

WHITE PAPER

The Journey to the Private Cloud - Taking the First Steps

Sponsored by: EMC Corporation & Brocade Communication Systems, Inc.

Benjamin S. Woo

May 2010

EXECUTIVE SUMMARY

The modern IT organization is changing. IT organizations need to increasingly deliver IT through a services orientated model. As such, leveraging consolidated and convergent infrastructure will lead to the desired cost efficiencies and deliver IT service to the required and agreed upon service levels.

IT functions will increasingly be automated so that its delivery can be more predictable, repeatable and thus more reliable to users. IT organizations looking to accomplish this and become true and efficient service organizations must look to the sky: to achieve these objectives, they must leverage the benefits that can be found in a private cloud computing environment.

The private cloud affords the opportunity to create the virtualized IT enterprise architecture of the future, on an organization's own terms, yet with the backbone of the Internet facilitating it. The applications reside on the organization's hardware, within its network, as does the data. The IT infrastructure is distributed across the enterprise LANs and WANs. Unlike the public cloud, private cloud computing requires your own build-and-sustain efforts, but with that responsibility comes the benefits of centralized management, the promise of a virtualized computing environment and control of endpoints, and protection and security.

IDC views private cloud computing as maturation of the evolution of the IT datacenter, and sees virtualization as the necessary stepping stone to the private cloud environment. While public cloud computing raises issues of reliability, data security, system protection, compliance and governance, none of these concerns are as prominent with the private cloud.

Moreover, the private cloud can be more easily managed, since it tends to leverage existing known processes and practices. The private cloud data center of the future is based upon the concepts of agility, flexibility, leveraging assets, and creating an open but secure computing environment. Working with these concepts, the new data center model can be accomplished using three working principles: consolidation, virtualization, and protection. Once these three principles are implemented, it is possible to have a fully automated data center that delivers IT as a reliable and

sustainable service to enterprise users all across the private cloud. Although this is a considerable undertaking, the rewards are great, and solutions exist to help navigate to the objective. This white paper describes the process through the three working principles and how they configure the automation process, and one solution based on experienced, tested technologies.

Building the Data Center of the Future

In today's service-oriented economy, the mantra is to listen to the customers. Just as the business cannot function without IT, so IT understands its mission is to support the business – and that means providing the highest-value services to its customer, the technology user. IT has learned in recent years that its relationship to the customer is where it forges the bond of service, and that in order to sustain and improve that relationship; its systems must be agile, flexible, and leveraged. These concepts are familiar to all, but what do they mean in practical terms?

□ **Open:** Today's open IT system differs from what has been conventionally considered open in the past, by virtue of the cloud. The concept of open today means more than simply installed equipment from different vendors: it means providing infrastructure support for multiple applications, servers and operating systems, networking interfaces and storage capabilities that all work together seamlessly. This level of openness, facilitated by private cloud computing, makes it possible to add new applications and services with ease.

□ **Agility:** An agile IT system supports its existing informational infrastructure, is smoothly integrated across fixed and networked assets, is diverse in its application portfolio, is based upon open-system practices, and is built for continuous development and improvement. An agile IT environment can be physical, virtual, or, ideally, both.

□ **Flexibility:** A flexible IT system architecture takes advantage of its diverse servers, ensures open cross-functionality, delivers access across the network, and supports whatever needs users currently have or may request in the future. Its services are proven and tested, and afford different deployment options based on the agile architecture and adaptable configurations previously mentioned.

□ **Fully Leveraged:** A fully leveraged IT system takes maximum advantage of existing assets, even if they are all fixed physical assets. Because of its agility and flexibility, it is an adaptable system that can be reconfigured as a virtual system, accessible via a private cloud. By virtue of its design, recovery, security and data integrity are assured.

IT executives understand they cannot allow their services to stand still or falter in today's competitive, and often perilous, business environment. They are like the cross-country runner who races through a natural environment fraught with danger: mud, stones, hidden tree roots, inclement weather, and a strenuous terrain, while constantly trying to stay ahead of the other runners. For both, the tactical must always be measured and balanced against the strategic, for nothing stays the same for long.

Moving forward, IDC believes four of the greatest challenges for IT organizations are:

- Cloud computing - especially the private cloud
- The completely virtualized data center

- Virtual workgroups using virtual applications and distributed data across the cloud, and
- Protection and security issues surrounding challenges one through three.

While these may at first appear to be separate problems to solve, they are interrelated, and solutions to solve these problems already exist. IDC believes the importance of cloud computing – especially the private cloud – cannot be overemphasized, particularly for geographically dispersed enterprises. If IT cannot deliver a private cloud for the enterprise, an outside vendor may be called to step in and provide it. In the aggregate, the solution can be summed up thusly:

- Consolidation of physical and network resources
- Virtualization of the data center operations
- Protection of physical, virtual, and network resources and data security, and
- Automation of all the above

Step One: Consolidation

Most enterprise data centers are comprised of a variety of hardware, software, and network components from many different vendors. Patchwork data centers, cobbled together over years and years of changes and additions, are often kludgy and inefficient, not just in terms of wasted cycles or redundant equipment, but energy usage as well.

Consolidation can create efficiencies of scale while reducing costs, eliminating waste and underutilization, all the while moving the data center toward the cloud computing model. Central to effective consolidation is recognizing that it applies to the three pillars on which IT relies – compute, networking and storage.

Storage as a key aspect of consolidation, can often be overlooked. A centralized networking environment for processing also benefits from consolidating storage resources. Higher storage utilization means headroom allocation can be reduced, which means additional storage capacity can be purchased on an as-needed - rather than a, in-case-it's-needed-basis. In addition, hierarchical or tiered storage can significantly reduce costs because of data storage prioritization. In short, most, if not all, the benefits of server consolidation apply to storage consolidation as well: productivity increases, personnel costs decrease, system uptime improves, and operational costs decline significantly. The steps in consolidation are to first consolidate the data center networks, then tier network storage, followed by integrating IT management.

Step Two: Virtualization

Most IT executives are aware of the benefits that can accrue from virtualization, yet the cost and complexity of the transition from physical to virtual can seem daunting. Unfortunately, that perception is mired in the physical IT infrastructure, which becomes more flexible and scalable once it is married to the virtualized infrastructure. Even so, the necessity of integrating the old physical data center into the new virtual data center is essential if IT is to move to the private cloud. Once the limitations of the physical environment have been transcended, the two ideally complement one another. Virtualization makes most IT functions simpler to address and resolve, while

improving efficiencies for common data center tasks such as hardware provisioning, migrating applications, and often data protection as well. By moving away from the one-to-one relationships between various physical resources, virtualization increases capacity and utilization while reducing CAPEX and OPEX.

Virtualization, in the past often regarded as strictly a server or OS enhancement, can be meaningfully deployed across the entire IT infrastructure. This is, indeed, the idea. However, perhaps its greatest potential lies in tiered network storage across multiple storage devices and platforms, facilitating writing data from multiple servers with dependable integrity and coherency. IT managers who plan to virtualize are usually tasked with first virtualizing their servers, then the network, followed by a tiered storage network. Data stored in a multitude of physical locations can now be accessed as a single virtual storage resource across the IT platform.

With consolidation achieved, virtualization moves the promise of the private cloud in the data center forward by adding agility and flexibility, thus increasing utilization and streamlining management.

Step Three: Protecting the Data Center Physical Resources

Protecting applications and securing the proprietary information they produce is a key concern and ongoing task for IT. As every IT professional knows and understands, there is a tradeoff between the need for accessibility and the restrictiveness of security. IT must balance application protection and data security with maximizing IT resources, and minimizing unnecessary complexity or compromising system performance. Here again, consolidation affords an efficient solution that takes advantage of centralized data center management.

An attendant issue with regard to insuring 24/7 application availability is, of course, data security. IDC studies report that nearly all organizations have data protection and a security strategy that includes data encryption. It is the preferred method of securing valuable proprietary data, to safeguard intellectual property and information, and to be in compliance with company, industry, and government policies and regulations.

A core enterprise asset is data-at-rest. Not only is it the repository for an organization's digital assets, but it is essential to meet governance, regulatory and compliance management. Assuring its security is commonly facilitated by using encryption. Yet as good as it is, encryption cannot surmount the proliferation of problems caused by endpoint computing. Therefore, as the data center transitions from being exclusively physical to various stages of virtualization, the protection of data located remotely becomes an equal concern. Further, the ability to replicate applications and to provide near-instantaneous recovery in case of a disaster becomes mission-critical for the always-up IT infrastructure support of business practices. Clearly, as the IT infrastructure becomes more agile, flexible, leveraged and open, supporting more diverse uses at a variety of new endpoints, so does the need grow for strong, efficient consolidation and centralized data center management.

Protection and security are two sides of the same coin, and are inextricably part of the IT environment and mission. Protecting software assets in planned and unplanned situations - for example backup, remote replication and disaster recovery - can be designed as SAN extensions of the networking infrastructure, and should be. Secure

encryption can be integrated at the application layer in the IT environment so that it works consistently and reliably in the background, freeing users to concentrate on high-productivity work output. In so doing, the data center takes another significant step toward complete automation and delivering IT at the highest level of service quality.

Step Four: Complete Data Center Automation

Most IT environments manage their operations through systems and storage management software, these tools are insufficient to effectively achieve data center automation and thus, breaks one of the key attributes necessary for the private cloud. To properly address this issue requires new solutions that bring the physical and virtual data center into alignment. Among the benefits are:

- Support services that are designed for an open and flexible data center
- The IT focus shifts from maintaining hardware to sustained and distributed applications to a service orientated delivery of a complete hardware and software stack
- Hardware, networking and software achieve a far higher degree of integration
- Servers, networking and storage are all virtualized, assuring always-up, anywhere access
- Protection and security are integrated and embedded – in other words automated

Full data center automation leverages IT assets at a far higher degree of utilization, often resulting in significant and material cost savings. Simultaneously, highly virtualized data centers pave the way for the introduction and integration of newer, more efficient technologies over time.

Implementing the Big Picture

Virtualization is commonly touted as the next step forward, as if it were a technology bag to hang on the side of the box. Nothing could be further from the truth. In fact, virtualization needs an integration strategy in order to work effectively. That integration manifests on two levels. One is the technology level, which this white paper discusses. The second level is the organizational level. IDC does not believe that moving to the cloud is an undertaking an IT organization should do on its own. Rather, it requires a broad partnership inside and outside of the enterprise. Building out applications, converging data networks, tiering storage, embedding virtualization in networks – each is a disruptive technology or process in itself. And remember, the ideal transition from the physical data center to the private cloud is integrated, of a single piece.

How can this be best achieved? The first step is to examine the entire IT stack, getting a sense of its functionality, strengths and weaknesses. Performance tuning, replication, recovery, and other common tools in the IT toolkit will be used to monitor and maintain system integrity throughout the process. In addition, new tools will need to be introduced, along with new processes and practices. Some of these include:

- Integrated monitoring and management
- Virtualization-aware system tools
- Bi-directional access to performance data

- System views, not just up and down, but in cross-sections as well
- Reduced number of interfaces needed to manage the stack

A technology partner can help make implementing the big picture not only a practical reality but a sound investment. While many technology partners see a partial snapshot of the private cloud, one partnership has combined resources to partner with its customers in breaking through to the new consolidated, virtualized data center. EMC and Brocade have been partnering on solutions for customers for over a decade. The two firms have combined their thought leadership to create solutions that improve data center efficiency, lower costs, facilitate deployment of a robust new information infrastructure, and create a foundation for private cloud computing. The foundation is made of three building blocks discussed in this white paper:

- Consolidation
- Virtualization
- Protection

This structure is reinforced with the Brocade Integrated Data Center Fabric, that facilitates convergence of IP and FC SAN protocols. The Data Center Fabric integrates with the Brocade DCX backbone to provide the necessary technologies to achieve consolidation, virtualization, and protection. EMC and Brocade have developed simple, practical steps to consolidate, tier and centrally manage the data center from departmental to mission critical applications.

CHALLENGES/OPPORTUNITIES

Challenges

The opportunity to converge the currently isolated islands of networking infrastructure, such as those between compute layers and storage layers, offers users with many choices.

As a result, the networking partner of choice by the end user may be driven more by an existing group of network administrators. Network administrators are more likely to adopt a common physical interface (such as 10GbE) with a singular (say IP) network protocol as opposed to attempt to integrate SAN and LAN/WAN specific packets on a single interface or network.

Opportunities

With that said, for organizations that have already made significant investments in legacy Fibre Channel (FC) infrastructure, the introduction of complementary technologies that help bridge the gap between existing and emerging networking technologies make good sense. It enables convergence (which can sometimes be disruptive) to occur, while having minimal impact to the existing environment. At the same time, users will also benefit from being able to protect the investments that they already made.

CONCLUSION

IDC believes private cloud computing is a high-value play. It transforms IT into a service, or IaaS. Once servers, storage, and networking become IaaS, compute power can be turned on and off like water. Applications that data users create are instantly and always available, always current. IT resources are protected and IP is safe. These are highly appropriate objectives for moving ahead in the second decade of the new millennium.

It goes without saying that it makes the most sense to determine what your targeted solutions are, and to use existing technologies to move toward the private cloud. Envisioning the next-generation data center is equally straightforward. The existing technologies that will drive the migration include open systems, sustaining support for the current infrastructure, evolving into virtualization toolsets that inspire the consolidation process, making the IT architecture more flexible to accommodate the virtual propagation, and being ever-mindful of the need for protection and security.

Developing a bold and innovative relationship with a technology partner will assure that these steps occur in the proper order, at the proper place, and achieve your targeted solution success.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2010 IDC. Reproduction without written permission is completely forbidden.