Server Virtualization

Andrew Joiner

4/28/2009

NET-450
Senior Thesis Project
Instructor: J. Hoag

This research project is an overview of the components in creating a Virtual Infrastructure using VMware as the software company as well as experiencing a hands-on approach to learning about how the different components are interconnected.

Table of Contents

Problem Statement and Literature Review

Server Virtualization, while it may sound new, has in fact been around for ages in different forms. It can date back to when mainframe computers had the ability to use time slots for particular programs. With an increase of technology and computing power in today's information world, virtualization is becoming an increasingly popular use of technology.

The term virtualization has already been thrown around, but what is virtualization anyway? The term virtualization can be broken up to have better meaning. "Virtual" means nonexistent physically but in imagination or logically, something exists and "ization" just means the action of making something virtual. To relate this term back to technology, before virtualization, a new machine had to be purchased and/or in possession in order to perform tasks in another type of environment. This environment can range from differences in operating system, memory size, hard drive size, and variety of arrays. The modern way of utilizing the current infrastructure of machines to host multiple logical machines is through the use of virtualization.

The host machine, which is the physical machine that can be physically touched, can have multiple virtual machines (VM's), which are logical machines which cannot be physically touched. VM's have the ability to work completely independent from each other. This is achieved by using some sort of virtualization software which has been programmed to allow many diverse and unique types of VM's to share the same hardware while keeping each VM isolated from each other.

Two of the most popular corporations which have written virtualization software include Microsoft and VMware. Each different application has its pros and cons as well as software lines for the desktop virtualization and server virtualization but the leader thus far is VMware. Because of the strength and popularity of products from VMware, only their products will be explored into greater detail especially during the project phase.

Through the use of virtualization, companies don't have to purchase separate machines, thus saving them money. With the decrease in the number of physical machines, there are also savings in the amount of space required in a data center as well as savings in cooling and electricity.

The last and possibly the most important part to consider is the security standpoint of creating a virtual environment. While many organizations will enjoy the cost savings, many will not recognize the need for security until later.

Benefits of Virtualization

With virtualization, there can be many benefits to the organization including one of the most important factors, cost. While cost may mean money and generally is, there are many items that reduce the cost of the organization. Reducing the amount of physical server's decreases cost alone in a few ways. Having less physical servers in a room saves lots of space. As the number of servers decreases, the amount of energy required to power the servers also decreases. Cooling is a main concern in server rooms and if there are less servers generating heat, there doesn't need to be as much cooling, saving the company even more.

Nationwide Mutual Insurance Company is a prime example for demonstrating the benefits. The company has a plan to cut the amount of servers the company owns in half. Currently, the company has about 5,000 servers but plans to have 2,500 servers by using server virtualization technology. The company had many reasons to reduce the amount of servers. For three years now, the company was able to reduce the amount of physical space the servers take up putting the plan to expand the datacenter on hold. The company also has experienced a decrease in the electric bill and saved about $2.2 billion dollars in hardware costs. Typically, each physical server is hosting thirteen virtual servers but there are a few physical servers hosting as many as twenty virtual servers. The company is using VMware as the virtualization software and uses their popular VMotion tool to move a virtual server to another physical machine without disrupting the services on the virtual server (Thibodeau 8).

Why VMware Wins

When comparing VMware to products from Microsoft or other companies, there is a comparison between features and price. While a product may be cheaper in the short run, it can be more expensive in the long run due to maintenance costs. Microsoft decided to do a price comparison between their products to the price of VMware for five machines. Microsoft was able to virtualize the five servers for $21,200, meanwhile it would cost $61,400 to virtualize them with VMware (Smith 24).

While Microsoft was cheaper and their product would be easier to manage in their native MMC style, Microsoft is missing one important tool, VMware's VMotion tool. Although Microsoft claims that their next release of Hyper-V built on Windows Server 2008 in 2010 will have this functionality, VMware is ahead of the game offering this feature now. Companies are able to save maintenance costs in the long run from being able to use VMotion to move a virtual server to another physical box to do routine maintenance and utilize High Availability mode for when a machine fails (Smith 24).

In another side-to-side comparison, VMware has pulled ahead of Microsoft once again with comparison in performance testing's. *Network World* has an article which was published in September 2008 with its findings between the two popular companies. Each of the virtualization software's, VMware's ESX and Microsoft's Hyper-V were tested the same way with loading only all Windows Server 2008 VMs and then a separate test with only Novell SLES 10.2 VMs. Natively, VMware ESX was able to provide better performance in basic testing's. When Microsoft's Hyper-V was loaded with special drivers, it was finally able to support Novell SLES 10.2 (Henderson 42).

The first test that was conducted was to find the cost of virtualization between a machine just running as a regular traditional server and then with a cushion, the virtualization software between the operating system and the hardware. VMware won this round by a small margin (Henderson 44).

The second test tracked performance as VMs were added to a server. Performance was looked at with one, three, and six VMs being hosted on a server. The test for both one VM and three VMs were tested separate separately between the Windows guest operating systems and Linux guest operating systems. For each of the tests, VMware was ahead of the game by 1,400 bops with Windows and 1,800 bops off with Linux. As more VMs were added to the test of six, both Microsoft and VMware were struggling; however, Microsoft was able to stay afloat better as it was able to allocate hypervisor resources more effectively. Since extremely powerful servers were not being used for the test, the number of VMs were limited than if it were tested on a sever that can handle more resources (Henderson 44)

The third test examined the load of the hard drive input/output speeds. Each of the four tests, VMware with Windows Server 2008 and SLES Linux then Microsoft with Windows Server 2008 and SLES Linux were loaded with six VMs. The purpose of loading a large number of VMs is to test how the virtualization software will perform with a large amount of data to and from the hard drive. In testing SLES Linux, Microsoft was able to perform 5% more I/O’s per second than VMware. With testing Windows Server 2008, Microsoft was choking as VMware was able to outperform Microsoft by about 860 million I/O per second (Henderson 46).

In an article from the same authors that performed three tests that was released later that month, they analyzed which product is better without the cost or performance put into play. One of the most important points that were brought out during the research is the compatibility of the types of operating systems which are supported by each (Henderson Virtual Winner 32).

Microsoft’s product Hyper-V works on top of an edition of Microsoft Windows Server 2008. In doing so, the hardware in the physical machine has to be supported by the core operating system as well as the VMs. Currently, only Windows Server 2008 and just the one flavor of Linux, Novell SUSE Linux Enterprise 10 SP1 or SP2 is supported (Henderson Virtual Winner 32).

In contrast, VMware's ESX server runs on a Linux operating system. It is able to support a variety of platforms in both Windows and Linux environments. To name a few that are supported include: XP, Vista, Server 2000, Server 2003, Server 2008, Windows NT, Red Hat Enterprise Linux, SUSE Linux, Ubuntu Linux, Free-BSD, and many more (Henderson Virtual Winner 32).

VMware ESX Server

One of the VMware's most popular features is its VMotion technology. VMotion has the ability to move a VM to another physical server without having to power off the VM. This is a great feature to have in making server management easier. If a particular physical machine is experiencing high load as VMs are starting to need more resources, an administrator can easily move the VM or a few VMs to another physical server to reduce contention. Because the VM can be transferred on-the-fly, the product VMotion satisfy's guarantee service in service-level agreements (McCain 5).

When VMotion moves a VM, it copies the registry and memory to the other physical machine. The old machine is able to properly close the other VM and then the new one is able to be started properly. In order for this transition to work, the types of processors need to match. For example, if a machine is running on an AMD processor and it is then transferred to a machine with Intel, there may be some problems with how the memory and registry settings interact with the processor to execute instructions. This can also be the case if transferring from a single core processor to a dual core processor and vice-versa. It is recommended to use similar types of architecture for the various VMs to better guarantee VMotion to work, but it is not required. If there are different types of processors in the virtual server environment, VMotion has to be tested to make sure compatibility is not an issue (Haletky 3).

As with any infrastructure and protocols, there are various layers which bottom layers serve the upper layers. In virtualization, the same is true. The bottom layer is for the physical hardware. This includes the CPU, memory, disk drives, network cards, and so on. The first layer is common for the traditional machine, but the second layer where the whole virtualization concept is starting to come into play (Marshall 10).

The second layer is the Virtualization Layer. This is the where the Hypervisor is located. In order for anything to work with the hardware, there needs to be some sort of operating system to have instructions on how to handle the various inputs and output devices. The Hypervisor has the role of being able to communicate to the hardware devices through the use of the operating system on the previous layer and at the same time to provide support to the various independent VMs on the third layer (Marshall 10).

The third layer, the VM layer then has sub layers. Just like regular machines, the bottom layer needs to have some sort of hardware. Since the physical hardware is being controlled by the virtualization layer, each VM has virtual hardware. On top of the virtual hardware is the operating system followed by the software applications running on the operating system (Marshall 10).

Just like any operating system, there is some sort of maximum limit for the amount of different devices. Although ESX isn’t considered an operating system, it can only support so much. Each VM can have up to 4 NICs, 64GB of RAM, 4 CPUs, and 10 remote consoles to the VM. For the physical machine, there can be 32 CPU cores and a maximum of 256GB of RAM (VMware Configuration Maximums 1, 3).

The first version of ESX server required an installation of Red Hat Linux as the foundation. Much has changed since 2001. Now, ESX server can be installed without an operating system at the base level. To make this possible, hypervisor level is built upon a VMkernel. Although there are commands that are the same as Linux, it isn’t exactly Linux (McCain 2).

The VMkernel controls the physical resources such as the CPU, hard drive, memory, and network connectivity to the VMs. (Marshall 17) The only user functionality behind the physical machine is to access the Service Console. This is installed to provide simple management tasks. The firewall can be configured and a simple web server can be enabled. Also in the Service Console is a way to enter the serial for the product as well as configure the IP address for the ESX machine (McCain 2).

In order to actually configure the physical machine to accept VMs and to configure the machine better for virtualization, there has to be a Virtual Infrastructure Client. This client, when installed on a machine, can remotely manage the ESX server. The reason for a simple web server is to provide a link to this package from any other machine connected to the network. Without a Virtual Center, each ESX server would have to be connected separately to be able to manage them. With Virtual Center, management is much easier. Just as Active Directory is installed on a Windows network to provide ease of management, Virtual Center is installed to manage ESX servers on a virtualization-type network (McCain 3).

Shared Storage Space

For any operating system to work, either on a physical machine or VM, there has to be some sort of storage volume to hold the data. For traditional machines, the hard drive in the physical machine is typically used. When virtualizing, the physical ESX machine can have the VMs stored on the local disk, but this is not preferred. Typically in an environment that wants fault tolerance, the data is stored on a network.

One of the reasons to use network storage is to make the popular VMotion tool work. Just as the section explained how VMotion is used, only the registry and RAM are copied to another machine. The reasoning behind that is that the virtual hard disk, the VMFS, is stored on a storage network and the disk is accessed directly over the network. By having a shared medium, each of the ESX machines will be able to access the same hard drive to be able to support the data and Operating Systems on the VMs.

Servers have a few different ways of using storage devices off of the network. The best way, which is also the most expensive option, is to use Fiber Channel Storage. In this environment, there are usually multiple hard drive volumes managed by a Fiber Controller. Each server will then have a Host Bus Adapter which is a hardware device that will connect directly into the fiber network. This will emulate the physical server of actually having a regular hard drive in it (McCain 97).

Another way to provide remote storage is through iSCSI Network Storage. This method is very similar to the Fiber Channel Storage environment except that the data runs on top of TCP/IP. Usually the iSCSI is on a separate network but iSCSI can run on the regular data network. Once again, there has to be a special hardware device for iSCSI to interpret the information (McCain 108).

The third way is to run a Network Attached Storage (NAS) using Network File System (NFS). The data to and from the remote disk is transferred directly over the typical network and can use the same network card that is used for regular traffic, however in best-practice, it is recommended to isolate regular traffic from NFS traffic. Having the data transferred across separate networks increases network performance (McCain 120).

Security

With any new technology, there is a need to research the security of the product and implement security strategies to protect the system.

Nail Roiter from *Information Security* magazine wrote an article about a couple of key topics. He indicates that companies quickly switched over to virtualization due to cost savings as if there was a gold rush. Unfortunate for them, the companies did not think about security until the later. VMware recognized this and has devoted resources in making security easy through the use of documentation as well as tools. One of the major problems is the time needed for a company to look over the security policies on the ESX servers especially when they are hundreds of them. VMware partnered up with Tripwire to have a free tool which is able to check the policies of the various ESX Servers. This program is called ConfigCheck and can be downloaded through Tripwire's website (Roiter 2008).

To address the security concern about network traffic, there are a couple of different network traffic types that is generated through the use of virtualization. It is recommended to have a completely different network for each of them. The ESX Server Management accepts connections through the Virtual Center Client and through the VI Web Access. The data passed is encrypted but this is also an area that can be connected to the internet to provide remote assistance (Security Best Practices).

The second type of network traffic is through the VMkernal ports. Traffic generated in this area includes VMotion and traffic to the datastore such as NFS or iSCSI. It is important to put each of these on a separate network because none of the traffic generated in each system is encrypted. If security is essential, hardware SSL can be used to protect the data (Security Best Practices).

The third type of traffic generated is from the actual Virtual Machines. This is the network connection that clients are able to utilize to reach the servers that are running as VMs. Virtual

LANs can also be created within ESX Server management to create an environment which closely relates to the environment the physical servers used to have (Security Best Practices).

On the management end, there needs to be documentation for how the virtual infrastructure is laid out. This includes the different networks and storage devices and system information. Monitoring systems should be used to trigger alarms for different types of events that are suitable for the company's policies. Another key management technique in security is through the use of creating snapshots of each of the virtual machines. This will enable a server to be reverted if there is a problem. Also system patches are extremely important in securing the system. This means patches for all components should be performed. This includes all of the ESX Servers, the individual VMs, the Virtual Server Center, and the individual clients on the network (Security Best Practices).

For each individual machine, there are a couple of best practice techniques that the program Tripwire will look for. As each ESX Server has a root account, a secure password should be used that only the essential administrators know. For the other administrators, another user account can be created to give them limited access (Security Best Practices).

The ESX Server Console should also not be mistaken for a regular Linux machine. In light of this, installations of extra packages on the ESX Server intended for the Linux platform should not be installed unless the software is known to provide support to the ESX Server. Network Time Protocol (NTP) should be used to synchronize the system time with an accurate clock so that auditing and logging can be more accurate. To provide administrator's access to the VMs, they should use RDP or VNC instead of using the VI client (Security Best Practices).

The Virtual Center is hosted on a Windows platform and therefore it is prone to attacks by itself. One way to limit problems is to disable services in the operating system that are not needed. Another standard to follow is to not browse the web or have an email client installed. This server should be kept as clean as possible to reduce the chances of it being at risk. By default, the database is created on the same machine as Virtual Center but the database can be stored on a different machine. To limit access, another network card should be used to connect only the database server to the Virtual Center. The database can be secured further with a password. By default, the Virtual Center has a generic SSL certificate but this should be replaced by one from the organization (Security Best Practices).

Just like how the ESX Servers should have different user accounts to limit access, the Virtual Center should also be limited to what administrators can do. There are three main components in creating permissions on what users can administer:

- *Privilege – The ability to perform a specific action or read a specific property. Examples include powering on a virtual machine and creating an alarm.*
- *Role – A collection of privileges. Roles provide a way to aggregate all the individual privileges that are required to perform a higher-level task, such as administer a virtual machine.*

- *Object – An entity upon which actions are performed. Virtual Center objects are datacenters, folders, resource pools, clusters, hosts, and virtual machines.* (Managing VMware Virtual Center Roles and Permissions 2007)

Each user or group of users can be assigned unique tasks in any way possible. To make management easier, there are a couple of predefined groups for most common tasks. The “Administrator” has complete control over the entire infrastructure. The “Datacenter Administrator” has roles for the datacenter hierarchy and the “Resource Pool Administrator” performs functions mainly for Resource Pool management. The “Virtual Machine Power User” is able to modify most of the settings of a VM such as snapshots, scheduled tasks, and configurations. The most restricted group is the “Virtual Machine User” which has the role of interacting with the VMs without the ability to change the current configuration (Managing VMware Virtual Center Roles and Permissions).

By observing a couple of practices, the security of the virtual infrastructure can be tightened. For each of the three types of network traffic, a dedicated network should be used. Documentation and patching of systems is also another important task in security. One of the most important parts in security is to limit the access by having users and groups to prevent harm from inside the network.

Project Experience and Results

The project portion will focus on implementing a simple Virtual Server Infrastructure to learn and experience how virtual servers work. In doing so, there are a couple of key systems to achieve this goal. There is a need to have a centralized storage, ESXi servers, a Virtual Center Server, and a Virtual Center Client. The end product in incorporating all of these elements will be an environment where multiple Virtual Machines can be run and be migrated to different ESXi servers.

Background Information

ESXi Servers can operate independently but to include a popular feature VMotion, there needs to be some sort of shared storage. VMware is extremely particular when it comes to sharing a drive over the network. As ESXi is closer related to Linux, they decided to use NFS to create a centralized storage. Many Network Attached Storage devices can be purchased from a store; however, many of them support SMB rather than NFS. To alleviate the cost as well as providing a solution to support NFS, alternatives were researched. FreeNAS, a Linux distribution, stood out and had promises with their features. FreeNAS is an extremely small package derived from FreeBSD that can either be run as a live image or installed to the hard drive. The interface on the host is extremely simple and gives options in a text format rather than providing a GUI. Simple tasks such as assigning an IP address, rebooting, and shutting down the system are available from the host. All of the other features in actually configuring the NAS are performed on a remote host by visiting the website for the assigned IP address of the Free NAS machine. FreeNAS has security features for shares including the ability to utilize existing groups and users from Active Directory and LDAP. Also included in FreeNAS are other sharing features such as NFS, SMB, BitTorrent, Web Server, iTunes, SSH, along with other forms of file sharing.

ESXi servers are the individual physical machines that host virtual machines. VMware actually has two types, ESX and ESXi servers. ESX server requires a paid license where ESXi can be granted free licenses with a valid email address. For this project, ESXi server will be implemented. The ESXi servers are basically the core of the whole virtualization task. This is because ESXi servers don't actually require a NAS or Virtual Center. The local disk can be utilized as the storage facility and each ESXi server can be managed one at a time. This can be good for a small office or home when failover technology is not required.

In order to connect all of the ESXi servers together, Virtual Center is used to manage them. Virtual Center can be installed on top of Windows XP or Windows Server 2003. For this project, Windows Server 2003 will be used to make sure the connection limit to the OS isn't exceeded. In order to connect to the Virtual Center, there needs to be a VMware Infrastructure Client to provide a nice GUI interface. This can be installed on any regular Windows Operating System to manage the ESXi servers. The client can either connect to the ESXi server directly by using the static IP address or machine name or a single connection can be made to the Virtual Center Server which manages all of the other ESXi servers.

Problems Faced

At first, three separate physical machines were tested to create a Virtual Server Infrastructure. The first machine was a Pentium D 3.0 GHz, 2GB RAM, with an Abit Motherboard. An attempt to install ESXi server on this machine failed as the hard drive controller was not supported. Due to this problem, Windows Server 2003 was installed on this machine to host the Virtual Center and to create a NFS share.

The second machine was a Pentium 4 2.66 GHz, 2GB RAM, with an Intel Motherboard and the third machine was a dual socket AMD 2.33GHz, 1GB RAM, with an unknown motherboard. Each of the two machines was able to install ESXi server with ease and connect to the shared NFS datastore.

When it came time to explore the feature VMotion, there was a major problem, compatibility between processor types. As the preliminary research indicated, the processors in each of the ESXi servers should come from the same family. If they were not in the same family, they should be tested for compatibility before deployment. Since the one ESXi server had an Intel processor and the other had an AMD, the processor mismatch wasn’t even close and there was a need for another solution to better experience the features of VMware’s products.

Since there were two problems, compatibility for the hard drive controller and a mismatch in processor, VMware Workstation was then utilized to create the entire infrastructure. This solution ended up working extremely well as each of the ESXi servers had the same hardware, thus enabling VMotion compatibility.

FreeNAS

VMware Workstation was configured to the following settings:

Processor: Intel Quad Core 2.66 GHz

Number of Processors: 1

Memory: 256MB

Hard Drive: 120GB SCSI

Network Adapter: 1Gb/s

After VMware Workstation was configured, FreeNAS was loaded as an ISO image. The package automatically loaded as a live image. There was then a screen to install the package to the hard disk using easy user prompts. After FreeNAS is installed to the hard drive, the LAN IP address was configured to a static IP: 192.168.73.95/24.

The GUI web interface is extremely easy to navigate and configure. To begin configuring, a hard disk needs to be imported. To do this, “Disks – Management” is selected from the menu. After each change, the service has to be restarted which is provided by an easy button on the current page. After the disk is added, it now needs to be mounted. This is achieved by selecting “Disks – Mount Point”. After the disk is mounted, the NFS portion can now be enabled. This is found under “Services – NFS”. The service itself has to be enabled as well as the NFS share.

To be able to put ISO images to the NAS, SMB was also configured to allow a windows machine to access the same shared folder as the ESXi servers. This is easily configurable by going to “Services – SMB”. The service was enabled then the share was created.

ESXi Server

Three ESXi servers were installed onto VMware Workstation with the following settings:

Processor: Intel Quad Core 2.66 GHz

Number of Processors: 1

Memory: 1024MB

Hard Drive: 8GB SCSI

Network Adapter: 1Gb/s

Just like FreeNAS, each server was booted from an ISO CD image. The install itself is simple with easy onscreen prompts. Also just like FreeNAS, the console on the screen itself does not have many options. It does however has the option to change the password and configure the network settings. This is achieved by pressing <F2> and selecting the proper titles for the categories. Each of the ESXi servers were configured with the username: root and password: vmware. The IP addresses of each were configured with this IP addressing schema: ESXi01 - 192.168.73.60/24; ESXi02 - 192.168.73.65; and ESXi03 - 192.168.73.70.

Virtual Center

Server 2003 was installed onto VMware Workstation with the following settings:

Processor: Intel Quad Core 2.66 GHz

Number of Processors: 1

Memory: 256MB

Hard Drive: 8GB SCSI

Network Adapter: 1Gb/s

Installation for Server 2003 was performed with all of the default settings. After it was installed, Virtual Center was then installed on top of Server 2003. For installation of Virtual Center, all of the default settings were selected. This allows a SQL database to be installed to handle all of the data from the ESXi servers. During installation, it will ask for the Server 2003 administrator username and password so that new user accounts can be created for the database and other operations for Virtual Center.

VMware Infrastructure Client

VMware Infrastructure Client was installed on Windows Vista on a desktop as well as on XP on a laptop. Each of the two machines were able to configure the virtual environment but the client on XP performed better and had no lockups when compared to the client installed on Vista which had numerous lockups.

Piecing Everything Together

Now that all of the pieces of the puzzle are present, it is time to put them all together. By this point, there is a NFS share using FreeNAS, three ESXi servers, and Virtual Center installed on Server 2003.

The first step it to add the ESXi servers to Virtual Center. To do this, VMware Infrastructure Client is used to connect to Virtual Center. Once connected, there is an Explorer Tree view on the left panel. Right click the Virtual Center host and add a datacenter. After the datacenter is added, that can now be right clicked to add ESXi servers. The IP address of each ESXi server is now entered along with the username and password to each of the three.

Now that the ESXi servers are added to Virtual Center, each ESXi server can be managed through the same screen inorder to add the shared NFS volume. To do this, click the first host and go to the configuration tab. There is now an option to add storage. A prompt will then ask what kind of storage to add. Since it is a NFS volume, NFS is selected. It will ask for the IP address for the NFS server and the path. The IP address is 192.168.73.95 and the path to mount is /mnt/VMDataBank. This has to be added for each of the three ESXi servers.

The next step is to add ISO images to the shared storage. The SMB share can be used from a Windows machine to copy over the ISO images. After the images are copied over, VMware Infrastructure Client can be used to install the OS onto the ESXi servers. To do this, click on a single ESXi server and click “Add Virtual Machine”. A prompt will then come up for the name of the VM, location, hard drive size, memory allocation, and location of the ISO image. After the VM is created, it can then be booted and displayed on the Console tab. The operating system can then be installed as if it were on a regular machine.

After the Operating System is installed, it can then be powered off and used as a template. In the power off stage, the VM can be right clicked and converted into a template. The template can then be used to quickly make copies of the same type of VM without having to install it from scratch.

When many VM's are created, VMotion can then be configured to provide the ability for VMs to be transferred to another ESXi server. To enable VMotion, there is a network properties option on the configuration tab. Under the properties, VMotion has to be enabled. After it has been enabled on all of the ESXi servers, a VM can easily be moved to another ESXi server by just dragging and dropping the VM from the current ESXi server to another one. It took approximately two minutes to migrate the VM to the other server in this environment.

Discussion and Future Research

As the senior project was only one semester long, there was only time to research key items to make server virtualization work. A couple of features, High Availability and Distributed Scheduling of System Resources are two extremely popular features that were not covered in this project. Also, the project portion did not cover anything about the performance and security in virtualizing.

High Availability (HA) is a feature from VMware that enables a fault tolerance capability for when an ESXi server goes down. Basically, there is a heartbeat from the Virtual Center Server that monitors the condition of the ESXi servers. When the heartbeat fails, the VMs are able to be migrated automatically to another ESXi server. Unfortunately, this feature was unable to be explored. There were a few problems that require more research because of a couple of problems. There was a lack of understanding exactly how HA works and how it can be enabled effectively. Also, there is a need to have more ESXi servers so that there are enough resources for the VMs to be transferred evenly between various ESXi servers.

Another feature VMware offers is DRS (Distributed Scheduling of System Resources). What this feature can do is automatically calculate which VM should be run on each of the ESXi servers. While an administrator can manually choose which server a VM can run on, the system can make management easier by being able to dynamically adjust where the VMs are run as stress is applied to the ESXi servers. This would have been a great feature to research but just like the problem with HA, there wasn’t enough information on how it actually works and the lack of resources to run multiple ESXi servers.

The first part of the paper had research about the performance between Microsoft's product Hyper-V and VMware's product ESXi server. It would be great to be able to replicate the results as well as test in different ways the performance of a virtual environment. For future research, this in itself can be an extremely detailed and effective research by itself.

Security is extremely big in the information age and as detailed in the first part of the paper, there are many ways to increase security on the system. The main goal for the project portion was to get the system to actually work. In doing so, security was not even though of and the implementation would be much different in the future to follow some of the security guidelines.

Overall, this project was an extremely beneficial learning experience. Although the first part focused on theory, it was beneficial to have a good background to go by in thinking about what kind of project should be done. The project portion only focused on the basics which could be expanded to specific areas in the future.

Works Cited

Dodge, John, Michael Burke and Rob Daly. VMware Infrastructre 3 Security Best Practices. 20 April 2009 <http://www.datadr.net/download/Whitepapers/Security-Best-Practices-VI3_Foedus.pdf>.

Haletky, Edward L. VMware ESX Server in the Enterprise. Boston: Pearson Education, Inc., 2008.

Henderson, Tom and Brendan Allen. "Virtual winner: VMware's ESX KOs a roughly built Hyper-V package." Network World (September 29, 2008): 28-34.

Henderson, Tom and Brendan Allen. "VMware edges microsoft in virtualization performance test." Network World (September 1, 2008): 42-46.

Marshall, David, Stephen S Beaver and Jason W McCarty. VMware ESX Essentials in the Virtual Data Center. Boca Raton: Taylor & Francis Group, LLC, 2009.

McCain, Chris. Mastering VMware Infrastructure 3. Indianapolis: Wiley Publishing, Inc., 2008 .

Roiter, Neil. Virtualization tool assesses VMware security configurations. 2005 June 2008. 20 April 2009 <http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gcil316324,00.html>.

Smith, Roger. "Virtualization: Microsoft's Price Versus VMware's Features." InformationWeek (September 15, 2008): 24-26.

Thibodeau, Patrick. "Nationwide Aims to Cut Its Server Count in Half." Computerworld (November 2, 2008): 8.

VMware. Managing VMware Virtual Center Roles and Permissions. 20 April 2009 <http://www.vmware.com/pdf/vi3_vc_roles.pdf>.

—. "Configuration Maximums." 2008. <http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_config_max.pdf>.