Developing a Network Infrastructure to Support Cloud Computing

eWEEK

Level (3) COMMUNICATIONS IS NOW CenturyLink®

Contents...

Developing a Network Infrastructure to Support Cloud Computing

2 Cloud Application Growth Requires Re-Thinking Network Connectivity

5 Optimizing Cloud Applications with Efficient Network Solutions

7 Increase Control and Security of Cloud Applications

9 How Level 3 Can Help

Cloud Application Growth Requires Re-Thinking Network Connectivity

The appetite for businesses and their IT departments to move toward cloud computing seems insatiable. You're unlikely to find an IT organization that hasn't at least explored cloud computing, and there isn't an IT vendor around that doesn't offer cloud-based products or services. Cloud computing comes in many different flavors — software as a service, infrastructure as a service, and platform as a service, for starters — that it seems to have something for everyone.

There is no question why organizations of all types are moving to cloud infrastructure to deliver richer, higher-quality services to their business and retail customers. They are much the same reasons why most people obtain electricity from the grid instead of buying and operating generators.

With the cloud:

- You don't have to design, purchase, set up, maintain and manage the infrastructure.
- Capacity can rapidly scale up or down in response to demand.
- You don't have to pay for mostly idle servers just to ensure you have the capacity to meet peak loads.
- There can be huge economies of scale in equipment purchasing.
- A cloud provider can have a team of specialists that would be prohibitively expensive for a customer to bring on board.
- Cloud services can be more resilient.

- With a consumption-based pricing model, customers save money by only paying for their actual usage.

These advantages have produced an explosive growth rate for the cloud services industry. In February 2014, IHS Technology reported global business spending for cloud infrastructure and services would reach $174.2 billion in 2014, a 20 percent increase over last year, and that enterprise spending on the cloud would hit $235 billion in 2017, triple the amount spent in 2011.

Mission-Critical Apps Move to the Cloud

We see the results of this cloud build out every time we stream media to our television, check our bank account balances, or let our smartphone give us turn-by-turn directions. It is great having all these public-facing

applications at our beck and call, but the question is whether we should trust the cloud with our mission-critical systems that don't require public access.

Here, there is considerably more reluctance to give up control, but the movement is in that direction. To begin with, many large enterprise application vendors are now in the cloud. There are, of course, the pure cloud vendors such as Salesforce.com, which brought in $4 billion in 2013 through its signature Customer Relationship Management (CRM) system and other offerings. Traditional in-house vendors are also increasingly moving their enterprise software to the cloud. SAP has cloud versions of Human Capital Management (HCM) software – through its acquisition of SuccessFactors – as well as Financial, Procurement, Sales, Marketing and Supply Chain. Oracle similarly has cloud versions of its HCM, Financial, Project Management, Business Intelligence and Supply Chain software. It also offers a multitenant cloud version of Oracle Database 11g, and is planning to offer dedicated virtual machines running Oracle Database 11g or 12c.

Then there are companies that specialize in providing Infrastructure as a Service (IaaS). A leader in this area is Amazon Web Services (AWS). Gartner's most recent Magic Quadrant for Cloud Infrastructure as a Service (May 2014) evaluated 15 vendors. Microsoft Azure and AWS were the only vendors positioned in its Leaders quadrant. AWS was positioned the furthest for ability to execute and completeness of vision.[i]

But vendors are continuing to solidify their cloud offerings, and more customers are willing to trust their mission-critical applications to the cloud. IDC conducts an annual Global CloudTrack Survey of more than 1,000 companies. In 2012, it found that 71 percent of companies were "using, planning or researching cloud," that 30 percent of organizations expected that the majority of their IT capability would be delivered through the cloud within five years and that 45.5 percent would be delivered through a public, private or hybrid cloud within three years. The 2013 survey found that 60 percent of companies "were already using or had firm plans to use cloud services." It also found that 31 percent wanted to have a cloud-first strategy within the next 24 months. Looking at deployment of five enterprise applications – CRM for call centers, CRM for marketing and sales automation, financial ERP, HR ERP and supply chain and logistics – on-premises deployments had declined by 5.5 percent to 7.0 percent, with that work shifting to cloud deployments.

Cloud Liabilities

There are few questions as to why cloud usage is growing and more enterprises are moving their back-office, mission-critical applications to the cloud. But there are challenges involved in enabling a successful cloud operating environment. Employees and customers have certain expectations when it comes to application uptime and performance. Business users, for example, are accustomed to working with on-premise applications that are very responsive. Many applications are very sensitive to poor or inconsistent network performance so that when there is latency, it can cause an application like a database or email server to stall or even time-out.

This can be a problem in-house. Even when only a few feet separate data center components and the users are in the same building, applications can still time-out. But add in a cloud provider, and hundreds of thousands of miles are added to each round-trip loop. The distance itself adds latency. Even with a fiber-optic connection — where the signals travel about two-thirds the speed of light — using a cloud service that is 1,000 miles away adds more than 15ms latency – not particularly noticeable to the end user, but an eternity for a database server. And it is not just the distance that matters. Each router, gateway, switch, firewall and load balancer along the way adds its own little bit to the latency.

Because of this, any company considering a cloud initiative needs to closely consider network performance between users, applications and their cloud services. While many businesses have been sold on the idea of cloud services, connectivity is frequently overlooked — even though this is where critical performance issues come into play.

The Role of Private Networks

The Internet can be very egalitarian: your mission-critical application is no more critical than someone else's marathon game session. The cyberhighway is also host to lots of drivers you don't want share the same road with: in 2013 Kapersky Labs detected an average of 315,000 new malicious files per day, up from 200,000 the year before.[ii]

Just as your organization relies on a private network when running in-house applications, you should consider the same approach when moving your critical functions offsite. Unlike a public internet connection, private networks allow businesses to control how data moves between users and the cloud by providing guaranteed throughput and consistent latency. Performance and availability is predictable on private networks, even when managing large workloads. Private networks offer deterministic performance and guaranteed bandwidth. Private networks also have end-to-end security built in, so you don't have to worry about moving your data offsite. In the next two articles, we will take a greater look at the issues of efficiency and security as they relate to cloud computing and private networks.

Optimizing Cloud Applications with Efficient Network Solutions

In the first article, we discussed how organizations are increasingly moving, not only their public-facing applications, but their mission-critical applications to the cloud. To ensure performance, reliability and security, they should consider private networks as an alternative to the public Internet. But there is one other factor that is key: efficiency.

IT is under continual pressure to deliver greater flexibility and operational value while cutting costs. When Gartner surveyed 2,339 CIOs about their priorities for 2014 as part of its report Taming the Dragon: The 2014 *CIO Agenda*[iii], efficiency was listed as the No. 1 priority. That shouldn't be surprising: efficiency was No. 1 in the 2009 and 2013 surveys as well. The report explained: "In terms of management's mood, CIOs report a gradual but undeniable shift toward growth. But despite the need to grow, there is pressure on budgets. The global weighted average expected change in CIO IT budgets is +0.2%. This lack of significant uptick presents challenges for the CIO and IT organization since there is a need to simultaneously renovate the core of IT systems and services, and exploit new technology options."

To meet this demand for efficiency, there has been an ongoing move toward virtualization and consolidation. Many data centers are now using VMware, XenServer, and/or Microsoft Hyper-V, reducing the number of servers the organization has to purchase, but also slashing ongoing costs for support, floor space, licensing, power and cooling. Next was storage consolidation, replacing direct attached storage with Storage Array Networks and Network Attached Storage. Some have gone as far as consolidating the number of data centers they operate.

But virtualization and consolidation can only go so far and many organizations have achieved most of the benefit they will get from these activities. 451 Research's TheInfoPro service reported in 2012 that 51 percent of x86 servers were already virtualized. IDC predicts that around 80 percent of x86 server loads that can be virtualized will be by the end of the decade.

Switching from CapEx to OpEx

Switching to hardware virtualization increases utilization and cuts expenses, but there is a more fundamental shift that has been taking place in IT. Driven in part by the adoption of the Information Technology Infrastructure Library (ITIL) methodology, instead of being viewed as an infrastructure provider, IT is expected to provide the services that the business needs to grow and prosper. Where those services come from is not as important as the quality, cost or effectiveness of the services rendered.

Since companies are paying for services rather than infrastructure, more IT expenditures have shifted to outsourcing. Specialist programmers brought in for a particular project can do it faster, cheaper and better than in-house generalists. Software as a Service (SaaS) has lower upfront costs and is easier to maintain than when one owns the software.

There has also been a switch from a CapEx to an OpEx viewpoint when it comes to storage and computing resources. While virtualization did improve the utilization levels, that is nothing compared to what can be achieved by averaging utilization across a broad customer base. Some speculate that this is what led Amazon to get into the cloud services market to begin with. It is believed that the company needed a huge infrastructure to deal with the short holiday season traffic peak, which would be wasted the rest of the year.[v] Amazon could afford to build an infrastructure that could easily manage the peak loads without glitching by selling its excess capacity.

Its customers, meanwhile, got access to world-class computing resources when needed, without incurring the capital expenses and ongoing operating expenses required for such a system. Instead, they just paid for the services they actually consumed.

Bringing Efficiency to the Network

The idea of paying for consumption with bursting, when needed, is part of the appeal of the cloud. You never have to pay to build and maintain an infrastructure robust enough to handle rarely seen peaks, nor do you have to worry about running out of capacity since the cloud is infinitely scalable.

But there is one point where companies have fallen down in their cloud implementations: the network. Just as computing needs are highly variable, so are networks. Cloud backups, moving data to or from a remote data center, reporting and other functions can produce high-bandwidth bursts. In order to access cloud services, companies have been overbuilding their WAN connections in order to avoid any slowdowns during peak traffic periods. And, if they are using a public internet connection, they have to oversize their connection even further to try to compensate for delays caused by other users of this shared resource. Even so, they have no guarantee that their traffic will get through.

The same concepts that have driven the adoption of cloud computing can be applied to virtual private network services, which are reliable and secure. Private network services are physically separate from the public Internet and they provide guaranteed throughput, availability and latency. Done right, they also improve efficiency by:

- **Streamlining Security:** With private network services, you can keep the most sensitive applications and data cordoned off from the outside world. This gives your application developers a controlled environment to create and test new applications in the cloud without exposing your internal network and assets. Then, when you finally deploy your applications in the cloud, you can use private network services for your most important data and apps, limiting public ports and minimizing your security overhead.

- **Maintaining Productivity:** Because private network services offer guaranteed throughput and deterministic performance, you get the bandwidth you need to move large workloads in and out of the cloud with the latency required by the applications and end users. By comparison, the public Internet moves information on a best-efforts basis, so during times of heavy congestion, packets can be dropped, data may need to be re-transmitted, and applications may timeout causing an inefficient and potentially costly use of bandwidth and lost productivity.

- **Pay Just for What You Use:** With virtual private network (VPN) services, you can scale up and down dynamically and pay for only what you use, which is perfect for unpredictable or inherently variable workloads.

With a private network connecting to cloud resources, the enterprise gets a better, more predictable experience. Performance benchmarks and user expectations are met and frustration is eliminated. The company can support continued growth in data and the systems to manage it while avoiding the high upfront cost and long lead times associated with private data center build outs. Offices spread across the globe can be connected to company data centers as well as cloud resources via this dedicated private network. They can deliver cloud-based applications quickly and without interruption while realizing greater efficiencies.

Increase Control and Security of Cloud Applications

In addition to concerns over performance, the other main concern that enterprises have when moving mission-critical applications to the cloud is security. Mission-critical applications always carry sensitive data. Even if the data itself is not confidential, it is still essential to business operations and so, if the data is intercepted or corrupted en route, it can disrupt operations. The network can also serve as an attack vector into the backend servers and storage systems.

The public Internet is the most common conduit to the cloud and firewalls and data encryption are good enough for securing many cloud services. For some organizations it is not, however, secure enough for mission-critical data and applications. If open ports expose an enterprise's network and IT environment to the public Internet, there are vulnerability issues to contend with. Anyone that detects an opening can launch an attack on your site or application and bring it down. Many companies are able to manage this on their own, but as the number and complexity of cloud applications increase, so does the need for more diligence. Any minor security lapse can be cause for concern, and security issues directly impact network performance and availability.

Cost of Security Breaches

Data breaches can be extremely expensive. In August 2014, Target Corporation reported that the theft of customer credit card information in 2013 cost the company $148 million.[vi] That, however, was just the hard costs: it doesn't count the reputational damage and lost sales that resulted from breaching the public's trust. And that is just one company. The Director General of Britain's MI5 security agency reported in 2012 that one unnamed major firm listed on the London Stock Exchange lost about $1.3 billion due to hostile state cyberattack.[vii]

A June 2014 report prepared by the Center for Strategic and International Studies on behalf of McAfee, Inc. came up with an annual figure of $375 billion to $575 billion annually in global cybercrime losses, including direct costs, lost intellectual property, reputational losses and costs of additional security following the breach.[viii]

Keep in mind, however that these high costs don't mean that cloud computing is any less secure than keeping things in-house. To begin with, the major cloud service

providers have greater security resources and systems in place than many of their customers could afford. And, one can note, that the cyberattacks do not necessarily entail cloud vulnerabilities. For example, the Target data breach involved someone gaining access to the computers of a small company in Philadelphia that did air conditioning work for Target, using the electronic billing system to access Targets computers, and then swiping data from the point of sale system.[ix] The biggest classified data security breach recently was carried out by an employee, Edward Snowden, downloading top secret files onto a thumb drive and walking out the door.[x]

Building a Secure Network

Cybersecurity requires defense in depth: finding and eliminating weak points. This includes making sure internal systems are secure and proper measures are taken to secure your resources in the cloud. However, too often the connection between the two is overlooked.

Public networks are inherently exposed to the public and require more vigilant security measures. When dealing with public-facing applications, this cannot be avoided, but most mission-critical applications are not available to the public. In such a case, a private network that is physically isolated from other networks offers both greater control and better defenses.

The correct solution is to architect the network with the connection type that makes the most sense for the applications and users and that minimizes security and management overhead. Consolidate the public connections so security can be closely managed and use private network services everywhere else.

How Level 3 Can Help

Cloud computing gives companies a simple way to scale their IT services, pay only for what they need and quickly deploy new services. Without a solid network strategy, successful migration to a cloud solution is virtually impossible.

Since 1998, Level 3 has been innovating network and communication services. It offers a comprehensive portfolio of cloud, data center, network, security, video, voice, unified communication and collaboration solutions.

Level 3® Cloud Connect Solutions make it simple to establish private connections to private and public cloud services. With pre-established connectivity to leading cloud service and data centers around the world, Level 3 makes it easy to attach a new cloud service to an enterprise's WAN. Level 3 offers both dedicated and VPN services to enable a range of solutions that fit into your desired network architecture — from aggregating cloud traffic and controlling routing over a few high-bandwidth connections to deploying several right-sized connections between multiple, regionally distributed offices and cloud distribution points.

Level 3® Cloud Connect Solutions create a secure path between your offices and the cloud or data center providers of your choice. Level 3 Cloud Connect Solutions include:

- Pre-established interconnects that enable you to quickly add or change connections between your WAN and different public, private, and hybrid cloud resources.
- Global, end-to-end fiber network with low-latency options and class of service guarantees for reliable, high-performing, secure cloud ecosystems.

- Dynamic bandwidth and usage-based billing allows your organization to consume the network with the same efficiency of the cloud services it delivers.
- Point-to-point transport gives Level 3 customers full transparency and routing control so they can build and manage their own high-speed, high-performance backbones with guaranteed throughput and defined latency.
- Point-to-multi-point and any-to-any VPN services provide greater efficiency at lower speeds, dynamic

bandwidth, guaranteed class of service and usage-based billing. Regardless of the customer's architecture, they have complete control.

Level 3's network is global, so regardless of where your offices are, chances are Level 3 can offer local connectivity to local cloud resources so you don't need to navigate multiple service providers across time-zones and languages.

As enterprises continue to migrate and operate their business applications in the cloud, create more and more data and demand greater analytical, processing and storage capabilities, Level 3 is ready to assist with the network connections that help make it all possible. Cloud adoption and growth is occurring at blinding speed. There is a lot to know and a lot to think about. Level 3 can help you with your business's needs and objectives, and build the network solutions that make them all possible.

[i]*Note: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.*

[ii]*http://www.kaspersky.com/about/news/virus/2013/number-of-the-year*

[iii]*Taming the Dragon: The 2014 CIO Agenda, Jan. 2014. http://www.gartner.com/imagesrv/cio/pdf/cio_agenda_insights2014.pdf*

[iv]*http://www.serverwatch.com/server-trends/survey-51-of-x86-servers-now-virtualized.html*

[v]*http://web.stanford.edu/class/ee204/Publications/Amazon-EE353-2008-1.pdf*

[vi]*http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html?_r=0*

[vii]*http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9354373/Cyber-crime-a-global-threat-MI5-head-warns.html*

[viii]*http://csis.org/files/attachments/140609_McAfee_PDF.pdf*

[ix]*http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/*

[x]*http://articles.latimes.com/2013/jun/13/news/la-pn-snowden-nsa-secrets-thumb-drive-20130613*

WVM12347-USEN-00