A DISCUSSION OF VIRTUALISATION TECHNOLOGIES: THE HEART OF CLOUD COMPUTING

Dr Stilianos Vidalis & Hamse Yuusuf
Newport Business School
University of Wales, Newport, United Kingdom
Stilianos.Vidalis@newport.ac.uk, Hamse.Yuusuf@students.newport.ac.uk

ABSTRACT

The success of cloud computing would not be possible without the advances in virtualization. The basic concept is to have one resource pretend to be another. Its implementation is applicable to many areas of computing. Virtualization allows a computer to become several different computers, or one software package to emulate another.

Although virtualization technology has been around for many years, it is only now beginning to be fully deployed. One of the reasons for this is the increase in processing power and advances in hardware technology. As the benefits of virtualization are realised, we can observe the benefits to a wide range of users, from IT professionals, to large businesses and government organizations.

Firstly this paper aims to discuss the key technology behind virtualisation, secondly analyse current threats and vulnerabilities, and finally propose corresponding countermeasures of Virtualisation threats and vulnerabilities, in order to facilitate the implementation of Virtualization Technologies for organizations.

Keywords: ***Virtualisation Technology, Cloud Computing and Virtualisation Security.***

1 WHAT IS VIRTUALIZATION?

One of the most important ideas behind cloud computing is scalability, and the key technology that makes that possible is virtualization. Virtualization, in its broadest sense, is the emulation of one of more workstations/servers within a single physical computer. Put simply, virtualization is the emulation of hardware within a software platform. This allows a single computer to take on the role of multiple computers. This type of virtualization is often referred to as full virtualization, allowing one physical computer to share its resources across a multitude of environments. This means that a single computer can essentially take the role of multiple computers.

However, virtualization is not limited to the simulation of entire machines. There are many different types of virtualization, each for varying purposes. One of these is in use by almost all modern machines today and is referred to as virtual memory. Although the physical locations of data may be scattered across a computers RAM and Hard Drive, the process of virtual memory makes it appear that the data is stored contiguously and in order. RAID (Redundant Array of Independent Disks) is also a form of virtualization along with disk partitioning, processor virtualization and many other virtualization techniques.

Virtualization allows the simulation of hardware via software. For this to occur, some type of virtualization software is required on a physical machine. The most well-known virtualization software in use today is VMware. VMware will simulate the hardware resources of an x86 based computer, to create a fully functional virtual machine. An operating system and associated applications can then be installed on this virtual machine, just as would be done on a physical machine. Multiple virtual machines can be installed on a single physical machine, as separate entities. This eliminates any interference between the machines, each operating separately.

2 WHY VIRTUALISE?

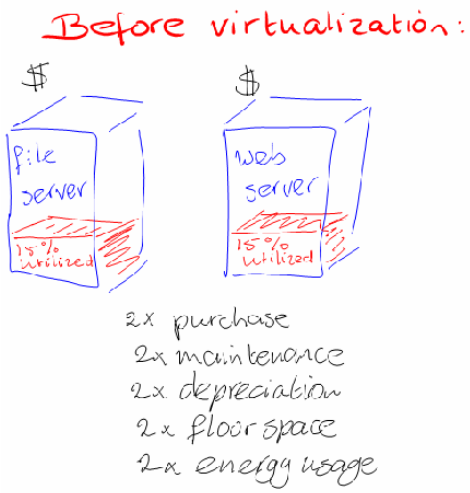

Fig 1. Before Virtualisation

There are four main objectives to virtualization, demonstrating the value offered to organizations:

• Increased use of hardware resources;
• Reduced management and resource costs;
• Improved business flexibility; and
• Improved security and reduced downtime.

2.1 Increased use of Hardware Resources

With improvements in technology, typical server hardware resources are not being used to their full capacity. On average, only 5-15% of hardware resources are being utilized. One of the goals of virtualization is to resolve this problem. By allowing a physical server to run virtualization software, a server's resources are used much more efficiently. This can greatly reduce both management and operating costs. For example, if an organization used 5 different servers for 5 different services, instead of having 5 physical servers, these servers could be run on a single physical server operating as virtual servers.

2.2 Reduced Management and Resource Costs

Due to the sheer number of physical servers/workstations in use today, most organizations have to deal with issues such as space, power and cooling. Not only is this bad for the environment but, due to the increase in power demands, the construction of more buildings etc is also very costly for businesses. Using a virtualized infrastructure, businesses can save large amounts of money because they require far fewer physical machines.

2.3 Improved Business Flexibility

Whenever a business needs to expand its number of workstations or servers, it is often a lengthy and costly process. An organisation first has to make room for the physical location of the machines. The new machines then have to be ordered in, setup, etc. This is a time consuming process and wastes a business's resources both directly and indirectly.
Virtual machines can be easily setup. There are no additional hardware costs, no need for extra physical space and no need to wait around. Virtual machine management software also makes it easier for administrators to setup virtual machines and control access to particular resources, etc.

2.4 Improved Security and Reduced Downtime
When a physical machine fails, usually all of its software content becomes inaccessible. All the content of that machine becomes unavailable and there is often some downtime to go along with this, until the problem is fixed. Virtual machines are separate entities from one another. Therefore if one of them fails or has a virus, they are completely isolated from all the other software on that physical machine, including other virtual machines. This greatly increases security, because problems can be contained.
Another great advantage of virtual machines is that they are not hardware dependent.
What this means is that if a server fails due to a hardware fault, the virtual machines stored on that particular server can be migrated to another server. Functionality can then resume as though nothing has happened, even though the original server may no longer be working.

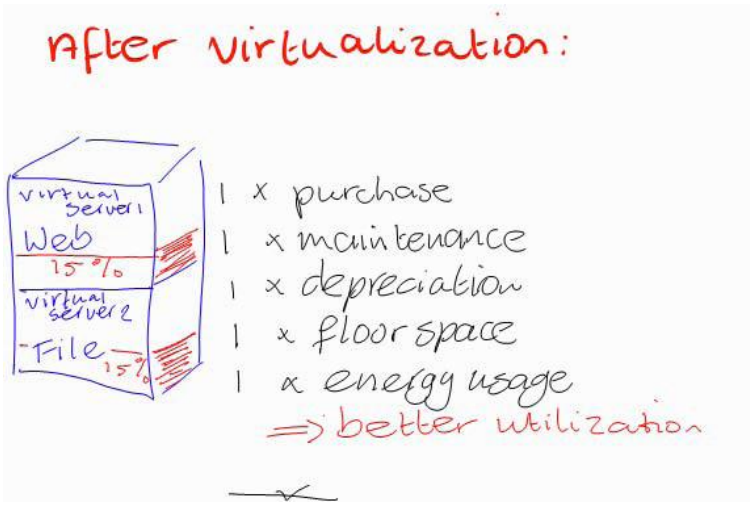

Fig 2 after Virtualisation

3. OVERVIEW VIRTUALISATION TECHNOLOGIES

VMware and Microsoft have a strong footing in virtualized technology and are perhaps the most well known companies involved with virtualization. However, now that virtualization technology has begun to stabilize and its advantages have been proven, plenty of other companies have started emerging. Below is a comprehensive guide on some of the most popular and widely used virtualization technologies.

3.1 VMware

VMware is one of the most widely known virtualization companies. Its brand is easily recognizable and they offer a number of virtualization programs. Their most popular virtualization applications are briefly detailed below.

3.1.1 Desktop Editions

VMware Workstation – Initially launched in 1999, VMware workstation is one of the longest running modern day virtualization applications. It allows users to create multiple x86-based virtual machines on a single physical machine. A wide number of guest operating systems such as Windows, Linux and MAC OS X can then be installed on to these virtual machines.

VMware Fusion – This is similar to VMware Workstation, the only difference is that
VMware Fusion was designed for users of the Mac Intel hardware platform. It is fully compatible with all virtual machines created by other VMware applications.

VMware Player – This application is a freeware application and is offered to users who do not have a licence to run VMware Workstation or VMware Fusion. Unlike the other two applications, VMware Player cannot create virtual machines, however it can run them.

3.1.2 Server Editions

VMware ESX Server – This is an enterprise level virtualization product that is offered by VMware. It does not require a host OS to be installed as it is installed directly onto a server's hardware (i.e. is a bare metal virtualization solution). This is unlike the desktop editions which are installed as applications from within their host OS. VMware ESX Server is much more efficient than other virtualization technologies because it has lower system overheads and interacts with its hardware directly.

VMware ESXi – This application is similar to the VMware ESX Server application. The only difference is that it takes up less memory, because its Service Console is replaced with a simpler interface. As of July 2008, VMware ESXi is available to download for free.

VMware Server – This is VMware's free server virtualization application. It is an application which needs to be installed onto a host OS that is either Window or Linux based. Due to this fact it is not as efficient as the other VMware server editions, which are installed directly on their hardware. However VMware Server does allow you to create multiple virtual machines which can have a number of different guest operating systems installed.

VMware offer a number of different virtualization applications. Each one has its own advantages and disadvantages, depending on the scenarios they are used in. VMware Workstation would be best utilized in an environment which contains multiple end user desktops. These desktops could be virtualized into a few physical machines. VMware ESX Server would be best used to create high performance virtual servers which provide important services. VMware Server is offered for free, however it is not as efficient as VMware ESX Server.

However it would still be great to use for the virtualization of less mission-critical servers. Which virtualization solution a business should go for really depends upon their current scenario; for example how large they are, whether their servers are resource-intensive and what their future prospects are. Once a business determines these things they can go about choosing a suitable virtualization solution.

Although VMware is the dominant brand in virtualization, other companies are now starting to catch up. Microsoft has released their new Hyper-V software, which is a direct competitor to VMware's own ESX Server edition. At the moment, tests show that performance wise, ESX Server Edition currently leads the way. However many virtualization companies are improving their technologies and you can now even download powerful open source virtualization technologies for free.

3.2 Citrix

Citrix systems specialises in application delivery infrastructure that can be used as a found of both public and private cloud computing. The Citrix Xen hypervisor powers many of the world's largest cloud providers today. NetScaler delivers web applications to a large proportion of all internet users each day. Building on these technologies, Citrix has extended its offering into the cloud with its Citrix Cloud Centre (C3) solution, an integrated portfolio of Citrix delivery infrastructure products packaged and marketed to the cloud service provider market.

The Citrix C3 solution gives cloud providers a set of service delivery infrastructure building blocks for hosting, managing and delivering cloud-based computing service. It includes reference

architecture that combines the individual capabilities of several Citrix product lines to offer a service-based infrastructure suited to large-scale, on demand delivery of bot IT infrastructure and application services. This architecture consists of five key components: Platform, Desktop Services, Delivery, Bridge and Orchestration.

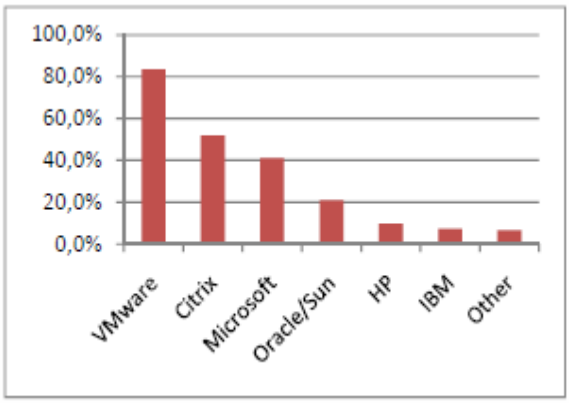

Fig. 3: current virtualisation providers

3.3 Microsoft

Windows Server is Microsoft's premier server OS. Its latest version, Windows Server 2008 is Windows first OS that is integrated with full virtualization. This feature is known as WSV (Windows Server Virtualization).
Along with its previous server roles, Windows Server 2008 has a new Hyper-V role. Selecting this role allows you to create a virtualized server environment. Within this environment you can then create multiple virtual servers. Hyper-V is much more efficient than standalone virtual server applications because it is actually integrated into the Windows Server 2008 operating system.

WSV offers many of the benefits that you would expect to receive from virtualization technology, such as rapid server deployment and the ability to take snapshots for backup purposes, etc. However it also offers a few extra features. For example it can offer up to 32 GB of RAM and up to 4 processors per guest OS. It also provides support for virtual LANs and can run both 32bit and 64bit virtual machines. WSV has plenty of resources and can be flexibly administered by IT professionals. WSVs main competitor is VMware ESX edition. They are both very strong virtualization technologies and both companies have a solid footing in the virtualization market area. WSVs main advantage is that it supports more hardware than VMware ESX currently does. As long as you can install Windows Server 2008 on a machine, you should be able to run WSV.

VMware however, has a much larger feature set than WSV and it is a tried and tested virtualization solution. It will be interesting to see how things will develop between these two companies in the future and whether VMware can continue to remain the market leader in virtualization technology.

3.4 Oracle /Sun

Oracle's main virtualization application is known as Oracle VM. This is a virtualization application that offers support for Oracle and even non-Oracle applications. Benchmark tests have shown that Oracle VM can be up to three times more efficient than other virtualization applications in certain aspects. It can support both Windows and Linux distributions as guest operating systems and also includes a web-based management console, making it easier for administrators to manage their virtual environment.
Along with their virtualization application, Oracle also offers what is known as Oracle VM templates. Oracle VM templates are effectively images (or snapshots) of pre-installed and pre-configured enterprise software. This makes setting up and configuring new machines much easier for administrators, because all they have to do is copy over an Oracle VM template which contains the software that they require.

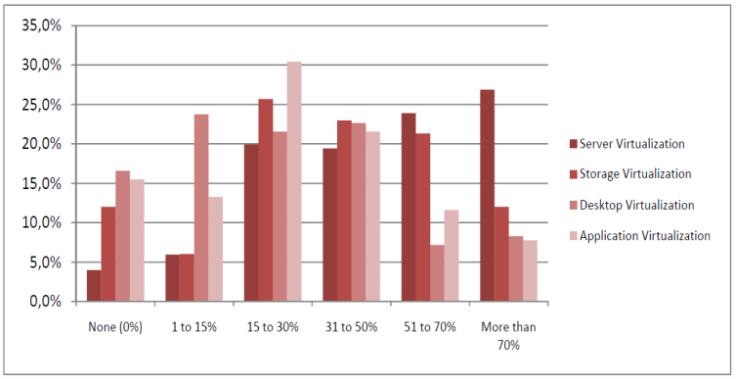

Fig.4: Implementation of virtualisation by end of 2010

4. CHALLENGES OF VIRTUALIZATION MANAGEMENT

4.1 Virtual Machine to Virtual Machine (V-V) Threat

Inter-VM traffic brings about new security problems, as a number of VMs run on a single server. If one VM gets infected by viruses, the

other VMs which are communicating with the infected one can also get infected.
One of the vulnerabilities could be insufficient isolation between different virtual machines, virtual networks, virtual storages, etc. Such security issue potentially facilitates viruses to make virtual machines get infected rapidly. Another reason could be partial understanding and improper utilization of virtualization products. For example, VMware ESXi does not have its own firewalls, so it demands users to add firewalls to its infrastructure to guard the virtual machines running on the server, in order to strengthen security.

4.2 Administrator Causes Hidden Danger

There is no doubt that administrator takes an indispensable role in the management of virtualization, and also plays a significant role relating to security management in virtual environment. Nevertheless, this makes administrators possess too many privileges, which causes hidden danger to the security management potentially.

Take the management of hypervisor for example. The administrator has the right to access any of the virtual servers installed on one hypervisor, along with that hypervisors have more access to the hardware compared with other traditional applications. In addition, virtual servers function differently as web server, mail server, or database, and each of them contains their own sensitive information. Under such circumstances, an untrustworthy administrator could breach the security of virtualization management and do harm to the whole virtual infrastructure built on the hypervisor. What is worse, it is unfeasible to solve such problem merely depending on virtual technology nowadays.

4.2 Lack of Discretionary Security Level

New virtual technology in products functions as the enabler to adoption and implementation of virtualization. However, it sometimes acts as the hindrance referring to security management of virtualization. Such security breach comes from the hot spot--hypervisor in virtualization.
The virtual servers on the same hypervisor can only be set at the same security level, though they take on distinct tasks varying from web services to data storage. Such technical limitation causes it unfeasible to establish different security levels according to different security demands on the same hypervisor. Such limitation also restricts the consolidation of virtualization, as it requires dividing various security zones according to the functions of virtual servers running on one hypervisor.

5 COUNTERMEASURES

5.1 Security Policies:

Security policies state the type of security and which security level is required to protect the system varying from personal use to organizational use.
Security policies take effect as the logical model to build up a security culture impacting human behavior. Security policies vary from one organization to another, so it is difficult to give a concrete sample of such policies.

However, certain principles can be taken into account when set up security policies for the organization in general. For instance, principle of least privilege means the entities can only be given the privileges they need to complete their tasks. The principle of separation of privilege means different roles are responsible for their own separated duties especially referring to critical tasks. Policies are based on both macroscopic and microscopic aspects, because they also refer to specific sub-fields in security management like access control, communication operation, and so on.

5.2 Standards of security management:

International standards relating to security management can also provide operational and administrative guidelines for management in virtual environment. It facilitates virtualization management with certain processes from a macroscopic aspect. International standards like COBIT, SOX, ISO/IEC 27000 Series, etc, all take significant roles in their own impacting areas.

ISO/IEC 27002, derived from ISO 17799, is named Information technology-Security techniques-Code of practice for information security management. ISO 17799 is comprised of such key chapters as follows: Security Policy, Organization of Information Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communications and Operations Management, Access Control, Information Systems Acquisition, Development and Maintenance, Information Security Incident Management, Business Continuity Management, Compliance

5.3 Defence in depth

It derives from information assurance and it takes advantage of a plurality of layers to enhance the security of IT systems. Defence in depth is also applicable to virtual environment, combing with the countermeasures like firewalls, DMZ, IDS etc. Furthermore, defence in depth can be also implemented with access control. In order to guard virtualization hosts, access control can be utilized for authentication and authorization using such limit like hostname, IP address, time of day, and so on. Certain techniques are also required to assist such access control.

6 CONCLUSIONS

Virtualization technology has begun to stabilize and its advantages have been proven. Building up a secure virtual infrastructure can be implemented by utilizing a good combination of security technology at hand with new virtual security technology. Technical and no-technical aspects in virtualization management also play an indispensable role in security of virtualization.

This paper sought for discussing different Virtualisation Technologies, collected security threats and vulnerabilities in virtualization, and analysed them according to their different categories.

This paper also focused on corresponding countermeasures to the threats and vulnerabilities and proposed corresponding countermeasures of Virtualisation threats and vulnerabilities, in order to facilitate the implementation of Virtualization Technologies for organizations.

Furthermore, this paper reaches the main research goal that Virtualisation Technology provides quicker implementations and lower costs while providing greater scalability, adaptability, and reliability to Cloud environment. Especially in terms of web applications, a solution can be available at any time, in any location on the planet, by any person. As use of the application increases or decreases, the cloud solution adjusts accordingly.

7 REFERENCES

[1] Ronald L. Krutz and Russell Dean Vines, Cloud Security, A comprehensive guide to Secure Computing

[2] Microsoft, Securing Microsoft's Cloud Infrastructure," *White Paper*, 2009, http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf Accessed April 2011

[3] Gary Anthesm, Security in the Cloud (2010) Communication of the ACM Vol. 53 No.11

[3] Karen Scafone, Murugiah Souppaya, Paul Hoffman. Guide to Security for full Virtualisation Technology. NIST, January 2011, Special Publication 800-125

[4] Virtualization from the Datacenter to the Desktop. (2007). White paper, Microsoft virtualization Resources.

[5] Dr Achrin Luhn , Michael Jaekel. Cloud Computing – Business Models, Value Creation Dynamics and Advantages for Customers

[6] Luis Vaquero, Luis Rodero-Merino, Juan Caceres, et al, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, pp. 50-55, 2009.

[7] Microsoft Research, Securing Microsoft's Cloud Infrastructure," White Paper, 2009, http://www.globalfoundationservices.com/security/documents/SecuringtheMSCloudMay09.pdf Accessed April 2011

[8] Michael Armbrust, Armando Fox. Above the Clouds: A Berkeley View of Cloud Computing. Technical Report, February 10, 2009

[9] B. D. Payne, M. Carbone, M. Sharif, and W. Lee. Lares: An architecture for secure active monitoring using Virtualization. Security and Privacy, IEEE Symposium on, 0:233–247, 2008.

[10] Gartner, Radically Transforming Security and Management in a Virtualized World: Concepts, Neil MacDonald, 2008

[11] NIST Guide to Intrusion Detection and Prevention Systems, http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf