Netzwerkkonfiguration

Enterprise applications

NetApp
May 09, 2024

Inhalt

Netzwerkkonfiguration

Design der logischen Schnittstelle für Oracle-Datenbanken

Oracle Datenbanken benötigen Zugriff auf den Storage. Logische Schnittstellen (LIFs) sind die Netzwerk-Rohrleitungen, die eine Storage Virtual Machine (SVM) mit dem Netzwerk und damit der Datenbank verbinden. Ein angemessenes LIF-Design ist erforderlich, um sicherzustellen, dass für jeden Datenbank-Workload ausreichend Bandbreite vorhanden ist. Das Failover führt nicht zu einem Verlust von Storage-Services.

Dieser Abschnitt bietet einen Überblick über die wichtigsten LIF-Designprinzipien. Eine ausführlichere Dokumentation finden Sie im "Dokumentation zum ONTAP-Netzwerkmanagement". Wie andere Aspekte der Datenbankarchitektur hängen die besten Optionen für die Storage Virtual Machine (SVM, in der CLI als vServer bezeichnet) und das Design der logischen Schnittstelle (LIF) stark von den Skalierungsanforderungen und den geschäftlichen Anforderungen ab.

Berücksichtigen Sie bei der Entwicklung einer LIF-Strategie die folgenden primären Themen:

- **Leistung.** ist die Netzwerkbandbreite ausreichend?
- **Ausfallsicherheit.** gibt es Single Points of Failure im Design?
- **Verwaltbarkeit.** kann das Netzwerk unterbrechungsfrei skaliert werden?

Diese Themen beziehen sich auf die End-to-End-Lösung, vom Host über die Switches bis zum Speichersystem.

LIF-Typen

Es gibt mehrere LIF-Typen. "ONTAP-Dokumentation zu LIF-Typen" Stellen Sie umfassendere Informationen zu diesem Thema bereit, LIFs können jedoch aus funktionaler Sicht in die folgenden Gruppen unterteilt werden:

- **Cluster- und Node-Management-LIFs.** LIFs, die zum Verwalten des Storage-Clusters verwendet werden.
- **SVM-Management-LIFs.** Schnittstellen, die den Zugriff auf eine SVM über die REST-API oder ONTAPI (auch bekannt als ZAPI) für Funktionen wie Snapshot-Erstellung oder Volume-Anpassung erlauben. Produkte wie SnapManager für Oracle (SMO) müssen Zugriff auf eine SVM-Management-LIF haben.
- **Daten-LIFs.** Schnittstellen für FC, iSCSI, NVMe/FC, NVMe/TCP, NFS, oder SMB/CIFS-Daten.

> Eine logische Datenschnittstelle für NFS-Datenverkehr kann durch Änderung der Firewallrichtlinie von auch zum Management verwendet werden `data` Bis `mgmt` Oder eine andere Richtlinie, die HTTP, HTTPS oder SSH erlaubt. Diese Änderung kann die Netzwerkkonfiguration vereinfachen, indem die Konfiguration jedes Hosts für den Zugriff auf die LIF der NFS-Daten und eine separate Management-LIF vermieden wird. Es ist nicht möglich, eine Schnittstelle für iSCSI- und Managementverkehr zu konfigurieren, obwohl beide ein IP-Protokoll verwenden. In iSCSI-Umgebungen ist eine separate Management-LIF erforderlich.

Design von SAN LIF

Das LIF-Design in einer SAN-Umgebung ist aus einem Grund relativ einfach: Multipathing. Alle modernen SAN-Implementierungen ermöglichen es einem Client, über mehrere unabhängige Netzwerkpfade auf Daten

zuzugreifen und den optimalen Pfad oder die besten Pfade für den Zugriff auszuwählen. So lässt sich die Performance in Bezug auf LIF-Design einfacher bewältigen, da SAN-Clients automatisch den I/O-Lastausgleich über die besten verfügbaren Pfade durchführen.

Wenn ein Pfad nicht mehr verfügbar ist, wählt der Client automatisch einen anderen Pfad aus. Das daraus resultierende einfache Design macht SAN LIFs im Allgemeinen einfacher zu managen. Das bedeutet nicht, dass eine SAN-Umgebung immer einfacher zu managen ist, da viele andere Aspekte des SAN-Storage viel komplizierter sind als NFS. Es bedeutet schlichtweg, dass das LIF-Design von SAN einfacher ist.

Leistung

Der wichtigste Aspekt bei der LIF-Performance in einer SAN-Umgebung ist die Bandbreite. In einem ONTAP AFF-Cluster mit zwei Nodes mit zwei 16-GB-FC-Ports pro Node können beispielsweise bis zu 32 GB Bandbreite von jedem Node bereitgestellt werden.

Ausfallsicherheit

SAN LIFs führen keinen Failover auf einem AFF Storage-System durch. Wenn eine SAN-LIF aufgrund eines Controller-Failovers ausfällt, erkennt die Multipathing-Software des Clients den Verlust eines Pfads und leitet den I/O an eine andere LIF um. Bei ASA Storage-Systemen wird für LIFs nach kurzer Verzögerung ein Failover durchgeführt. Die I/O wird jedoch nicht unterbrochen, da auf dem anderen Controller bereits aktive Pfade vorhanden sind. Der Failover-Prozess erfolgt, um den Hostzugriff auf allen definierten Ports wiederherzustellen.

Managebarkeit

Die LIF-Migration ist in einer NFS-Umgebung viel üblicher, da die LIF-Migration häufig mit dem Verschieben von Volumes innerhalb des Clusters verknüpft ist. Wenn Volumes innerhalb des HA-Paars verschoben werden, ist keine Migration einer LIF in eine SAN-Umgebung erforderlich. Der Grund dafür ist, dass ONTAP nach Abschluss der Volume-Verschiebung eine Benachrichtigung über eine Pfadänderung an das SAN sendet, die die SAN-Clients automatisch neu optimieren. Die LIF-Migration mit SAN steht in erster Linie in Verbindung mit größeren Änderungen an physischer Hardware. Wenn beispielsweise ein unterbrechungsfreies Upgrade der Controller erforderlich ist, wird eine SAN LIF auf die neue Hardware migriert. Wenn ein FC-Port defekt ist, kann eine LIF zu einem nicht verwendeten Port migriert werden.

Designempfehlungen

NetApp gibt die folgenden Empfehlungen:

- Erstellen Sie nicht mehr Pfade, als erforderlich sind. Eine übermäßige Anzahl von Pfaden erschwert das gesamte Management und kann zu Problemen mit dem Pfad-Failover auf einigen Hosts führen. Darüber hinaus weisen einige Hosts unerwartete Pfadeinschränkungen für Konfigurationen wie das Booten von SAN auf.
- Nur sehr wenige Konfigurationen sollten mehr als vier Pfade zu einem LUN erfordern. Der Wert von mehr als zwei Nodes, um LUNs bekannt zu machen, ist beschränkt, da das Aggregat, das eine LUN hostet, nicht zugänglich ist, wenn der Node, der Eigentümer der LUN und dessen HA-Partner ausfällt. In solch einem Szenario ist es nicht hilfreich, Pfade auf anderen Nodes als dem primären HA-Paar zu erstellen.
- Obwohl die Anzahl der sichtbaren LUN-Pfade durch Auswählen der in FC-Zonen enthaltenen Ports gemanagt werden kann, ist es im Allgemeinen einfacher, alle potenziellen Zielpunkte in die FC-Zone aufzunehmen und die LUN-Sichtbarkeit auf ONTAP-Ebene zu kontrollieren.
- In ONTAP 8.3 und höher ist die Funktion für die selektive LUN-Zuordnung (SLM) die Standardeinstellung. Bei SLM wird jede neue LUN automatisch von dem Node bereitgestellt, dem das zugrunde liegende Aggregat und der HA-Partner des Node gehören. Durch diese Anordnung müssen keine Portsätze erstellt

oder Zoning konfiguriert werden, um den Zugriff auf den Port zu beschränken. Jede LUN ist mit der Mindestanzahl der Nodes verfügbar, die für eine optimale Performance und Stabilität erforderlich sind. *Falls eine LUN außerhalb der beiden Controller migriert werden muss, können die zusätzlichen Knoten mit dem hinzugefügt werden `lun mapping add-reporting-nodes` Befehl, sodass die LUNs auf den neuen Nodes angekündigt werden. Dadurch werden zusätzliche SAN-Pfade zu den LUNs für die LUN-Migration erstellt. Der Host muss jedoch einen Erkennungsvorgang durchführen, um die neuen Pfade verwenden zu können.

- Seien Sie nicht übermäßig besorgt über indirekten Verkehr. Es empfiehlt sich, in einer sehr I/O-intensiven Umgebung, in der jede Mikrosekunde von großer Latenz ist, indirekten Verkehr zu vermeiden, aber der sichtbare Performance-Effekt ist bei typischen Workloads zu vernachlässigen.

LIF-Design von NFS

Im Gegensatz zu SAN-Protokollen kann bei NFS nur bedingt mehrere Pfade zu Daten definiert werden. Die parallelen NFS-Erweiterungen (pNFS) zu NFSv4 beheben diese Einschränkung. Da die ethernet-Geschwindigkeit jedoch 100 GB erreicht hat, ist das Hinzufügen weiterer Pfade selten ein Nutzen.

Performance und Ausfallsicherheit

Obwohl die Messung der LIF-Performance in erster Linie dazu dient, die gesamte Bandbreite von allen primären Pfaden zu berechnen, muss die Bestimmung der Performance von NFS LIF genau die Netzwerkkonfiguration durchgeführt werden. Beispielsweise können zwei 10-Gbit-Ports als physische Rohports konfiguriert oder als LACP-Interface-Gruppe (Link Aggregation Control Protocol) konfiguriert werden. Wenn sie als Schnittstellengruppe konfiguriert sind, stehen mehrere Load-Balancing-Richtlinien zur Verfügung, die je nachdem, ob der Datenverkehr geswitcht oder geroutet wird, unterschiedlich funktionieren. Oracle Direct NFS (dNFS) bietet Load-Balancing-Konfigurationen, die derzeit in keinen NFS-Clients des Betriebssystems vorhanden sind.

Im Gegensatz zu SAN-Protokollen erfordern NFS-Filesysteme Ausfallsicherheit auf Protokollebene. Beispielsweise wird eine LUN immer mit aktiviertem Multipathing konfiguriert, was bedeutet, dass dem Storage-System mehrere redundante Kanäle zur Verfügung stehen, von denen jeder das FC-Protokoll verwendet. Ein NFS-Dateisystem hingegen hängt von der Verfügbarkeit eines einzelnen TCP/IP-Kanals ab, der nur auf der physischen Ebene geschützt werden kann. Diese Anordnung ist, warum Optionen wie Port-Failover und LACP Port-Aggregation existieren.

In einer NFS-Umgebung werden sowohl Performance als auch Ausfallsicherheit auf der Netzwerkprotokollebene bereitgestellt. Dadurch sind beide Themen miteinander verflochten und müssen gemeinsam diskutiert werden.

Binden Sie LIFs an Portgruppen

Um ein LIF an eine Portgruppe zu binden, ordnen Sie die LIF-IP-Adresse einer Gruppe physischer Ports zu. Die primäre Methode zur Aggregation physischer Ports ist LACP. Die Fehlertoleranz-Funktion von LACP ist ziemlich einfach. Jeder Port in einer LACP-Gruppe wird überwacht und im Falle einer Störung aus der Portgruppe entfernt. Es gibt jedoch viele Missverständnisse darüber, wie LACP in Bezug auf Performance funktioniert:

- Für LACP ist keine Konfiguration auf dem Switch erforderlich, um mit dem Endpunkt übereinstimmen zu können. Beispielsweise kann ONTAP mit IP-basiertem Lastausgleich konfiguriert werden, während ein Switch MAC-basierten Lastausgleich verwenden kann.
- Jeder Endpunkt, der eine LACP-Verbindung verwendet, kann den Port für die Paketübertragung unabhängig auswählen, jedoch nicht den für den Empfang verwendeten Port auswählen. Das bedeutet, dass Datenverkehr von ONTAP zu einem bestimmten Ziel an einen bestimmten Port gebunden ist, und der Rückverkehr könnte auf einer anderen Schnittstelle eintreffen. Dies verursacht jedoch keine Probleme.

- LACP verteilt den Datenverkehr nicht ständig gleichmäßig. In einer großen Umgebung mit vielen NFS-Clients wird normalerweise sogar alle Ports in einer LACP-Aggregation genutzt. Jedoch ist jedes ein NFS-Dateisystem in der Umgebung auf die Bandbreite von nur einem Port beschränkt, nicht die gesamte Aggregation.
- Obwohl LACP-Richtlinien für die Robin-Lösung auf ONTAP verfügbar sind, adressieren diese Richtlinien nicht die Verbindung von einem Switch zu einem Host. Beispielsweise ist eine Konfiguration mit einem LACP Trunk mit vier Ports auf einem Host und einem LACP Trunk mit vier Ports auf einem ONTAP immer noch nur in der Lage, ein Filesystem über einen einzelnen Port zu lesen. Obwohl ONTAP Daten über alle vier Ports übertragen kann, sind derzeit keine Switch-Technologien verfügbar, die über alle vier Ports vom Switch an den Host gesendet werden. Es wird nur eine verwendet.

In größeren Umgebungen, die aus vielen Datenbank-Hosts bestehen, ist der geläufigste Ansatz, mithilfe eines IP-Lastausgleichs ein LACP Aggregat mit einer entsprechenden Anzahl von 10 GB (oder schneller) Schnittstellen zu erstellen. Mit diesem Ansatz kann ONTAP sogar die Nutzung aller Ports ermöglichen, sofern genügend Clients vorhanden sind. Der Lastausgleich wird unterbrochen, wenn weniger Clients in der Konfiguration vorhanden sind, da LACP Trunking die Last nicht dynamisch neu verteilt.

Wenn eine Verbindung hergestellt wird, wird der Datenverkehr in eine bestimmte Richtung nur an einem Port platziert. Beispielsweise liest eine Datenbank, die einen vollständigen Tabellenscan gegen ein NFS-Dateisystem durchführt, das über einen LACP-Trunk mit vier Ports verbunden ist, Daten über nur eine Netzwerkkarte (NIC). Wenn sich nur drei Datenbankserver in einer solchen Umgebung befinden, ist es möglich, dass alle drei vom gleichen Port lesen, während die anderen drei Ports inaktiv sind.

Binden Sie LIFs an physische Ports

Das Binden einer LIF an einen physischen Port führt zu einer granulareren Kontrolle der Netzwerkkonfiguration, da eine gegebene IP-Adresse auf einem ONTAP-System jeweils nur mit einem Netzwerk-Port verknüpft ist. Stabilität wird dann durch die Konfiguration von Failover-Gruppen und Failover-Richtlinien erreicht.

Failover-Richtlinien und Failover-Gruppen

Das Verhalten von LIFs wird während der Netzwerkunterbrechung durch Failover-Richtlinien und Failover-Gruppen gesteuert. Die Konfigurationsoptionen wurden mit den verschiedenen Versionen von ONTAP geändert. Konsultieren Sie die "ONTAP Netzwerkmanagement-Dokumentation für Failover-Gruppen und Richtlinien" Finden Sie spezifische Details zur implementierten Version von ONTAP.

ONTAP 8.3 und höher ermöglichen das Management von LIF-Failovers basierend auf Broadcast-Domänen. Daher kann ein Administrator alle Ports definieren, die Zugriff auf ein bestimmtes Subnetz haben, und ONTAP erlauben, eine entsprechende Failover-LIF auszuwählen. Einige Kunden verwenden diesen Ansatz durchaus, weist jedoch aufgrund der mangelnden Planbarkeit in einer Storage-Netzwerkumgebung mit hoher Geschwindigkeit Einschränkungen auf. Beispielsweise kann eine Umgebung sowohl 1-Gbit-Ports für routinemäßigen Filesystem-Zugriff als auch 10-Gbit-Ports für Datendatei-I/O. Wenn beide Ports in derselben Broadcast-Domäne vorhanden sind, kann ein LIF-Failover dazu führen, Datendatei-I/O von einem 10-GB-Port auf einen 1-GB-Port zu verschieben.

Zusammenfassend lassen sich die folgenden Vorgehensweisen berücksichtigen:

1. Konfigurieren Sie eine Failover-Gruppe als benutzerdefiniert.
2. Füllen Sie die Failover-Gruppe mit Ports am Partner-Controller für Storage Failover (SFO), damit die LIFs beim Storage Failover den Aggregaten folgen. Dadurch wird die Erstellung indirekter Verkehrsströme vermieden.
3. Verwenden Sie Failover-Ports, deren Performance-Merkmale mit der ursprünglichen logischen Schnittstelle übereinstimmen. Beispielsweise sollte eine LIF auf einem einzelnen physischen 10-Gbit-Port eine Failover-

Gruppe mit einem einzelnen 10-Gbit-Port enthalten. Ein LACP LIF mit vier Ports sollte ein Failover auf eine andere LACP LIF mit vier Ports durchführen. Diese Ports wären eine Teilmenge der Ports, die in der Broadcast-Domäne definiert sind.

4. Setzen Sie die Failover-Richtlinie auf nur SFO-Partner. Dadurch wird sichergestellt, dass die LIF während des Failovers dem Aggregat folgt.

Autom. Rücksetzung

Stellen Sie die ein `auto-revert` Parameter wie gewünscht. Die meisten Kunden bevorzugen es, diesen Parameter auf zu setzen `true` Um das LIF auf seinen Home Port zurückzusetzen. In einigen Fällen haben Kunden dies jedoch auf `false `so gesetzt, dass ein unerwartetes Failover untersucht werden kann, bevor eine LIF an ihren Home Port zurückgegeben wird.

LIF-Volume-Verhältnis

Ein weit verbreitetes Missverständnis ist, dass es eine 1:1 Beziehung zwischen Volumes und NFS LIFs geben muss. Diese Konfiguration ist zwar erforderlich, um ein Volume ohne zusätzlichen Interconnect-Verkehr an eine beliebige Stelle in einem Cluster zu verschieben, ist jedoch kategorisch keine Anforderung. Der Intercluster-Datenverkehr muss berücksichtigt werden, aber die bloße Anwesenheit von Intercluster-Datenverkehr verursacht keine Probleme. Viele der für ONTAP veröffentlichten Benchmarks sind überwiegend indirekte I/O-Vorgänge

Ein Datenbankprojekt mit einer relativ kleinen Anzahl Performance-kritischer Datenbanken, für die nur insgesamt 40 Volumes benötigt wurden, könnte beispielsweise eine LIF-Strategie für das 1:1 Volume rechtfertigen. Dieses Arrangement würde 40 IP-Adressen erfordern. Jedes Volume könnte dann zusammen mit der zugehörigen LIF an jeden beliebigen Ort im Cluster verschoben werden. Der Datenverkehr würde dann immer direkt erfolgen, wodurch jede Latenzquelle sogar auf Mikrosekunden-Ebene minimiert wird.

Zählerbeispiel: Eine große, gehostete Umgebung kann durch eine 1:1:1-Beziehung zwischen Kunden und LIFs einfacher gemanagt werden. Im Laufe der Zeit muss ein Volume möglicherweise auf einen anderen Node migriert werden, was zu einem indirekten Traffic führen würde. Der Performance-Effekt sollte jedoch nicht nachweisbar sein, es sei denn, die Netzwerk-Ports auf dem Interconnect-Switch sind voll ausgelastet. Falls Bedenken bestehen, kann eine neue LIF auf zusätzlichen Nodes erstellt werden, und der Host kann im nächsten Wartungsfenster aktualisiert werden, um indirekten Traffic aus der Konfiguration zu entfernen.

TCP/IP- und ethernet-Konfiguration für Oracle-Datenbanken

Viele Kunden von Oracle auf ONTAP verwenden ethernet, das Netzwerkprotokoll von NFS, iSCSI, NVMe/TCP sowie insbesondere die Cloud.

Einstellungen für das Host-Betriebssystem

Die Dokumentation der meisten Anwendungsanbieter enthält bestimmte TCP- und ethernet-Einstellungen, die sicherstellen sollen, dass die Anwendung optimal funktioniert. Diese Einstellungen reichen in der Regel aus, um auch eine optimale IP-basierte Speicherleistung zu erzielen.

Ethernet-Flusskontrolle

Mit dieser Technologie kann ein Client verlangen, dass ein Sender die Datenübertragung vorübergehend stoppt. Dies geschieht normalerweise, weil der Empfänger eingehende Daten nicht schnell genug verarbeiten kann. Die Anforderung, dass ein Sender die Übertragung abbricht, war zu einem Zeitpunkt weniger störend, als dass ein Empfänger Pakete verwirft, weil die Puffer voll waren. Dies ist bei den heute in Betriebssystemen verwendeten TCP-Stacks nicht mehr der Fall. Tatsächlich verursacht die Flusskontrolle mehr Probleme als sie

löst.

Leistungsprobleme, die durch die Ethernet-Flusssteuerung verursacht werden, haben in den letzten Jahren zugenommen. Der Grund dafür ist, dass die Ethernet-Flusssteuerung auf der physischen Ebene ausgeführt wird. Wenn eine Netzwerkkonfiguration es einem Host-Betriebssystem ermöglicht, eine Ethernet-Datenflusssteuerungsanforderung an ein Storage-System zu senden, führt dies zu einer I/O-Pause für alle verbundenen Clients. Da immer mehr Clients von einem einzelnen Storage Controller bedient werden, steigt die Wahrscheinlichkeit, dass ein oder mehrere dieser Clients Flow Control-Anfragen senden. Das Problem ist bei Kundenstandorten mit umfassender Betriebssystemvirtualisierung häufig aufgetreten.

Eine NIC auf einem NetApp-System sollte keine Anfragen zur Flusskontrolle empfangen. Die Methode, mit der dieses Ergebnis erzielt wird, hängt vom Hersteller des Netzwerk-Switches ab. In den meisten Fällen kann die Flusssteuerung auf einem Ethernet-Switch eingestellt werden `receive desired` Oder `receive on`, Das bedeutet, dass eine Durchflussregelanforderung nicht an den Speichercontroller weitergeleitet wird. In anderen Fällen lässt die Netzwerkverbindung auf dem Storage Controller möglicherweise die Deaktivierung der Flusssteuerung nicht zu. In diesen Fällen müssen die Clients so konfiguriert werden, dass sie keine Flow-Control-Anforderungen senden, entweder indem sie auf die NIC-Konfiguration auf dem Host-Server selbst oder auf die Switch-Ports wechseln, mit denen der Host-Server verbunden ist.

NetApp empfiehlt sicherzustellen, dass NetApp-Speicher-Controller keine Ethernet-Flow-Control-Pakete empfangen. Dies kann im Allgemeinen durch Einstellen der Switch Ports geschehen, an die der Controller angeschlossen ist. Bei einigen Switch-Hardware bestehen jedoch Einschränkungen, die stattdessen clientseitige Änderungen erfordern können.

MTU-Größen

Der Einsatz von Jumbo Frames hat gezeigt, dass sich die Performance in 1-GB-Netzwerken durch Reduzierung des CPU- und Netzwerk-Overheads verbessert. Die Vorteile sind jedoch in der Regel nicht signifikant.

NetApp empfiehlt, wenn möglich Jumbo Frames zu implementieren, sowohl um potenzielle Leistungsvorteile zu realisieren als auch um die Lösung zukunftssicher zu machen.

Die Verwendung von Jumbo Frames in einem 10-Gbit-Netzwerk ist fast zwingend erforderlich. Der Grund dafür ist, dass die meisten 10-GB-Implementierungen vor Erreichen der 10-GB-Marke ohne Jumbo-Frames eine Grenze von Paketen pro Sekunde erreichen. Die Verwendung von Jumbo Frames verbessert die Effizienz bei der TCP/IP-Verarbeitung, da Betriebssystem, Server, NICs und Speichersystem weniger, aber größere Pakete verarbeiten können. Die Leistungsverbesserung variiert von NIC zu NIC, ist jedoch signifikant.

Bei Jumbo-Frame-Implementierungen besteht die allgemeine, aber falsche Annahme, dass alle verbundenen Geräte Jumbo-Frames unterstützen müssen und dass die MTU-Größe End-to-End entsprechen muss Stattdessen verhandeln die beiden Netzwerkendpunkte beim Herstellen einer Verbindung die höchste für beide Seiten akzeptable Frame-Größe. In einer typischen Umgebung ist ein Netzwerk-Switch auf eine MTU-Größe von 9216, der NetApp-Controller auf 9000 und die Clients auf 9000 und 1514 eingestellt. Clients, die eine MTU von 9000 unterstützen, können Jumbo-Frames verwenden, und Clients, die nur 1514 unterstützen, können einen niedrigeren Wert aushandeln.

Probleme mit dieser Anordnung sind in einer komplett geschalteten Umgebung selten. Achten Sie jedoch in einer gerouteten Umgebung darauf, dass kein Zwischenrouter gezwungen ist, Jumbo-Frames zu fragmentieren.

NetApp empfiehlt die Konfiguration folgender Komponenten:

- Jumbo Frames sind wünschenswert, jedoch nicht erforderlich mit 1Gb Ethernet (GbE).
- Jumbo Frames sind für maximale Performance mit 10 GbE und schneller erforderlich.

TCP-Parameter

Drei Einstellungen sind oft falsch konfiguriert: TCP-Zeitstempel, selektive Bestätigung (SACK) und TCP-Fenster-Skalierung. Viele veraltete Dokumente im Internet empfehlen, einen oder mehrere dieser Parameter zu deaktivieren, um die Leistung zu verbessern. Vor vielen Jahren war diese Empfehlung verdienlich, als die CPU-Kapazitäten wesentlich geringer waren und der Overhead für die TCP-Verarbeitung, wenn möglich, reduziert werden konnte.

Bei modernen Betriebssystemen führt die Deaktivierung dieser TCP-Funktionen jedoch in der Regel nicht zu nachweisbaren Vorteilen und kann gleichzeitig die Leistung beeinträchtigen. In virtualisierten Netzwerkumgebungen sind Performance-Schäden besonders wahrscheinlich, da diese Funktionen für eine effiziente Handhabung von Paketverlusten und Änderungen der Netzwerkqualität erforderlich sind.

NetApp empfiehlt, TCP-Zeitstempel, SACK und TCP-Fenster-Skalierung auf dem Host zu aktivieren, und alle drei dieser Parameter sollten in jedem aktuellen Betriebssystem standardmäßig aktiviert sein.

FC-Konfiguration für Oracle-Datenbanken

Bei der Konfiguration von FC SAN für Oracle-Datenbanken geht es in erster Linie um die Umsetzung der täglichen SAN Best Practices.

Dazu gehören typische Planungsmaßnahmen wie die Sicherstellung einer ausreichenden Bandbreite auf dem SAN zwischen dem Host und dem Speichersystem, die Überprüfung, ob alle SAN-Pfade zwischen allen erforderlichen Geräten vorhanden sind, unter Verwendung der FC-Port-Einstellungen, die Ihr FC-Switch-Anbieter benötigt, um ISL-Konflikte zu vermeiden, und ordnungsgemäße Überwachung des SAN-Fabrics verwenden.

Zoning

Eine FC-Zone sollte nie mehr als einen Initiator enthalten. Eine solche Anordnung mag zunächst zu funktionieren scheinen, doch Crosstalk zwischen Initiatoren beeinträchtigt letztendlich die Performance und Stabilität.

Multitarget-Zonen werden allgemein als sicher angesehen, obwohl in seltenen Fällen das Verhalten von FC-Zielports unterschiedlicher Anbieter Probleme verursacht hat. Es ist beispielsweise zu vermeiden, die Ziel-Ports von einem NetApp und einem nicht-NetApp Storage-Array in derselben Zone zu integrieren. Darüber hinaus besteht mit noch größerer Wahrscheinlichkeit die Gefahr, dass ein NetApp Storage-System und ein Bandgerät in dieselbe Zone platziert werden.

Oracle-Datenbank und ONTAP-Konnektivität mit Direktverbindung

Storage-Administratoren ziehen es manchmal vor, ihre Infrastruktur zu vereinfachen, indem sie Netzwerk-Switches von der Konfiguration entfernen. Dies kann in einigen

Szenarien unterstützt werden.

ISCSI und NVMe/TCP

Ein Host, der iSCSI oder NVMe/TCP verwendet, kann direkt mit einem Storage-System verbunden werden und ordnungsgemäß ausgeführt werden. Der Grund dafür ist Pathing. Direkte Verbindungen zu zwei verschiedenen Storage Controllern ergeben zwei unabhängige Pfade für den Datenfluss. Der Verlust von Pfad, Port oder Controller verhindert nicht, dass der andere Pfad verwendet wird.

NFS

Direct-Connected NFS Storage kann genutzt werden, aber mit einer erheblichen Einschränkung - Failover funktioniert nicht ohne einen erheblichen Scripting-Aufwand, der in der Verantwortung des Kunden liegt.

Der Grund, warum ein unterbrechungsfreier Failover mit direkt verbundenem NFS-Storage kompliziert ist, ist das Routing auf dem lokalen Betriebssystem. Angenommen, ein Host hat eine IP-Adresse von 192.168.1.1/24 und ist direkt mit einem ONTAP-Controller mit einer IP-Adresse von 192.168.1.50/24 verbunden. Während eines Failovers kann diese 192.168.1.50-Adresse ein Failover auf den anderen Controller durchführen, und sie wird für den Host verfügbar sein. Wie erkennt der Host jedoch sein Vorhandensein? Die ursprüngliche 192.168.1.1-Adresse ist noch auf der Host-NIC vorhanden, die keine Verbindung mehr zu einem Betriebssystem herstellt. Der für 192.168.1.50 bestimmte Datenverkehr würde weiterhin an einen nicht funktionsfähigen Netzwerkport gesendet.

Die zweite BS-NIC könnte als 19 konfiguriert werden 2.168.1.2 und wäre in der Lage, mit der Failed Over 192.168.1.50-Adresse zu kommunizieren, aber die lokalen Routing-Tabellen würden standardmäßig eine **und nur eine**-Adresse verwenden, um mit dem Subnetz 192.168.1.0/24 zu kommunizieren. Ein Sysadmin könnte ein Skript-Framework erstellen, das eine fehlerhafte Netzwerkverbindung erkennt und die lokalen Routing-Tabellen ändert oder Schnittstellen hoch- und herunterfahren würde. Das genaue Verfahren hängt vom verwendeten Betriebssystem ab.

In der Praxis haben NetApp-Kunden NFS direkt verbunden, aber normalerweise nur für Workloads, bei denen IO-Pausen während Failover akzeptabel sind. Wenn harte Mounts verwendet werden, sollte es während solcher Pausen keine IO-Fehler geben. Die E/A-Vorgänge sollten so lange hängen bleiben, bis Dienste wiederhergestellt werden, entweder durch ein Failback oder durch einen manuellen Eingriff, um IP-Adressen zwischen NICs auf dem Host zu verschieben.

FC-Direktverbindung

Es ist nicht möglich, einen Host direkt über das FC-Protokoll mit einem ONTAP Storage-System zu verbinden. Der Grund dafür ist die Verwendung von NPIV. Der WWN, der einen ONTAP FC-Port mit dem FC-Netzwerk identifiziert, verwendet eine Art Virtualisierung, die als NPIV bezeichnet wird. Jedes Gerät, das an ein ONTAP-System angeschlossen ist, muss einen NPIV-WWN erkennen können. Es gibt derzeit keine HBA-Anbieter, die einen HBA anbieten, der auf einem Host installiert werden kann, der ein NPIV-Ziel unterstützen könnte.