Filing Information: May 2009, IDC #IDCWP10R

Virtualisation and Business Continuity

Claus Egge
Giorgio Nebuloni
Nathaniel Martinez
Chris Ingle

IDC EMEA, 389 Chiswick High Road, London, W4 4AE, U.K. Tel.+44.20.8987.7100 www.idc.com

WHITE PAPER

Virtualisation and Business Continuity

Sponsored by: EMC and VMware

Claus Egge | Nathaniel Martinez
Giorgio Nebuloni | Chris Ingle

May 2009

IDC OPINION

The adoption rate for server virtualisation has been high as customers strive to cut costs and maximise the return on their existing investments. IDC research shows that many customers are turning their attention to an enhancement of their business continuity (BC) infrastructure as the next phase in their virtualisation roadmap.

At one end of the scale, BC means having the appropriate plans for an organisation to cope with major disasters such as a flood or extended power outage. At the other end, BC means having an agile IT environment that is able to deal with a host of relatively minor yet potentially costly disruptions. Faced with flat budgets and complex infrastructures, IT professionals are increasingly looking for a more agile and flexible approach to BC that is straightforward to manage and introduces greater levels of automation and resilience. In either scenario, IDC believes that once protection levels have been raised, IT is unlikely to bring them back down.

Server virtualisation offers a powerful and flexible new approach to business continuity, giving IT managers tools to enhance their BC capability and make better use of the resources and budgets that are available. We advise users, irrespective of their familiarity with server virtualisation, to explore the many benefits it can bestow on BC operations.

It may be tempting to rush into virtualisation to reap the benefits of a more agile and automated environment, but for BC plans dealing with disaster scenarios it is advisable to move ahead with thoughtful consideration. BC plans must be robust and properly tested and staff involved must be comfortable that their execution of the plan is predictable and effective.

IDC believes that in order to maximise the benefits on offer, a virtualisation BC roadmap for the company, based on a methodical and holistic assessment of the IT infrastructure should be drawn up, using the guidelines and recommendations presented in this paper.

IDC EMEA, 389 Chiswick High Road, London, W4 4AE, U.K. Tel.+44.20.8987.7100 www.idc.com

TABLE OF CONTENTS

P

LIST OF FIGURES

P

METHODOLOGY

This document uses the research methodology from the latest *IDC Server and Software Taxonomies* and includes results from the *IDC European Server Virtualisation Survey* conducted last year as well as the latest *IDC Annual European Storage Survey*. It also refers to server installed base estimates presented in *European Server Installed Base Market Shares and Forecasts, 2007–2012*.

IN THIS WHITE PAPER

This IDC paper is focused on the potential impact that x86 server virtualisation is having on business continuity practices in datacentres. It provides detailed analysis of the shift from traditional datacentre protection to BC plans in virtualised server environments. Furthermore, it examines the issues and potential benefits that organisations should consider in formulating a virtualisation roadmap.

SITUATION OVERVIEW

What is Virtualisation and Business Continuity?

In this section, we look at the definitions of business continuity, disaster recovery (DR), high availability (HA) and server virtualisation and why virtualisation requires a different approach to BC.

Business Continuity

The term business continuity is used in many different contexts. In its most thorough interpretation, business continuity planning spans the whole organisation, including all of its employees, its vital business processes and not least its physical facilities. The best-known example is the BS25999 standard, which has been led by the British Standards Institution.

For the purpose of this document, we will use the term BC to refer specifically to IT practices.

We will also refer to different types of contingency scenario:

- High-availability, in which the aim is to minimise downtime as well as provide IT environments designed for automated seamless failover.
- Disaster recovery, which sets out to enable an organisation to cope with the loss of its main IT-site(s)
- SLA provision, in which the IT department implements processes to enable the recovery of resources and applications to conform with service level agreements

Traditionally, BC solutions have been based on variable combinations of:

- **Redundant hardware** geographically distributed in DR scenarios, or hosted in the same facility in HA scenarios
- **Special editions of software** (OS and apps) supporting high-end needs (e.g., clustering) and/or specific storage management products able to replicate

standard software environments (examples include HP Integrity, IBM System Cluster, IBM GPFS)

- **Data replication**. Producing copies of information on different types of media on disparate computing platforms and in separate locations has been exploited from the infancy of computing. Data replication has continually evolved, adding sophistication and efficiency, frequently through virtualisation at the storage layer.

Server Virtualisation

Server virtualisation introduces a software layer between the physical server and operating system(s). This layer removes the traditional dependency of an operating system on its physical host. In this way, operating systems and applications can run as virtual machines (VMs) concurrently on a server while being isolated from each other.

Server virtualisation drives potentially transformational benefits for the IT function, offering the possibility of rapid and significant cost reductions concurrently with "game-changing" increases in performance and productivity.

There are many potential benefits of server virtualisation:

- Higher average CPU utilisation rates of physical servers
- Servers consolidated from many to few
- Applications can be migrated seamlessly between physical servers
- Raising IT professionals' ability and agility in systems and application management
- Improved energy efficiency
- Resolving compatibility problems of aged hardware and legacy applications

Due to these benefits, x86 virtualisation is progressing quickly from early test and development projects, to large-scale adoption in production environments and widespread recognition in the market.

IDC's global research group forecasts that the installed base of virtualised servers will grow 33% CAGR from $16.3 million in 2008 to $51.3 million in 2012.

Such is the appreciation of server virtualisation that of those European IT professionals who had *not* implemented it yet, 81% were nonetheless familiar with it (*2008 European Server Virtualization Survey: Fast Growth and Wider Range of Applications*, IDC #GE56Q, June 2008), and a further 54% had plans to implement virtualisation over the subsequent 12–24 months.

Irrespective of the initial reason for implementing server virtualisation, IT professionals will soon have to consider its impact on existing BC, and more importantly the potential additional benefits a virtualised environment can offer. However, the ultimate benefits can only be realised with a fresh strategic approach to BC.

Virtualisation Requires a Fresh Approach

IDC believes that companies should approach virtualisation plans with a holistic view in order to:

- Explore the new functions and capabilities that a virtualised server environment offers
- Review the BC and DR plans to fully exploit a virtualised environment
- Evaluate the new skills required by IT staff in managing virtualised environments
- Carefully consider, and plan for, the potential impact on data storage protection, security and information governance

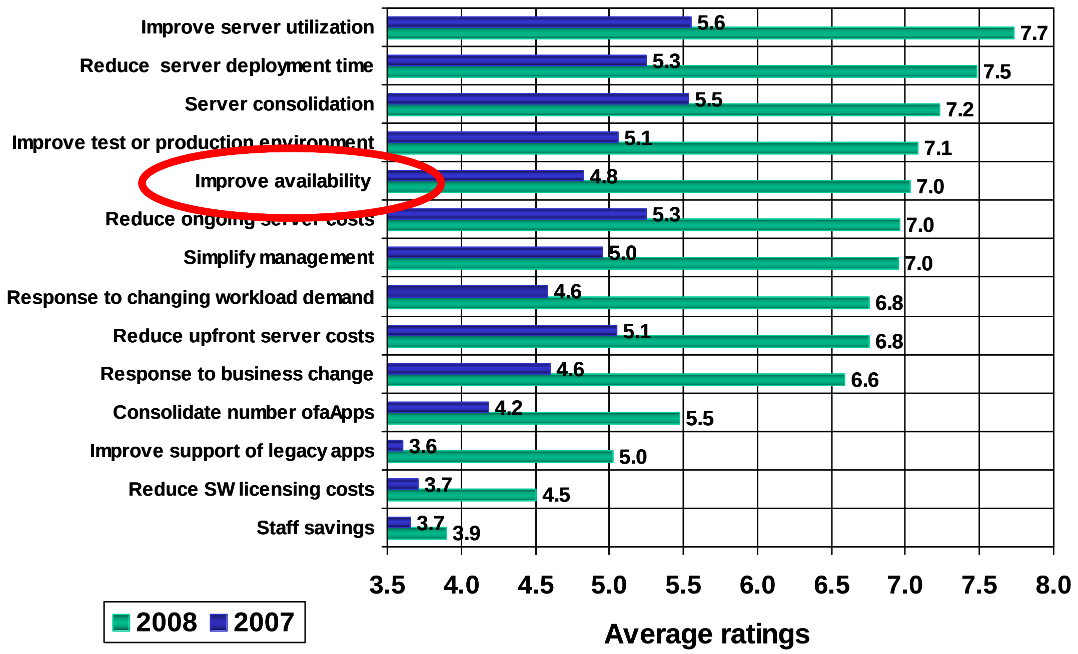
Virtualisation as a Driver for BC

IT professionals are rapidly becoming aware of the potential offered by virtualisation in the BC arena. In our 2008 server virtualisation survey, 27% of European companies identified availability as one of the three main reasons to proceed with virtualisation. This represented a significant increase from 2007, when only 8% did. Also, companies rated the importance of availability as one of the top 5 drivers for embarking on virtualisation projects (see Figure 1, survey cit.).

FIGURE 1

Availability is a Key Driver for Virtualisation

Rate the following criteria for their importance in your decision to virtualise your servers



Source: IDC European Server Virtualisation Survey, 2008

As mentioned previously, it is the separation of operating systems (and their applications) from the physical server that makes virtualisation such a compelling proposition. This so-called abstraction layer liberates software from the confines of hardware. In this section, we detail the reasons for exploiting the virtualisation benefits in the context of BC.

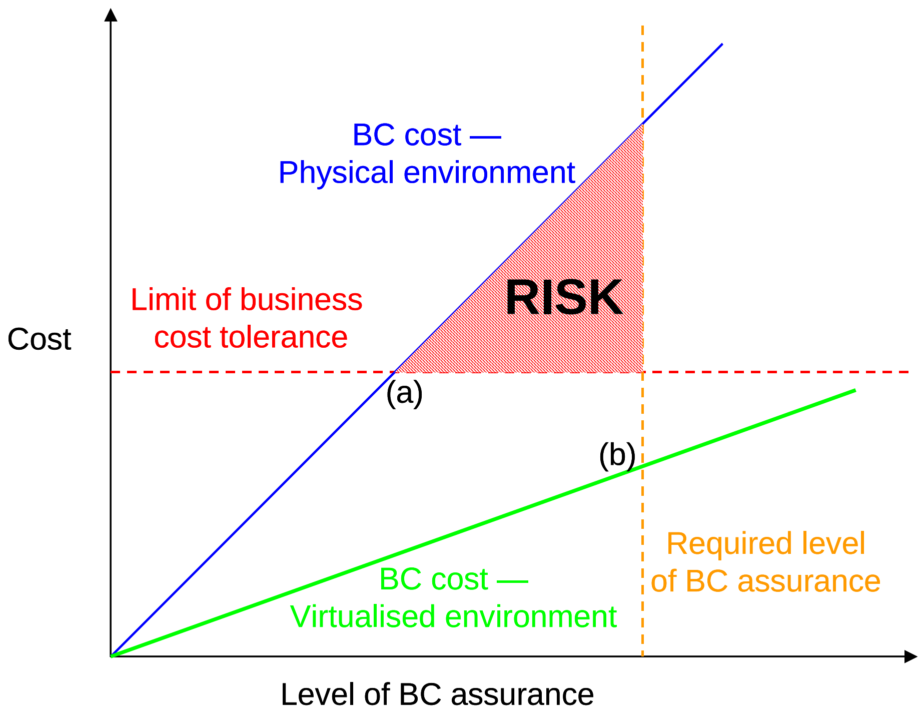
Another way to appreciate how easy it is to manage virtual compared to physical machines is the way that the state of the VM can be stored as a relatively small file. Such a file contains the entire identity of a system at a given time, encapsulating the operating system and application(s). As with any other file, it can be copied easily and ported to run on other machines controlled by hypervisors. Furthermore, because VMs run under the control of the hypervisor, they are hardware-agnostic, meaning that they can be deployed on almost any x86 server, provided that it is virtualised.

From a BC standpoint, the characteristics of virtual machines — encapsulation and portability — make them simpler to back up, replicate and restore. Protecting a complete system can be just a matter of protecting a few files. The files that make up a virtual machine can be recovered to any compatible virtualised server platform without requiring any changes because virtual machines are hardware-independent. These characteristics mean that tasks such as server migration, backup and recovery, and replication can increasingly be thought of as simple data migrations or file copy operations.

As we will examine in this section, this enables the IT department to provision for levels of business continuity that would have been unaffordable in a purely physical environment, as illustrated in Figure 2.

FIGURE 2

Business Continuity Assurance Versus Cost



Source: IDC, 2009

Figure 2 illustrates the relationship between cost (vertical axis) and levels of BC assurance (horizontal axis).

Every business has a "tolerance ceiling" of cost for BC assurance (red horizontal dotted line) above which it is unwilling to invest. However, the business also has an optimum level of BC assurance it needs to provide if it is to properly provision for BC (gold vertical dotted line).

The cost of BC in a physical environment (blue line) frequently exceeds the "tolerance ceiling" (at point A), making it impossible for IT to provision adequate levels of BC, creating risk (red zone)

Virtualisation offers the possibility of keeping the BC cost curve (green line) below the "tolerance ceiling" of the business, making it possible for IT to provision fully adequate BC (at point B) to de-risk the business.

BC in a Virtualised Environment

Ensuring that the business is able to function continuously means that the IT department is prepared to deal with a wide range of potential disruptions. There are a number of common disruption scenarios in a traditional environment. In the following sections we demonstrate why virtualisation can deliver on the "breakthrough" promise of doing more with less when compared with traditional, physical environments.

Planned Downtime — Server Maintenance

Most downtime is planned, as it is required by many operating environments for the maintenance and implementation of new features.

In a virtualised environment, virtual machines with running applications can be moved to other servers without any disruption to service levels. This means that maintenance can be performed at any time of day and IT staff can finally speculate about operating with zero scheduled downtime.

VMs can be moved from a host that is scheduled for maintenance and then restored back to the original host once the work is completed. The VM movement can be automated including full rebalancing after maintenance.

The implications of these capabilities are profound, driving rapid, significant, predictable and quantifiable business returns.

Unplanned Downtime — Server Failure

Unplanned downtime arising from hardware or software failure can be very costly to the business.

In a physical environment, an operating system and the applications it supports are highly dependant on the server on which they are hosted. If the server fails, and there is no failover provision, the application will be taken out of operation until the server can be restored.

In a virtual environment, virtual machines can be created in pairs that run in lockstep but on different physical servers — a passive machine essentially mirroring the active one. To the external world, they appear as one instance (one IP address, one application) — but they are fully redundant instances.

In the event of an unexpected hardware failure that causes the active, primary VM to fail, the secondary, formerly passive VM immediately picks up where the primary left off, and continues to run, uninterrupted, and without loss of network connections or transactions.

This technology will also work across any application and OS without modifications or scripting, and provides a more cost-effective way of running mission-critical workloads than fault-tolerant hardware dedicated entirely to individual applications.

Unplanned Downtime — Workload Management

Less visible than server failure, but often just as costly over time, is the issue of workload management. High levels of utilisation can significantly affect the ability of an application to perform, with costly consequences where the application is performing a mission-critical function.

In a physical environment, the application is entirely dependant on the resources of the server on which it operates. Either server capacity has to be provisioned at all times to cope with peaks in activity — meaning wasted resources at all other times — or the business has to incur the cost of degraded performance or even failure at times of peak activity.

In a virtual environment, virtual machines that require more processing capacity than is being provided to them by the server on which they reside can be redeployed, with no interruption, to other hosts, affording them greater performance. This process is typically automated, with preset business rules dictating at what point and to which destinations overloaded VMs will be redeployed. This reduces both the cost of outage itself and the cost of staff required to manage the rebalancing of workloads.

The dynamic, automated management of workloads extends beyond the server and into the wider information infrastructure. In just the same way as server virtualisation allows the fluid balancing of VM requirements across the full pool of server capacity, so storage virtualisation allows the automated, seamless provisioning of storage capacity to VMs in line with their requirements.

Fully capable storage virtualisation also recognises the imperative of tiered storage, reallocating stored data to more or less costly storage platforms in line with business requirements reflected in preset business rules.

Large-Scale Disaster

Although large-scale disaster recovery is rarely invoked, the potential impact of such a disaster may be enough to risk putting the company out of business.

Virtualisation can dramatically reduce the costs associated with provisioning for, and executing, disaster recovery processes in two main areas:

- Cost of the recovery environment. In a physical environment, a full mirror site has to be maintained in the event of partial or total failure of the main production site. This can be prohibitively expensive. In a virtual environment, the seamless portability of virtual machines means that different (physically separate) parts of the production environment can be used to host mirror copies of VMs from other parts. This makes the provisioning of the recovery environment more cost-effective in terms of both cost of infrastructure and cost of management. This is obviously best practiced across multiple sites.

- Cost of recovery process: By providing a fully automated framework for disaster recovery, the DR process in a virtualised environment is far faster and easier than in a physical environment, where installation, reconfiguration and testing of restored OS and applications is a laborious process.

Also, a virtual environment can potentially recover a system in hours rather than days. A traditional system can take many hours to rebuild the operating system and application configuration. In the case of virtualised systems, the backup of the complete virtual machine can be directly restored without OS or application reinstall, requiring much less testing.

Integration With the Wider Information Infrastructure

From the discussion so far it will hopefully be clear why virtualisation can bring about significant improvements to business continuity performance, optimising levels of assurance to the business within the limits of acceptable spend.

However, the benefits of server virtualisation with regard to high availability and data protection may be severely compromised if the wider information infrastructure is not adequately prepared. Also, improving the processes and performance of the server platform puts increased focus on the networked storage platform in order for it to match and complement a faster and more flexible server environment. A defining benefit of virtualisation is the significant increase in server utilisation rates. But this means that if, for example, a virtualised server increases its average utilisation from 20% to 70%, its spare processing capacity is no longer available as a performance buffer. Backup and replication processes of databases and application files still demand time and processing bandwidth, which should not impede the performance of a highly utilised server.

Inefficient data replication is often caused by

- Inefficient storage infrastructure
- Unnecessary (duplicated) data replication
- Inefficient restore processes

An integrated review of these three areas should form an essential part of any virtualisation roadmap.

There are increased adoption rates of both backup to disk and data deduplication on the secondary or even primary storage tiers as essential components of a high-performance information infrastructure environment.

Less appreciated perhaps is the critical nature of backup and restoration processes, which frequently require a minimal and inflexible amount of available capacity across an inflexible schedule of backup windows.

A key objective of the virtualisation roadmap should be to deliver fully automated and "intelligent" backup processes in which scheduling and provisioning are driven dynamically in real time by predefined business rules, and applications are restored in an order that reflects their importance to the business.

Intelligent process automation will be essential to help the IT function deliver the full benefit of server virtualisation to the business in the form of optimised levels of business continuity assurance at acceptable cost.

By combining server virtualisation with a highly efficient and automated data management infrastructure, the IT function is able to move beyond the ineffective and wasteful policy of equal BC provisioning for all applications.

In this scenario, provisioning can fall short of real requirements for highly critical applications (creating risk) and conversely can be unnecessarily high for non-critical applications (creating waste).

Further Considerations

Compliance and Management

A growing number of organisations find themselves compelled to adopt and gain accreditation for BC standards. This is due to industry-specific governance regulations or because they are suppliers to organisations that demand such accreditation.

These organisations can benefit from virtualisation as it impacts the overall management of BC as a practice. Even in companies without accreditation, IT professionals with responsibility for DR plans will have experience in contributing content to the company-wide DR and/or BC plans. In traditional server environments, these plans frequently provide instructions for manual processes.

In the world of virtualised servers in the situations we have described above, the ability to automate features highly. This is of great benefit to BC managers in the event that the BC plans kick into action. A problem with BC plans is often the low frequency with which they can be tested due to the common demand for IT running around the clock. For example, porting VMs across physical servers is likely to become a routine, if not automated, task in most virtualised server environments. It is also a function central to the execution of the large scale BC plan.

The planning of BC and DR is both easier when dealing with frequently used processes and also more likely to succeed where these can be automated and practiced frequently.

Improved BC for the Virtual Desktop

As organisations develop their virtualisation strategies, virtual desktop infrastructure (VDI) is emerging as one of the key areas of interest.

A full discussion of VDI is out of the scope of this document. In essence, however, VDI involves the hosting of the operating systems, applications and data in the datacentre rather than on the PC workstation or laptop; the latter operating as a "thin client".

In this scenario, in which the traditional backup of data across the many user PCs no longer exists, it is self-evident that business continuity provisions around the datacentre, and the considerations set out in this document, take on an even greater level of importance.

Management Processes in the Context of Virtualised BC

The plans and underlying processes for business continuity in the context of dealing with serious incidents is likely to undergo significant change in a virtualised server environment. It is therefore important to undertake an in-depth assessment of the many options that server virtualisation offers to improve BC and DR processes.

Our research shows that customers expect virtualisation to help them improve availability, as mentioned. IDC believes that many IT departments have sincere intentions to raise the quality and speed of their BC, and just as applications are tested thoroughly before going into production, new improved BC features must be tested rigorously, ensuring that they are robust. There should also be extensive pre-testing of features, as they are being considered (if possible), to ensure that they perform predictably and reliably.

The IT department will be executing BC plans involving people (internal and external), in a mix of manual and automated procedures. It is key that the operational readiness of all parties is assessed upfront in the planning stage. This will ensure successful execution of the plan and that everyone involved will feel comfortable with their own roles, and everybody else's for that matter.

Building a Virtualisation Roadmap for Your Business

As virtualisation grows in importance and is applied across IT infrastructure, we recommend that organisations develop a coherent roadmap for virtualisation in their organisation.

IDC has observed four distinct phases of customer adoption with regard to server virtualisation. These phases are distinguishable by significant changes in customer behaviour across six organisational areas.

Organisational Impact of Server Virtualisation

The six major organisational changes that result from server virtualisation are as follows:

- **Application usage**: There are generally measurable differences in the types of applications that are deployed on virtual servers as maturity increases in a customer site.
- **Lines of business**: With increasing use of virtualisation in an organisation, the interface with the lines of business also changes.
- **IT process**: As with any new technology, IT governance rules and processes will need to change to accommodate the impacts of virtualisation. Customers are usually required to make some formal changes before virtual machines are used in any type of production environment.
- **Financial impact**: The business justification for server virtualisation activities changes quite dramatically across the maturity cycle. Business cases are often initially based on hardware savings but quickly move to encapsulate softer costs such as availability and time to market. Operational and staff time savings are also a key driver.

- **Technology usage**: As customers become more comfortable with virtualisation technologies, their desire to push the limitations of features and functionality increases. Today, customers are already seeking more sophisticated tools to help manage their virtualised resources, with automation expected to play a strong role for the next 18 months.
- **Staff skills**: As more complex technologies are deployed along the virtualisation maturity cycle, the impact on IT staff moves from that of manual tasks to higher levels of automation. At the same time, staff usually take on business-orientated tasks that include educating and justifying the use of virtual machines to line-of-business owners and application owners.

Although these organisational impacts are not necessarily exhaustive, they cover the major implications for businesses as they mature their use of server virtualisation. The changes that customers make in each of these areas evolve as they enter a new phase of virtualisation and therefore enable IT infrastructure managers to both identify their level of maturity and set goals for future strategies.

IDC Server Maturity Index

Server virtualisation is following the same classic curve of maturity that many enterprise technologies have followed in the past, with one major exception — the rapidity with which customers are adopting this technology for use with their x86 systems and seeking to drive it into their new server purchases.

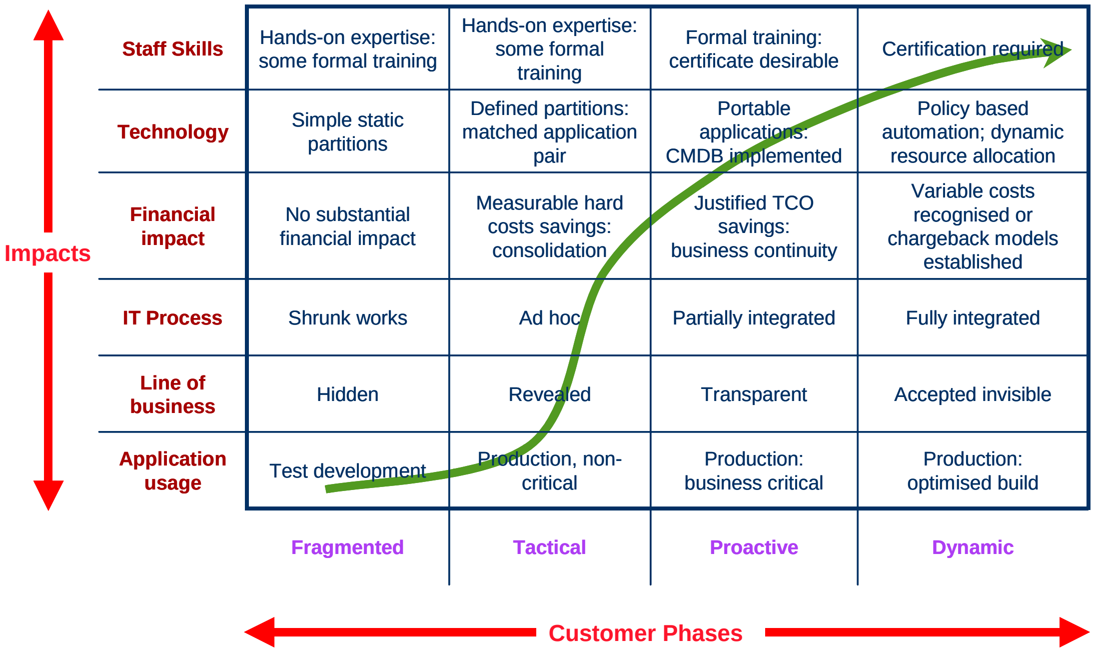
Although much of the early server virtualisation adoption went hand in hand with application development environments and consolidation or migration projects, IDC has already observed that the primary driver for virtualisation is now often associated with availability solutions and disaster recovery programs.

Most notably, customers are just as likely to measure the time-to-market and flexibility advantages of server virtualisation as they are the cost savings from hardware when developing a virtualisation business case.

This evolution in customer behaviour depends largely on how much experience an IT organisation has with server virtualisation technologies and the successes it has had in lowering costs, improving software support, and increasing its responsiveness to the business. The progression of adoption in an organisation is best described by IDC's Server Virtualisation Maturity Index, which highlights the four major phases of adoption and provides a market model for the maturing use of server virtualisation in customer accounts (see Figure 3).

FIGURE 3

Server Maturity Index



Source: IDC, 2009

Phase 1: Fragmented

For many customers, the initial phase of server virtualisation typically begins within the application development organisation. Lab or development systems are ideally suited to both test virtualisation technologies and leverage the ability to quickly deploy virtual machines and exploit hardware resources that are often underutilised. This phase is typically the skunkworks project of one or two individuals and has little financial impact on the organisation. During this nascent stage, virtualisation is often not part of formal IT processes and procedures, and is almost always unseen or hidden from line-of-business owners. Staff skill sets are immature, and from a technology aspect, customers are typically focused on simple partitioning and deployment activities, although they may begin to dabble in more sophisticated mobility tools as they move toward their use in production environments.

Phase 2: Tactical

Moving from the fragmented phase to the tactical phase is significant in that customers move from a test environment to a production environment. For customers it is not so much a technology challenge as a cultural challenge. The IT department is almost exclusively the sales vehicle for driving virtualisation from test environments to production, and during this phase, virtualisation often becomes visible to the lines of business. IT staff may have built up good technical competencies through hands-on experience and some formal training, but they are not necessarily prepared for the cultural resistance they may face by introducing this shared infrastructure model to a non-technical audience. They will find themselves actively engaged with application owners and business managers in selling the cost benefits of virtualisation and in guaranteeing service levels.

The projects chosen for taking virtualisation to this next step will usually be visible enough to garner attention if successful, but they are not likely to be the most mission-critical or strategic in the IT portfolio. Given the limited use of virtualisation at this stage, alterations are made to change control procedures, but widespread changes to IT policies and governance procedures happen later.

As companies move toward the end of this phase, success stories are critical to drive adoption to a broader organisational setting. IT staff will find themselves rapidly ramping up their skills and will actively be looking for tools that help them make the best choices for pairing applications on the same physical server. They will probably have tested portability tools that allow movement of virtual machines from one physical server to another.

Phase 3: Proactive

The proactive phase is distinct from the tactical phase because of its broad use across IT systems. Based on previous successes and internal advocates, IT organisations are using virtualisation as a basis for multiple IT projects and application deployments. Its credibility is now high enough in the IT organisation and in the lines of business such that mission-critical applications are deployed on virtual machines. Much of the resistance from the lines of business is overcome and the IT organisation is able to build convincing business cases that not only incorporate savings on hardware, but also account for better availability or disaster recovery.

By the end of this phase, server virtualisation is built into IT policies, practices and governance rules, and a change management database (CMDB) is often implemented. This step is critical because portability is usually in place and is a precursor for breaking down manual tasks. Toward the end of this phase, IT staff are technically adept and are even certified to manage virtual environments. Server, storage, and networking groups are actively engaged in modifying their workflow policies to achieve higher levels of automation. IT staff are comfortable communicating the value of virtualisation to the business and are laying out a strategic plan for the future that changes their mindset from asking themselves, "why virtualise?" to asking themselves, "why not virtualise?".

Phase 4: Dynamic

This last and most important of all phases is the dynamic phase of virtualisation. During this phase, virtualisation is a foundational building block for what many have termed a utility computing model or an on-demand environment. This is where IT systems, applications and business processes are tied together via policy automation rules so that changes in the business are rapidly and appropriately reflected in IT resources.

During this phase, virtualisation is optimised for application performance and is a standard build for the IT systems group. The lines of business are well educated on the benefits of shared infrastructure and actually ask for it due to cost savings and improved availability and flexibility. Virtualisation is fully integrated within IT processes and policies, and a variable chargeback model is deployed where the business has decided that this is the most appropriate IT financial model. IT staff across multiple units are certified for virtual environments.

Supporting Technologies for Business Continuity in Virtualised Environments

While virtualisation solutions include more tools to solve backup, disaster recovery and high availability needs, they need to be matched and supported by specific technologies on the storage side — both hardware- and software-based.

Tools for the backup or replication of virtual machines can now be found from all major storage suppliers, either bundled with storage hardware or sold as standalone software products. Storage products that are able to make the most of virtualised server pools regarding replication include: Symantec Backup Exec and NetBackup, EMC NetWorker, IBM Tivoli Storage Manager, Acronis True Image, and NetApp SnapMirror. As virtualisation continues to extend its footprint in datacenters, more solutions will be VM-compatible, although not all of them will be able to support any virtualisation technology.

It is also noteworthy that the virtualisation vendors themselves are focusing on storage by embedding a growing number of backup functions in their virtualisation management suites. For example, VMware Virtual Infrastructure includes VMware Consolidated Backup, while Microsoft offers backup with Microsoft System Centre Data Protection Manager.

The most common way to proceed with VM backup is to execute snapshots and then replicate them to disk or tape devices. However, performance often arises as a potential issue, as I/O constraints may limit the ability to access VMs and shared storage/server resources may generate workload contentions. Users backing up VMware VMDK files to disk with deduplication capabilities may find that particularly high levels of deduplication may be possible.

On the server side, virtualisation vendors are tackling this issue with tools that enable dynamic resource allocations to more or less demanding VMs, while on the storage side, suppliers provide new use tools to measure and prioritise I/O optimisation in a storage system.

FUTURE OUTLOOK

IDC believes that virtualisation remains a key factor in the way organisations design and plan their business continuity strategy, as the virtualised portion of the datacenter grows and customers become increasingly familiar with the technology. The advantages ensured by using virtualisation to raise the quality of BC are increasingly visible to customers, not least thanks to the expanding portfolio of products from storage and system vendors.

The lower price point of virtualisation-based BC compared to higher end solutions is making BC more viable for computing platforms where it was previously perceived to be unaffordable, most typically in the midmarket.

CONCLUSION

The benefits of server virtualisation are transforming the way IT departments provision IT to their customers. If the first wave of x86 virtualisation was mostly focused on improvements in utilisation, then IDC believes that the second major wave will focus on the enhancement of business continuity and DR capability.

Virtualisation offers to bring significantly improved BC practices to a broader spectrum of IT environments, IDC advises companies that evaluate BC plans involving virtualisation to draw up a roadmap that envisions the potential effects of a wide virtualisation of their x86 installed base, while at the same time taking into account the necessary interaction between the virtualised and non-virtualised environments, in terms of both system management and of common governance policies. As demonstrated in this document, without integration, most of the advantages of a virtualised BC are at risk of being lost.

Furthermore, it must be recalled that any kind of BC project pivots around people and processes. IDC recommends that organisations build plans that encompass not only the technology aspects, but also the processes and the people that revolve around them.

On the IT side, redundancy is crucial to a well-built BC plan. Although high utilisation rates of computing resources are made possible by virtual infrastructures, IT managers may need to allocate spare hardware for mission-critical applications — even within virtualised environments. Also, IDC counsels avoiding single points of failure by protecting the top of the virtualisation stack (i.e., the virtualisation management console) with appropriate failover options.

APPENDIX

Expanded Definition of Business Continuity

According to its full definition; business continuity planning is the holistic approach of an organisation to:

- Assess potential risks
- Eliminate risks where possible
- Protect the organisation's staff and assets

This is done by implementing the relevant processes for staff to execute in order to ensure the organisation's continued operation should incidents occur.

Disaster recovery planning is a subset of BC and relates to business-critical IT infrastructure and processes.

BC as a practice is therefore not restricted to IT, but DR protection of IT resources clearly dominates in most organisations' BC planning.

Nevertheless, IDC recommends that all organisations, irrespective of their size, explore the concept of BC at a pan-organisational level. Only with the recognition and support from senior management will BC stand a good chance of being implemented well in an organisation.

Disaster Recovery

Disaster recovery spans several areas, such as hardware, software, and service providers in scenarios of planned and unplanned downtime.

IT managers should consider how to protect next-generation IT infrastructure, and how to ensure uptime for mission-critical business applications — even if any given hardware or software component of the infrastructure goes offline.

In summary, market drivers for business continuity solutions include:

- End-to-end applications that span the enterprise and rely on highly available data
- 24 x 7 business operations
- Downtime means lost revenue for business
- Need to support end users and consumers
- Need to comply with regulations
- Internet access has reduced the worldwide window for server platform planned downtime
- User expectation of always-on infrastructure

Choosing the right business continuity solution is a decision that needs to be based on the level of risk and disruption that can be tolerated by the different parts of the business.

Prevention is Better Than Cure

The best measures to ensure an organisation's continued operation lie in prevention rather than picking up the pieces when something goes wrong. The selection of sites away from danger, incorporating features countering potential threats such as emergency power supplies, is a superior measure ensuring smooth, uninterrupted operation.

Copyright Notice