



Configuración de red

Enterprise applications

NetApp
May 09, 2024

Tabla de contenidos

- Configuración de red 1
 - Diseño de interfaz lógica para bases de datos de Oracle 1
 - Configuración TCP/IP y ethernet para bases de datos Oracle 5
 - Configuración de FC para bases de datos de Oracle 7
 - Base de datos Oracle y conectividad ONTAP de conexión directa 8

Configuración de red

Diseño de interfaz lógica para bases de datos de Oracle

Las bases de datos de Oracle necesitan acceder al almacenamiento. Las interfaces lógicas (LIF) son las tuberías de red que conecta una máquina virtual de almacenamiento (SVM) a la red y, por tanto, a la base de datos. Es necesario diseñar un LIF adecuado para garantizar que exista un ancho de banda suficiente para cada carga de trabajo de la base de datos. La conmutación por error no conlleva la pérdida de los servicios de almacenamiento.

En esta sección se ofrece una descripción general de los principios clave del diseño de LIF. Para obtener documentación más completa, consulte "[Documentación de gestión de red de ONTAP](#)". Al igual que otros aspectos de la arquitectura de bases de datos, las mejores opciones para las máquinas virtuales de almacenamiento (SVM, conocidas como Vserver en la CLI) y el diseño de la interfaz lógica (LIF) dependen en gran medida de los requisitos de escalado y las necesidades empresariales.

Tenga en cuenta los siguientes temas principales al crear una estrategia de LIF:

- **Rendimiento.** ¿Es suficiente el ancho de banda de la red?
- **Resiliencia.** ¿Hay algún punto de falla en el diseño?
- **Capacidad de gestión.** ¿Se puede escalar la red de forma no disruptiva?

Estos temas se aplican a la solución completa, desde el host, los switches y el sistema de almacenamiento.

Tipos de LIF

Hay varios tipos de LIF. "[Documentación de ONTAP sobre tipos de LIF](#)" Puede proporcionar información más completa sobre este tema, pero desde una perspectiva funcional, los LIF se pueden dividir en los siguientes grupos:

- **LIF de administración de clúster y nodos.** LIF utilizadas para administrar el clúster de almacenamiento.
- **LIF de administración de SVM.** Interfaces que permiten el acceso a una SVM a través de la API REST o ONTAPI (también conocida como ZAPI) para funciones como la creación de instantáneas o el redimensionamiento de volúmenes. Productos como SnapManager para Oracle (SMO) deben tener acceso a una LIF de gestión de SVM.
- **LIF de datos.** Interfaces para FC, iSCSI, NVMe/FC, NVMe/TCP, NFS, o datos SMB/CIFS.



También puede utilizarse una LIF de datos que se utiliza para el tráfico NFS al cambiar la política de firewall de `data` para `mgmt` o cualquier otra política que permita HTTP, HTTPS o SSH. Este cambio puede simplificar la configuración de red ya que evita la configuración de cada host para obtener acceso a tanto a la LIF de datos de NFS como a una LIF de gestión separada. No se puede configurar una interfaz para iSCSI y para el tráfico de gestión, a pesar de que ambos usen un protocolo IP. En los entornos iSCSI, se requiere una LIF de gestión separada.

Diseño de LIF SAN

El diseño de LIF en un entorno SAN es relativamente sencillo por una de las razones: La multivía. Todas las

implementaciones de SAN modernas permiten a un cliente acceder a los datos a través de múltiples rutas de red independientes y seleccionar la mejor ruta o las mejores rutas para acceder. Como resultado, el rendimiento con respecto al diseño de las LIF es más sencillo de abordar porque los clientes SAN equilibran automáticamente la carga de I/O en las mejores rutas disponibles.

Si una ruta deja de estar disponible, el cliente selecciona automáticamente una ruta diferente. La simplicidad resultante del diseño hace que los LIF SAN sean generalmente más gestionables. Esto no significa que un entorno SAN siempre se gestione con mayor facilidad, ya que existen otros muchos aspectos del almacenamiento SAN que son mucho más complicados que NFS. Simplemente significa que el diseño de LIF SAN es más sencillo.

Rendimiento

El aspecto más importante con respecto al rendimiento de LIF en un entorno SAN es el ancho de banda. Por ejemplo, un clúster ONTAP AFF de dos nodos con dos puertos FC de 16GB Gb por nodo permite hasta 32GB Gbps de ancho de banda hacia/desde cada nodo.

Resiliencia

Los LIF DE SAN no conmutan al nodo de respaldo en un sistema de almacenamiento AFF. Si falla un LIF de SAN debido a la recuperación tras fallos de la controladora, el software multivía del cliente detecta la pérdida de una ruta y redirige las I/O a otro LIF. Con los sistemas de almacenamiento de ASA, los LIF conmutarán por error tras un breve retraso, pero esto no interrumpe las I/O porque ya hay rutas activas en la otra controladora. El proceso de conmutación por error tiene lugar para restaurar el acceso de host en todos los puertos definidos.

Gran capacidad de administración

La migración de LIF es una tarea mucho más común en un entorno NFS porque la migración de LIF suele asociarse con la reubicación de volúmenes en el clúster. No es necesario migrar un LIF en un entorno SAN cuando se reubican volúmenes en el par de alta disponibilidad. Esto se debe a que, una vez finalizado el movimiento de volúmenes, ONTAP envía una notificación a la SAN sobre un cambio en las rutas y los clientes SAN vuelven a optimizarse automáticamente. La migración de LIF con SAN está asociada principalmente a los grandes cambios de hardware físico. Por ejemplo, si es necesaria una actualización sin interrupciones de las controladoras, se migra un LIF SAN al nuevo hardware. Si se encuentra que un puerto FC está defectuoso, puede migrarse un LIF a un puerto no utilizado.

Recomendaciones de diseño

NetApp hace las siguientes recomendaciones:

- No cree más rutas de las necesarias. Un número excesivo de rutas complica la gestión general y puede provocar problemas en la conmutación al nodo de respaldo de rutas en algunos hosts. Además, algunos hosts tienen limitaciones inesperadas de la ruta para configuraciones como el arranque SAN.
- Muy pocas configuraciones deberían requerir más de cuatro rutas a una LUN. El valor de tener más de dos nodos de rutas de publicidad para los LUN es limitado porque no se puede acceder al agregado que aloja una LUN si se produce un error en el nodo propietario de la LUN y su partner de alta disponibilidad. La creación de rutas en nodos que no sean el par de alta disponibilidad primario no es útil en esta situación.
- Aunque puede gestionar el número de rutas visibles de LUN si selecciona qué puertos se incluyen en las zonas FC, suele ser más fácil incluir todos los puntos de destino potenciales en la zona FC y controlar la visibilidad de la LUN a nivel de ONTAP.
- En ONTAP 8,3 y versiones posteriores, la función de asignación selectiva de LUN (SLM) es la opción

predeterminada. Con SLM, cualquier nuevo LUN se anuncia automáticamente desde el nodo propietario del agregado subyacente y el partner de alta disponibilidad del nodo. Esta disposición evita la necesidad de crear conjuntos de puertos o configurar la división en zonas para limitar la accesibilidad del puerto. Cada LUN está disponible en el número mínimo de nodos necesarios, tanto para un rendimiento óptimo como para una resiliencia.

*En el caso de que una LUN deba migrarse fuera de los dos controladores, los nodos adicionales se pueden agregar con el `lun mapping add-reporting-nodes` Comando para que las LUN se anuncien en los nodos nuevos. Al hacerlo, se crean rutas de SAN adicionales a las LUN para la migración de la LUN. Sin embargo, el host debe realizar una operación de detección para utilizar las rutas nuevas.

- No se preocupe demasiado por el tráfico indirecto. Es mejor evitar el tráfico indirecto en un entorno con un gran volumen de I/O para el que cada microsegundo de latencia es crucial, pero el efecto de rendimiento visible es insignificante para las cargas de trabajo típicas.

Diseño de LIF NFS

A diferencia de los protocolos SAN, NFS tiene una capacidad limitada de definir varias rutas para los datos. Las extensiones paralelas de NFS (pNFS) instaladas en NFSv4 solucionan esta limitación, pero, como las velocidades de ethernet han alcanzado los 100GB GbE y más allá, rara vez hay valor en añadir rutas adicionales.

Rendimiento y resiliencia

Aunque medir el rendimiento de LIF de SAN se trata, principalmente, de calcular el ancho de banda total de todas las rutas principales, determinar el rendimiento de LIF NFS requiere observar con más detenimiento la configuración de red exacta. Por ejemplo, se pueden configurar dos puertos 10Gb GbE como puertos físicos sin configurar o como grupo de interfaces del protocolo de control de agregación de enlaces (LACP). Si se configuran como un grupo de interfaces, hay varias políticas de equilibrio de carga disponibles que funcionan de forma diferente en función de si el tráfico se conmuta o se enruta. Por último, Oracle Direct NFS (dNFS) ofrece configuraciones de equilibrio de carga que no existen en ningún cliente NFS del sistema operativo en este momento.

A diferencia de los protocolos SAN, los sistemas de archivos NFS requieren resiliencia en la capa de protocolo. Por ejemplo, un LUN siempre está configurado con multivía habilitado, lo que significa que hay varios canales redundantes disponibles para el sistema de almacenamiento, cada uno de los cuales utiliza el protocolo FC. Un sistema de archivos NFS, por otro lado, depende de la disponibilidad de un único canal TCP/IP que solo se puede proteger en la capa física. Esta disposición es el motivo por el cual existen opciones como la conmutación por error de puerto y la agregación de puertos LACP.

En un entorno NFS, se proporciona rendimiento y flexibilidad en la capa de protocolo de red. Como resultado, ambos temas están entrelazados y deben discutirse juntos.

Enlace las LIF a grupos de puertos

Para enlazar una LIF a un grupo de puertos, asocie la dirección IP de LIF con un grupo de puertos físicos. El principal método para añadir puertos físicos juntos es LACP. La funcionalidad de tolerancia a fallos de LACP es bastante sencilla; cada puerto de un grupo de LACP se supervisa y se elimina del grupo de puertos en caso de que se produzca un funcionamiento incorrecto. No obstante, existen muchos conceptos erróneos sobre cómo funciona LACP con respecto al rendimiento:

- LACP no requiere que la configuración del switch coincida con el extremo. Por ejemplo, ONTAP puede configurarse con balanceo de carga basado en IP, mientras que un switch puede utilizar balanceo de carga basado en MAC.
- Cada punto final que utiliza una conexión LACP puede elegir de forma independiente el puerto de transmisión de paquetes, pero no puede elegir el puerto utilizado para la recepción. Esto significa que el

tráfico de ONTAP a un destino en particular está vinculado a un puerto en particular, y el tráfico de retorno podría llegar a una interfaz diferente. Sin embargo, esto no causa problemas.

- LACP no distribuye el tráfico de manera uniforme en todo momento. En un entorno de gran tamaño con muchos clientes NFS, el resultado suele utilizarse incluso en todos los puertos de una agregación de LACP. Sin embargo, cualquier sistema de archivos NFS en el entorno está limitado al ancho de banda de un solo puerto, no a toda la agregación.
- Si bien las políticas LACP de robin-robin están disponibles en ONTAP, estas políticas no abordan la conexión desde un switch a un host. Por ejemplo, una configuración con un tronco LACP de cuatro puertos en un host y un tronco LACP de cuatro puertos en ONTAP solo puede leer un sistema de archivos utilizando un único puerto. Aunque ONTAP puede transmitir datos a través de los cuatro puertos, actualmente no hay tecnologías de switches disponibles que se envíen del switch al host a través de los cuatro puertos. Solo se utiliza uno.

El enfoque más común en entornos de mayor tamaño que consisten en muchos hosts de base de datos es crear un agregado LACP de un número adecuado de interfaces 10Gb (o más rápidas) mediante el equilibrio de carga de IP. Este enfoque permite a ONTAP ofrecer un uso uniforme de todos los puertos, siempre y cuando existan suficientes clientes. El equilibrio de carga se desglosa cuando hay menos clientes en la configuración porque la conexión troncal LACP no redistribuye la carga de forma dinámica.

Cuando se establece una conexión, el tráfico en una dirección determinada se coloca en un solo puerto. Por ejemplo, una base de datos que realiza una exploración de tabla completa en un sistema de archivos NFS conectado a través de un tronco LACP de cuatro puertos lee los datos aunque solo una tarjeta de interfaz de red (NIC). Si sólo hay tres servidores de base de datos en un entorno de este tipo, es posible que los tres estén leyendo desde el mismo puerto, mientras que los otros tres puertos estén inactivos.

Enlazar LIF a puertos físicos

La vinculación de una LIF a un puerto físico provoca un control más granular sobre la configuración de red, ya que una dirección IP determinada en un sistema ONTAP solo está asociada con un puerto de red a la vez. A continuación, la resiliencia se lleva a cabo mediante la configuración de grupos de conmutación al respaldo y las políticas de conmutación por error.

Políticas de conmutación por error y grupos de conmutación por error

El comportamiento de las LIF durante la interrupción de la red está controlado por las políticas de conmutación por error y los grupos de recuperación tras fallos. Las opciones de configuración han cambiado con las distintas versiones de ONTAP. Consulte la ["Documentación de gestión de redes de ONTAP para políticas y grupos de conmutación por error"](#) Para obtener detalles específicos de la versión de ONTAP que se va a poner en marcha.

ONTAP 8,3 y superiores permiten la gestión de recuperación tras fallos de LIF en función de dominios de retransmisión. Por lo tanto, un administrador puede definir todos los puertos que tienen acceso a una subred determinada y permitir que ONTAP seleccione una LIF de conmutación al nodo de respaldo adecuada. Algunos clientes pueden utilizar este enfoque, pero tiene limitaciones en un entorno de red de almacenamiento de alta velocidad debido a la falta de previsibilidad. Por ejemplo, un entorno puede incluir ambos puertos 1GB para acceso rutinario al sistema de archivos y puertos 10Gb para las operaciones de I/O del archivo de datos Si ambos tipos de puertos existen en el mismo dominio de retransmisión, la conmutación por error de LIF puede provocar que se muevan las operaciones de I/O del archivo de datos de un puerto 10Gb a un puerto 1GB.

En resumen, tenga en cuenta las siguientes prácticas:

1. Configure un grupo de failover como definido por el usuario.

2. Rellenar el grupo de recuperación tras fallos con puertos en el controlador asociado de recuperación tras fallos de almacenamiento (SFO) de modo que los LIF sigan a los agregados durante una conmutación al nodo de respaldo de almacenamiento. Esto evita la creación de tráfico indirecto.
3. Utilice puertos de conmutación por error con las características de rendimiento correspondientes a la LIF original. Por ejemplo, un LIF en un único puerto físico 10Gb debería incluir un grupo de conmutación por error con un único puerto 10Gb. Un LIF LACP de cuatro puertos debe conmutar por error a otro LIF LACP de cuatro puertos. Estos puertos serían un subconjunto de los puertos definidos en el dominio de retransmisión.
4. Establezca la política de recuperación tras fallos únicamente en SFO-partner. Al hacerlo, se asegura de que el LIF siga al agregado durante la recuperación tras fallos.

Reversión automática

Ajuste la `auto-revert` parámetro como desee. La mayoría de los clientes prefieren establecer este parámetro en `true` Para que la LIF vuelva a su puerto de inicio. Sin embargo, en algunos casos, los clientes han establecido esto en 'false' para que se pueda investigar una conmutación por error inesperada antes de devolver una LIF a su puerto de origen.

Proporción de LIF a volumen

Un concepto erróneo común es que debe haber una relación de 1:1 GbE entre los volúmenes y los LIF de NFS. Aunque esta configuración es necesaria para mover un volumen a cualquier punto de un clúster mientras no se crea tráfico de interconexión adicional, no es categóricamente un requisito. Hay que tener en cuenta el tráfico entre clústeres, pero la mera presencia del tráfico entre clústeres no crea problemas. Muchas de las pruebas de rendimiento publicadas creadas para ONTAP incluyen I/O predominantemente indirectas

Por ejemplo, un proyecto de base de datos que contiene una cantidad relativamente pequeña de bases de datos críticas para el rendimiento que solo requerían un total de 40 volúmenes podría justificar un volumen de 1:1 GB para la estrategia LIF, una disposición que requeriría 40 direcciones IP. Posteriormente, cualquier volumen se podría mover a cualquier parte del clúster junto con la LIF asociada; el tráfico siempre sería directo, minimizando todas las fuentes de latencia incluso a niveles de microsegundos.

Como ejemplo por contador, un entorno alojado de gran tamaño se podría gestionar más fácilmente con una relación de 1:1:1 entre clientes y las LIF. Con el tiempo, es posible que se deba migrar un volumen a un nodo diferente, lo cual provocaría cierto tráfico indirecto. Sin embargo, el efecto de rendimiento debe ser indetectable a menos que los puertos de red en el conmutador de interconexión estén saturados. Si hay algún problema, se puede establecer un nuevo LIF en nodos adicionales y el host puede actualizarse en la siguiente ventana de mantenimiento para eliminar el tráfico indirecto de la configuración.

Configuración TCP/IP y ethernet para bases de datos Oracle

Muchos clientes de Oracle en ONTAP utilizan ethernet, el protocolo de red de NFS, iSCSI, NVMe/TCP y, especialmente, el cloud.

Configuración del sistema operativo host

La mayoría de la documentación del proveedor de aplicaciones incluye configuraciones TCP y ethernet específicas para garantizar que la aplicación funcione de manera óptima. Estas mismas configuraciones suelen ser suficientes para ofrecer también un rendimiento óptimo del almacenamiento basado en IP.

Control de flujo Ethernet

Esta tecnología permite a un cliente solicitar que un remitente detenga temporalmente la transmisión de datos. Esto suele hacerse porque el receptor no puede procesar los datos entrantes con la suficiente rapidez. Al mismo tiempo, solicitar que un remitente cesara la transmisión era menos perjudicial que tener un receptor descarte de paquetes porque los buffers estaban llenos. Este ya no es el caso con las pilas TCP utilizadas en los sistemas operativos actualmente. De hecho, el control de flujo causa más problemas de los que resuelve.

Los problemas de rendimiento causados por el control de flujo de Ethernet han aumentado en los últimos años. Esto se debe a que el control de flujo Ethernet funciona en la capa Physical. Si una configuración de red permite que un sistema operativo del host envíe una solicitud de control de flujo de Ethernet a un sistema de almacenamiento, el resultado es una pausa en las operaciones de I/O de todos los clientes conectados. Debido a que una única controladora de almacenamiento atiende cada vez más a un número de clientes, la probabilidad de que uno o varios de estos clientes envíen solicitudes de control de flujo aumenta. El problema se ha observado con frecuencia en las instalaciones de los clientes con una amplia virtualización del SO.

Una NIC de un sistema NetApp no debe recibir solicitudes de control de flujo. El método utilizado para lograr este resultado varía según el fabricante del conmutador de red. En la mayoría de los casos, el control de flujo en un conmutador Ethernet se puede establecer en `receive desired` o `receive on`, lo que significa que una solicitud de control de flujo no se reenvía al controlador de almacenamiento. En otros casos, la conexión de red en la controladora de almacenamiento puede no permitir la deshabilitación de control de flujo. En estos casos, los clientes deben configurarse para que nunca envíen solicitudes de control de flujo, ya sea cambiando a la configuración de NIC en el propio servidor host o a los puertos de switch a los que está conectado el servidor host.



NetApp recomienda asegurarse de que los controladores de almacenamiento NetApp no reciban paquetes de control de flujo Ethernet. Por lo general, esto puede realizarse mediante la configuración de los puertos del switch a los que está conectada la controladora, pero algunas limitaciones en el hardware del switch pueden requerir cambios en el lado del cliente.

Tamaños de MTU

Se ha demostrado que el uso de tramas gigantes ofrece alguna mejora del rendimiento en las redes 1GB al reducir la sobrecarga de la CPU y de la red, pero el beneficio no suele ser significativo.



NetApp recomienda implementar marcos jumbo cuando sea posible, tanto para obtener beneficios potenciales de rendimiento como para preparar la solución para el futuro.

El uso de tramas gigantes en una red 10Gb es casi obligatorio. Esto se debe a que la mayoría de las implementaciones de 10Gb alcanzan un límite de paquetes por segundo sin tramas gigantes antes de alcanzar la marca de 10Gb. El uso de tramas gigantes mejora la eficiencia del procesamiento TCP/IP porque permite que el sistema operativo, el servidor, las NIC y el sistema de almacenamiento procesen menos paquetes, pero más grandes. La mejora del rendimiento varía de NIC a NIC, pero es significativa.

En las implementaciones de tramas gigantes, existe la creencia común, aunque incorrecta, de que todos los dispositivos conectados deben admitir tramas gigantes y que el tamaño de MTU debe coincidir de extremo a extremo. En su lugar, los dos extremos de red negocian el tamaño de trama más alto mutuamente aceptable al establecer una conexión. En un entorno típico, un switch de red se establece con un tamaño de MTU de 9216, la controladora NetApp se establece en 9000 y los clientes se configuran con una combinación de 9000 y 1514. Los clientes que admiten un MTU de 9000 pueden utilizar tramas gigantes, y los clientes que solo puedan admitir 1514 pueden negociar un valor inferior.

Los problemas con esta disposición son raros en un entorno completamente conmutado. Sin embargo, tenga

cuidado en un entorno enrutado que ningún enrutador intermedio se vea forzado a fragmentar tramas gigantes.



NetApp recomienda configurar lo siguiente:

- Las tramas gigantes son deseables, pero no se requieren con Ethernet de 1GB Gb (GbE).
- Se requieren tramas gigantes para lograr el máximo rendimiento, con 10GbE y más rápido.

Parámetros de TCP

A menudo hay tres ajustes mal configurados: Marcas de tiempo TCP, reconocimiento selectivo (SACK) y escalado de ventana TCP. Muchos documentos desactualizados en Internet recomiendan deshabilitar uno o varios de estos parámetros para mejorar el rendimiento. Había algo de mérito en esta recomendación hace muchos años, cuando las capacidades de la CPU eran mucho menores y había un beneficio en reducir la sobrecarga en el procesamiento TCP siempre que fuera posible.

Sin embargo, con los sistemas operativos modernos, deshabilitar cualquiera de estas características de TCP generalmente no resulta en ningún beneficio detectable, a la vez que también puede dañar el rendimiento. Los daños en el rendimiento son especialmente probables en entornos de red virtualizados, ya que estas características son necesarias para gestionar eficazmente la pérdida de paquetes y los cambios en la calidad de la red.



NetApp recomienda habilitar las marcas de tiempo TCP, EL SACK y el escalado de la ventana TCP en el host, y los tres parámetros deben estar activados por defecto en cualquier sistema operativo actual.

Configuración de FC para bases de datos de Oracle

La configuración de SAN FC para bases de datos de Oracle consiste principalmente en seguir prácticas recomendadas diarias de SAN.

Esto incluye medidas de planificación típicas, como asegurar que exista suficiente ancho de banda en la SAN entre el host y el sistema de almacenamiento, comprobar que existan todas las rutas de SAN entre todos los dispositivos requeridos, mediante la configuración de puertos FC requerida por el proveedor de switches FC, para evitar la contención de ISL, y con una supervisión adecuada del tejido SAN.

División en zonas

Una zona de FC nunca debe contener más de un iniciador. Tal arreglo puede parecer funcionar inicialmente, pero la comunicación entre iniciadores finalmente interfiere con el rendimiento y la estabilidad.

Las zonas multidestino se consideran generalmente seguras, aunque en raras ocasiones el comportamiento de los puertos de destino FC de diferentes proveedores ha causado problemas. Por ejemplo, evite incluir los puertos de destino de una cabina de almacenamiento NetApp y otra que no sea de NetApp en la misma zona. Además, es aún más probable que la ubicación de un sistema de almacenamiento NetApp y un dispositivo de cinta en la misma zona cause problemas.

Base de datos Oracle y conectividad ONTAP de conexión directa

A veces, los administradores de almacenamiento prefieren simplificar sus infraestructuras eliminando los switches de red de la configuración. Esto puede ser soportado en algunos escenarios.

ISCSI y NVMe/TCP

Un host que utilice iSCSI o NVMe/TCP se puede conectar directamente a un sistema de almacenamiento y funcionar normalmente. El motivo son las rutas. Las conexiones directas a dos controladoras de almacenamiento diferentes dan como resultado dos rutas independientes para el flujo de datos. La pérdida de una ruta, un puerto o una controladora no impide que se utilice la otra ruta.

NFS

Se puede utilizar el almacenamiento NFS conectado directamente, pero con una limitación considerable: El fallo no funcionará si no se realiza una ejecución significativa de secuencias de comandos, que sería responsabilidad del cliente.

El motivo por el que la recuperación tras fallos sin interrupciones se complica gracias al almacenamiento NFS de conexión directa es el enrutamiento que se produce en el sistema operativo local. Por ejemplo, supongamos que un host tiene una dirección IP de 192.168.1.1/24 y está directamente conectado a una controladora ONTAP con la dirección IP 192.168.1.50/24. Durante la conmutación al nodo de respaldo, esa dirección 192.168.1.50 puede conmutar al nodo de respaldo a la otra controladora y estará disponible para el host, pero ¿cómo detecta el host su presencia? La dirección 192.168.1.1 original todavía existe en la NIC host que ya no se conecta a un sistema operativo. El tráfico destinado a 192.168.1.50 seguiría enviándose a un puerto de red inoperable.

La segunda NIC del SO podría configurarse como 192.168.1.2 y sería capaz de comunicarse con la dirección fallida en 192.168.1.50, pero las tablas de enrutamiento locales tendrían un valor predeterminado de usar una dirección **y solo una** para comunicarse con la subred 192.168.1.0/24. Un administrador de sistema podría crear un marco de scripting que detectara una conexión de red fallida y alterara las tablas de enrutamiento locales o activara o desactivara las interfaces. El procedimiento exacto dependerá del sistema operativo en uso.

En la práctica, los clientes de NetApp disponen de NFS conectado directamente, pero normalmente solo para cargas de trabajo en las que se pueden pausar I/O durante las recuperaciones tras fallos. Cuando se utilizan montajes duros, no debe haber ningún error de E/S durante dichas pausas. El I/O se debe bloquear hasta que los servicios se restauren, ya sea mediante una conmutación de retorno tras recuperación o intervención manual para mover las direcciones IP entre las NIC del host.

Conexión directa FC

No es posible conectar directamente un host a un sistema de almacenamiento ONTAP mediante el protocolo FC. La razón es el uso de NPIV. El WWN que identifica un puerto ONTAP FC con la red de FC utiliza un tipo de virtualización denominado NPIV. Cualquier dispositivo conectado a un sistema ONTAP debe poder reconocer un WWN de NPIV. No hay proveedores de HBA actuales que ofrezcan un HBA que se pueda instalar en un host que admita un destino NPIV.

Información de copyright

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

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

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

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

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

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

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

Información de la marca comercial

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