mib`)

ONTAP admite MIB de IPv6 (RFC 2465), TCP (RFC 4022), UDP (RFC 4113) e ICMP (RFC 2466), que muestran datos de IPv4 e IPv6.

ONTAP también proporciona una breve referencia cruzada entre identificadores de objeto (OIDs) y nombres cortos de objetos en el `traps.dat` archivo.

> Las versiones más recientes de los archivos ONTAP MIBs y "traps.dat" están disponibles en el sitio de soporte de NetApp. Sin embargo, las versiones de estos archivos en el sitio de soporte no corresponden necesariamente a las capacidades SNMP de su versión de ONTAP. Estos archivos se proporcionan para ayudarle a evaluar las funciones SNMP en la última versión de ONTAP.

Capturas SNMP

Las capturas SNMP capturan información de supervisión del sistema que se envía como una notificación asíncrona desde el agente SNMP al administrador SNMP.

Hay tres tipos de capturas SNMP: Estándar, integrado y definido por el usuario. ONTAP no admite capturas definidas por el usuario.

Una captura se puede utilizar para comprobar periódicamente si existen umbrales o errores operativos definidos en el MIB. Si se alcanza un umbral o se detecta un fallo, el agente SNMP envía un mensaje (captura) a los hosts de capturas para alertarlos del evento.

ONTAP admite capturas de SNMPv1 y SNMPv3. ONTAP no admite capturas SNMPv2c ni informa.

Capturas SNMP estándar

Estos solapamientos se definen en RFC 1215. Hay cinco capturas SNMP estándar que son compatibles con ONTAP: Coldstart, warwStart, linkdown, linkup y authenticationFailure.

La captura de autenticación por fallo está deshabilitada de forma predeterminada. Debe utilizar `system snmp authtrap` el comando para habilitar la captura. Obtenga más información sobre `system snmp authtrap` en el "Referencia de comandos del ONTAP".

Capturas SNMP integradas

Las capturas integradas están predefinidas en ONTAP y se envían automáticamente a las estaciones de administración de red en la lista de capturas si se produce un evento. Estas capturas, como diskFailedShutdown, cpuTooBusy y volumeNearlyFull, se definen en la MIB personalizada.

Cada captura integrada se identifica mediante un código de captura único.

Cree comunidades SNMP para la red ONTAP

Es posible crear una comunidad SNMP que actúa como mecanismo de autenticación entre la estación de gestión y la máquina virtual de almacenamiento (SVM) cuando se usa SNMPv1 y SNMPv2c.

Al crear comunidades SNMP en una SVM de datos, puede ejecutar comandos, `snmpwalk` como y `snmpget` en las LIF de datos.

Acerca de esta tarea

- En las nuevas instalaciones de ONTAP, SNMPv1 y SNMPv2c se desactivan de forma predeterminada.

  Se habilitan SNMPv1 y SNMPv2c después de crear una comunidad SNMP.

- ONTAP admite comunidades de solo lectura.
- De forma predeterminada, la política de firewall de «datos» que se asigna a las LIF de datos tiene el servicio SNMP establecido en `deny`.

  Debe crear una nueva política de firewall con el servicio SNMP establecido en `allow` cuando cree un usuario SNMP para una SVM de datos.

  A partir de ONTAP 9.10.1, las políticas de firewall están obsoletas y sustituidas por completo por políticas de servicios LIF. Para obtener más información, consulte "Configurar políticas de firewall para LIF".

- Es posible crear comunidades SNMP para los usuarios de SNMPv1 y SNMPv2c para la SVM admin y la SVM de datos.
- Puesto que una SVM no forma parte del estándar SNMP, las consultas sobre LIF de datos deben incluir el OID raíz de NetApp (1,3.6,1.4,1.789), por ejemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Pasos

1. Cree una comunidad SNMP mediante `system snmp community add` el comando. El siguiente comando muestra cómo crear una comunidad SNMP en la SVM de administrador cluster-1:

```
system snmp community add -type ro -community-name comty1 -vserver
cluster-1
```

   El siguiente comando muestra cómo crear una comunidad SNMP en la SVM de datos vs1:

```
system snmp community add -type ro -community-name comty2 -vserver vs1
```

2. Verifique que se hayan creado las comunidades mediante el comando System snmp Community show.

   El siguiente comando muestra las dos comunidades creadas para SNMPv1 y SNMPv2c:

```
system snmp community show
cluster-1
rocomty1
vs1
rocomty2
```

3. Compruebe si SNMP está permitido como servicio en la política de firewall de datos mediante el `system services firewall policy show` comando.

   El siguiente comando muestra que el servicio snmp no está permitido en la política de firewall predeterminada "data" (el servicio snmp se permite únicamente en la política de firewall "mgmt"):

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. Cree una nueva política de firewall que permita el acceso mediante `snmp` `system services firewall policy create` el servicio mediante el comando.

   Los siguientes comandos crean una nueva política de firewall de datos llamada “data1” que permite el `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. Aplique la política de firewall a una LIF de datos mediante `network interface modify` el comando con el parámetro -firewall-policy.

El siguiente comando asigna la nueva política de firewall "data1" a la LIF "datalif1":

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

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

Configure SNMPv3 usuarios en un clúster de ONTAP

SNMPv3 es un protocolo seguro en comparación con SNMPv1 y SNMPv2c. Para utilizar SNMPv3, debe configurar un usuario SNMPv3 para ejecutar las utilidades SNMP desde el administrador SNMP.

Paso

Utilice el `security login create` Comando para crear un usuario SNMPv3.

Se le pedirá que introduzca la siguiente información:

- ID del motor: El valor predeterminado y recomendado es ID del motor local
- Protocolo de autenticación
- Contraseña de autenticación
- Protocolo de privacidad
- Contraseña del protocolo de privacidad

Resultado

El usuario SNMPv3 puede iniciar sesión desde el administrador SNMP mediante el nombre de usuario y la contraseña y ejecutar los comandos de la utilidad SNMP.

Parámetros de seguridad SNMPv3

SNMPv3 incluye una función de autenticación que, cuando se selecciona, requiere que los usuarios escriban sus nombres, un protocolo de autenticación, una clave de autenticación y el nivel de seguridad deseado al invocar un comando.

En la siguiente tabla se enumeran los parámetros de seguridad de SNMPv3 :

Parámetro	Opción de línea de comandos	Descripción
ID de motor	-E Ingeniería	ID de motor del agente SNMP. El valor predeterminado es EngineID local (recomendado).
SecurityName	-U Nombre	El nombre de usuario no debe superar los 32 caracteres.

Protocolo de autenticación	-A {none	MD5
SHA	SHA-256}	El tipo de autenticación puede ser none, MD5, SHA o SHA-256.
Clave de autenticación	-UNA FRASE DE PASO	Frase de contraseña con un mínimo de ocho caracteres.
Nivel de seguridad	-L {authNoprivilegios	authpriv
noAuthprivilegios}	El nivel de seguridad puede ser autenticación, sin privacidad, autenticación, privacidad o sin autenticación, Sin privacidad.	PrivProtocol
-x { none	des	aes128}
El protocolo de privacidad puede ser none, des o aes 128	PrivPassword	-X contraseña

Ejemplos de diferentes niveles de seguridad

Este ejemplo muestra cómo un usuario SNMPv3 creado con diferentes niveles de seguridad puede utilizar los comandos SNMP del lado del cliente, `snmpwalk` como , para consultar los objetos del cluster.

Para obtener un mejor rendimiento, debe recuperar todos los objetos de una tabla en lugar de un solo objeto o algunos objetos de la tabla.

Debe utilizar `snmpwalk` 5.3.1 o posterior cuando el protocolo de autenticación es SHA.

Nivel de seguridad: Authpriv

El siguiente resultado muestra la creación de un usuario SNMPv3 con el nivel de seguridad authpriv.

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Modo FIPS

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

Prueba snmpwalk

El siguiente resultado muestra al usuario SNMPv3 que ejecuta el comando snmpwalk:

Para obtener un mejor rendimiento, debe recuperar todos los objetos de una tabla en lugar de un solo objeto o algunos objetos de la tabla.

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nivel de seguridad: AuthNoprivilegios

El siguiente resultado muestra la creación de un usuario SNMPv3 con el nivel de seguridad authNoprivilegios.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

Modo FIPS

FIPS no le permite elegir **none** para el protocolo de privacidad. Como resultado, no es posible configurar un usuario authNoPriv SNMPv3 en modo FIPS.

Prueba snmpwalk

El siguiente resultado muestra al usuario SNMPv3 que ejecuta el comando snmpwalk:

Para obtener un mejor rendimiento, debe recuperar todos los objetos de una tabla en lugar de un solo objeto o algunos objetos de la tabla.

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Nivel de seguridad: NoAuthNoprivilegios

El siguiente resultado muestra la creación de un usuario SNMPv3 con el nivel de seguridad noAuthNoprivilegios.

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

Modo FIPS

FIPS no le permite elegir **none** para el protocolo de privacidad.

Prueba snmpwalk

El siguiente resultado muestra al usuario SNMPv3 que ejecuta el comando snmpwalk:

Para obtener un mejor rendimiento, debe recuperar todos los objetos de una tabla en lugar de un solo objeto o algunos objetos de la tabla.

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

Configure los hosts de capturas para SNMP en la red ONTAP

Puede configurar el host de capturas (administrador SNMP) para recibir notificaciones (PDU de captura SNMP) cuando se generan capturas SNMP en el clúster. Es posible especificar el nombre de host o la dirección IP (IPv4 o IPv6) del host de capturas de SNMP.

Antes de empezar

- Se debe habilitar SNMP y las capturas de SNMP en el clúster.

> SNMP y las capturas de SNMP se habilitan de forma predeterminada.

- El DNS debe haberse configurado en el clúster para resolver los nombres de host de capturas.
- IPv6 debe estar habilitado en el clúster para configurar los hosts de capturas de SNMP mediante direcciones IPv6.
- Al crear hosts de capturas, debe haber especificado la autenticación de un modelo de seguridad predefinido basado en el usuario (USM) y las credenciales de privacidad.

Paso

Añada un host de capturas de SNMP:

```
system snmp traphost add
```

> Las capturas solo se pueden enviar cuando se especifica al menos una estación de administración SNMP como un host de capturas.

El siguiente comando añade un nuevo host de capturas SNMPv3 llamado yyy.example.com con un usuario USM conocido:

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

El siguiente comando añade un host de capturas mediante la dirección IPv6 del host:

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

Compruebe el sondeo de SNMP en un clúster de ONTAP

Después de configurar SNMP, debe verificar que puede sondear el clúster.

Acerca de esta tarea

Para sondear un cluster, debe utilizar un comando de terceros como `snmpwalk` .

Pasos

1. Envíe un comando SNMP para sondear el clúster desde un clúster diferente.

   En el caso de los sistemas que ejecutan SNMPv1, utilice el comando de la CLI `snmpwalk -v version -c community_stringip_address_or_host_name system` para detectar el contenido de la MIB (base de información de gestión).

   En este ejemplo, la dirección IP de la LIF de administración del clúster que está sondeando es 10.11.12.123. El comando muestra la información solicitada de la MIB:

   ```
   C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

   SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
              Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
   SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
   DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
   19:47:24.48
   SNMPv1-MIB::sysContact.0 = STRING:
   SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
   SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
   SNMPv1-MIB::sysServices.0 = INTEGER: 72
   ```

   En el caso de los sistemas que ejecutan SNMPv2c, utilice el comando de la CLI `snmpwalk -v version -c community_stringip_address_or_host_name system` para detectar el contenido de la MIB (base de información de gestión).

   En este ejemplo, la dirección IP de la LIF de administración del clúster que está sondeando es 10.11.12.123. El comando muestra la información solicitada de la MIB:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

En el caso de los sistemas que ejecutan SNMPv3, utilice el comando de la CLI `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` para detectar el contenido de la MIB (base de información de gestión).

En este ejemplo, la dirección IP de la LIF de administración del clúster que está sondeando es 10.11.12.123. El comando muestra la información solicitada de la MIB:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

Comandos de ONTAP para gestionar SNMP, capturas y hosts de capturas

Es posible usar `system snmp` los comandos para gestionar SNMP, capturas y hosts de capturas. Puede usar `security` los comandos para gestionar usuarios de SNMP por SVM. Es posible usar `event` los comandos para gestionar eventos relacionados con capturas SNMP.

Comandos para configurar SNMP

Si desea…	Se usa este comando…

Habilite SNMP en el clúster	`options -option-name snmp.enable -option-value on` Se debe permitir el servicio SNMP bajo la política del firewall de gestión (gestión). Puede verificar si se permite SNMP mediante el comando system Services firewall policy show.
Deshabilite SNMP en el clúster	`options -option-name snmp.enable -option-value off`

Comandos para gestionar usuarios de SNMP v1, v2c y v3

Si desea…	Se usa este comando…
Configurar usuarios SNMP	`security login create`
Mostrar usuarios SNMP	`security snmpusers`y `security login show -application snmp`
Eliminar usuarios SNMP	`security login delete`
Modifique el nombre de rol de control de acceso de un método de inicio de sesión para los usuarios SNMP	`security login modify`

Comandos para proporcionar información de contacto y ubicación

Si desea…	Se usa este comando…
Mostrar o modificar los detalles de contacto del clúster	`system snmp contact`
Muestra o modifica los detalles de ubicación del clúster	`system snmp location`

Comandos para gestionar comunidades SNMP

Si desea…	Se usa este comando…
Añada una comunidad de solo lectura (ro) para una SVM o para todas las SVM del clúster	`system snmp community add`
Elimine una comunidad o todas las comunidades	`system snmp community delete`
Mostrar la lista de todas las comunidades	`system snmp community show`

Dado que los SVM no forman parte del estándar SNMP, las consultas sobre LIF de datos deben incluir el OID raíz de NetApp (1,3.6,1.4,1.789), por ejemplo, `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`.

Comando para mostrar valores de opciones de SNMP

Si desea…	Se usa este comando…
Mostrar los valores actuales de todas las opciones de SNMP, incluido el contacto del clúster, la ubicación de contacto, si el clúster está configurado para enviar capturas, la lista de hosts de capturas y la lista de comunidades y el tipo de control de acceso	`system snmp show`

Comandos para gestionar las capturas y los hosts de capturas de SNMP

Si desea…	Se usa este comando…
Habilite las capturas de SNMP que se envían desde el clúster	`system snmp init -init 1`
Deshabilite las capturas de SNMP enviadas desde el clúster	`system snmp init -init 0`
Añada un host de capturas que reciba notificaciones SNMP para eventos específicos en el clúster	`system snmp traphost add`
Eliminar un host de capturas	`system snmp traphost delete`
Mostrar la lista de hosts de capturas	`system snmp traphost show`

Comandos para gestionar eventos relacionados con capturas SNMP

Si desea…	Se usa este comando…
Mostrar los eventos para los que se generan capturas SNMP (integradas)	`event route show` Utilice `-snmp-support true` el parámetro para ver solo eventos relacionados con SNMP. Utilice el `instance -messagename <message>` parámetro para ver una descripción detallada del motivo por el que puede haber ocurrido un evento y cualquier acción correctiva. No se admite el enrutamiento de eventos de captura SNMP individuales a destinos de host de capturas específicos. Todos los eventos de captura SNMP se envían a todos los destinos de host de capturas.

Mostrar una lista de registros del historial de capturas SNMP, que son notificaciones de eventos que se han enviado a capturas SNMP	`event snmphistory show`
Elimine un registro del historial de capturas SNMP	`event snmphistory delete`

Información relacionada

- "snmp del sistema"
- "usuarios de seguridad"
- "seguridad"
- "evento"
- "inicio de sesión de seguridad"

Gestione el enrutamiento en una SVM

Obtenga información sobre el enrutamiento de SVM en la red ONTAP

La tabla de enrutamiento de una SVM determina la ruta de red que la SVM utiliza para comunicarse con un destino. Es importante comprender cómo funcionan las tablas de enrutamiento para evitar problemas de red antes de que ocurran.

Las reglas de enrutamiento son las siguientes:

- ONTAP enruta el tráfico por la ruta disponible más específica.
- ONTAP enruta el tráfico por una ruta de puerta de enlace predeterminada (con 0 bits de máscara de red) como último recurso, cuando no hay más rutas específicas disponibles.

En el caso de rutas con el mismo destino, máscara de red y métrica, no hay garantía de que el sistema utilice la misma ruta después de un reinicio o después de una actualización. Esto es especialmente un problema si ha configurado varias rutas predeterminadas.

Se recomienda configurar una sola ruta predeterminada para una SVM. Para evitar interrupciones, debe asegurarse de que la ruta predeterminada pueda llegar a cualquier dirección de red a la que no pueda acceder una ruta más específica. Para obtener más información, consulte"Base de conocimientos de NetApp : SU134: El acceso a la red podría verse interrumpido por una configuración de enrutamiento incorrecta en ONTAP en clúster"

Cree rutas estáticas para la red ONTAP

Puede crear rutas estáticas dentro de una máquina virtual de almacenamiento (SVM) para controlar cómo usan las LIF la red para el tráfico de salida.

Cuando se crea una entrada de ruta asociada a una SVM, todas las LIF son propiedad de la SVM especificada y que se encuentran en la misma subred que la puerta de enlace usarán.

Paso

Utilice `network route create` el comando para crear una ruta.

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

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

Habilite el enrutamiento multivía para la red ONTAP

Si varias rutas tienen la misma métrica para un destino, sólo se selecciona una de las rutas para el tráfico saliente. Esto lleva a que otras rutas no se utilicen para enviar tráfico saliente. Puede activar el enrutamiento multivía para equilibrar la carga en todas las rutas disponibles en proporción a sus métricas, en lugar del enrutamiento ECMP, que equilibra la carga entre las rutas disponibles de la misma métrica.

Pasos

1. Inicie sesión en el nivel de privilegio avanzado:

   `set -privilege advanced`

2. Habilitar enrutamiento multivía:

   `network options multipath-routing modify -is-enabled true`

   El enrutamiento multivía está habilitado para todos los nodos del clúster.

   ```
   network options multipath-routing modify -is-enabled true
   ```

   Obtenga más información sobre `network options multipath-routing modify` en el "Referencia de comandos del ONTAP".

Elimine rutas estáticas de la red ONTAP

Es posible eliminar una ruta estática innecesaria de una máquina virtual de almacenamiento (SVM).

Paso

Utilice el `network route delete` comando para eliminar una ruta estática.

En el ejemplo siguiente se elimina una ruta estática asociada a SVM vs0 con una puerta de enlace 10.63.0.1 y una dirección IP de destino 0.0.0.0/0:

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

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

Ver información de enrutamiento de ONTAP

Puede ver información sobre la configuración de enrutamiento de cada SVM del clúster. Esto puede ayudarle a diagnosticar problemas de enrutamiento relacionados con problemas de conectividad entre aplicaciones o servicios de cliente y una LIF en un nodo del clúster.

Pasos

1. Utilice `network route show` el comando para mostrar las rutas dentro de una o más SVM. En el siguiente ejemplo, se muestra una ruta configurada en la SVM vs0:

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. Utilice `network route show-lifs` el comando para mostrar la asociación de rutas y las LIF dentro de una o más SVM.

   En el ejemplo siguiente se muestran las LIF con rutas propiedad de la SVM vs0:

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

   Obtenga más información sobre `network route show` y `network route show-lifs` en el "Referencia de comandos del ONTAP".

3. Utilice `network route active-entry show` el comando para mostrar las rutas instaladas en uno o más nodos, SVM, subredes o las rutas con destinos especificados.

   En el siguiente ejemplo, se muestran todas las rutas instaladas en una SVM específica:

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
```

```
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
11 entries were displayed.
```

Obtenga más información sobre `network route active-entry show` en el "Referencia de comandos del ONTAP".

Elimine las rutas dinámicas de las tablas de enrutamiento de la red ONTAP

Cuando se reciben redirecciones ICMP para IPv4 e IPv6, se agregan rutas dinámicas a la tabla de enrutamiento. De forma predeterminada, las rutas dinámicas se eliminan tras 300 segundos. Si desea mantener rutas dinámicas durante un período de tiempo diferente, puede cambiar el valor de tiempo de espera.

Acerca de esta tarea

Puede ajustar el valor del tiempo de espera de 0 a 65,535 segundos. Si establece el valor en 0, las rutas nunca caducan. La eliminación de rutas dinámicas evita la pérdida de conectividad causada por la persistencia de rutas no válidas.

Pasos

1. Muestra el valor de tiempo de espera actual.
   - Para IPv4:

     ```
     network tuning icmp show
     ```

   - Para IPv6:

     ```
     network tuning icmp6 show
     ```

2. Modifique el valor del tiempo de espera.
   - Para IPv4:

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - Para IPv6:

     ```
     network tuning icmp6 modify -node node_name -redirect-v6-timeout
     timeout_value
     ```

3. Compruebe que el valor del tiempo de espera se ha modificado correctamente.
   - Para IPv4:

     ```
     network tuning icmp show
     ```

   - Para IPv6:

     ```
     network tuning icmp6 show
     ```

Obtenga más información sobre `network tuning icmp` en el "Referencia de comandos del ONTAP".

Información de red de ONTAP

Ver la información de la red ONTAP

Mediante la CLI, puede ver información relacionada con los puertos, las LIF, las rutas, las reglas de conmutación por error, los grupos de conmutación por error, reglas de firewall, DNS, NIS y conexiones. A partir de ONTAP 9,8, también puede descargar los datos que se muestran en System Manager sobre su red.

Esta información puede ser útil en situaciones como volver a configurar la configuración de red o al solucionar problemas del clúster.

Si es un administrador de clúster, puede ver toda la información de redes disponible. Si es un administrador de SVM, puede ver solo la información relacionada con las SVM que tiene asignadas.

En System Manager, cuando se muestra información en una *Vista de lista*, puede hacer clic en **Descargar** y se descarga la lista de objetos que se muestra.

- La lista se descarga en formato de valores separados por comas (CSV).
- Sólo se descargan los datos de las columnas visibles.
- El nombre de archivo CSV tiene formato con el nombre del objeto y una Marca de hora.

Ver información del puerto de red de ONTAP

Puede ver información sobre un puerto específico o acerca de todos los puertos de todos los nodos del clúster.

Acerca de esta tarea

Se muestra la siguiente información:

- Nombre del nodo
- Nombre de puerto
- Nombre del espacio IP
- Nombre de dominio de retransmisión
- Estado del enlace (activo o inactivo)
- Ajuste MTU
- Configuración de velocidad del puerto y estado operativo (1 Gigabit o 10 gigabits por segundo)
- Configuración de negociación automática (verdadero o falso)
- Modo doble y estado operativo (mitad o completo)
- El grupo de interfaces del puerto, si corresponde
- La información de etiqueta de VLAN del puerto, si corresponde
- Estado del puerto (estado o degradado)
- Motivos para que un puerto se marque como degradado

Si los datos de un campo no están disponibles (por ejemplo, el dúplex operativo y la velocidad de un puerto inactivo no estarían disponibles), el valor del campo aparece como `-`.

Paso

Muestra información del puerto de red mediante `network port show` el comando.

Puede mostrar información detallada de cada puerto especificando `-instance` el parámetro o obtener información específica especificando nombres de campo con el `-fields` parámetro.

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

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

Consulte la información de VLAN de ONTAP

Puede ver información sobre una VLAN específica o sobre todas las VLAN del clúster.

Acerca de esta tarea

Puede mostrar información detallada de cada VLAN especificando `-instance` el parámetro. Puede mostrar información específica especificando nombres de campo con el `-fields` parámetro.

Paso

Mostrar información sobre las VLAN mediante `network port vlan show` el comando El siguiente comando muestra información sobre todas las VLAN del clúster:

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

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

Ver la información del grupo de interfaces de ONTAP

Puede mostrar información sobre un grupo de interfaces para determinar su configuración.

Acerca de esta tarea

Se muestra la siguiente información:

- Nodo en el que está ubicado el grupo de interfaces
- Lista de puertos de red que se incluyen en el grupo de interfaces
- Nombre del grupo de interfaces
- Función de distribución (MAC, IP, puerto o secuencial)
- La dirección Media Access Control (MAC) del grupo de interfaces

- Estado de la actividad portuaria; es decir, si todos los puertos agregados están activos (participación completa), si algunos están activos (participación parcial) o si ninguno está activo

Paso

Mostrar información sobre los grupos de interfaces mediante `network port ifgrp show` el comando.

Puede mostrar información detallada de cada nodo especificando `-instance` el parámetro. Puede mostrar información específica especificando nombres de campo con el `-fields` parámetro.

El siguiente comando muestra información sobre todos los grupos de interfaces del clúster:

```
network port ifgrp show
         Port     Distribution                    Active
Node     IfGrp    Function     MAC Address        Ports   Ports
-------- -------- ------------ -----------------  ------- --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

El siguiente comando muestra información detallada del grupo de interfaces de un solo nodo:

```
network port ifgrp show -instance -node cluster-1-01

                Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

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

Consulte la información de LIF de ONTAP

Puede ver información detallada sobre una LIF para determinar su configuración.

También puede ver esta información para diagnosticar problemas básicos de LIF, como comprobar las direcciones IP duplicadas o verificar si el puerto de red pertenece a la subred correcta. Los administradores de

máquinas virtuales de almacenamiento (SVM) pueden ver solo la información acerca de las LIF asociadas con la SVM.

Acerca de esta tarea

Se muestra la siguiente información:

- La dirección IP asociada con la LIF
- Estado administrativo de la LIF
- Estado operativo de la LIF

  El estado operativo de los LIF de datos viene determinado por el estado de la SVM con la que están asociadas los LIF de datos. Cuando se detiene la SVM, el estado operativo de la LIF cambia a inactivo. Cuando se inicia de nuevo la SVM, el estado operativo cambia a up

- Y el puerto en el que reside el LIF

Si los datos de un campo no están disponibles (por ejemplo, si no hay información de estado ampliada), el valor del campo aparece como `-`.

Paso

Mostrar la información de LIF mediante `network interface show` el comando.

Puede ver la información detallada de cada LIF especificando el parámetro -instance o obtener información específica especificando nombres de campo con el parámetro -fields.

El siguiente comando muestra información general acerca de todas las LIF de un clúster:

```
network interface show
            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
example
            lif1         up/up    192.0.2.129/22   node-01
                                                                e0d
false
node
            cluster_mgmt up/up    192.0.2.3/20     node-02
                                                                e0c
false
node-01
            clus1        up/up    192.0.2.65/18    node-01
                                                                e0a
true
            clus2        up/up    192.0.2.66/18    node-01
                                                                e0b
true
            mgmt1        up/up    192.0.2.1/20     node-01
                                                                e0c
true
node-02
            clus1        up/up    192.0.2.67/18    node-02
                                                                e0a
true
            clus2        up/up    192.0.2.68/18    node-02
                                                                e0b
true
            mgmt2        up/up    192.0.2.2/20     node-02
                                                                e0d
true
vs1
            d1           up/up    192.0.2.130/21   node-01
                                                                e0d
false
            d2           up/up    192.0.2.131/21   node-01
                                                                e0d
true
            data3        up/up    192.0.2.132/20   node-02
                                                                e0c
true
```

El siguiente comando muestra información detallada sobre una única LIF:

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                  Data Protocol: nfs,cifs
                      Home Node: node-01
                      Home Port: e0c
                   Current Node: node-03
                   Current Port: e0c
               Operational Status: up
                  Extended Status: -
                          Is Home: false
                  Network Address: 192.0.2.128
                          Netmask: 255.255.192.0
            Bits in the Netmask: 18
                  IPv4 Link Local: -
                      Subnet Name: -
           Administrative Status: up
                 Failover Policy: local-only
                 Firewall Policy: data
                     Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

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

Ver información de enrutamiento para la red ONTAP

Puede mostrar información sobre las rutas dentro de una SVM.

Paso

En función del tipo de información de enrutamiento que desee ver, introduzca el comando correspondiente:

Para ver información acerca de…	Introduzca…
Rutas estáticas, por SVM	`network route show`

LIF en cada ruta, por SVM	`network route show-lifs`

Puede visualizar información detallada de cada ruta especificando el `-instance` parámetro. El siguiente comando muestra las rutas estáticas dentro de las SVM en cluster- 1:

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

El siguiente comando muestra la asociación de rutas estáticas e interfaces lógicas (LIF) dentro de todas las SVM del clúster-1:

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

Obtenga más información sobre `network route show` y `network route show-lifs` en el "Referencia de comandos del ONTAP".

Ver las entradas de la tabla de hosts DNS de ONTAP

Las entradas de la tabla de hosts DNS asignan nombres de host a direcciones IP. Puede mostrar los nombres de host y los nombres de alias, y la dirección IP a la que se asignan para todas las SVM de un clúster.

Paso

Visualice las entradas de nombre de host de todas las SVM mediante el comando vserver Services NAME-service dns hosts show.

En el ejemplo siguiente se muestran las entradas de la tabla de hosts:

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ---------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

Puede usar `vserver services name-service dns` el comando para habilitar DNS en una SVM y configurarlo para que utilice DNS para la resolución de nombre de host. Los nombres de host se resuelven mediante servidores DNS externos.

Ver la información de configuración del dominio DNS de ONTAP

Puede mostrar la configuración de dominios DNS de una o varias máquinas virtuales de almacenamiento (SVM) en el clúster para verificar que está configurada correctamente.

Paso

Ver la configuración del dominio DNS con `vserver services name-service dns show` el comando.

El siguiente comando muestra las configuraciones de DNS de todas las SVM del clúster:

```
vserver services name-service dns show
                                                    Name
Vserver         State     Domains                   Servers
--------------- --------- ------------------------- -------------
cluster-1        enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs1             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs2             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs3             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
```

El siguiente comando muestra información detallada de la configuración de DNS para SVM vs1:

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

Ver información sobre el grupo de conmutación por error de ONTAP

Puede ver información acerca de los grupos de conmutación por error, incluida la lista de nodos y puertos de cada grupo de conmutación por error, tanto si la conmutación por error está habilitada como deshabilitada, así como el tipo de política de conmutación por error que se aplica a cada LIF.

Pasos

1. Mostrar los puertos de destino de cada grupo de failover mediante `network interface failover-groups show` el comando.

   El siguiente comando muestra información sobre todos los grupos de conmutación al nodo de respaldo en un clúster de dos nodos:

   ```
   network interface failover-groups show
                                Failover
   Vserver          Group       Targets
   ---------------  ----------- --------------------------------
   Cluster
                    Cluster
                                cluster1-01:e0a, cluster1-01:e0b,
                                cluster1-02:e0a, cluster1-02:e0b
   vs1
                    Default
                                cluster1-01:e0c, cluster1-01:e0d,
                                cluster1-01:e0e, cluster1-02:e0c,
                                cluster1-02:e0d, cluster1-02:e0e
   ```

   Obtenga más información sobre `network interface failover-groups show` en el "Referencia de comandos del ONTAP".

2. Muestra los puertos de destino y el dominio de retransmisión de un grupo de conmutación por error específico mediante `network interface failover-groups show` el comando.

   El siguiente comando muestra información detallada acerca de los datos del grupo de conmutación al nodo de respaldo 12 para SVM vs4:

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. Muestre la configuración de conmutación al respaldo utilizada por todas las LIF mediante `network interface show` el comando.

   El siguiente comando muestra la política de conmutación por error y el grupo de conmutación por error que utiliza cada LIF:

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy         failover-group
--------  -------------------  ----------------------  --------------
Cluster   cluster1-01_clus_1   local-only              Cluster
Cluster   cluster1-01_clus_2   local-only              Cluster
Cluster   cluster1-02_clus_1   local-only              Cluster
Cluster   cluster1-02_clus_2   local-only              Cluster
cluster1  cluster_mgmt         broadcast-domain-wide   Default
cluster1  cluster1-01_mgmt1    local-only              Default
cluster1  cluster1-02_mgmt1    local-only              Default
vs1       data1                disabled                Default
vs3       data2                system-defined          group2
```

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

Ver los destinos de recuperación tras fallos de LIF de ONTAP

Puede tener que comprobar si las políticas de conmutación por error y los grupos de conmutación por error de una LIF están configurados correctamente. Para evitar la configuración incorrecta de las reglas de conmutación al nodo de respaldo, puede mostrar los destinos de conmutación por error para una única LIF o para todas las LIF.

Acerca de esta tarea

Mostrar los destinos de conmutación por error de LIF permite comprobar lo siguiente:

- Si los LIF están configurados con el grupo de conmutación por error y la normativa de recuperación tras fallos correctos
- Si la lista resultante de puertos de destino de conmutación por error es adecuada para cada LIF

- Si el destino de conmutación al nodo de respaldo de una LIF de datos no es un puerto de gestión (e0M)

Paso

Muestre los destinos de conmutación al nodo de respaldo de una LIF mediante `failover` la opción `network interface show` del comando.

El siguiente comando muestra información acerca de los destinos de conmutación por error para todas las LIF de un clúster de dos nodos. La `Failover Targets` fila muestra la lista (priorizada) de combinaciones de nodo-puerto para una LIF determinada.

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

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

Ver los LIF de ONTAP en una zona de equilibrio de carga

Puede verificar si una zona de equilibrio de carga está configurada correctamente mostrando todas las LIF que pertenecen a ella. También puede ver la zona de equilibrio de carga de una LIF determinada o las zonas de equilibrio de carga de todas las LIF.

Paso

Muestre las LIF y los detalles de equilibrio de carga que desee mediante uno de los comandos siguientes

Para mostrar…	Introduzca…
LIF en una zona de equilibrio de carga en particular	`network interface show -dns-zone zone_name` `zone_name` especifica el nombre de la zona de equilibrio de carga.
La zona de equilibrio de carga de una LIF determinada	`network interface show -lif lif_name -fields dns-zone`
Las zonas de equilibrio de carga de todas las LIF	`network interface show -fields dns-zone`

Ejemplos de mostrar zonas de equilibrio de carga para las LIF

El siguiente comando muestra los detalles de todas las LIF de la zona de equilibrio de carga storage.company.com para SVM vs0:

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network            Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask       Node      Port    Home
--------- ---------- ---------- ------------------ --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20   ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20    ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20    ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20    ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20    ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20    ndeux-21  e0c     true
```

El siguiente comando muestra los detalles de la zona DNS de los datos de la LIF.3:

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

El siguiente comando muestra la lista de todas las LIF del clúster y sus zonas DNS correspondientes:

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

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

Ver las conexiones de clústeres de ONTAP

Puede mostrar todas las conexiones activas del clúster o un recuento de conexiones activas en el nodo por cliente, interfaz lógica, protocolo o servicio. También puede mostrar todas las conexiones de escucha en el clúster.

Mostrar conexiones activas por cliente (solo administradores de clúster)

Puede ver las conexiones activas por cliente para verificar el nodo que está utilizando un cliente específico y para ver los posibles desequilibrios entre el número de clientes por nodo.

Acerca de esta tarea

El número de conexiones activas por cliente es útil en las siguientes situaciones:

- Búsqueda de un nodo ocupado o sobrecargado.
- Determinar por qué el acceso de un cliente en particular a un volumen es lento.

  Puede ver detalles sobre el nodo al que accede el cliente y después compararlo con el nodo en el que reside el volumen. Si acceder al volumen requiere recorrer la red del clúster, es posible que los clientes experimenten una reducción del rendimiento debido al acceso remoto al volumen en un nodo remoto sobresuscritos.

- Comprobación de que todos los nodos se están utilizando igualmente para el acceso a los datos.
- Búsqueda de clientes que tienen un número alto de conexiones inesperadamente.
- Comprobar si determinados clientes tienen conexiones a un nodo.

Paso

Mostrar un recuento de las conexiones activas por cliente en un nodo mediante `network connections active show-clients` el comando.

Obtenga más información sobre `network connections active show-clients` en el "Referencia de comandos del ONTAP".

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253                1
        vs0             192.0.2.252                2
        Cluster         192.10.2.124               5
node1   vs0             192.0.2.250                1
        vs0             192.0.2.252                3
        Cluster         192.10.2.123               4
node2   vs1             customer.example.com       1
        vs1             192.0.2.245                3
        Cluster         192.10.2.122               4
node3   vs1             customer.example.org       1
        vs1             customer.example.net       3
        Cluster         192.10.2.121               4
```

Mostrar las conexiones activas por protocolo (solo administradores de clúster)

Puede mostrar un recuento de las conexiones activas por protocolo (TCP o UDP) en un nodo para comparar el uso de protocolos dentro del clúster.

Acerca de esta tarea

El número de conexiones activas por protocolo es útil en las siguientes situaciones:

- Encontrar los clientes UDP que están perdiendo su conexión.

  Si un nodo está cerca de su límite de conexión, los clientes UDP son los primeros en caer.

- Comprobando que no se está utilizando ningún otro protocolo.

Paso

Mostrar un recuento de las conexiones activas por protocolo en un nodo mediante `network connections active show-protocols` el comando.

Obtenga más información sobre `network connections active show-protocols` en el "Referencia de comandos del ONTAP".

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

Mostrar conexiones activas por servicio (sólo administradores de clúster)

Puede mostrar un recuento de las conexiones activas por tipo de servicio (por ejemplo, por NFS, SMB, montaje, etc.) para cada nodo de un clúster. Esto resulta útil para comparar el uso de los servicios del clúster, lo que ayuda a determinar la carga de trabajo principal de un nodo.

Acerca de esta tarea

El recuento de conexiones activas por servicio es útil en los siguientes casos:

- Comprobar que todos los nodos se están utilizando para los servicios adecuados y que el equilibrio de carga de ese servicio está funcionando.
- Verificando que no se está utilizando ningún otro servicio. Muestra un recuento de las conexiones activas por servicio en un nodo mediante `network connections active show-services` el comando.

Obtenga más información sobre `network connections active show-services` en el "Referencia de comandos del ONTAP".

```
network connections active show-services
Node        Vserver Name    Service    Count
---------   -------------   ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

Muestre las conexiones activas por LIF en un nodo y una SVM

Puede mostrar un número de conexiones activas para cada LIF, por nodo y máquina virtual de almacenamiento (SVM), para ver los desequilibrios de conexión entre las LIF dentro del clúster.

Acerca de esta tarea

El número de conexiones activas por LIF es útil en las siguientes situaciones:

- Buscar un LIF sobrecargado mediante la comparación del número de conexiones en cada LIF.
- Comprobar que el equilibrio de carga de DNS funciona en todos los LIF de datos.
- Comparación del número de conexiones con las distintas SVM para encontrar las SVM que más se usan.

Paso

Muestre un recuento de conexiones activas para cada LIF por SVM y nodo mediante `network connections active show-lifs` el comando.

Obtenga más información sobre `network connections active show-lifs` en el "Referencia de comandos del ONTAP".

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

Muestra las conexiones activas en un clúster

Puede mostrar información acerca de las conexiones activas de un clúster para ver la LIF, el puerto, el host remoto, el servicio, las máquinas virtuales de almacenamiento (SVM) y el protocolo que utilizan las conexiones individuales.

Acerca de esta tarea

Ver las conexiones activas en un clúster es útil en las siguientes situaciones:

- Verificar que los clientes individuales están usando el protocolo y el servicio correctos en el nodo correcto.
- Si un cliente tiene problemas para acceder a los datos mediante una cierta combinación de nodo, protocolo y servicio, puede utilizar este comando para encontrar un cliente similar para la comparación de la configuración o el seguimiento de paquetes.

Paso

Muestre las conexiones activas en un clúster mediante `network connections active show` el comando.

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

El siguiente comando muestra las conexiones activas del nodo 1:

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

El siguiente comando muestra las conexiones activas en la SVM vs1:

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

Muestra las conexiones de escucha en un clúster

Puede mostrar información acerca de las conexiones de escucha en un clúster para ver las LIF y los puertos que aceptan conexiones para un protocolo y un servicio dados.

Acerca de esta tarea

Ver las conexiones de escucha en un clúster es útil en las siguientes situaciones:

- Verificación de que el protocolo o servicio deseado están escuchando en una LIF si las conexiones de cliente con esta LIF fallan de forma consistente.
- Comprobar que se abre un listener de UDP/rclopcp en cada LIF de clúster si se produce un error en el acceso remoto a datos a un volumen de un nodo a través de una LIF en otro nodo.
- Comprobación de que se abre un agente de escucha UDP/rclopcp en cada LIF del clúster si se producen errores en las transferencias de SnapMirror entre dos nodos del mismo clúster.
- Comprobar que se ha abierto un agente de escucha TCP/ctlopcp en cada LIF de interconexión de clústeres si se producen fallos en las transferencias de SnapMirror entre dos nodos en clústeres diferentes.

Paso

Muestre las conexiones de escucha por nodo con `network connections listening show` el comando.

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

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

Comandos de la ONTAP para diagnosticar problemas de red

Puede diagnosticar problemas en su red mediante comandos `ping`, `traceroute`, `ndp`, como y. `tcpdump` También puede usar comandos `ping6` como y `traceroute6` para diagnosticar problemas IPv6.

Si desea…	Introduzca este comando…
Compruebe si el nodo puede llegar a otros hosts de su red	`network ping`
Probar si el nodo puede llegar a otros hosts en su red IPv6	`network ping6`
Rastree la ruta que los paquetes IPv4 toman a un nodo de red	`network traceroute`
Rastree la ruta que los paquetes IPv6 toman a un nodo de red	`network traceroute6`
Gestión del protocolo de descubrimiento cercano (NDP)	`network ndp`
Mostrar estadísticas sobre los paquetes que se reciben y se envían en una interfaz de red especificada o en todas las interfaces de red	`run -node` *`node_name`* `ifstat` **Nota**: Este comando está disponible desde el nodeshell.

Muestra información sobre los dispositivos vecinos que se detectan de cada nodo y puerto del clúster, incluido el tipo de dispositivo remoto y la plataforma de dispositivos	`network device-discovery show`
Ver los vecinos de CDP del nodo (ONTAP solo admite anuncios de CDPv1)	`run -node node_name cdpd show-neighbors` **Nota**: Este comando está disponible desde el nodeshell.
Realice el seguimiento de los paquetes que se envían y se reciben en la red	`network tcpdump start -node node-name -port port_name` **Nota**: Este comando está disponible desde el nodeshell.
Mida la latencia y el rendimiento entre nodos entre clústeres o dentro del clúster	`network test -path -source-node source_nodename local -destination -cluster destination_clustername -destination-node destination_nodename -session-type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer` Para obtener más información, consulte la "Gestión del rendimiento".

Información relacionada

- "Referencia de comandos del ONTAP"
- "ping de red"
- "ruta de acceso de red"
- "espectáculo de detección de dispositivos de red"
- "ndp de red"

Vea la conectividad de red con los protocolos de detección de vecinos

Vea la conectividad de red ONTAP con protocolos de detección de vecinos

En un centro de datos, puede utilizar protocolos de descubrimiento de vecinos para ver la conectividad de red entre un par de sistemas físicos o virtuales y sus interfaces de red. ONTAP admite dos protocolos de detección de vecinos: El protocolo de descubrimiento de Cisco (CDP) y el protocolo de detección de nivel de enlace (LLDP).

Los protocolos de detección de vecinos permiten detectar y ver automáticamente información sobre los dispositivos habilitados para protocolos conectados directamente en una red. Cada dispositivo anuncia la identificación, las capacidades y la información de conectividad. Esta información se transmite en tramas Ethernet a una dirección MAC de multidifusión y la reciben todos los dispositivos vecinos habilitados por protocolo.

Para que dos dispositivos se conviertan en vecinos, cada uno debe tener un protocolo activado y configurado correctamente. La funcionalidad del protocolo de detección se limita a redes conectadas directamente. Los vecinos pueden incluir dispositivos habilitados para protocolos, como switches, routers, puentes, etc. ONTAP admite dos protocolos de detección de vecinos, que se pueden utilizar por separado o juntos.

Cisco Discovery Protocol (CDP)

CDP es un protocolo de capa de enlace patentado desarrollado por Cisco Systems. Está habilitado de forma predeterminada en ONTAP para los puertos de clúster, pero debe habilitarse explícitamente para los puertos de datos.

Protocolo de detección de nivel de enlace (LLDP)

LLDP es un protocolo neutral en cuanto a proveedores especificado en el documento estándar IEEE 802.1AB. Debe habilitarse explícitamente para todos los puertos.

Utilice CDP para detectar la conectividad de red ONTAP

El uso de CDP para detectar la conectividad de red consiste en revisar las consideraciones de implementación, habilitarlo en puertos de datos, ver dispositivos vecinos y ajustar los valores de configuración de CDP según sea necesario. De forma predeterminada, CDP está habilitado en los puertos de clúster.

También es necesario habilitar CDP en cualquier switch y enrutador para poder mostrar la información acerca de los dispositivos vecinos.

Versión de ONTAP	Descripción
9.10.1 y anteriores	El monitor de estado del switch de clúster también utiliza el CDP para detectar automáticamente los switches de red de gestión y clúster.
9.11.1 y posterior	El monitor de estado del switch de clúster también utiliza el CDP para detectar automáticamente los switches de red de clúster, almacenamiento y gestión.

Información relacionada

"Administración del sistema"

Consideraciones para usar CDP

De forma predeterminada, los dispositivos compatibles con CDP envían anuncios de CDPv2. Los dispositivos compatibles con CDP envían anuncios de CDPv1 sólo cuando reciben anuncios de CDPv1. ONTAP solo es compatible con CDPv1. Por lo tanto, cuando un nodo ONTAP envía anuncios de CDPv1, los dispositivos vecinos que cumplen con CDP devuelven anuncios de CDPv1.

Debe considerar la siguiente información antes de habilitar CDP en un nodo:

- CDP es compatible con todos los puertos.
- Los anuncios de CDP son enviados y recibidos por los puertos que están en el estado up.
- CDP debe estar activado en los dispositivos de transmisión y recepción para enviar y recibir anuncios de CDP.
- Los anuncios de CDP se envían a intervalos regulares y puede configurar el intervalo de tiempo.
- Cuando cambian las direcciones IP de una LIF, el nodo envía la información actualizada en el siguiente anuncio de CDP.
- ONTAP 9.10.1 y anteriores:
  - CDP está siempre habilitado en los puertos de clúster.

    - De forma predeterminada, CDP está deshabilitado en todos los puertos que no son de clúster.
- ONTAP 9.11.1 y posteriores:
    - CDP está siempre habilitado en los puertos de clúster y de almacenamiento.
    - De forma predeterminada, CDP está deshabilitado en todos los puertos que no son de clúster y que no están relacionados con el almacenamiento.

> A veces, cuando se cambian las LIF en el nodo, la información de CDP no se actualiza en el lado del dispositivo receptor (por ejemplo, un switch). Si encuentra este problema, debe configurar la interfaz de red del nodo con el estado inactivo y, a continuación, con el estado activo.

- Sólo las direcciones IPv4 están anunciadas en los anuncios de CDP.
- Para los puertos de red físicos con VLAN, se anuncian todas las LIF configuradas en las VLAN de ese puerto.
- Para los puertos físicos que forman parte de un grupo de interfaces, todas las direcciones IP configuradas en ese grupo de interfaces se anuncian en cada puerto físico.
- Para un grupo de interfaces que aloja VLAN, todas las LIF configuradas en el grupo de interfaces y las VLAN se anuncian en cada uno de los puertos de red.
- Debido a que los paquetes CDP están restringidos a no más de 1500 bytes, en los puertos configurados con un gran número de LIF sólo se puede informar en el switch adyacente un subconjunto de estas direcciones IP.

Habilite o deshabilite CDP

Para detectar y enviar anuncios a dispositivos vecinos compatibles con CDP, es necesario habilitar CDP en cada nodo del clúster.

De manera predeterminada en ONTAP 9.10.1 y versiones anteriores, CDP está habilitado en todos los puertos de clúster de un nodo y está deshabilitado en todos los puertos que no son de clúster de un nodo.

De forma predeterminada en ONTAP 9.11.1 y versiones posteriores, CDP está habilitado en todos los puertos de clúster y almacenamiento de un nodo, y está deshabilitado en todos los puertos que no son de clúster y que no son de almacenamiento de un nodo.

Acerca de esta tarea

`cdpd.enable`La opción controla si CDP está habilitado o deshabilitado en los puertos de un nodo:

- Para ONTAP 9.10.1 y versiones anteriores, en habilita CDP en puertos que no son de clúster.
- Para ONTAP 9.11.1 y versiones posteriores, el habilita CDP en puertos que no son de clúster y que no son de almacenamiento.
- Para ONTAP 9.10.1 y versiones anteriores, OFF deshabilita CDP en puertos que no son de clúster; no puede deshabilitar CDP en los puertos de clúster.
- Para ONTAP 9.11.1 y versiones posteriores, OFF deshabilita CDP en puertos que no son de clúster y que no son de almacenamiento; no puede deshabilitar CDP en puertos de clúster.

Cuando CDP está desactivado en un puerto conectado a un dispositivo compatible con CDP, es posible que el

tráfico de red no esté optimizado.

Pasos

1. Muestra la configuración actual de CDP para un nodo o para todos los nodos de un clúster:

Para ver la configuración CDP de…	Introduzca…
Un nodo	`run - node <node_name> options cdpd.enable`
Todos los nodos de un clúster	`options cdpd.enable`

2. Habilite o deshabilite CDP en todos los puertos de un nodo o en todos los puertos de todos los nodos de un clúster:

Para habilitar o deshabilitar CDP en…	Introduzca…
Un nodo	`run -node node_name options cdpd.enable {on or off}`
Todos los nodos de un clúster	`options cdpd.enable {on or off}`

Consulte la información sobre vecinos de CDP

Puede ver información acerca de los dispositivos vecinos que están conectados a cada puerto de los nodos del clúster, siempre que el puerto esté conectado a un dispositivo compatible con CDP. Puede utilizar `network device-discovery show -protocol cdp` el comando para ver la información del vecino. Obtenga más información sobre `network device-discovery show` en el "Referencia de comandos del ONTAP".

Acerca de esta tarea

En ONTAP 9.10.1 y versiones anteriores, como el CDP siempre está habilitado para los puertos de clúster, la información de vecinos CDP siempre se muestra para esos puertos. CDP debe estar habilitado en puertos que no son de clúster para que aparezca la información de cercanía para esos puertos.

En ONTAP 9.11.1 y versiones posteriores, como el CDP está siempre habilitado para el clúster y los puertos de almacenamiento, la información de vecino de CDP siempre se muestra para esos puertos. Para que aparezca la información relacionada con los puertos, CDP debe estar habilitado en puertos que no sean de clúster y que no sean de almacenamiento.

Paso

Muestra información sobre todos los dispositivos compatibles con CDP que están conectados a los puertos de un nodo del clúster:

```
network device-discovery show -node node -protocol cdp
```

El siguiente comando muestra los vecinos que están conectados a los puertos en el nodo sti2650-212:

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

El resultado enumera los dispositivos Cisco que están conectados a cada puerto del nodo especificado.

Configure el tiempo de espera para los mensajes CDP

El tiempo de espera es el período de tiempo durante el cual los anuncios de CDP se almacenan en la caché en los dispositivos vecinos que cumplen con CDP. El tiempo de mantenimiento se anuncia en cada paquete CDPv1 y se actualiza cada vez que un nodo recibe un paquete CDPv1.

- El valor de `cdpd.holdtime` la opción debe establecerse con el mismo valor en ambos nodos de un par de alta disponibilidad.
- El valor de tiempo de espera predeterminado es de 180 segundos, pero puede introducir valores que oscilan entre 10 segundos y 255 segundos.
- Si se elimina una dirección IP antes de que caduque el tiempo de retención, la información CDP se almacena en caché hasta que caduque el tiempo de retención.

Pasos

1. Muestre el tiempo de espera actual de CDP para un nodo o para todos los nodos de un clúster:

Para ver el tiempo de espera de…	Introduzca…
Un nodo	`run -node node_name options cdpd.holdtime`

Todos los nodos de un clúster	`options cdpd.holdtime`

2. Configure el tiempo de retención de CDP en todos los puertos de un nodo o en todos los puertos de todos los nodos de un clúster:

Para establecer el tiempo de espera activado:	Introduzca…
Un nodo	`run -node node_name options cdpd.holdtime holdtime`
Todos los nodos de un clúster	`options cdpd.holdtime holdtime`

Establezca el intervalo para enviar anuncios CDP

Los anuncios de CDP se envían a los vecinos de CDP a intervalos periódicos. Es posible aumentar o reducir el intervalo para enviar anuncios de CDP en función del tráfico de red y los cambios en la topología de red.

- El valor de `cdpd.interval` la opción debe establecerse con el mismo valor en ambos nodos de un par de alta disponibilidad.
- El intervalo predeterminado es de 60 segundos, pero puede introducir un valor entre 5 segundos y 900 segundos.

Pasos

1. Muestre el intervalo de tiempo de anuncio de CDP actual para un nodo o para todos los nodos de un clúster:

Para ver el intervalo de…	Introduzca…
Un nodo	`run -node node_name options cdpd.interval`
Todos los nodos de un clúster	`options cdpd.interval`

2. Configure el intervalo para enviar anuncios CDP para todos los puertos de un nodo o para todos los puertos de todos los nodos de un clúster:

Para establecer el intervalo para…	Introduzca…
Un nodo	`run -node node_name options cdpd.interval interval`
Todos los nodos de un clúster	`options cdpd.interval interval`

Ver o borrar estadísticas de CDP

Es posible ver las estadísticas de CDP de los puertos de clúster y no de clúster en cada nodo para detectar posibles problemas de conectividad de red. Las estadísticas de CDP son acumulativas a partir del momento en que se borraron por última vez.

Acerca de esta tarea

En ONTAP 9.10.1 y versiones anteriores, como CDP está siempre habilitado para los puertos, las estadísticas de CDP siempre se muestran para el tráfico de esos puertos. CDP debe estar habilitado en los puertos para que aparezcan las estadísticas para esos puertos.

En ONTAP 9.11.1 y versiones posteriores, como el CDP está siempre habilitado para los puertos de clúster y de almacenamiento, las estadísticas de CDP siempre se muestran para el tráfico de esos puertos. CDP debe estar habilitado en puertos que no sean de clúster o que no sean de almacenamiento para que las estadísticas aparezcan para esos puertos.

Paso

Muestre o borre las estadísticas actuales de CDP para todos los puertos en un nodo:

Si desea…	Introduzca…
Consulte las estadísticas de CDP	`run -node node_name cdpd show-stats`
Borre las estadísticas de CDP	`run -node node_name cdpd zero-stats`

Ejemplo de mostrar y borrar estadísticas

El siguiente comando muestra las estadísticas de CDP antes de borrarlas. El resultado muestra el número total de paquetes que se enviaron y recibieron desde la última vez que se borraron las estadísticas.

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

El siguiente comando borra las estadísticas de CDP:

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:            0  | Csum Errors:       0  | Unsupported Vers:     0
 Invalid length:     0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:       0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:            0  | Xmit fails:        0  | No hostname:          0
 Packet truncated:   0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:      0
```

Una vez borradas las estadísticas, comienzan a acumularse después de que se envía o recibe el próximo anuncio de CDP.

Conexión a switches Ethernet que no admiten CDP

Varios conmutadores de proveedores no admiten CDP. Ver el"Base de conocimientos de NetApp : La detección de dispositivos ONTAP muestra los nodos en lugar del conmutador" Para más detalles.

Existen dos opciones para resolver este problema:

- Deshabilite CDP y habilite LLDP, si es compatible. Consulte "Use LLDP para detectar la conectividad de red" para obtener más información.
- Configure un filtro de paquetes de direcciones MAC en los switches para borrar anuncios CDP.

Utilice LLDP para detectar la conectividad de red ONTAP

El uso de LLDP para detectar la conectividad de red consiste en revisar consideraciones de implementación, habilitarlo en todos los puertos, ver dispositivos vecinos y ajustar los valores de configuración de LLDP según sea necesario.

También es necesario habilitar LLDP en cualquier switch y enrutador para poder mostrar la información acerca de los dispositivos vecinos.

ONTAP informa actualmente de las siguientes estructuras de longitud de valor de tipo (TLV):

- ID del chasis
- Identificador del puerto
- Tiempo de vida (TTL)
- Nombre del sistema

  El TLV del nombre del sistema no se envía en los dispositivos CNA.

Ciertos adaptadores de red convergentes (CNA), como el adaptador X1143 y los puertos UTA2 integrados, contienen compatibilidad con la descarga para LLDP:

- La descarga de LLDP se utiliza para la creación de puentes en centros de datos (DCB).
- La información mostrada podría diferir entre el clúster y el switch.

  Los datos del identificador del chasis y del identificador del puerto que muestra el switch podrían ser diferentes para los puertos CNA y no CNA.

Por ejemplo:

- Para puertos que no son CNA:
  - El identificador de chasis es una dirección MAC fija de uno de los puertos en el nodo
  - Port ID es el nombre de puerto del puerto correspondiente en el nodo
- Para puertos CNA:
  - Los identificadores de chasis y de puerto son las direcciones MAC de los respectivos puertos en el nodo.

Sin embargo, los datos que muestra el clúster son consistentes para estos tipos de puerto.

La especificación LLDP define el acceso a la información recogida a través de una MIB SNMP. Sin embargo, ONTAP no admite actualmente la MIB de LLDP.

Habilite o deshabilite LLDP

Para detectar y enviar anuncios a dispositivos vecinos compatibles con LLDP, es necesario habilitar LLDP en cada nodo del clúster. A partir de ONTAP 9.7, LLDP está habilitado en todos los puertos de un nodo de manera predeterminada.

Acerca de esta tarea

Para ONTAP 9.10,1 y versiones anteriores, la `lldp.enable` opción controla si LLDP está habilitado o deshabilitado en los puertos de un nodo:

- `on` Activa LLDP en todos los puertos.
- `off` Desactiva LLDP en todos los puertos.

Para ONTAP 9.11,1 y versiones posteriores, la `lldp.enable` opción controla si LLDP está habilitado o deshabilitado en los puertos que no son del clúster y que no son de almacenamiento de un nodo:

- `on` Activa LLDP en todos los puertos que no son del clúster y que no son de almacenamiento.
- `off` Desactiva LLDP en todos los puertos que no son del clúster y que no son de almacenamiento.

Pasos

1. Muestra la configuración actual de LLDP para un nodo o para todos los nodos de un clúster:
   - Un nodo: `run -node node_name options lldp.enable`
   - Todos los nodos: Opciones `lldp.enable`
2. Habilite o deshabilite LLDP en todos los puertos de un nodo o en todos los puertos de todos los nodos de un clúster:

Para habilitar o deshabilitar LLDP en…	Introduzca…
Un nodo	`run -node node_name options lldp.enable {on
off}`	Todos los nodos de un clúster
`options lldp.enable {on	off}`

- Un solo nodo:

```
run -node node_name options lldp.enable {on|off}
```

- Todos los nodos:

```
options lldp.enable {on|off}
```

Consulte la información sobre vecinos de LLDP

Puede ver información sobre los dispositivos vecinos que están conectados a cada puerto de los nodos del clúster, siempre y cuando el puerto esté conectado a un dispositivo compatible con LLDP. Puede utilizar el comando network device-Discovery show para ver información de los vecinos.

Paso

1. Muestra información sobre todos los dispositivos compatibles con LLDP que están conectados a los puertos de un nodo del clúster:

```
network device-discovery show -node node -protocol lldp
```

El siguiente comando muestra los vecinos que están conectados a los puertos en el nodo cluster-1_01. La salida enumera los dispositivos habilitados para LLDP que están conectados a cada puerto del nodo especificado. Si se `-protocol` omite la opción, la salida también muestra los dispositivos habilitados para CDP.

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

Ajuste el intervalo para la transmisión de anuncios de LLDP

Los anuncios de LLDP se envían a intervalos periódicos. Es posible aumentar o reducir el intervalo para enviar anuncios de LLDP en función del tráfico de red y los cambios en la topología de red.

Acerca de esta tarea

El intervalo predeterminado recomendado por IEEE es de 30 segundos, pero puede introducir un valor de 5 segundos a 300 segundos.

Pasos

1. Muestre el intervalo de tiempo de anuncio de LLDP actual para un nodo o para todos los nodos de un clúster:
   - Un solo nodo:

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - Todos los nodos:

     ```
     options lldp.xmit.interval
     ```

2. Ajuste el intervalo para enviar anuncios de LLDP para todos los puertos de un nodo o para todos los puertos de todos los nodos de un clúster:
   - Un solo nodo:

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - Todos los nodos:

     ```
     options lldp.xmit.interval <interval>
     ```

Ajuste el tiempo de respuesta de los anuncios de LLDP

El tiempo de vida (TTL) es el período de tiempo durante el cual los anuncios de LLDP se almacenan en la caché en dispositivos vecinos compatibles con LLDP. TTL se anuncia en cada paquete LLDP y se actualiza cada vez que un nodo recibe un paquete LLDP. TTL puede modificarse en tramas LLDP salientes.

Acerca de esta tarea

- TTL es un valor calculado, el producto del intervalo de transmisión (`lldp.xmit.interval`) y el multiplicador de retención (`lldp.xmit.hold`) más uno.
- El valor predeterminado del multiplicador de retención es 4, pero puede introducir valores que oscilen entre 1 y 100.
- Por lo tanto, el valor predeterminado TTL es de 121 segundos, como recomienda el IEEE, pero al ajustar el intervalo de transmisión y mantener los valores multiplicadores, puede especificar un valor para los fotogramas salientes de 6 segundos a 30001 segundos.
- Si se elimina una dirección IP antes de que caduque el TTL, la información de LLDP se almacena en caché hasta que caduque el TTL.

Pasos

1. Muestre el valor actual de contener multiplicador para un nodo o para todos los nodos de un clúster:
   - Un solo nodo:

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

   - Todos los nodos:

     ```
     options lldp.xmit.hold
     ```

2. Ajuste el valor de multiplicador de mantenimiento en todos los puertos de un nodo o en todos los puertos de todos los nodos de un clúster:
   - Un solo nodo:

     ```
     run -node <node_name> options lldp.xmit.hold <hold_value>
     ```

   - Todos los nodos:

     ```
     options lldp.xmit.hold <hold_value>
     ```

Ver o borrar estadísticas de LLDP

Es posible ver las estadísticas de LLDP de los puertos de clúster y no de clúster en cada nodo para detectar posibles problemas de conectividad de red. Las estadísticas de LLDP son acumulativas a partir del momento en que se borraron por última vez.

Acerca de esta tarea

Para ONTAP 9.10.1 y versiones anteriores, como LLDP siempre están habilitadas para puertos del clúster, siempre se muestran las estadísticas de LLDP para el tráfico de esos puertos. LLDP debe estar habilitado en puertos que no son del clúster para que se muestren estadísticas de esos puertos.

Para ONTAP 9.11.1 y versiones posteriores, como LLDP siempre está habilitado para los puertos de clúster y de almacenamiento, siempre se muestran las estadísticas de LLDP para el tráfico de esos puertos. LLDP deben estar habilitadas en puertos que no sean del clúster y en puertos del almacenamiento para que se muestren estadísticas de esos puertos.

Paso

Muestre o borre las estadísticas actuales de LLDP para todos los puertos en un nodo:

Si desea…	Introduzca…
Consulte las estadísticas de LLDP	`run -node node_name lldp stats`
Borre las estadísticas de LLDP	`run -node node_name lldp stats -z`

Ejemplo de estadísticas show y clear

El siguiente comando muestra las estadísticas de LLDP antes de borrarlas. El resultado muestra el número total de paquetes que se enviaron y recibieron desde la última vez que se borraron las estadísticas.

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

El siguiente comando borra las estadísticas de LLDP.

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

Una vez borradas las estadísticas, comienzan a acumularse después de que se envía o recibe el próximo anuncio de LLDP.