Server Virtualization Products

And Information Security

William J. Sparks
Daniel G. James
ICTN 6883
Semester Project
4/8/2008

Author Bio's

Daniel G. James is a fulltime employee/fulltime graduate student working in the higher education and healthcare industries. He is currently employed in Winston-Salem, NC as a Systems Administrator. He has been working in the IT field for the past 8 years. He is currently working on a Master's degree in Technology Systems with a concentration in Information security via the distance education program of East Carolina University in Greenville, NC. He is scheduled to graduate in May 2008. Research interests include virtualization and digital forensics.

William J. Sparks is a full time graduate student in the Technology Systems program with a concentration in Information Security at East Carolina University in Greenville, North Carolina. He is employed by East Carolina University as a video production assistant in the Global Understanding Department. He received his Baccalaureate in Information and Computer Technology from East Carolina University with dual concentrations in Information Security and Information Technology. Research interests include application security and penetration testing.

Abstract

Virtualization is an emerging technology that is still being evaluated for usefulness and cost effectiveness by many companies. We will discuss the two largest server virtualization products on the market today. These products are VMware and Microsoft Virtual Server 2005 R2. We will do a comprehensive review of these products outlining the features and costs of each. We will also touch on the benefits of server virtualization and how it can save money. Also covered in this area will be some examples of how server virtualization may not be a good choice for certain server configurations. We will outline the pros and cons of each product and also talk about the security risks and threats that arise from virtualization. We will also cover the

misconception that virtualization actually reduces security risks. The fact is that virtualization has its own set of security risks and may not be a good option for certain types of servers.

Virtualization and Its Benefits

Server virtualization technology is utilized to construct multiple virtual servers (i.e., virtual machines) on one physical server. An operating system can operate and an application system can run on each of these virtual servers, just as on a physical server. Virtual machines can be built by dividing a physical server in terms of hardware and software. When the physical server is divided by hardware, server virtualization offers a special advantage: a hardware error or high load occurring in one divided section does not affect the other sections. In contrast, when the physical server is divided by software, server virtualization offers other advantages, such as allowing the CPU, memory, I/O devices, and other hardware resources to be assigned to virtual machines, and the resource assignment status changed even during operation. Moreover, when the physical server is divided by software (through server virtualization), the hardware resources can be shared by and assigned among multiple virtual machines, as well as being used exclusively by a specific virtual machine. The following mainly describes server virtualization by software. Given the recent background of significant increases in application-system construction costs (in terms of actual expenses, time needed, locations, etc.), there are great expectations for server virtualization technology. In other words, there is an urgent need to quickly and flexibly satisfy a variety of changing business environment conditions, and systems should be built in service units and flexibly interlinked according to application conditions. Service Oriented Architecture (SOA) embodies such flexible design techniques. In this case, the construction of a total application system must usually consist of multiple systems. Building a total application system based solely on physical servers entails the expensive purchase of

physical servers. Moreover, these physical servers must offer high levels of performance to accommodate peak loads during operation, but which may result in a low hardware usage rate and ineffective use of resources during other periods. At times requiring the high availability of system operation, a standby system must also be prepared to continue processing in case of an error occurring. [1]

Therefore, building and maintaining such a standby system that will be rarely used under ordinary circumstances also necessitate additional costs. Introducing server virtualization technology can resolve such problems. When multiple virtual machines are built by software and exist on one physical server the installation cost and time needed can be dramatically reduced compared to a case where multiple physical servers are deployed. Moreover, building multiple systems having low hardware resource usage rates (e.g., CPU usage rate) on the same physical server will result in more effective use of server resources. The ratio of resources distributed to low-load jobs and standby systems can also be kept low as in usual operation, though the distribution rate may abruptly increase in case of a higher load or error occurrence. Thus, server virtualization technology reduces the TCO and makes rapid system configuration changes possible under changing use conditions. [1]

Below in figure 1 you can see a graphical representation of virtualization and how it can take several physical servers that are not being efficiently utilized and turn them into several very efficient virtual machines on one physical server. It is important to note that this is just one instance where server virtualization makes sense and can save money and support costs. However, virtualization may not be a good choice for every type of server or application. It is important to check with the vendor or creator of the application(s) before installing it in a virtual environment as vendor support and warranties may be voided as a result.

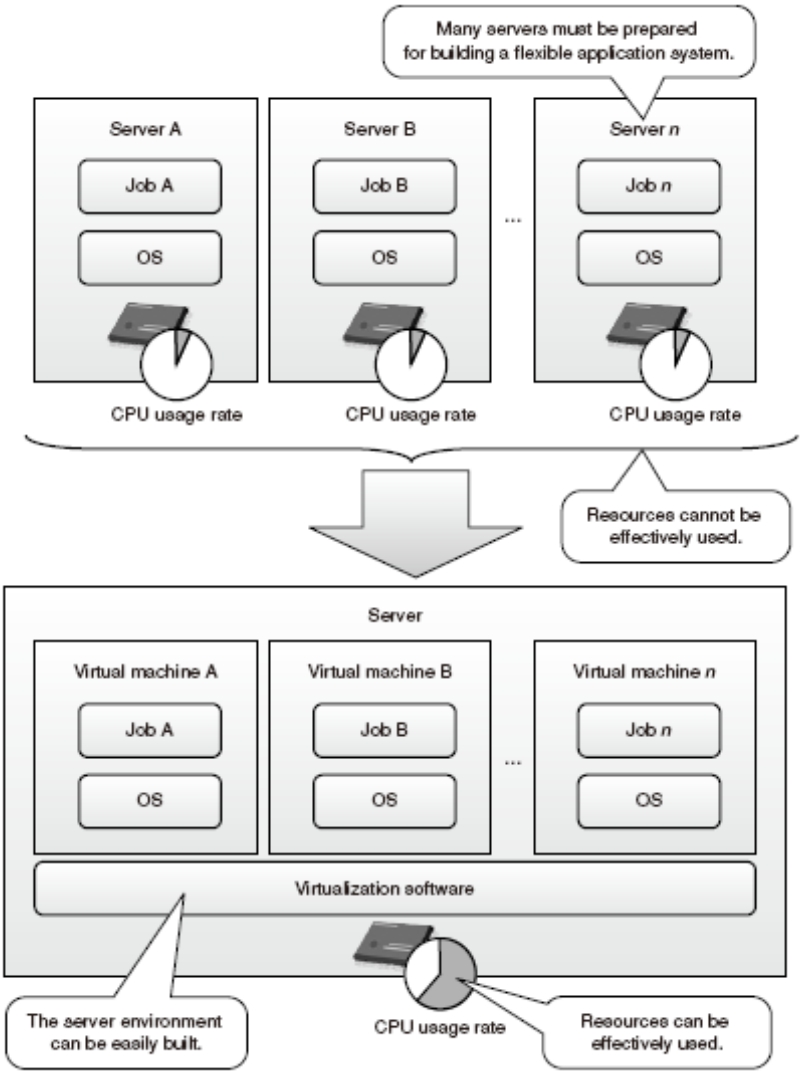

Figure 1 - Virtualization in Action [1]

Choices for Virtualization

In conjunction with Windows Server 2003, Virtual Server 2005 R2 SP1 provides a virtualization platform that runs most major x86 operating systems in a guest environment, and is supported by Microsoft as a host for Windows Server operating systems and Windows Server System applications. Virtual Server 2005 R2's comprehensive COM API, in combination with the Virtual Hard Drive (VHD) format and support for virtual networking, provide administrators

complete scripted control of portable, connected virtual machines and enable easy automation of deployment, and ongoing change and configuration. [2]

Additionally, its integration with a wide variety of existing Microsoft and third-party management tools allows administrators to seamlessly manage a Virtual Server 2005 R2 SP1 environment with their existing physical server management tools. A wide array of complementary product and service offerings are available from Microsoft and its partners to help businesses plan for, deploy, and manage Virtual Server 2005 R2 SP1 in their environment. [2] You can see from the figures below some of the features and benefits associates with this product.

New Features in Virtual Server R2 SP1	
Benefit	**Description**
Hardware-assisted virtualization	Supports both Intel Virtualization Technology (Intel VT) and AMD Virtualization (AMD-V) hardware-assisted virtualization.
VHD Mount Command-line Tool and APIs	Provides the ability to mount a virtual hard disk file (.vhd file) as a virtual disk device on another operating system.
Support for Volume Shadow Copy Service	Allows back-up of Virtual Server and its running virtual machines without needing to install backup agents inside the guest operating system of the virtual machines.
Larger default size for dynamically expanding virtual hard disks	The default size for dynamically expanding virtual hard disks has been changed from 16 GB to 127 GB, making the VHD file format even more useful for enterprise production, test, and disaster-recovery workloads.
Support for greater than 64 virtual machines on x64-based hosts	Virtual Server can run more than 64 virtual machines on x64-based hosts. The 64 virtual machine limit remains when running on 32-bit hosts.
Host clustering step-by-step guide	Host clustering allows you to extend the high-availability benefits of clustering to non-cluster-aware applications and workloads.
Virtual SCSI fix for Linux guests	This fix resolves an issue some customers encountered when trying to install certain Linux distributions inside a virtual machine on the emulated SCSI bus.

New Features in Virtual Server R2 SP1	
Benefit	**Description**
VMRC ActiveX control and Internet Explorer Security Zones	The Virtual Machine Remote Control (VMRC) ActiveX control now uses the security zone information in Internet Explorer to determine whether to prompt you for your credentials when you load the control.
Service Publication using Active Directory Service Connection Points	Virtual Server service now publishes its binding information in Active Directory as a Service Connection Point (SCP) object.

Figure 2 – New features in Microsoft Virtual Server 2005 R2 SP1 [2]

Increased Utilization of Hardware Resources	
Benefit	**Description**
Virtualization	Virtualization for operating system and application isolation on a fully tested and qualified Microsoft stack. • Broad x86 guest operating system compatibility: Runs most major x86 operating systems in the virtual machine guest environment. • Windows Server guest operating system performance optimization: Add-ins provide even greater CPU and IO performance for Windows Server guest operating systems and certain third-party x86 operating systems. • x64 host support: Natively runs within a 64-bit Windows host operating system, providing increased performance and memory headroom.
Availability	Flexible clustering scenarios provide high availability for mission critical environments while improving patching and hardware maintenance processes. • Guest to guest: iSCSI clustering for guests to guest across physical machines. • Host to host: Cluster all virtual machines running on a host.
Resource Management	Policy-based control for balanced workload management. • CPU resource allocation: Supports both weighting and constraint methods for fine-grained control. • Memory resource allocation: Supports memory resizing at virtual machine boot time.
Enhanced IT Productivity and Responsiveness	
Benefit	**Description**
Rapid Deployment	Complete scripted control of portable, connected virtual machines enables automated

Enhanced IT Productivity and Responsiveness	
Benefit	**Description**
and Provisioning	configuration and deployment. • VHDs: Encapsulates virtual machines in portable Virtual Hard Disks (VHDs), enabling flexible configuration, versioning, and deployment. • Virtual networking: Enables flexible networking with guest-to-guest, guest-to-host, and guest-to-net connectivity. • Comprehensive COM API: Enables complete scripted control of virtual machine environments. • PXE Boot: Network boot allows for provisioning of virtual machines in the same way as physical servers.
Manage and Migrate	Use existing server management tools to administer virtual machines running on a familiar host operating system. • Virtual Server Web console: Enables authenticated administration and client remote access. • Microsoft Operations Manager 2005 Management Pack for Virtual Server: Provides extensible guest-host mapping for event and performance management. • Microsoft Systems Management Server 2003 SP1: Reports virtual to physical machine relationships for inventory purposes. • Automated Deployment Services and Virtual Server Migration Toolkit: Provides command-line tools for converting from physical to virtual or virtual to virtual, easing migration to a virtual machine environment.
Cost-Effective and Reliable Solution from a Trusted Platform Vendor	
Benefit	**Description**
Integrated Innovation	Comprehensive testing and support for Virtual Server in conjunction with Windows Server operating systems and Microsoft server applications. • Windows–qualified drivers: Virtual machines utilize the Windows host operating systems qualified device drivers, ensuring robust and stable device support and broad device compatibility. • Operating system support: Microsoft extensively tests Virtual Server in conjunction with Windows Server 2003 and Windows 2000 Server. • Windows Server System family support: The Windows Server System Common Engineering Criteria 2005 states, “To help customers improve the utilization of hardware resources, all server products will support Microsoft Virtual Server 2005. Each product must be capable of running from within a virtual instance. • Active Directory integration: Enables delegated administration and authenticated

Cost-Effective and Reliable Solution from a Trusted Platform Vendor	
Benefit	**Description**
	guest access.
Ecosystem Support	Independent software vendors (ISVs) and customers can integrate their offerings with Virtual Server for enhanced functionality and manageability. • Management interface: Comprehensive COM management interfaces are published and utilized by management tool vendors. • VHD: The Microsoft VHD file format is available under royalty-free license, enabling ISVs such as security and management vendors to natively interoperate with Virtual Server.

Figure 3 – Benefits of Microsoft Virtual Server 2005 R2 SP1 [2]

Virtual Security Concerns

As virtual servers move into production, IT needs to address security and compliance issues. Unfortunately, most participants in the benchmark, when asked how they secure their virtual servers, say they treat them like physical servers as much as possible! Sensibly, they use host-based security such as antivirus and anti-malware agents. However, they also use network tools to protect virtual servers exactly as if they were simply very thin, very densely stacked rack mount boxes. [3]

While treating virtual servers simply as dense blades may work as a system administration policy, it is lacking as a security policy, as it fails to address the added layers of complexity virtualization creates and the decreased visibility of inter-VM network traffic. In a virtual environment there are also virtual network switches. These software switches offer VLAN capabilities and can be stacked to create quite complex virtual networks. Virtualized servers might contain entire virtual network architectures with n-tier application components such as application servers, Web servers, even databases contained inside the virtual machines.

From the perspective of a traditional security appliance sitting outside this virtual network architecture, none of the network traffic between these servers is visible or auditable. If network traffic traverses from virtual switch to virtual switch it may never touch a physical switch. The virtual environment becomes almost completely opaque. A security breach in any one of the virtual servers can go unnoticed, and worse, it can spread unencumbered to other virtual machines. Another key issue with virtualization is compliance. The common element most regulatory frameworks impose is a requirement to control and audit who has accessed what and when. This "who, what, when" question is often addressed with network enforcement and monitoring appliances. Unfortunately these traditional security measures are, for the most part, not virtualization-aware and therefore have limited or no visibility into the traffic traveling between virtual servers. Thus, compliance becomes a critical barrier to adoption of virtualization and is cited often in our research as a reason why virtualization adoption is aborted or stalled. [3]

Any company implementing virtualization is bound to have a mixed environment. Some servers will be virtual, some physical. Part of the network will be running over physical switches, while part of it will only exist inside virtual switches. In such an environment there are a variety of risks that can only be mitigated by a flexible and comprehensive security strategy. A number of different security controls can be applied to virtual infrastructures, including:

- Host-based security, such as HIPS and anti-virus within the guest operating systems.
- Virtual LAN (VLAN) segmentation reaching into the virtual network to separate traffic between virtual machines.
- Security implemented as a plug-in to the hypervisor software.
- Virtual appliances running alongside other guest operating systems and providing inline network security.
- Switch-based or appliance-based security outside the virtual network.

Each of these approaches adds to the security of virtual infrastructures, but none is sufficient in itself. Companies need to combine these methods to provide defense in depth across a heterogeneous data center that contains both virtual and physical systems. [3]

Putting host-based security software such as intrusion-prevention systems on each guest OS in a virtualized environment provides the same benefits as doing so on physical hosts: it creates a perimeter-of-one security boundary that can be tailored to the host. Because it relies on no other system, it has the greatest resiliency. However, it has the same shortcomings as host-based security in the physical realm. Security software competes with production software for resources such as memory and processor cycles, for example, and in a virtualized environment that burden is multiplied by the number of virtual hosts involved, and simultaneously increases competition for those primary shared resources. Also, each installation of the software is another configuration item to track and manage, creating greater overhead and increasing the risk of individual machines being misconfigured and so falling out of compliance and possibly increasing the risk of compromise. The management burden is increased by the multiplication of virtual hosts as well, since each guest system added potentially requires not just its own configuration, but also the reconfiguration of all the existing instances. The ability to freeze and thaw instances, and to move them from infrastructure to infrastructure, only complicates this tracking and management issue further. So, while virtual host-based security is a necessary technique for preventing security breaches, it can't be the only one and if using traditional tools, should be deployed tactically to address special security or auditing needs, rather than strategically as a primary method. Any major deployment of host-based security in a virtual environment must be built around a mature and enterprise-minded management system that minimizes complications, and is robust in the face of a dynamic environment. [3]

The obvious place to address security in the virtual environment's network infrastructure is in its backplane equivalent– the hypervisor. All traffic to and from the virtual environment

and among virtual machines within it must pass through the hypervisor. However, none of the major hypervisor vendors has implemented robust security for hosted environments in their hypervisors. Unfortunately, the interfaces available to third parties for inserting a hypervisor are still new, and so lack maturity and proven stability and reliability. Introducing layered software within the hypervisor framework also increases the size of the hypervisor, rendering it fatter and slowing it down as the security functionality competes with the other components for resources. And of course, any addition of code to the hypervisor increases the probability that vulnerability will be introduced as well: introducing security modules could directly decrease security! Using hypervisor-level security should be approached with caution, then, and with the goal of decreasing the burden on guest systems (having a function provided centrally instead of on every guest) and of decreasing the need to have traffic leave the environment solely in order for its security needs to be addressed by external systems. [3]

VMware

At this point, the analysis will be turned to VMware; the alternative to Microsoft's Virtual Server 2005. VMware is another option to consider in the server virtualization market. VMware, the global leader in virtualization, recently made headlines with the VMware Lifecycle Manager. "The Lifecycle Manager provides control over the virtual environment, showing who owns a virtual machine, when it was requested, where it is deployed, how long it has been in operation and when it is scheduled to be decommissioned. " [4] VMware virtual machines radically improve system security, availability and performance of the applications hosted, and operating systems. Automation and control of virtual machines through a central control point reduce repetitive tasks, thereby reducing errors, and enabling IT staff to remain in compliance with standards and policies. VMware machines are ideal for capturing and automating processes such as service delivery. "VMware Lifecycle Manager allows companies to implement a

consistent and automated process for requesting, approving, deploying, updating, and retiring virtual machines." [4]

VMware covers all applications necessary for complete virtualization of an organization's systems including security provisions, business continuity and system optimizations. Below, the different VMware server-side applications are divided into 3 categories.

- **Management and Automation**
    - Infrastructure Optimization
        - VMware Virtual Center: Allows a user to automate routine management tasks, and monitor use of physical machines.
        - VMware Converter: Allows the user to convert his/her existing physical system into a virtual machine.
        - VMware Capacity Planner: Views resource utilization and plans server containment and consolidation.
    - Business Continuity
        - VMware Site Recovery Manager: Allows the user to automate disaster recovery in the Data Center using virtualization.
    - IT Service Delivery
        - VMware Lab Manager: Combines servers and networking storage, and shares them across development teams.
        - VMware Stage Manager: Accelerates transition of IT services into integration, testing and user acceptance phases.

        - VMware Lifecycle Manager: Facilitates IT administration and allows companies to deploy consistent approval, update and retirement of virtual machines.

- **Virtual Infrastructure**
    - Resource management
        - VMware DRS: Monitors resource usage and allocates machine resources appropriately.
    - Availability
        - VMware High Availability: Delivers high availability across the IT network without clustering
        - VMware Consolidated Backup: Provides a centralized backup utility that uses a proxy server and reduces load on the production server.
    - Mobility
        - VMware Storage Vmotion: Enables live migration of virtual machine disk files across storage arrays.
    - Security
        - VMware Update Manager: Automates updates and patching for VMware Servers as well as Microsoft and Linux virtual machines.
- **Virtualization Platforms**
    - VMware ESX: VMware hypervisor allocates hardware resources
    - VMware Virtual SMP: Uses up to four physical processors in a single virtual machine.
    - VMware VMFS: High performance cluster file system optimized for virtual machines. [4]

The VMware ESX server is a data center class virtual machine platform that is able to maintain servers in a high performance, high throughput network. The ESX server is appropriate for corporate IT concerns and service providers. Security is covered in the by ESX server in the following ways:

- Design of virtual machines
- Network security and VLANs
- Independent security audits [5]

The VMware kernel is highly secure. It was developed for running virtual machine images in a high capacity server environment. The VMkernel controls hardware and resource usage among virtual machines and the service console. The VMkernel has no public interfaces and cannot execute a process in the conventional sense the way a physical operation system would. This lack of ability to execute processes enhances security because there are no public interfaces. All VMware virtual machines residing on a host computer are isolated from each other. One virtual machine cannot see any other machine except for the virtual machine monitor or service console. This enables virtual machines to run securely while still being able to share hardware. If one operating system crashes on the same hard drive, the other software/operating systems will continue to run unaffected. The only method of enabling communications between a virtual machine and another computer whether it's virtual or physical, is through the network connection. A virtual machine that follows organizational security policies is protected by firewalls, intrusion detection and any other security measures employed. Isolation of virtual machines occurs at the hardware level, so there is no way to access outside systems without the ESX server system administrator permission. [5]

One possible security threat to a VMware ESX server is when an attacker burdens the system by using as much of the system resources as possible in and attempt to deny service to

other virtual machines on the same network. This can be prevented by configuring the hardware resources a machine can use. For instance, the system administrator can allocate 10 percent of the processor cycles to the intended virtual machine so, in effect, there will automatically be ten percent processor resources no matter what the other machines do. DMZ's can be used in conjunction with VMware ESX server to prevent higher level security breaches. DMZ in a box is a term used by VMware that creates a perimeter network whereby the firewall inside the virtual machine is used to verify traffic from the external network. If the traffic is authorized by the firewall it is routed through the DMZ switch and allowed to pass. So if one virtual machine was compromised by a virus or worm, it would not be allowed to spread to other machines on the network. [5]

The VMware ESX server service console is a stripped down version of Linux based on Red Hat 7.2. The service console is the administration point for the entire ESX server. If the service console is compromised, the entire virtual network could be controlled, so the ESX service console runs only services essential to the administration of the virtual environment. Programs compatible with Red Hat 7.2 are able to run on the service console and thus can be exploited. VMware supplies a list of services that are recommended and using outside programs is highly discouraged. [5]

VMware employs the use of VMsight to enable monitoring of virtual machines and network resources. VMsight allows real time monitoring of security policies in the virtual network. It also provides reporting capabilities and alerts which can be integrated with Microsoft Active Directory. Monitoring can be applied at the user or group levels and activity between virtual or physical machines can be logged. VMsight has very little effect on system throughput. Monitoring can be scheduled, further providing convenience to the administrator. VMsight ensures compliance with the Health Insurance Portability and Accountability Act

(HIPPA) and the Payment Card Industry Data Security Standard (PCI DSS) in the following ways. [6]

- Ensures communications for sensitive information are sent through encrypted channels.
- Support of regulations that require network restrictions, documentation, and justification for the use of secure and insecure protocols.
- Support of work station requirements that align with regulations on how sensitive systems may be accessed. [6]

The major components of the VMware security structure are:

- The virtualization layer, which consists of the VMkernel and the virtual machine monitor. The virtualization layer combines four hardware components to create the virtualization platform that the operating system can run on. The virtualization layer is actually the VMkernel. The VMkernel alternates between all the virtual hosts operating on the physical disk. Virtualization performance is made possible by binary translation which is a technique used to increase the efficiency of the CPU.
- The virtual machines: Virtual machines are “containers” in which operating systems run. A user with administrator or kernel level access on a virtual machine is unable to access another virtual machine due to the layer of isolation between virtual machines. Virtual machines can have resources reserved on the ESX host. This adds another layer of security by denying excessive use of resources by ill-intentioned users.
- The ESX server service console: The ESX server service console allows the administrator to control the virtual environment. The default ESX server service console is installed with a high security setting. All communications from clients are encrypted with 256 bit SSL. Services like FTP and Telnet are disabled by default.

- The ESX server virtual networking layer: The virtual networking layer is made up of virtual network devices, where the ESX server service console and the other virtual machines interface with the network. The virtual networking layer includes virtual network adapters and virtual switches. The virtual switch consists of:
    - The core layer 2 forwarding engine
    - VLAN tagging, stripping, and filtering units
    - Virtual port capabilities
    - Level security, checksum and offload segmentation units.

  ESX Server supports VLANS as well for increased security.
- Virtualized Storage: ESX Server implements a path to high speed storage networks for good input/output performance.
- Virtual Center: Management activities are performed in the Virtual Center. Virtual Center uses Windows security tools. It is role based and tied to Active Directory. Virtual Center manages the creation of resource pools which divide system resources and allocate them to their respective systems. [9]

In summary, both Microsoft Virtual Server 2005 and VMware ESX Server are excelling in technology and services offered and becoming more popular. There are security advantages and disadvantages to using server virtualization as opposed to conventional hardware servers. The greater security of virtual systems make server virtualization technologies an attractive option. Complete host isolation is one security selling point that will be considered by those deciding on whether to go the route of server virtualization. VMware is the world leader in system virtualization technology. It remains to be seen whether or not Microsoft can compete in the virtualization market.

Works Cited

[1] Y. Oguchi and T. Yamamoto, Server Virtualization Technology and Its Latest Trends, FUJITSU Science Technical Journal, 44, 1,p.46-52 (January 2008).

[2] A. Antonopoulos and J. Burke, Practical Virtual Security, Nemertes Research.

[3] Microsoft Corporation. Technical specifications for Microsoft Virtual Server 2005 R2 SP1 http://www.microsoft.com/windowsserversystem/virtualserver/default.aspx

[4] VMware http://www.vmware.com/

[5] VMware Resources. ESX Server2 Security. http://www.vmware.com/resources/techresources/cat/91,98 9/24/2004

[6] VMware Resources. Using VMware VDI and VMsight for Stronger more Sustainable HIPPA and PCI Compliance. http://www.vmware.com/resources/techresources/cat/91,98 1/27/2008

[7] VMware Resources. Virtual Networking Concepts. http://www.vmware.com/resources/techresources/cat/91,98 7/29/2007

[8] VMware Resources. Managing VMware Virtual Center Roles and Permissions. http://www.vmware.com/resources/techresources/cat/91,98 4/16/2007

[9] VMware Resources. Security Design of the VMware Infrastructure 3 Architecture. http://www.vmware.com/resources/techresources/cat/91,98 2/22/2007

[10] VMware Resources. VMware Infrastructure 3 Security Hardening. http://www.vmware.com/resources/techresources/cat/91,98 2/21/2007

[11] Muller, Al; Seburn, Wilson; Happe, Don; Humphrey, Gary J. Virtualization with VMware ESX Server. Syngress Publishing. Rockland, MA. 2005