



F5 White Paper

Bau einer Hybrid-ADN-Architektur mit virtuellen und physischen ADCs

Die Virtualisierung der Infrastruktur von Netzwerken und Anwendungsnetzwerken ist die zweite Welle des Virtualisierungs-Tsunamis, die die Küste des Datenzentrums trifft. Im Gegensatz zu einer Server-Virtualisierung hat eine Virtualisierung des Controllers zur Anwendungsbereitstellung (Application Delivery Controller, ADC) aufgrund dessen einzigartiger Rolle im Datenzentrum Auswirkungen auf die Architektur selbst, die einen simplen Austausch virtuell gegen physisch nicht annehmbar machen. Es gibt allerdings geeignete Stellen im Datenzentrum und der Unternehmensorganisation, an denen virtualisierte ADCs als Stand-alone-Lösungen eingesetzt werden können - auch in Kombination mit dem physischen Vorgänger -, um ein Datenzentrum dynamischer zu machen, ohne Kompromisse in Bezug auf Zuverlässigkeit, Skalierbarkeit und Performance eingehen zu müssen.

von Lori MacVittie

Technical Marketing Manager, Application Services



Inhalt

Einleitung

Wer sollte einen vADC einsetzen?

- Bereitstellung im Datenzentrum eines Unternehmens
 - Unabhängige Software-Anbieter
 - Cloud-Computing-Umgebungen
-

Architektonische Herausforderungen

- Skalierbarkeit
 - Anpassbarkeit
 - Mobilität
-

Empfohlene Best Practices

- Überlegungen zu einer Architektur mit einem virtuellen ADC
 - Überlegungen zu einer Architektur mit einem physischen ADC
-

Schlussfolgerung



Einleitung

Virtualisierung ist inzwischen keine neue Technologie für Datenzentren mehr, sondern ein Standardbereitstellungswerkzeug in Unternehmen jeder Größe und Branche. Eine von Rackspace im August 2007 durchgeführte Umfrage zum Thema Virtualisierung ließ ein starkes Vertrauen in die Virtualisierung erkennen, da 72 Prozent der Befragten angaben, virtualisierte Anwendungen in einer Produktionsumgebung bereitstellen zu wollen.¹ Eine vor kurzem durchgeführte Umfrage von Shavlik Technologies ergab, dass 75 Prozent der Befragten die Hälfte ihrer Produktionsserver bereits virtualisiert hatten.² Andere aktuelle Umfragen, darunter auch solche von bekannten Analystenfirmen, bestätigen diese Trends, und die Einführungsquote der Virtualisierung beweist, dass fast alle Unternehmen auf die Virtualisierung ihrer Datenzentren setzen.

Trotz der breiten Einführung ist eine Virtualisierung immer noch mit vielen Herausforderungen verbunden. Eine von CIO.com Anfang 2008 durchgeführte Untersuchung deckte zahlreiche Herausforderungen sowohl bei der Bereitstellung als auch bei der Verwaltung von virtualisierten Umgebungen auf. Spitzenreiter mit 64 Prozent ist hier die Herausforderung, die Serverauslastung auszugleichen und die Anwendungs-Performance aufrechtzuerhalten.³

Mit zunehmender Verbreitung von virtualisierten Technologien beschäftigen sich viele Unternehmen auch verstärkt damit, andere Komponenten des Datenzentrums zu virtualisieren, um die IT-Agilität zu erhöhen und besser auf wechselnde Geschäftsanforderungen reagieren zu können. Anbieter von Netzwerken und Anwendungsnetzwerken stehen unter Druck und müssen virtualisierte Versionen von herkömmlichen physischen Geräten für das Datenzentrum auf den Markt bringen, was zu einem breiteren Angebot im Bereich virtuelle Netzwerkgeräte führen wird.

Der erfolgreiche Einsatz dieser virtuellen Netzwerkgeräte (Virtual Network Appliances, VNAs) kann ohne entsprechende Informationen zur Architektur jedoch schwierig sein. Eine Server-Virtualisierung hat nur minimalen Einfluss auf die Gesamtarchitektur eines Datenzentrums. VNAs dagegen können wegen der Abhängigkeiten der verschiedenen Komponenten in der Infrastruktur des Netzwerks zum Problem werden. In einigen Fällen bietet es sich nicht an oder ist technisch nicht machbar, ein herkömmliches physisches Gerät durch ein VNA zu ersetzen. So wie manche Arbeitslasten nicht zu einer Server-Virtualisierung passen, sollte auch nicht jede Netzwerkkomponente durch ein VNA ersetzt werden. Daher bleibt den Unternehmen nichts anderes übrig, als mit einer Netzwerkarchitektur zu arbeiten, die sowohl aus physischen wie auch virtuellen Versionen einer Lösung besteht. Architekturen dieser Art sind notwendig, um die von Unternehmen geforderte



White Paper

Bau einer Hybrid-ADN-Architektur mit virtuellen und physischen ADCs

Flexibilität und Skalierbarkeit zu sichern, ohne Einschränkungen bei Zuverlässigkeit und Verfügbarkeit machen zu müssen.

Die Verfügbarkeit eines virtuellen Controllers zur Anwendungsbereitstellung (virtual Application Delivery Controller, vADC) ermöglicht Unternehmen, eine solche Lösung auf unterschiedliche Art und an allen Stellen im Entwicklungszyklus einer Anwendung einzubauen. In vielen Fällen ändert die Verwendung eines vADCs anstelle seines physischen Pendanten wenig oder überhaupt nichts an der Architektur. In anderen Fällen dagegen kann es problematisch werden, wenn man in einem vorhandenen Netzwerk einen physischen Controller zur Anwendungsbereitstellung (physical Application Delivery Controller, pADC) durch einen vADC ersetzt.

Unternehmen mit 500 oder mehr Mitarbeitern tendieren eher dazu, Erfolg auf der Grundlage verbesserter Unternehmens-Agilität zu bewerten.

Quelle: Server Virtualization Life Cycle Report von CDW, Januar 2010

Wer sollte einen vADC einsetzen?

Es gibt verschiedene Organisationstypen, die vom Einsatz eines vADC profitieren:

- Datenzentren von Unternehmen
- Unabhängige Software-Anbieter
- Cloud- und Hosting-Anbieter

Bereitstellung im Datenzentrum eines Unternehmens

Netzwerkadministratoren und -architekten

Administratoren und Architekten von Netzwerken profitieren am meisten von einem vADC, wenn dieser in Test- und QS-Umgebungen eingesetzt wird. In Kombination mit einer Server-Virtualisierung ermöglicht ein vADC einem Unternehmen, Produktionsumgebungen ohne erhebliche Investitionen in physische Komponenten zu replizieren. Durch eine Virtualisierung aller Komponenten in der Architektur kann das Testen neuer Lösungen und die Optimierung vorhandener Richtlinien in einer isolierten Umgebung erfolgen und dann in die Produktion migriert werden.

Entwickler und Anwendungsarchitekten

Entwickler und Anwendungsarchitekten wissen um die Vorteile, die eine Integration von Technologien zur Anwendungsbereitstellung in Anwendungen bietet, doch bis jetzt haben die Kosten einer für Entwickler zugänglichen physischen Komponente die Einführung verhindert. Die Verwendung eines pADC in der Produktionsumgebung wird - aus gutem Grund - nicht empfohlen, sodass die Integration von Technologien zur Anwendungsbereitstellung bis jetzt weitgehend unerforscht geblieben ist. Die Möglichkeit, durch die Verwendung eines vADC diese Technologien nutzen zu



White Paper

Bau einer Hybrid-ADN-Architektur mit virtuellen und physischen ADCs

können, ebnet Entwicklern den Weg dazu, bei Entwicklung und Bereitstellung ihrer Anwendungen von Beschleunigung, Sicherheit, Optimierung und Anpassung der Plattform zur Anwendungsbereitstellung profitieren zu können.

Unabhängige Software-Anbieter

Der Mangel an Verwaltungs- und Orchestrierungssystemen, die sowohl physische als auch virtuelle Anwendungs- und Netzwerkkomponenten verwalten können, erschwert die Einführung vieler Virtualisierungs- und Cloud-Computing-Modelle. Viele Vorteile von Cloud-Computing und Virtualisierung ergeben sich aus der Möglichkeit zur Automatisierung und Orchestrierung von IT-Prozessen, die mit On-Demand-Provisioning zusammenhängen. Ebenso wie Entwickler und Architekten eines Unternehmens von einem vADC profitieren können, steht unabhängigen Software-Anbietern mit einem vADC eine kostengünstige Lösung zur Verfügung, um Anwendungsbereitstellung in Verwaltungslösungen zu integrieren und neue, innovative Verwendungsmöglichkeiten für Technologien zur Anwendungsbereitstellung zu entwickeln.

Cloud-Computing-Umgebungen

Anbieter von Cloud- und herkömmlichen Hosting und damit auch deren Kunden können genauso - wenn nicht sogar noch mehr - von einem vADC profitieren wie Unternehmen. Der hochdynamische Charakter solcher Umgebungen verlangt die Flexibilität und schnelle Skalierbarkeit von virtualisierten Lösungen. Während herkömmliche pADC-Komponenten sowohl Flexibilität als auch schnelle Skalierbarkeit bieten, sind sie weniger in der Lage, die Richtlinien zur Anwendungsbereitstellung von tausenden von Kunden effizient zu isolieren.

Cloud- und Hosting-Anbieter können einen vADC verwenden, um sich mit ihren Angeboten vom Wettbewerb abzusetzen, und den Kunden dadurch die Möglichkeit geben, in Verbindung mit ihren Cloud-basierten Anwendungen Unternehmens- und Carrier-Class-Bereitstellungstechnologien zu verwenden. Wenn Kunden die Möglichkeit haben, ihren eigenen vADC zu verwenden, verringert dies für den Anbieter die Notwendigkeit, den eigenen pADC für Kunden zu öffnen. Auf diese Weise können Bedenken hinsichtlich der Isolierung von Konfiguration und Komponenten innerhalb der Infrastruktur des Cloud-Computing-Anbieters zerstreut werden.

Um virtuelle Netzwerke flexibel und verwaltbar zu machen, ist die Programmierbarkeit der Netzwerkelemente von größter Bedeutung. Nur durch programmierbare Netzwerkelemente können die Service-Anbieter kundenspezifische Protokolle implementieren und verschiedene Services bereitstellen. Daher muss es auf die konzeptionellen Entscheidungen "wie viel Programmierbarkeit soll sein" und "wie soll diese zugänglich sein" befriedigende Antworten geben.

Quelle: "A Survey of Network Virtualization", Oktober 2008, N.M Mosharaf Kabir Chowdhury et al.



White Paper

Bau einer Hybrid-ADN-Architektur mit virtuellen und physischen ADCs

Die Kunden von Cloud- und Hosting-Anbietern können die Funktionalität von Best-in-Class pADCs in virtueller Form nutzen. Mit einem vADC in der Ziel-Cloud-Umgebung ist die Migration von Anwendungen, die unter Umständen der Sicherheit wegen von Technologien zur Bereitstellung von Anwendungen abhängen, erheblich einfacher. In einigen Fällen muss die Anwendung dann nicht mehr für eine Cloud-Umgebung umgeschrieben werden, es genügt, stattdessen einfach die Anwendung und den vADC bereitzustellen. Durch die Bündelung der Anwendungsbereitstellungstechnologie mit der Anwendung haben Unternehmen mehr Möglichkeiten bei der Auswahl eines Anbieters, da sie, was den Zugang zu Komponenten zur Anwendungsbereitstellung angeht, nicht mehr länger vom Anbieter abhängig sind.

Architektonische Herausforderungen

Es wäre verfrüht, anzunehmen, dass virtualisierte Controller zur Anwendungsbereitstellung ihre vorhandenen Pendanten - physische Controller zur Anwendungsbereitstellung - ersetzen werden. In einigen Fällen mag eine reine Austauschstrategie möglich sein, doch in anderen Fällen hätte dies so weitreichende Auswirkungen, dass empfohlen wird, weiterhin mit einem pADC zu arbeiten (oder einen solchen anzuschaffen) und dessen Funktionalität über einen vADC zu verbessern.

Die optimale Architektur zur Anwendungsbereitstellung nutzt die Vorteile von physischen und virtuellen Controllern zur Anwendungsbereitstellung, um die für ein dynamisches Datenzentrum erforderliche Mobilität, Skalierbarkeit und Anpassbarkeit zu erreichen. Ein Hybrid-Ansatz für den Bau eines flexiblen und anpassbaren, aber dennoch hochskalierbaren und hochperformanten Netzwerks zur Anwendungsbereitstellung ist für Unternehmen, die auf die Virtualisierung von Netzwerk und Netzwerkkomponenten zur Anwendungsbereitstellung setzen, am Erfolg versprechendsten.

Skalierbarkeit

Skalierbarkeit - insbesondere On-Demand- oder "Auto-Skalierbarkeit" - treibt den größten Teil der Nachfrage nach VNAs. Dies liegt vor allem daran, dass ein pADC nach Erreichen der Kapazitätsgrenzen entweder als Ersatz in physischer Form oder als zusätzliche Bereitstellung skaliert wird. Dass zum Erwerb eines physischen Ersatz unter Umständen viel Zeit benötigt wird, wird allerdings als störend empfunden.



White Paper

Bau einer Hybrid-ADN-Architektur mit virtuellen und physischen ADCs

Man geht davon aus, dass der Übergang schneller, preisgünstiger und nahtloser wäre, wenn man bei Kapazitätsproblemen einfach ein "Spin-up" von zusätzlichen vADCs durchführen könnte. Die Skalierung auf einen vADC wäre zwar schneller und weniger kostenaufwendig, aber nicht weniger zeitaufwendig. Genau genommen kann sich der Übergang negativ auf die Performance und die Verfügbarkeit von Netzwerk und bereitgestellten Anwendungen auswirken.

Aufgrund der Skalierbarkeit von VNAs geht man automatisch davon aus, dass sie auch Anforderungen/Datenverkehr über mehr Instanzen des virtuellen Geräts hinweg verteilen können - eine Aufgabe, die in der Regel einem dafür geeigneten pADC zugewiesen wird. Diese Aufgabe migriert jedoch nicht automatisch vom pADC zum VNA, nur weil der Controller jetzt virtualisiert ist. Daher wird man zur Skalierung von vADCs und VNAs im Allgemeinen auch in Zukunft einen pADC brauchen.

Horizontale Skalierung (Scale-Out)

Aufgrund der Art, in der Netzwerkkomponenten andere Komponenten virtualisieren - z.B. wie sie den Datenverkehr auf mehrere Instanzen eines Geräts verteilen - werden Rollen nicht automatisch migriert. Bei einer vollständig virtualisierten Architektur wird häufig angenommen, dass ein Scale-Out möglich ist, indem man einfach ein neues virtuelles Gerät anlaufen lässt, was dann zu einer sogenannten Active/Active (oder n-Active)-Konfiguration führt, bei der alle Instanzen aktiv akzeptieren und Datenverkehr/Anforderungen verarbeiten. Und hier liegt das Problem: Alle Instanzen akzeptieren und verarbeiten Datenverkehr/Anforderungen, denn um eine solche Konfiguration aus der Sicht eines Netzwerks zu implementieren, müssen alle Instanzen eine gemeinsame MAC-Adresse haben, an die der gesamte Datenverkehr/alle Anforderungen weitergeleitet werden. Die einzelnen Lösungen müssen dann entscheiden, welche Instanz den Datenverkehr/die Anforderung verarbeiten soll. Im Grunde genommen macht diese Architektur aus Upstream-Switches Hubs und dupliziert den Netzwerkverkehr. Je mehr eine Lösung horizontal skaliert wird, desto mehr Bandbreite wird durch dieses Broadcast-Verhalten verbraucht. Dies kann sich negativ auf die Netzwerkkapazität und die Performance auswirken, ganz zu schweigen davon, dass die Fehlersuche schwieriger wird, vor allem in Umgebungen wie z.B. Cloud-Computing, bei denen die Sichtbarkeit bereits eingeschränkt ist.

Vertikale Skalierung (Scale-Up)

Beim Scale-Up spielen Netzwerkprobleme keine Rolle, da zur Ausweitung der Kapazität zusätzliche Rechenressourcen verwendet werden. Dieser Ansatz



White Paper

Bau einer Hybrid-ADN-Architektur mit virtuellen und physischen ADCs

hat zwar seine Berechtigung, aber auch Grenzen, und ist im Gegensatz zum Scale-Out genauso unterbrechungsanfällig wie ein Scale-Up herkömmlicher Netzwerkkomponenten. Zur Erhöhung von Rechenressourcen wird häufig neue Hardware benötigt, und ob man nun Standardhardware oder spezialisierte Hardware austauscht, macht keinen Unterschied.

Darüber hinaus gibt es für eine vertikale Skalierung eine feste obere Kapazitätsgrenze, die ein VNA nicht überschreiten kann. Begrenzungen hinsichtlich des adressierbaren Arbeitsspeichers und inhärente Leistungsverschlechterungen schränken die Skalierbarkeit ein. Diese Leistungsverschlechterungen werden von Netzwerksoftware verursacht, die sich notwendigerweise auf die interne Pflege der verbindungsorientierten "Listen" konzentriert, auf die, wenn sie zu groß werden, der Zugriff immer länger dauert.

Beim Scale-Up eines VNA werden Verbesserungen von Performance und Effizienz, die durch die Integration in spezialisierte Hardware gewonnen wurden, wieder zunichte gemacht. Packet-Processing-Engines, algorithmische Beschleunigung und Protokolloptimierungen von spezialisierter Hardware können bei einer Verschiebung auf Standardhardware nicht die gleichen Performance-Raten erzielen.

Hybrid-Skalierbarkeit

Um herauszufinden, ob die Bereitstellung eines pADC oder eines vADC (oder eines beliebigen VNA im Vergleich zu seinem physischen Pendant) sinnvoll ist, hat es sich als gute Faustformel erwiesen, die Kernfunktionalität des Geräts festzulegen. Wenn die Lösung Datenverkehr/Anforderungen kumuliert und auf Geräte oder Netzwerke wie Routers und Load-Balancing verteilt, ist sie aufgrund der mit einer Skalierung von VNAs verbundenen Schwierigkeiten kein guter Kandidat für eine Virtualisierung. Eine zweite Orientierungshilfe: Wenn es bereits einen pADC gibt, der als Load-Balancer für die Lösung fungiert, wird mit ziemlicher Sicherheit auch dann noch ein pADC gebraucht, wenn diese in virtueller Form umgesetzt wird. Selbst wenn für die Lösungen - z.B. eine Netzwerk-Firewall - aktuell kein Load-Balancing durchgeführt wird, kann es notwendig sein, eine Load-Balancing-Lösung zu implementieren, um das VNA beim Wechsel von einer physischen zu einer virtuellen Bereitstellung zu skalieren.

Das bedeutet nicht, dass in einer Produktionsumgebung kein Platz für einen vADC ist. Ganz im Gegenteil, ein vADC ergänzt einen pADC und andere VNAs sehr gut. Bei einigen Funktionen ist es jedoch architektonisch gesehen nicht von Vorteil, virtualisierte Versionen einzusetzen, um diese Funktionen zu unterstützen.



Anpassbarkeit

Anpassbarkeit oder Flexibilität wird oft als Grund für die Implementierung von virtuellen Lösungen genannt. Es ist mit Sicherheit einfacher - und schneller - einen vADC als einen pADC bereitzustellen, wenn ein Problem aus betrieblichen oder technischen Gründen schnell gelöst werden muss. Dies gilt insbesondere für Fälle, in denen eine provisorische Lösung notwendig ist. Durch die Möglichkeit des dynamischen Einsatzes von Technologien zur Bereitstellung von Anwendungen - z.B. Webanwendungssicherheit auf Anforderung - kann die IT ohne größere Unterbrechungen an wechselnde betriebliche und technische Anforderungen angepasst werden.

Die Verwendung eines vADC zur Verbesserung vorhandener pADC-Implementierungen trägt zu einer bedarfsorientierten Trennung der Funktionalität auf Anwendungs- oder Abteilungsebene bei. Die Trennung verhindert, dass unterschiedliche Anforderungen innerhalb der Unternehmensorganisation sich gegenseitig überschreiben. Diese Architektur ähnelt der Architektur eines Cloud-Computing- oder Hosting-Anbieters, bei der eine Multi-Mandanten-Lösung durch die Kombination eines pADC mit spezialisierten oder kundenspezifischen, in einer getrennten Anwendungsbereitstellungsschicht eingesetzten vADCs implementiert wird.

Mobilität

Mobilität kann sich sowohl auf Benutzer als auch auf Anwendungen beziehen. Geht es um Benutzer, besteht die Herausforderung einer Anwendungsbereitstellung darin, für jede Anwendung abhängig vom Benutzerkontext - Standort, Gerät, Netzwerkbedingungen usw. - die richtige Bereitstellungsstrategie zu identifizieren und anzuwenden. In einer Umgebung, in der ein pADC eingesetzt ist, können diese Kontextinformationen über mehrere Funktionsmodule zur Anwendungsbereitstellung hinweg geteilt werden, um sicherzustellen, dass der richtige Zugang erlaubt - oder gesperrt - wird, und um auf der Grundlage dieses Kontextes die entsprechenden Beschleunigungs- und Optimierungsrichtlinien anzuwenden. Ein vADC hätte zwar die gleichen Funktionalität, es ist jedoch fraglich, ob die zugehörige physische Hardware die Ressourcen zur Verfügung stellen würde, die notwendig sind, um die gleichen Funktionen in einer einzigen Instanz bereitzustellen. Auf die Architektur bezogen ist die Trennung von Funktionalität durch die Bereitstellung mehrerer vADCs sicher eine vernünftige Entscheidung, doch diese Trennung verhindert zwangsläufig, dass Kontext über die Funktionalität hinweg geteilt wird, während es gleichzeitig zu Leistungsverschlechterungen kommt, da erheblich mehr Verbindungen oder "Hops" entlang des Datenweges



White Paper

Bau einer Hybrid-ADN-Architektur mit virtuellen und physischen ADCs

benötigt werden. Hier muss genau überlegt werden, um entscheiden zu können, welche Funktionen Zugang zum Benutzerkontext brauchen und welche nicht, bevor Funktionen auf eine getrennte vADC-Instanz verschoben werden.

Empfohlene Best Practices

Die empfohlene Best Practice für eine dynamische Infrastruktur besteht darin, pADCs als Schlüssel-Aggregationspunkte bereitzustellen, um Offloading-Funktionen für Server und Anwendung durchzuführen, Anwendungsauslastungen mit hohem Durchsatz zu unterstützen und im Fall von komplexen Bereitstellungen mehrere fortgeschrittene ADC-Funktionen wie Anwendungssicherheit, Webbeschleunigung und Zugangssteuerung zu verwenden. vADCs sollten für bestimmte Anwendungsauslastungen eingesetzt werden, bei denen eine komplexere und rechenintensive Verarbeitung wie z.B. Scripting auf Netzwerkebene für die Anwendung erforderlich ist. In diesem Fall wird eine dedizierte Verarbeitung für die einzelne Auslastung empfohlen, um über die Zuordnung von Rechenressourcen Skalierbarkeit zu ermöglichen. Diese vADCs sollten in einer Schicht hinter den pADCs bereitgestellt werden, in der Offloading-Funktionen ausgeführt werden.

vADCs eignen sich am besten für Labor- und QS-Umgebungen, um eine schnelle Entwicklung, und Integration zu ermöglichen und die Einführungszeit zu verkürzen. Darüber hinaus verbessern vADCs in diesen Umgebungen die Zusammenarbeit zwischen Netzwerk-, Sicherheits- und Anwendungsteams, da diese Technologie einem breiteren Publikum zugänglich gemacht werden kann, ohne dass dabei die Investitions- und Verwaltungskosten für einen pADC anfallen.

Am besten berücksichtigt man die spezifischen Anforderungen der Umgebung, wägt die Vor- und Nachteile ab, die der Einsatz eines vADC oder pADC jeweils hat, und beschäftigt sich zudem noch mit den Vorteilen einer Hybrid-Architektur, die von beiden Formfaktoren profitieren kann. Um die Entscheidung für einen vADC oder einen pADC zu vereinfachen, wurde folgende Tabelle mit den Vor- und Nachteilen jedes Geräts zusammengestellt:



Überlegungen zu einer Architektur mit einem virtuellen ADC

Vorteile	Beschreibung
Schnelle Bereitstellung	Als Softwarelösung kann ein vADC im Entwicklungsprozess erheblich schneller bereitgestellt und integriert werden als ein physisches Gerät.
Wirtschaftlichkeit für bestimmte Auslastungen	Da für ein physisches Gerät je nach Anwendungstyp, Verwendung und Bereitstellungsszenario hohe Kosten anfallen können, müssen sich Unternehmen manchmal zwischen Nichtstun und dem Betrieb einer suboptimalen Infrastruktur entscheiden. Mit einem vADC können die Kosten einfacher auf eine bestimmte Anwendungsauslastung verteilt werden, zudem kann der vADC dieser Auslastung zugeordnet werden.
Fehlereingrenzung	Für den Fall, dass der Ausfall einer bestimmten Anwendungskonfiguration den Ausfall eines physischen Geräts verursacht, das als Front-End für viele Anwendungen dient, wird ein Failover zum redundanten Gerät durchgeführt. Davon können dann jedoch alle Anwendungen betroffen sein. Wenn der vADC bestimmten Anwendungsauslastungen zugeordnet ist, wird bei Ausfällen eine bessere Eingrenzung erreicht.
Verwaltung	Da der vADC zum Verwaltungs-Framework des Hypervisor-Herstellers gehört, wird Verschieben und Verwalten des vADC einfacher. Durch die Kopplung eines vADC mit bestimmten Anwendungen lässt sich dieser besser in das Gesamt-Ökosystem integrieren.
Nachteile	Beschreibung
Hohe Verfügbarkeit	Die hohe Verfügbarkeit, die mit einem speziellen pADC erzielt wird, lässt sich mit Standard-Serverhardware nicht erreichen.
Sicherheit	Anstelle eines vollständig gehärteten Systems wird eine geteilte Umgebung verwendet, in der die Sicherheit der virtuellen Anwendungen vom Hypervisor-Hersteller und dem Hersteller des Standardserver abhängt.
Skalierbarkeit	Bestimmte High-Performance-Offloading-Services haben keinen direkten Zugang zu Hardware. Auch Standardserver haben keine speziellen ASICs für das Offloading. Beides beeinflusst Skalierung und Durchsatz eines vADC.



Überlegungen zu einer Architektur mit einem physischen ADC

Vorteile	Beschreibung
Hohe Verfügbarkeit	pADC Hardware-Designs sind Carrier-gehärtet, was ein schnelles Failover und Zuverlässigkeit garantiert. Redundante Komponenten (Hochleistungslüfter, RAID und Hardware-Watchdogs) und seriell-basiertes Failover sorgen für extrem hohe Betriebszeiten und MTBF-Zahlen. Standardhardware dieser Art ist teuer und wird nicht mit der ADC-Software integriert.
Sicherheit	Die meisten pADC-Geräte und -Systeme sind sicherheitsgehärtet und herstellerspezifisch. pADCs hängen nicht von der Sicherheitsimplementierung anderer Hersteller oder deren Fehlen ab. Bei Hypervisoren gibt es bekannte und potenziell unbekannt Sicherheitschwachstellen. Bis zu einem gewissen Grad hängt die virtuelle Anwendungssicherheit daher vom Hypervisor-Hersteller ab.
Skalierbarkeit	Einige pADCs verfügen über eine High-Speed-Bridge und Offload-ASICs für Funktionen wie High-Performance-L4-Verarbeitung, SSL und Komprimierung, was sie zu einem kostengünstigen Aggregationspunkt für viele Anwendungen oder High-Performance-Anwendungen mit hohem Durchsatz macht, bei denen die Latenz eine große Rolle spielt.
Verwaltung	Ein pADC verfügbar über eine spezielle LOM-Funktionalität (Lights-Out-Management), daher sind Zugang, Diagnose und Reparatur unabhängig vom physischen Gerät möglich. Die Verwaltung kann weniger komplex erfolgen, da die Anwendungsbereitstellungsfunktionen nicht über das Datenzentrum verteilt, sondern in einem einzigen Gerät zentralisiert sind.
Nachteile	Beschreibung
Schnelle Bereitstellung	Der Versand eines physischen Produkts, Racking, Stacking und Verkabelung sind zeitaufwendig und bedeuten zusätzliche Kosten für die Bereitstellung. Es eignet sich daher weniger gut für agile Entwicklungsumgebungen und QS-Labore.
Fehlereingrenzung	Für den Fall, dass der Ausfall einer bestimmten Anwendungskonfiguration den Ausfall eines physischen Geräts verursacht, das als Front-End für viele Anwendungen dient, wird ein Failover zum redundanten Gerät durchgeführt. Davon können dann jedoch alle Anwendungen betroffen sein. Daher kann die Kombination eines physischen ADCs mit einem virtuellen ADC sowohl für Fehlereingrenzung als auch für Skalierung sorgen.



White Paper

Bau einer Hybrid-ADN-Architektur mit virtuellen und physischen ADCs

Schlussfolgerung

Die Verfügbarkeit von virtuellen Netzwerkgeräten ist sicher ein Schritt in die richtige Richtung, und vADCs sind hier keine Ausnahme. Man muss jedoch im Gedächtnis behalten, dass mit der Virtualisierung von Netzwerkkomponenten andere technische Herausforderungen einhergehen als mit der Virtualisierung von Servern, und dass sich diese Herausforderungen fast immer auf die Architektur beziehen.

Es gibt viele Umgebungen und Verwendungsmöglichkeiten innerhalb eines Unternehmens, für die vADCs unmittelbar von Vorteil sind: Testen, Entwicklung, Integrierung, QS und Staging von Richtlinien zur Anwendungsbereitstellung. Andere, wie etwa Produktionsnetzwerke, auf die Unternehmen und Kunden vertrauen, können, müssen aber nicht für einen vADC geeignet sein, und sind mit Sicherheit keine guten Kandidaten, bevor nicht alle potenziellen Probleme mit der Architektur identifiziert und gelöst sind. Obwohl viele Herausforderungen in allen Unternehmen und Branchen auftreten, werden viele andere nur in einzelnen Datenzentren auftreten, abhängig von Anforderungen, Anwendungen und bereits vorhandenen Architekturen.

¹ <http://www.rackspace.com/downloads/surveys/VirtualizationSurvey.pdf>

² <http://www.channelinsider.com/c/a/Virtualization/Virtualization-a-Driver-for-2010-Server-Refresh-360526/>

³ http://www.cio.com/article/168401/Virtualization_in_the_Enterprise_Survey_Your_Virtualized_State_in_2008?page=2&taxonomyId=3112

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
info.asia@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

WP-Dynamisch-IT 05/10

© 2010 F5 Networks, Inc. All rights reserved. F5, F5 Networks, the F5 logo, BIG-IP, FirePass, iControl, TMOS, and VIPRION are trademarks or registered trademarks of F5 Networks, Inc. in the U.S. and in certain other countries.