Configurazione di rete

Enterprise applications

NetApp
May 09, 2024

Sommario

Configurazione di rete

Progettazione dell'interfaccia logica per i database Oracle

I database Oracle devono accedere allo storage. Le interfacce logiche (LIF) sono le tubazioni di rete che collegano una Storage Virtual Machine (SVM) alla rete e a loro volta al database. La corretta progettazione della LIF è necessaria per garantire una larghezza di banda sufficiente per ogni carico di lavoro del database e il failover non comporta una perdita dei servizi storage.

Questa sezione offre una panoramica dei principali principi di progettazione della LIF. Per una documentazione più completa, vedere "Documentazione di gestione della rete ONTAP". Come per altri aspetti dell'architettura dei database, le migliori opzioni per la progettazione di una Storage Virtual Machine (SVM, nota come vserver all'interfaccia della CLI) e di un'interfaccia logica (LIF) dipendono in gran parte dai requisiti di scalabilità e dalle esigenze di business.

Durante la creazione di una strategia LIF, prendi in considerazione i seguenti argomenti principali:

- **Performance.** la larghezza di banda della rete è sufficiente?
- **Resilienza.** ci sono singoli punti di guasto nel progetto?
- **Gestibilità.** la rete può essere scalata senza interruzioni?

Gli argomenti trattati sono relativi alla soluzione end-to-end, dall'host fino agli switch fino al sistema storage.

Tipi di LIF

Esistono diversi tipi di LIF. "Documentazione ONTAP sui tipi di LIF" Fornisci informazioni più complete su questo argomento, ma da un punto di vista funzionale le LIF possono essere divise in gruppi:

- **LIF di gestione cluster e nodi.** LIF utilizzati per gestire il cluster storage.
- **LIF di gestione SVM.** interfacce che consentono l'accesso a una SVM tramite l'API REST o ONTAPI (nota anche come ZAPI) per funzioni come la creazione di snapshot o il ridimensionamento del volume. Prodotti come SnapManager for Oracle (SMO) devono avere accesso a una LIF di gestione SVM.
- **Interfacce LIF dati** per FC, iSCSI, NVMe/FC, NVMe/TCP, NFS, o dati SMB/CIFS.

> Una LIF dati utilizzata per il traffico NFS può anche essere utilizzata per la gestione cambiando la policy del firewall da `data` a. `mgmt` O un'altra policy che consente HTTP, HTTPS o SSH. Questa modifica può semplificare la configurazione di rete evitando la configurazione di ciascun host per l'accesso sia alla LIF dati NFS che a una LIF di gestione separata. Non è possibile configurare un'interfaccia sia per iSCSI che per il traffico di gestione, nonostante entrambi utilizzino un protocollo IP. Negli ambienti iSCSI è necessaria una LIF di gestione separata.

Progettazione della SAN LIF

Il design di LIF in un ambiente SAN è relativamente semplice per un motivo: Il multipathing. Tutte le moderne implementazioni SAN consentono a un client di accedere ai dati su più percorsi di rete indipendenti e di selezionare i percorsi migliori per l'accesso. Di conseguenza, le performance rispetto alla progettazione LIF sono più semplici da gestire, perché i client SAN bilanciano automaticamente il carico dell'i/o nei migliori percorsi disponibili.

Se un percorso non è disponibile, il client seleziona automaticamente un percorso diverso. Grazie alla sua semplicità di progettazione, le LIF SAN sono generalmente più gestibili. Ciò non significa che un ambiente SAN sia sempre più facile da gestire, poiché vi sono molti altri aspetti dello storage SAN che sono molto più complicati di NFS. Significa semplicemente che la progettazione della SAN LIF è più semplice.

Performance

La considerazione più importante riguardo le performance di una LIF in un ambiente SAN è la larghezza di banda. Ad esempio, un cluster ONTAP AFF a due nodi con due porte FC da 16GB GB per nodo offre fino a 32GB Gbps di larghezza di banda da/per ciascun nodo.

Resilienza

Le LIF SAN non eseguono il failover su un sistema storage AFF. In caso di guasto di una LIF SAN a causa del failover del controller, il software multipath del client rileva la perdita di un percorso e reindirizza l'i/o a una diversa LIF. Con i sistemi storage ASA, il failover delle LIF dopo un breve ritardo, ma ciò non interrompe l'io perché ci sono percorsi già attivi sull'altro controller. Il processo di failover viene eseguito per ripristinare l'accesso dell'host su tutte le porte definite.

Gestibilità

La migrazione LIF è un task molto più comune in un ambiente NFS, perché la migrazione LIF è spesso associata alla riallocazione dei volumi nel cluster. Non è necessario migrare una LIF in un ambiente SAN quando i volumi vengono ricollocati nella coppia ha. Questo perché, una volta completato lo spostamento del volume, ONTAP invia una notifica alla SAN in merito a una modifica dei percorsi e i client SAN vengono automaticamente risottimizzati. La migrazione LIF con SAN è associata principalmente a importanti modifiche hardware fisiche. Ad esempio, per eseguire un upgrade senza interruzioni dei controller, viene eseguita la migrazione di una SAN LIF nel nuovo hardware. Se una porta FC è guasta, una LIF può essere migrata a una porta inutilizzata.

Raccomandazioni di progettazione

NetApp formula i seguenti consigli:

- Non creare più percorsi di quelli richiesti. Un numero eccessivo di percorsi complica la gestione complessiva e può causare problemi con il failover del percorso su alcuni host. Inoltre, alcuni host hanno limitazioni inattese del percorso per configurazioni come l'avvio SAN.
- Un numero molto ridotto di configurazioni deve richiedere più di quattro percorsi a un LUN. Il valore di avere più di due nodi che pubblicizzano i percorsi delle LUN è limitato perché l'aggregato che ospita un LUN è inaccessibile in caso di guasto del nodo proprietario del LUN e del partner ha. In una situazione del genere, la creazione di percorsi su nodi diversi dalla coppia ha primaria non è d'aiuto.
- Sebbene il numero di percorsi LUN visibili possa essere gestito selezionando le porte incluse nelle zone FC, in genere è più semplice includere tutti i potenziali punti di destinazione nella zona FC e controllare la visibilità delle LUN a livello ONTAP.
- In ONTAP 8,3 e versioni successive, la funzione SLM (Selective LUN mapping) è quella predefinita. Con SLM, ogni nuova LUN viene automaticamente pubblicizzata dal nodo proprietario dell'aggregato sottostante e del partner ha del nodo. Questa disposizione evita la necessità di creare set di porte o configurare la suddivisione in zone per limitare l'accessibilità delle porte. Ogni LUN è disponibile sul numero minimo di nodi necessari per performance e resilienza ottimali.
  *Nel caso in cui sia necessario migrare un LUN all'esterno dei due controller, è possibile aggiungere i nodi aggiuntivi con `lun mapping add-reporting-nodes` In modo che le LUN vengano pubblicizzate sui nuovi nodi. In questo modo si creano ulteriori percorsi SAN alle LUN per la migrazione delle LUN. Tuttavia, l'host deve eseguire un'operazione di rilevamento per utilizzare i nuovi percorsi.

- Non preoccupatevi eccessivamente del traffico indiretto. Si consiglia di evitare il traffico indiretto in un ambiente i/o-intensive per il quale è critico ogni microsecondo di latenza, ma l'effetto visibile delle performance è trascurabile per i workload tipici.

Progettazione della LIF NFS

A differenza dei protocolli SAN, NFS ha una capacità limitata di definire percorsi multipli ai dati. Le estensioni Parallel NFS (pNFS) a NFSv4 risolvono questo limite, ma poiché le velocità ethernet hanno raggiunto 100GB Mbps e oltre, raramente è utile aggiungere altri percorsi.

Performance e resilienza

Sebbene la misurazione delle performance SAN LIF si debba principalmente calcolare la larghezza di banda totale da tutti i percorsi primari, la determinazione delle performance NFS LIF richiede un'analisi più approfondita dell'esatta configurazione di rete. Ad esempio, è possibile configurare due porte 10Gb come porte fisiche grezze oppure come gruppo di interfacce LACP (link Aggregation Control Protocol). Se sono configurati come gruppo di interfacce, sono disponibili più criteri di bilanciamento del carico che funzionano in modo diverso a seconda che il traffico sia commutato o instradato. Infine, Oracle Direct NFS (DNFS) offre configurazioni di bilanciamento del carico attualmente inesistenti in nessun client NFS del sistema operativo.

A differenza dei protocolli SAN, i file system NFS richiedono resilienza al livello del protocollo. Ad esempio, un LUN è sempre configurato con il multipathing attivato, ovvero sono disponibili più canali ridondanti per il sistema storage, ciascuno dei quali utilizza il protocollo FC. Un file system NFS, invece, dipende dalla disponibilità di un unico canale TCP/IP che può essere protetto solo a livello fisico. Questa disposizione è il motivo per cui esistono opzioni quali il failover della porta e l'aggregazione della porta LACP.

In un ambiente NFS, performance e resilienza sono fornite a livello del protocollo di rete. Di conseguenza, entrambi gli argomenti sono intrecciati e devono essere discussi insieme.

Associare le LIF ai gruppi di porte

Per associare una LIF a un gruppo di porte, associare l'indirizzo IP della LIF a un gruppo di porte fisiche. Il metodo principale per aggregare insieme le porte fisiche è LACP. La capacità di fault tolerance di LACP è abbastanza semplice; ogni porta di un gruppo LACP viene monitorata e rimossa dal gruppo di porte in caso di malfunzionamento. Esistono, tuttavia, molte idee sbagliate sul funzionamento di LACP in relazione alle prestazioni:

- LACP non richiede che la configurazione sullo switch corrisponda all'endpoint. Ad esempio, ONTAP può essere configurato con il bilanciamento del carico basato su IP, mentre uno switch può utilizzare il bilanciamento del carico basato su MAC.
- Ogni endpoint che utilizza una connessione LACP può scegliere indipendentemente la porta di trasmissione del pacchetto, ma non può scegliere la porta utilizzata per la ricezione. Ciò significa che il traffico da ONTAP a una destinazione specifica è legato a una porta specifica e il traffico di ritorno potrebbe arrivare su un'interfaccia diversa. Ciò non causa tuttavia problemi.
- LACP non distribuisce uniformemente il traffico in ogni momento. In un ambiente di grandi dimensioni con molti client NFS, il risultato è generalmente l'utilizzo di tutte le porte in un'aggregazione LACP. Tuttavia, qualsiasi file system NFS nell'ambiente è limitato alla larghezza di banda di una sola porta, non all'intera aggregazione.
- Sebbene i criteri LACP di robin-robin siano disponibili su ONTAP, questi criteri non indirizzano la connessione da uno switch a un host. Ad esempio, una configurazione con un trunk LACP a quattro porte su un host e un trunk LACP a quattro porte su ONTAP è ancora in grado di leggere un file system utilizzando una sola porta. Sebbene ONTAP sia in grado di trasmettere dati attraverso tutte e quattro le porte, non sono attualmente disponibili tecnologie di switch che inviano dallo switch all'host attraverso tutte

e quattro le porte. Ne viene utilizzato uno solo.

L'approccio più comune in ambienti di grandi dimensioni costituiti da molti host di database è quello di creare un aggregato LACP di un numero appropriato di interfacce 10Gb (o più veloce) utilizzando il bilanciamento del carico IP. Questo approccio consente a ONTAP di garantire l'uso uniforme di tutte le porte, purché esistano un numero sufficiente di client. Il bilanciamento del carico si interrompe quando nella configurazione sono presenti meno client, poiché il trunking LACP non ridistribuisce dinamicamente il carico.

Quando viene stabilita una connessione, il traffico in una determinata direzione viene posizionato su una sola porta. Ad esempio, un database che esegue una scansione completa della tabella su un file system NFS collegato tramite un trunk LACP a quattro porte legge i dati tramite una sola scheda di interfaccia di rete (NIC). Se in un tale ambiente sono presenti solo tre server di database, è possibile che tutti e tre stiano leggendo dalla stessa porta, mentre le altre tre porte sono inattive.

Lega le LIF alle porte fisiche

L'associazione di una LIF a una porta fisica dà come risultato un controllo più granulare della configurazione di rete, in quanto un dato indirizzo IP su un sistema ONTAP è associato a una sola porta di rete alla volta. La resilienza viene quindi ottenuta tramite la configurazione di gruppi di failover e policy di failover.

Criteri di failover e gruppi di failover

Il comportamento delle LIF durante un'interruzione di rete è controllato da policy di failover e gruppi di failover. Le opzioni di configurazione sono state modificate con le diverse versioni di ONTAP. Consultare "Documentazione sulla gestione della rete di ONTAP per gruppi e policy di failover" Per informazioni specifiche sulla versione di ONTAP distribuita.

ONTAP 8,3 (e versioni successive) consente la gestione del failover LIF in base ai domini di broadcast. Pertanto, un amministratore può definire tutte le porte che hanno accesso a una data subnet e consentire a ONTAP di selezionare una LIF di failover appropriata. Questo approccio può essere utilizzato da alcuni clienti, ma presenta limitazioni in un ambiente di rete di storage ad alta velocità a causa della mancanza di prevedibilità. Ad esempio, un ambiente può includere sia porte 1Gb GbE per l'accesso di routine al file system sia porte 10Gb GbE per l'i/o del file dati Se nello stesso dominio di broadcast sono presenti entrambi i tipi di porte, il failover LIF può spostare l'i/o del file dati da una porta 10Gb a una porta 1Gb.

In sintesi, prendere in considerazione le seguenti pratiche:

1. Configurare un gruppo di failover come definito dall'utente.
2. Popola il gruppo di failover con le porte sul partner controller di failover dello storage (SFO), in modo che le LIF seguano gli aggregati durante un failover dello storage. In questo modo si evita di creare traffico indiretto.
3. Utilizza porte di failover con caratteristiche di performance corrispondenti alla LIF originale. Ad esempio, una LIF su una singola porta fisica di 10Gb deve includere un gruppo di failover con una singola porta 10Gb. Un LIF LACP a quattro porte deve eseguire il failover in un altro LIF LACP a quattro porte. Queste porte sono un sottoinsieme delle porte definite nel dominio di broadcast.
4. Impostare la policy di failover solo su partner SFO. Questo assicura che la LIF segua l'aggregato durante il failover.

Ripristino automatico

Impostare `auto-revert` parametro come desiderato. La maggior parte dei clienti preferisce impostare questo parametro su `true` Di ripristinare la porta home della LIF. Tuttavia, in alcuni casi, i clienti hanno impostato questo valore su `false' per poter esaminare un failover imprevisto prima di restituire una LIF alla porta home.

Rapporto LIF-volume

Un equivoco comune consiste nella necessità di una relazione 1:1:1 tra volumi e LIF NFS. Sebbene questa configurazione sia necessaria per spostare un volume ovunque in un cluster senza creare mai traffico di interconnessione aggiuntivo, non si tratta di un requisito categoricamente importante. Occorre considerare il traffico intercluster, ma la semplice presenza di traffico intercluster non crea problemi. Molti dei benchmark pubblicati per ONTAP includono principalmente l'i/o indiretto

Ad esempio, un progetto di database contenente un numero relativamente contenuto di database critici per le performance, che richiedevano solo un totale di 40 volumi, potrebbe giustificare un volume da 1:1 GB per la strategia LIF, una disposizione che richiederebbe 40 indirizzi IP. Quindi, è possibile spostare un qualsiasi volume nel cluster insieme alla LIF associata e il traffico sarebbe sempre diretto, minimizzando ogni origine di latenza anche a livelli di microsecondi.

Ad esempio, è possibile gestire più facilmente un ambiente di grandi dimensioni in hosting con una relazione di 1:1:1 tra clienti e LIF. Con il passare del tempo, potrebbe essere necessario migrare un volume su un nodo diverso, causando traffico indiretto. Tuttavia, l'effetto sulle prestazioni non dovrebbe essere rilevabile a meno che le porte di rete sullo switch di interconnessione non siano saturanti. In caso di problemi, è possibile stabilire una nuova LIF sui nodi aggiuntivi e l'host può essere aggiornato nella successiva finestra di manutenzione per rimuovere il traffico indiretto dalla configurazione.

Configurazione TCP/IP ed ethernet per database Oracle

Molti clienti di Oracle su ONTAP utilizzano ethernet, il protocollo di rete di NFS, iSCSI, NVMe/TCP e specialmente il cloud.

Impostazioni del sistema operativo host

La maggior parte della documentazione del fornitore di applicazioni include impostazioni TCP ed ethernet specifiche per garantire il funzionamento ottimale dell'applicazione. Queste stesse impostazioni sono in genere sufficienti per fornire anche prestazioni ottimali dello storage basato su IP.

Controllo di flusso Ethernet

Questa tecnologia consente a un client di richiedere che un mittente interrompa temporaneamente la trasmissione dei dati. Questa operazione viene solitamente eseguita perché il ricevitore non è in grado di elaborare i dati in ingresso abbastanza rapidamente. Una volta, la richiesta che un mittente cessi la trasmissione era meno disgregativa di avere pacchetti di scarto del destinatario perché i buffer erano pieni. Questo non è più il caso degli stack TCP utilizzati oggi nei sistemi operativi. Infatti, il controllo di flusso causa più problemi di quanti ne risolva.

Negli ultimi anni sono aumentati i problemi di prestazioni causati dal controllo di flusso Ethernet. Questo perché il controllo di flusso Ethernet opera al livello fisico. Se una configurazione di rete consente a qualsiasi sistema operativo host di inviare una richiesta di controllo di flusso Ethernet a un sistema di storage, il risultato è una pausa in i/o per tutti i client connessi. Poiché un numero crescente di client viene servito da un singolo storage controller, aumenta la probabilità che uno o più client inviino richieste di controllo di flusso. Il problema è stato riscontrato frequentemente presso le sedi dei clienti con un'ampia virtualizzazione del sistema operativo.

Una scheda NIC su un sistema NetApp non dovrebbe ricevere richieste di controllo di flusso. Il metodo utilizzato per ottenere questo risultato varia in base al produttore dello switch di rete. Nella maggior parte dei casi, il controllo di flusso su uno switch Ethernet può essere impostato su `receive desired` oppure `receive on`, il che significa che una richiesta di controllo di flusso non viene inoltrata al controller di

memorizzazione. In altri casi, la connessione di rete sul controller di storage potrebbe non consentire la disattivazione del controllo di flusso. In questi casi, i client devono essere configurati in modo da non inviare mai richieste di controllo di flusso, modificando la configurazione NIC sul server host stesso o le porte switch a cui è connesso il server host.

NetApp consiglia assicurarsi che i controller di archiviazione NetApp non ricevano pacchetti di controllo di flusso Ethernet. In genere, è possibile eseguire questa operazione impostando le porte dello switch a cui è collegato il controller, ma alcuni hardware dello switch presentano dei limiti che potrebbero richiedere modifiche sul lato client.

Dimensioni MTU

È stato dimostrato che l'utilizzo dei frame jumbo offre un certo miglioramento delle performance nelle reti 1Gb, riducendo l'overhead della CPU e della rete, ma i benefici non sono solitamente significativi.

NetApp consiglia l'implementazione di frame jumbo quando possibile, sia per ottenere potenziali vantaggi in termini di prestazioni sia per rendere la soluzione a prova di futuro.

L'utilizzo di frame jumbo in una rete 10Gb è quasi obbligatorio. Questo perché la maggior parte delle implementazioni 10Gb raggiungono un limite di pacchetti al secondo senza frame jumbo prima che raggiungano il contrassegno 10Gb. L'utilizzo di frame jumbo migliora l'efficienza dell'elaborazione TCP/IP, poiché consente a sistema operativo, server, schede di rete e sistema di storage di elaborare un numero inferiore di pacchetti, anche se di dimensioni maggiori. Il miglioramento delle prestazioni varia da scheda di rete a scheda di rete, ma è significativo.

Per le implementazioni jumbo-frame, esiste la convinzione comune, ma non corretta, che tutti i dispositivi connessi debbano supportare frame jumbo e che le dimensioni MTU debbano corrispondere end-to-end Al contrario, i due endpoint di rete negoziano la dimensione del frame più elevata reciprocamente accettabile quando si stabilisce una connessione. In un ambiente tipico, uno switch di rete è impostato su una dimensione MTU di 9216, il controller NetApp è impostato su 9000 e i client sono impostati su una combinazione di 9000 e 1514. I client in grado di supportare un valore MTU di 9000 possono utilizzare frame jumbo, mentre i client in grado di supportare solo 1514 possono negoziare un valore inferiore.

I problemi con questa disposizione sono rari in un ambiente completamente commutato. Tuttavia, in un ambiente con routing occorre assicurarsi che nessun router intermedio sia costretto a frammentare frame jumbo.

NetApp consiglia di configurare quanto segue:

- I frame jumbo sono desiderabili ma non necessari con 1Gb Ethernet (GbE).
- I frame jumbo sono necessari per ottenere le massime prestazioni con 10GbE e velocità.

Parametri TCP

Tre impostazioni spesso non sono configurate correttamente: Timestamp TCP, riconoscimento selettivo (SACK) e ridimensionamento finestra TCP. Molti documenti obsoleti su Internet consigliano di disabilitare uno o più di questi parametri per migliorare le prestazioni. Molti anni fa, questa raccomandazione ha avuto un certo merito quando le capacità della CPU erano molto inferiori e, quando possibile, vi era un vantaggio nel ridurre il sovraccarico sull'elaborazione TCP.

Tuttavia, con i sistemi operativi moderni, la disattivazione di una qualsiasi di queste funzioni TCP in genere non comporta alcun vantaggio rilevabile e, allo stesso tempo, può danneggiare le prestazioni. In ambienti di rete

virtualizzati, i danni alle prestazioni sono particolarmente probabili, poiché queste funzioni sono necessarie per gestire in modo efficiente la perdita di pacchetti e le modifiche della qualità della rete.

NetApp consiglia di abilitare timestamp TCP, SACCO e ridimensionamento finestra TCP sull'host, e tutti e tre questi parametri dovrebbero essere attivi per impostazione predefinita in qualsiasi sistema operativo corrente.

Configurazione FC per database Oracle

La configurazione di FC SAN per database Oracle riguarda principalmente le seguenti Best practice quotidiane SAN.

Sono incluse misure di pianificazione tipiche, quali la garanzia della presenza di una larghezza di banda sufficiente sulla SAN tra l'host e il sistema di storage, la verifica della presenza di tutti i percorsi SAN tra i dispositivi richiesti, l'utilizzo delle impostazioni della porta FC richieste dal fornitore dello switch FC, evitando conflitti ISL, e utilizzando un adeguato monitoraggio del fabric SAN.

Suddivisione in zone

Una zona FC non deve mai contenere più di un iniziatore. Una tale disposizione potrebbe sembrare funzionare inizialmente, ma la diafonia tra gli iniziatori interferisce eventualmente con le prestazioni e la stabilità.

Le zone MultiTarget sono generalmente considerate sicure, anche se in rare circostanze il comportamento delle porte target FC di fornitori diversi ha causato problemi. Ad esempio, evita di includere nella stessa zona le porte di destinazione di uno storage array NetApp e non NetApp. Inoltre, l'inserimento di un sistema di storage NetApp e di un dispositivo a nastro nella stessa zona è ancora più probabile che causino problemi.

Database Oracle e connettività ONTAP a collegamento diretto

Gli amministratori dello storage a volte preferiscono semplificare le loro infrastrutture rimuovendo gli switch di rete dalla configurazione. Questo può essere supportato in alcuni scenari.

ISCSI e NVMe/TCP

Un host che utilizza iSCSI o NVMe/TCP può essere collegato direttamente a un sistema storage e funzionare normalmente. La ragione è la pedata. Le connessioni dirette a due storage controller differenti offrono due percorsi indipendenti per il flusso di dati. La perdita di percorso, porta o controller non impedisce l'utilizzo dell'altro percorso.

NFS

È possibile utilizzare lo storage NFS con connessione diretta, ma con una limitazione significativa: Il failover non funzionerà senza una significativa attività di scripting, che sarà responsabilità del cliente.

Il motivo per cui il failover senza interruzioni è complicato con lo storage NFS connesso direttamente è il routing che si verifica sul sistema operativo locale. Ad esempio, si supponga che un host abbia un indirizzo IP 192.168.1.1/24 e che sia collegato direttamente a un controller ONTAP con un indirizzo IP 192.168.1.50/24. Durante il failover, l'indirizzo 192.168.1.50 può eseguire il failover sull'altro controller e sarà disponibile per l'host, ma in che modo l'host rileva la sua presenza? L'indirizzo 192.168.1.1 originale esiste ancora sulla

scheda di rete host che non si connette più a un sistema operativo. Il traffico destinato a 192.168.1.50 continuerebbe ad essere inviato a una porta di rete inutilizzabile.

La seconda scheda NIC del sistema operativo potrebbe essere configurata come 19 2.168.1.2 e sarebbe in grado di comunicare con l'indirizzo 192.168.1.50 non riuscito, ma le tabelle di routing locali avrebbero un valore predefinito di utilizzo di un solo indirizzo **e di un solo indirizzo** per comunicare con la subnet 192.168.1.0/24. Un amministratore di sistema potrebbe creare un framework di script che rilevi una connessione di rete non riuscita e alteri le tabelle di routing locali o che porti le interfacce verso l'alto e verso il basso. La procedura esatta dipende dal sistema operativo in uso.

In pratica, i clienti NetApp dispongono di NFS con connessione diretta, ma in genere solo per i workload in cui le pause io durante i failover sono accettabili. Quando si utilizzano i supporti rigidi, non devono verificarsi errori di i/o durante tali pause. L'io dovrebbe bloccarsi finché i servizi non vengono ripristinati, mediante failback o intervento manuale, per spostare gli indirizzi IP tra le schede NIC dell'host.

Connessione diretta FC

Non è possibile connettere direttamente un host a un sistema storage ONTAP utilizzando il protocollo FC. Il motivo è l'uso di NPIV. Il WWN che identifica una porta FC ONTAP per la rete FC utilizza un tipo di virtualizzazione chiamato NPIV. Qualsiasi dispositivo collegato a un sistema ONTAP deve essere in grado di riconoscere un WWN NPIV. Attualmente non vi sono fornitori di HBA che offrono un HBA che può essere installato in un host in grado di supportare un target NPIV.