



Configuração de rede em sistemas AFF/ FAS

Enterprise applications

NetApp

February 11, 2026

Índice

Configuração de rede em sistemas AFF/ FAS	1
Interfaces lógicas	1
Tipos de LIF	1
Design de SAN LIF	1
Design de LIF de NFS	3
Configuração TCP/IP e ethernet	5
Configurações do sistema operacional do host	5
Controle de fluxo Ethernet	5
Tamanhos de MTU	6
Parâmetros TCP	7
Configuração de FC SAN	7
Zoneamento	7
Rede de conexão direta	7
ISCSI e NVMe/TCP	7
NFS	8
Conexão direta FC	8

Configuração de rede em sistemas AFF/ FAS

Interfaces lógicas

Os bancos de dados Oracle precisam de acesso ao armazenamento. Interfaces lógicas (LIFs) são o encanamento de rede que conecta uma máquina virtual de armazenamento (SVM) à rede e, por sua vez, ao banco de dados. O design de LIF adequado é necessário para garantir que haja largura de banda suficiente para cada workload de banco de dados, e o failover não resulta em perda de serviços de storage.

Esta seção fornece uma visão geral dos principais princípios de design de LIF. Para obter documentação mais abrangente, consulte o ["Documentação do Gerenciamento de rede da ONTAP"](#). Assim como em outros aspectos da arquitetura de banco de dados, as melhores opções para o design de máquina virtual de storage (SVM, conhecido como vserver na CLI) e interface lógica (LIF) dependem muito dos requisitos de dimensionamento e necessidades de negócios.

Considere os seguintes tópicos principais ao criar uma estratégia de LIF:

- **Desempenho.** A largura de banda da rede é suficiente?
- **Resiliência.** Há algum ponto único de falha no projeto?
- **Capacidade de gerenciamento.** A rede pode ser dimensionada sem interrupções?

Esses tópicos se aplicam à solução completa, desde o host até os switches até o sistema de storage.

Tipos de LIF

Existem vários tipos de LIF. ["Documentação do ONTAP sobre tipos de LIF"](#) Forneça informações mais completas sobre este tópico, mas de uma perspectiva funcional os LIFs podem ser divididos nos seguintes grupos:

- **LIFs de gerenciamento de clusters e nós.** LIFs usadas para gerenciar o cluster de armazenamento.
- **LIFs de gerenciamento de SVM.** Interfaces que permitem o acesso a um SVM por meio da API REST ou ONTAPI (também conhecida como ZAPI) para funções como criação de snapshot ou redimensionamento de volume. Produtos como o SnapManager para Oracle (SMO) precisam ter acesso a um LIF de gerenciamento de SVM.
- **LIFs de dados.** Interfaces para dados FC, iSCSI, NVMe/FC, NVMe/TCP, NFS ou SMB/CIFS.

 Um LIF de dados usado para tráfego NFS também pode ser usado para gerenciamento alterando a política de firewall de data para mgmt ou outra política que permita HTTP, HTTPS ou SSH. Essa alteração pode simplificar a configuração de rede evitando a configuração de cada host para acesso ao LIF de dados NFS e a um LIF de gerenciamento separado. Não é possível configurar uma interface para iSCSI e tráfego de gerenciamento, apesar do fato de ambos usarem um protocolo IP. Um LIF de gerenciamento separado é necessário em ambientes iSCSI.

Design de SAN LIF

O design de LIF em um ambiente SAN é relativamente simples por um motivo: Multipathing. Todas as implementações de SAN modernas permitem que um cliente acesse dados em vários caminhos de rede

independentes e selecione o melhor caminho ou caminhos para acesso. Como resultado, o desempenho em relação ao design de LIF é mais simples de abordar, pois os clientes SAN equilibram automaticamente a e/S de carga nos melhores caminhos disponíveis.

Se um caminho ficar indisponível, o cliente selecionará automaticamente um caminho diferente. A simplicidade resultante do design torna os LIFs SAN geralmente mais gerenciáveis. Isso não significa que um ambiente SAN sempre seja gerenciado com mais facilidade, porque há muitos outros aspectos do storage SAN que são muito mais complicados do que o NFS. Isso significa simplesmente que o design de SAN LIF é mais fácil.

Desempenho

A consideração mais importante com o desempenho de LIF em um ambiente SAN é a largura de banda. Por exemplo, um cluster ONTAP AFF de dois nós com duas portas FC de 16GB GB por nó permite até 32GB Gbps de largura de banda de/para cada nó.

Resiliência

OS LIFs DE SAN não fazem failover em um sistema de storage da AFF. Se um LIF SAN falhar devido ao failover de controladora, o software multipathing do cliente deteta a perda de um caminho e redireciona e/S para um LIF diferente. Com os sistemas de armazenamento ASA, os LIFs serão falhados após um curto atraso, mas isso não interrompe a e/S porque já existem caminhos ativos no outro controlador. O processo de failover ocorre para restaurar o acesso do host em todas as portas definidas.

Capacidade de gerenciamento

A migração de LIF é uma tarefa muito mais comum em um ambiente NFS, pois a migração de LIF geralmente é associada à realocação de volumes no cluster. Não é necessário migrar um LIF em um ambiente SAN quando os volumes são transferidos para o par de HA. Isso ocorre porque, após a conclusão da movimentação de volume, o ONTAP envia uma notificação à SAN sobre uma alteração nos caminhos e os clientes SAN reotimizam automaticamente. A migração de LIF com SAN está associada principalmente a grandes alterações de hardware físico. Por exemplo, se uma atualização sem interrupções dos controladores for necessária, um LIF SAN é migrado para o novo hardware. Se uma porta FC estiver defeituosa, um LIF pode ser migrado para uma porta não utilizada.

Recomendações de design

A NetApp faz as seguintes recomendações:

- Não crie mais caminhos do que o necessário. O número excessivo de caminhos torna o gerenciamento geral mais complicado e pode causar problemas com failover de caminho em alguns hosts. Além disso, alguns hosts têm limitações de caminho inesperadas para configurações como inicialização por SAN.
- Poucas configurações devem exigir mais de quatro caminhos para um LUN. O valor de ter mais de dois nós anunciando caminhos para LUNs é limitado porque o host agregado de um LUN fica inacessível se o nó proprietário do LUN e seu parceiro de HA falhar. A criação de caminhos em nós que não o par de HA principal não é útil em tal situação.
- Embora o número de caminhos de LUN visíveis possa ser gerenciado selecionando quais portas estão incluídas nas zonas FC, geralmente é mais fácil incluir todos os pontos de destino potenciais na zona FC e controlar a visibilidade de LUN no nível ONTAP.
- No ONTAP 8,3 e posterior, o recurso de mapeamento de LUN seletivo (SLM) é o padrão. Com o SLM, qualquer novo LUN é automaticamente anunciado a partir do nó que é proprietário do agregado subjacente e do parceiro de HA do nó. Esse arranjo evita a necessidade de criar conjuntos de portas ou configurar o zoneamento para limitar a acessibilidade de portas. Cada LUN está disponível no número

mínimo de nós necessário para ter a melhor performance e resiliência. *Caso um LUN precise ser migrado para fora dos dois controladores, os nós adicionais podem ser adicionados com o `lun mapping add-reporting-nodes` comando para que os LUNs sejam anunciados nos novos nós. Isso cria caminhos SAN adicionais para os LUNs para migração de LUN. No entanto, o host deve executar uma operação de descoberta para usar os novos caminhos.

- Não se preocupe excessivamente com o tráfego indireto. É melhor evitar o tráfego indireto em um ambiente com uso intenso de e/S para o qual cada microsegundo de latência é crítico, mas o efeito de performance visível é insignificante para workloads típicos.

Design de LIF de NFS

Em contraste com os protocolos SAN, o NFS tem uma capacidade limitada de definir vários caminhos para os dados. As extensões NFS paralelas (pNFS) para NFSv4 abordam essa limitação, mas como as velocidades ethernet atingiram 100GBMbps e além raramente há valor na adição de caminhos adicionais.

Performance e resiliência

Embora a medição do desempenho do SAN LIF seja principalmente uma questão de calcular a largura de banda total de todos os caminhos principais, determinar o desempenho do NFS LIF requer uma visão mais detalhada da configuração exata da rede. Por exemplo, duas portas 10Gb podem ser configuradas como portas físicas brutas ou podem ser configuradas como um grupo de interfaces LACP (Link Aggregation Control Protocol). Se eles estiverem configurados como um grupo de interfaces, várias políticas de balanceamento de carga estarão disponíveis que funcionam de forma diferente, dependendo se o tráfego é comutado ou roteado. Por fim, o Oracle Direct NFS (DNFS) oferece configurações de balanceamento de carga que não existem em nenhum cliente NFS do sistema operacional no momento.

Diferentemente dos protocolos SAN, os sistemas de arquivos NFS exigem resiliência na camada do protocolo. Por exemplo, um LUN é sempre configurado com multipathing habilitado, o que significa que vários canais redundantes estão disponíveis para o sistema de storage, cada um dos quais usa o protocolo FC. Um sistema de arquivos NFS, por outro lado, depende da disponibilidade de um único canal TCP/IP que só pode ser protegido na camada física. Esse arranjo é o motivo pelo qual existem opções como failover de portas e agregação de portas LACP.

Em um ambiente NFS, a performance e a resiliência são fornecidas na camada de protocolo de rede. Como resultado, ambos os tópicos estão interligados e devem ser discutidos juntos.

Vincular LIFs a grupos de portas

Para vincular um LIF a um grupo de portas, associe o endereço IP de LIF a um grupo de portas físicas. O método principal para agregar portas físicas em conjunto é o LACP. A capacidade de tolerância a falhas do LACP é bastante simples; cada porta em um grupo LACP é monitorada e removida do grupo de portas em caso de mau funcionamento. Existem, no entanto, muitos equívocos sobre como o LACP funciona em relação ao desempenho:

- O LACP não requer a configuração no switch para corresponder ao endpoint. Por exemplo, o ONTAP pode ser configurado com平衡amento de carga baseado em IP, enquanto um switch pode usar平衡amento de carga baseado em MAC.
- Cada endpoint que usa uma conexão LACP pode escolher independentemente a porta de transmissão de pacotes, mas não pode escolher a porta usada para recebimento. Isso significa que o tráfego de ONTAP para um destino específico está vinculado a uma porta específica, e o tráfego de retorno pode chegar em uma interface diferente. No entanto, isso não causa problemas.
- O LACP não distribui uniformemente o tráfego o tempo todo. Em um ambiente grande com muitos clientes NFS, o resultado é normalmente até mesmo o uso de todas as portas em uma agregação LACP. No

entanto, qualquer sistema de arquivos NFS no ambiente é limitado à largura de banda de apenas uma porta, e não a agregação inteira.

- Embora as políticas LACP robin estejam disponíveis no ONTAP, essas políticas não abordam a conexão de um switch para um host. Por exemplo, uma configuração com um tronco LACP de quatro portas em um host e um tronco LACP de quatro portas no ONTAP ainda é capaz de ler apenas um sistema de arquivos usando uma única porta. Embora o ONTAP possa transmitir dados através das quatro portas, não há tecnologias de switch disponíveis que sejam enviadas do switch para o host através das quatro portas. Apenas um é usado.

A abordagem mais comum em ambientes maiores que consistem em muitos hosts de banco de dados é construir um agregado LACP de um número apropriado de interfaces 10Gb (ou mais rápidas) usando o balanceamento de carga IP. Essa abordagem permite que o ONTAP forneça uso uniforme de todas as portas, desde que existam clientes suficientes. O balanceamento de carga é interrompido quando há menos clientes na configuração porque o entroncamento LACP não redistribui dinamicamente a carga.

Quando uma conexão é estabelecida, o tráfego em uma determinada direção é colocado em apenas uma porta. Por exemplo, um banco de dados que executa uma verificação de tabela completa em um sistema de arquivos NFS conectado por meio de um tronco LACP de quatro portas lê dados através de apenas uma placa de interface de rede (NIC). Se apenas três servidores de banco de dados estiverem em tal ambiente, é possível que todos os três estejam lendo da mesma porta, enquanto as outras três portas estiverem ociosas.

Vincule LIFs a portas físicas

Vincular um LIF a uma porta física resulta em um controle mais granular sobre a configuração de rede, pois um determinado endereço IP em um sistema ONTAP está associado a apenas uma porta de rede de cada vez. A resiliência é então realizada por meio da configuração de grupos de failover e políticas de failover.

Políticas de failover e grupos de failover

O comportamento dos LIFs durante a interrupção da rede é controlado por políticas de failover e grupos de failover. As opções de configuração foram alteradas com as diferentes versões do ONTAP. Consulte o "[Documentação de gerenciamento de rede ONTAP para grupos e políticas de failover](#)" para obter detalhes específicos sobre a versão do ONTAP que está sendo implantado.

O ONTAP 8,3 e superior permitem o gerenciamento de failover de LIF com base em domínios de broadcast. Portanto, um administrador pode definir todas as portas que têm acesso a uma determinada sub-rede e permitir que o ONTAP selecione um LIF de failover apropriado. Essa abordagem pode ser usada por alguns clientes, mas tem limitações em um ambiente de rede de storage de alta velocidade devido à falta de previsibilidade. Por exemplo, um ambiente pode incluir ambas as portas 1Gb para acesso de rotina ao sistema de arquivos e portas 10Gb para e/S de arquivo de dados. Se ambos os tipos de portas existirem no mesmo domínio de broadcast, o failover de LIF pode resultar na movimentação de e/S de um arquivo de dados de uma porta 10Gb para uma porta 1Gb.

Em resumo, considere as seguintes práticas:

1. Configurar um grupo de failover conforme definido pelo usuário.
2. Preencha o grupo de failover com portas na controladora de parceiro de failover de storage (SFO) para que as LIFs sigam os agregados durante um failover de storage. Isso evita a criação de tráfego indireto.
3. Use portas de failover com características de desempenho correspondentes ao LIF original. Por exemplo, um LIF em uma única porta 10Gb física deve incluir um grupo de failover com uma única porta 10Gb. Um LIF LACP de quatro portas deve falhar para outro LIF LACP de quatro portas. Essas portas seriam um subconjunto das portas definidas no domínio de broadcast.
4. Defina a política de failover como somente parceiro SFO. Isso garante que o LIF siga o agregado durante

o failover.

Reversão automática

Defina auto-revert o parâmetro conforme desejado. A maioria dos clientes prefere definir este parâmetro para que true o LIF reverta para sua porta inicial. No entanto, em alguns casos, os clientes definiram isso como "falso" que um failover inesperado pode ser investigado antes de retornar um LIF à sua porta inicial.

Relação LIF-volume

Um equívoco comum é que deve haver uma relação do 1:1 entre volumes e LIFs NFS. Embora essa configuração seja necessária para mover um volume em qualquer lugar em um cluster, sem nunca criar tráfego de interconexão adicional, ela não é categoricamente um requisito. O tráfego entre clusters deve ser considerado, mas a mera presença de tráfego entre clusters não cria problemas. Muitos dos benchmarks publicados criados para o ONTAP incluem predominantemente I/O. indireto

Por exemplo, um projeto de banco de dados contendo um número relativamente pequeno de bancos de dados críticos ao desempenho que exigiam apenas um total de 40 volumes pode garantir um volume 1:1 para a estratégia LIF, um arranjo que exigiria 40 endereços IP. Qualquer volume poderia então ser movido para qualquer lugar do cluster junto com o LIF associado, e o tráfego sempre seria direto, minimizando cada fonte de latência, mesmo nos níveis de microssegundos.

Como um exemplo de contador, um ambiente grande e hospedado pode ser mais facilmente gerenciado com um relacionamento 1:1 entre clientes e LIFs. Com o tempo, um volume pode precisar ser migrado para um nó diferente, o que causaria algum tráfego indireto. No entanto, o efeito de desempenho deve ser indetectável, a menos que as portas de rede no switch de interconexão estejam saturando. Se houver problema, um novo LIF pode ser estabelecido em nós adicionais e o host pode ser atualizado na próxima janela de manutenção para remover o tráfego indireto da configuração.

Configuração TCP/IP e ethernet

Muitos clientes do Oracle no ONTAP usam ethernet, o protocolo de rede de NFS, iSCSI, NVMe/TCP e, especialmente, a nuvem.

Configurações do sistema operacional do host

A maioria da documentação do fornecedor de aplicativos inclui configurações específicas de TCP e ethernet destinadas a garantir que o aplicativo esteja funcionando de forma ideal. Essas mesmas configurações geralmente são suficientes para oferecer também um desempenho ideal de storage baseado em IP.

Controle de fluxo Ethernet

Esta tecnologia permite que um cliente solicite que um remetente pare temporariamente a transmissão de dados. Isso geralmente é feito porque o receptor não consegue processar os dados de entrada com rapidez suficiente. Ao mesmo tempo, solicitar que um remetente cessasse a transmissão era menos disruptivo do que ter um receptor descartar pacotes porque os buffers estavam cheios. Este não é mais o caso com as pilhas TCP usadas nos sistemas operacionais atuais. Na verdade, o controle de fluxo causa mais problemas do que resolve.

Os problemas de desempenho causados pelo controle de fluxo Ethernet têm aumentado nos últimos anos. Isso ocorre porque o controle de fluxo Ethernet opera na camada física. Se uma configuração de rede permitir que qualquer sistema operacional host envie uma solicitação de controle de fluxo Ethernet para um sistema de armazenamento, o resultado será uma pausa em e/S para todos os clientes conectados. Como um número

crescente de clientes é servido por um único controlador de armazenamento, a probabilidade de um ou mais desses clientes enviar solicitações de controle de fluxo aumenta. O problema tem sido visto frequentemente em sites de clientes com ampla virtualização de SO.

Uma NIC em um sistema NetApp não deve receber solicitações de controle de fluxo. O método utilizado para alcançar este resultado varia consoante o fabricante do comutador de rede. Na maioria dos casos, o controle de fluxo em um switch Ethernet pode ser definido como `receive desired receive on` ou , o que significa que uma solicitação de controle de fluxo não é encaminhada para o controlador de armazenamento. Em outros casos, a conexão de rede no controlador de armazenamento pode não permitir a desativação do controle de fluxo. Nesses casos, os clientes devem ser configurados para nunca enviar solicitações de controle de fluxo, seja alterando para a configuração da NIC no próprio servidor host ou para as portas de switch às quais o servidor host está conectado.

 **A NetApp recomenda** certificando-se de que os controladores de armazenamento NetApp não recebam pacotes de controle de fluxo Ethernet. Isso geralmente pode ser feito definindo as portas do switch às quais o controlador está conectado, mas alguns hardwares do switch têm limitações que podem exigir alterações no lado do cliente.

Tamanhos de MTU

O uso de quadros jumbo tem sido mostrado para oferecer alguma melhoria de desempenho em redes 1GBG, reduzindo a sobrecarga de CPU e rede, mas o benefício geralmente não é significativo.

 **A NetApp recomenda** a implementação de quadros jumbo quando possível, tanto para obter quaisquer benefícios potenciais de desempenho quanto para preparar a solução para o futuro.

Usar quadros jumbo em uma rede 10GbG é quase obrigatório. Isso ocorre porque a maioria das implementações 10Gb atingem um limite de pacotes por segundo sem quadros jumbo antes que atinjam a marca 10Gb. O uso de quadros jumbo melhora a eficiência no processamento TCP/IP porque permite que o sistema operacional, servidor, NICs e o sistema de armazenamento processem menos pacotes, mas maiores. A melhoria do desempenho varia de NIC para NIC, mas é significativa.

Para implementações de quadros jumbo, existe a crença comum, mas incorreta, de que todos os dispositivos conectados devem suportar quadros jumbo e que o tamanho da MTU deve corresponder de ponta a ponta. Em vez disso, os dois pontos de extremidade da rede negociam o tamanho de quadro mais alto mutuamente aceitável ao estabelecer uma conexão. Em um ambiente típico, um switch de rede é definido para um tamanho MTU de 9216, o controlador NetApp é definido como 9000 e os clientes são definidos como uma combinação de 9000 e 1514. Os clientes que podem suportar um MTU de 9000 podem usar quadros jumbo, e os clientes que só podem suportar 1514 podem negociar um valor mais baixo.

Problemas com este arranjo são raros em um ambiente completamente comutado. No entanto, tenha cuidado em um ambiente roteado que nenhum roteador intermediário é forçado a fragmentar quadros jumbo.

A NetApp recomenda configurando o seguinte:

- 
- Os quadros jumbo são desejáveis, mas não são necessários com Ethernet de 1GB GB (GbE).
 - Os quadros Jumbo são necessários para o máximo desempenho com 10GbE e mais rápido.

Parâmetros TCP

Três configurações geralmente são mal configuradas: Carimbos de data/hora TCP, reconhecimento seletivo (SACK) e escala de janela TCP. Muitos documentos desatualizados na Internet recomendam desativar um ou mais desses parâmetros para melhorar o desempenho. Havia algum mérito a esta recomendação há muitos anos, quando os recursos da CPU eram muito menores e havia um benefício para reduzir a sobrecarga no processamento TCP sempre que possível.

No entanto, com os sistemas operacionais modernos, desabilitar qualquer um desses recursos TCP geralmente resulta em nenhum benefício detetável, ao mesmo tempo em que potencialmente danifica o desempenho. Os danos no desempenho são especialmente prováveis em ambientes de rede virtualizados, pois esses recursos são necessários para o manuseio eficiente da perda de pacotes e alterações na qualidade da rede.

 **A NetApp recomenda** a ativação de timestamps TCP, SACK e escala de janelas TCP no host, e todos esses três parâmetros devem estar ativados por padrão em qualquer sistema operacional atual.

Configuração de FC SAN

A configuração do FC SAN para bancos de dados Oracle trata principalmente de seguir as práticas recomendadas diárias de SAN.

Isso inclui medidas de Planejamento típicas, como garantir a existência de largura de banda suficiente na SAN entre o host e o sistema de storage, verificar se todos os caminhos de SAN existem entre todos os dispositivos necessários, usar as configurações de porta FC exigidas pelo fornecedor do switch FC, evitar a contenção de ISL e usar o monitoramento adequado da malha SAN.

Zoneamento

Uma zona FC nunca deve conter mais de um iniciador. Tal arranjo pode parecer funcionar inicialmente, mas a conversa cruzada entre iniciadores eventualmente interfere com o desempenho e a estabilidade.

As zonas de destino múltiplo são geralmente consideradas seguras, embora em raras circunstâncias o comportamento das portas de destino FC de diferentes fornecedores tenha causado problemas. Por exemplo, evite incluir as portas de destino de um storage array NetApp e não NetApp na mesma zona. Além disso, é ainda mais provável que colocar um sistema de storage NetApp e um dispositivo de fita na mesma zona cause problemas.

Rede de conexão direta

Às vezes, os administradores de storage preferem simplificar suas infraestruturas removendo switches de rede da configuração. Isso pode ser suportado em alguns cenários.

iSCSI e NVMe/TCP

Um host usando iSCSI ou NVMe/TCP pode ser conectado diretamente a um sistema de storage e operar normalmente. A razão é pathing. Conexões diretas a dois controladores de storage diferentes resultam em dois caminhos independentes para o fluxo de dados. A perda de caminho, porta ou controlador não impede que o outro caminho seja usado.

NFS

O armazenamento NFS com conexão direta pode ser usado, mas com uma limitação significativa - o failover não funcionará sem um esforço significativo de script, o que seria da responsabilidade do cliente.

O motivo pelo qual o failover sem interrupções é complicado com o storage NFS com conexão direta é o roteamento que ocorre no sistema operacional local. Por exemplo, suponha que um host tenha um endereço IP de 192.168.1.1/24 e esteja conectado diretamente a um controlador ONTAP com um endereço IP de 192.168.1.50/24. Durante o failover, esse endereço 192.168.1.50 pode fazer failover para a outra controladora e estará disponível para o host, mas como o host deteta sua presença? O endereço 192.168.1.1 original ainda existe na NIC host que não se conecta mais a um sistema operacional. O tráfego destinado a 192.168.1.50 continuaria a ser enviado para uma porta de rede inoperável.

A segunda NIC do SO poderia ser configurada como 192.168.1.2 e seria capaz de se comunicar com o endereço 192.168.1.50 com falha, mas as tabelas de roteamento local teriam um padrão de usar um endereço **e apenas um** para se comunicar com a sub-rede 192.168.1.0/24. Um sysadmin poderia criar uma estrutura de script que detetaria uma conexão de rede com falha e alteraria as tabelas de roteamento local ou colocaria interfaces para cima e para baixo. O procedimento exato dependeria do SO em uso.

Na prática, os clientes da NetApp têm NFS com conexão direta, mas normalmente apenas para workloads em que as pausas de e/S durante failovers são aceitáveis. Quando os suportes rígidos são usados, não deve haver nenhum erro de e/S durante essas pausas. O IO deve travar até que os serviços sejam restaurados, seja por um fallback ou intervenção manual para mover endereços IP entre NICs no host.

Conexão direta FC

Não é possível conectar diretamente um host a um sistema de storage ONTAP usando o protocolo FC. A razão é o uso de NPIV. A WWN que identifica uma porta ONTAP FC para a rede FC usa um tipo de virtualização chamado NPIV. Qualquer dispositivo conectado a um sistema ONTAP deve ser capaz de reconhecer um NPIV WWN. Não há fornecedores atuais de HBA que ofereçam um HBA que possa ser instalado em um host que possa suportar um destino NPIV.

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.