https://doi.org/10.48009/2_iis_2009_218-225

THE ADVANTAGES OF VIRTUALIZING A UNIVERSITY COMPUTING INSTRUCTIONAL/RESEARCH DOMAIN

Corey Hemminger, Saint Cloud State University, heco0701@stcloudstate.edu
Paul Safonov, Saint Cloud State University, safonov@stcloudstate.edu
Dennis Guster, Saint Cloud State University, guster@stcloudstate.edu
Joseph Meunier, Saint Cloud State University, mejo0506@stcloudstate.edu
Christopher Schroeder, Saint Cloud State University, scch0305@stcloudstate.edu

ABSTRACT

The advent of distributed processing has drastically increased the number of hosts required to support an enterprise level computing domain. Often, each application such as accounting, DNS or WWW service is allocated its own dedicated host for performance and security reasons. While this scenario is effective from an enterprise computing perspective, it poses several disadvantages. These disadvantages include: high hardware cost, significant 110 volt power consumption, significant cooling costs and a complex computing environment to manage. To combat these disadvantages the concept of virtual hosts has been suggested. This paper explores, through a case study, how virtualization could be employed in a live computing domain to reduce the number of physical host by a factor of 9 while still maintaining adequate performance/security metrics. Further, while offering the advantages of ease of management, reduced power/space/cooling requirements and improved fault tolerance/backup.

Keywords: Virtualization, Green Computing, Enterprise Computing Management and Distributed Computing

INTRODUCTION

The traditional hardware model used in an enterprise computing domain typically features many different physical hosts. While this model is often complex and difficult to manage it was selected to provide a degree of separation among the applications run. This physical separation is typically undertaken for a variety of reasons such as gaining better performance, not disturbing a well functioning existing application or for security reasons. While the reasons cited do have a degree of merit, this physical model has several disadvantages such as it requires a lot of physical space to store multiple physical servers, the power consumption and heat generated can be substantial and the complexity and time required to manage multiple physical hosts can be problematic as well. To achieve physical separation for example, it is common to host DNS (domain name service), SMTP (email), WWW (web server) and whatever application servers there might be on completely separate physical hosts. Smith and Nair, [11] suggest that there is an alternative to this physical related model. Specifically, they state that virtualization can effectively support individual processes on a single physical machine that is logically divided into separate or "virtualized" zones.

Given the communication model used in the vast majority of today's enterprise systems in which local communication is provided via a LAN(local area network) and communication to the outside world is provided by a WAN(wide area network) Internet connection security is of paramount concern. Which means the concept of separation of applications cannot be abandoned. It is still possible to achieve this separation through the concept of logical rather than physical zones. Boyd and Dasgupta, [4] point out that virtual operating systems can provide isolation and allow those isolated zones to safely share the physical resources contained on a single physical computer.

To illustrate how the concept of virtualized hosts might be applied to an enterprise computing domain this paper will use the case study approach to delineate how a multi physical host environment could be converted to a single physical host, but multiple logical host environment.

REVIEW OF LITERATURE

The concept of a virtualized operating system is not new in fact on PC (personal computer) architecture it goes back at least 20 years [3]. However, it has only been in the last 5 years or so that the commonly

available design made the transition from best effort provisioning to stable platforms that did not compromise in regard to security and still were able to provide adequate performance and functionality [2].

A motivating factor to the increase in OS virtualization deals with the concept of sustainability and "green" IT solutions. Enterprise level computing experienced rapid growth to accommodate distributed systems that now have world-wide reach due to the Internet and the access it provides to support a global economy. Previous research related to virtualizing a computing domain has shown that in fact the number of physical computers can be reduced which in turn draws less power, generates less heat and takes up less physical space [1]. Further, because fewer computers are required in the computing domain advantages are also gained in regard to less physical maintenance and simplicity of design [10]. This may translate to fewer employees and given the highest cost within the IT budget is typically personnel this would be a most welcomed reduction.

In addition to the "greening" that fewer computers provides there are also other advantages that may result related to fault tolerance and performance. In the physical model, if a host failed only the application actually running on that host would fail. In the virtual model if the physical host fails all the virtual zones and their respective applications fail as well. So in a way the virtual model puts all of your "eggs" (running applications) in one basket. Therefore, for this model to be effective there needs to be multiple baskets [6]. Typically the main production virtualized host would be backed up at least twice. In other words, two exact copies (or as close as the updating delay would permit) would be keep, one on site and one off-site providing two degrees of fault tolerance. If the main site failed then the first replica would become the new production site. Besides offering this fault tolerance capability the replicas can also be used to increase performance by being configured for load balancing. In other words not all of the data inquiries would be sent to the main production server; rather they would be equally distributed among the main production host and the available replicas. Research has shown that the load balancing technique as would be expected can in fact help improve performance [9]. Given that the virtualized model in its basic form reduces an application's access to computer resources the concept of load balance through replicas helps off set that loss.

Certainly "greening" the computing enterprise, reducing complexity and enhancing fault tolerance make an excellent case for the concept of host virtualization. However, given the dire security consequences of being connected to the Internet perhaps it is virtualization's isolation of high profile services that is its best attribute. The work of Laureano, Maziero, and Jamhour [8] provides a striking illustration. In this work they describe the importance of intrusion detection applications to help safeguard against outside attacks and point out the application's vulnerability to external tampering or disabling when run in a straight unvirualized physical host. As one might expect intrusion detection is the cornerstone of any security strategy and should be protected to the utmost. Laureano, Maziero, and Jamhour [8] were able to use virtualization to successfully isolate the intrusion detection application in their domain thereby making it invisible and inaccessible to intruders.

MOTIVATION

The prime motivation for undertaking this project began with the problem of outgrowing available 110 volt power and cooling capacity. In the domain studied all of the primary missions are related to distributed processing and high performance computing. Therefore, the number of hosts that needed to be configured at one time usually exceeded 100. It quickly became clear that if the present physical space and its infrastructure were to remain viable a strategy other than the current one in which hosts were housed in separate physical computers needed to be undertaken. The virtualization option described herein provided a means to reduce the number of required physical hosts while offering benefits in regard to system management, fault tolerance and disaster recovery. Further given the push for "greener" IT infrastructure the timing of this project could not be better.

PROBLEM DESCRIPTION

In the computing domain serving this case study there are numerous physical production hosts that serve a variety of needs. They were originally placed in separate physical computers to provide isolation for security purposes. In all cases performance in the separate physical host model was for the most part excellent and unused CPU cycles were observed in all cases. Therefore, these core production hosts

offered an excellent test case for virtualized hosts. The assumption being that the virtual partitions would provide the isolation needed for security purposes and the performance requirements for any one host could be met in a shared resource environment. Specifically, it is assumed that since all hosts were using only a fraction of their available computing resources on their physical host that they would function at an acceptable level in a shared virtual host. In the case study 9 physical hosts are restructured as virtual machines into a single physical host. In theory that would mean that they would each be limited to 1/9 of the available computing resources. However, in the operating system utilized the resource allocation is dynamic meaning that the resources are viewed as a pool and any unused resources can be allocated to any virtual machine. This methodology works well as long as there are several fairly idle virtual machines. In the case of the unlikely scenario of intense workload across all 9 virtual machines performance would decay exponentially and a priority scheme would need to be used to control the resource allocation.

The purpose of each of the 9 original physical hosts described in partition numbers 1-9 follows in Table 1:

Table 1 Virtual machine partitions

Partition number	**Description**
Host	1000NTP Server, Virtual Machine host(Virtual Box), Ubuntu/Debian Mirror(apt-mirror)
1	Main Student Server. SSH login server(Firewall will forward all port22 traffic to)(Sun Java jre & jdk, TCPDump, Hping3, portmap, dig, trace-route)
2	Secondary SSH login server as backup if partition 1 locks up (Firewall will forward alternate port to partition2 port22)
3	LDAP/Kerberos Server (OpenLDAP/Kerberos5-mit)
4	DNS/DHCP Server (Bind9/DHCP3-Server-LDAP)
5	E-Mail Server (Ubuntu Mail Server install)
6	Web Server (Apache Tomcat)
7	NFS-Kernel-Server for Home folders
8	Network Installation Server (FAI-Server)
9	Head Node for Clusters (HA Cluster Tools)

The first entry in the partition number column describes the physical host for the 9 partitions to follow. The host itself contains the network time server that is used to synchronize all hosts both virtual and physical within the domain. For client/server and database applications it is critical

that all hosts be set with the same time for data integrity and security purposes. This physical host is configured with the Ubuntu/Debian release of the Linux operating system.

The first partition contains the main student server used to support instruction. One of the prime areas of instruction supported is computer security classes so a number of high risk commands are allowed on this virtual machine that would not be allowed on regular campus machines. Therefore, both incoming and outgoing traffic to this partition is tightly filtered at the firewall level and terminal access is only available through secure shell (ssh) which uses a robustly encrypted stream.

Virtual machine 2 which is housed in partition2 provides a secondary version of virtual machine 1. This machine is used for client/server related projects that require more than one server and as a general backup for partition 1. Because the domain uses a global authentication system single sign-on can be provided to users so that they are granted access to both partitions one and two, but only need to sign-on once.

The global authentication just described is supported in virtual machine 3. Global authentication is provided by lightweight directory access protocol which is well known for its robustness and scalability [5]. Further, this critical component in the IT security structure is hardened by Kerberos which means the encryption is very robust and that the password does not have to be sent remotely across the network.

The domain name service and the dynamic host configuration (protocol) services are hosted in virtual machine 4. This allows address resolution of network layer addressing to take place and client work stations to be allocated a temporary network (IP) address. Domain service is provided to all domains since in the enterprise illustrated there are .edu, .com and .net domain names supported.

Email services are provided by the virtual machine configured in partition 5. This virtual machine hosts a mail system which provides standard mail services and a browser based interface that is linked to a standard apache tomcat web server (hosted in partition 5). Both secure and unsecured services are supported. Standard web services are hosted in partition 6 and as previously stated apache tomcat is used as the web server software. This web server in addition to supporting browser based email, is also used to host domain related home pages and instructional activities such as Java applet programming.

Partition 7 houses the global file system which is supported by the network file system protocol. This file system then becomes the central depository of data for all users and allows all user data to be stored in a central location. Further, because it is global "it follows" a user no matter which host he/she is logged into. In other words, the user always has the same default directory no matter which host (virtual or otherwise) he/she is referencing. While centralizing all data at a single location provides many management advantages, it involves a certain degree of risk in that all the "eggs" (data) are in one basket. Therefore it is critical to have multiple baskets or in this case multiple host replicas to provide fault tolerance and backup.

Virtual machine 8 is contained in partition 8 and is used to store network retrievable images of software. Typically these are images that would need to be stored many times. Within the domain host/servers are constantly being configured for development and instructional purposes which means that several operating system images are stored in this partition and are installable via the network which is faster and more convenient as compared to installing from CDs.

The last partition contains the virtual machine that is used to manage the two main clusters in the domain. Each computing node in the clusters is configured to carry out calculations as a subpart of a team of processors. Therefore, the head node is the manager of that team, in that it schedules and assigns the work to be completed by each node in the completion of complex problem which would be segmented into subparts to improve performance.

VIRTUAL MACHINE CONFIGURATION DESCRIPTION

The details of the virtual hosts assigned to each partition are delineated in Table 2. The host of all the virtual machines is running Sun's Virtual Box 2.1 software. It's also the time server and is running NTP server since the NTP daemon needs direct access to the machines internal clock, which the virtual machines can not directly access. This host has 3 network cards configured for all 3 networks contained in the domain in which it operates. It also has the virtual machines operating system (OS) data

stored on its RAID1 root drive in addition to its own OS and it also has an Ubuntu/Debian mirror located on that same drive. The second RAID array is a RAID5 array with 1.5 terabytes of storage for home directories which are stored in the path /raid/users and this file system will also house domain level files and folders for different machine drivers, OS images, documentation, and other system level files.

All of the virtual machines have a local administration account to allow access to the machine if the authentication system goes down. All the machines also are running ufw firewall software to provide extra layers of protection. All the machines have a 10.0.0.0 (private) virtual network address assigned to them. Hosts that require direct Internet access have a second virtual network interface card (NIC) configured with an external Class C network addresses. Outside access is limited for security reasons to only certain services such as web hosting. All the other services can communicate with a NATed 10.0.0.0 network address.

The virtual machines were installed using Ubuntu images and configured using the minimal virtual machine install option and openssh-server. This strategy was invoked to minimize security risks and save system resources by not installing or running unneeded software. After this initial installation they were updated with the latest packages and virtual-box guest additions.

Partition 1 is the new student server to replace an old one which was configured as a standalone physical host. The new firewall will forward all port 22 (ssh) traffic to Partition 1 to create a choke point and protect other systems from being hacked. It thus becomes the main login system for the domain and will serve as a relay to get to and gain access to hosts only connected to the 10 network. It is configured with software used by instructors for various classes designed to support instruction in a distributed processing domain. It also has a script setup to be run from the root level for updating Kerberos. The script can be extremely valuable in global user maintenance. Basically it evaluates ldap's user accounts and reconciles differences. Specifically, it serves to coordinate communication between ldap (the user data base) and Kerberos (the user authentication system). This script is able to create/delete accounts in Kerberos that are already defined via ldap and assigns and manages passwords. It also will delete home folders for deleted accounts.

Partition 2 is the alternate ssh login server. The new firewall will have an alternate port forwarded to partition 2 via port 22 to allow domain logins by select administrators in the event that partition 1 is down. Once on partition 1 or partition 2, access to all other machines in the domain is available.

Partition 3 hosts the new authentication system running open LDAP which is hardened with Kerberos5. To simplify the creation of accounts the phpldapadmin package was also installed which provides a browser based GUI which can be used for account management. While logged in within the domain LAN it is possible to open a browser via a 10 address to use the GUI. All student accounts are created in the path /users/students. Staff accounts are created in /users/staff. The path /users/classes is used by professors that wish to share files with students. Further, the path /users/webspace is the folder used by all accounts so that they are able to host web pages for classes. Within each account upon first login the home folder is created automatically, and a www folder is provided via a symbolic link to the path /users/webspace/.

Partition 4 is the DNS/DHCP server that is running bind9 and dhcp3. It is the authoritative DHCP and the Domain controlling DNS.

Partition 5 is the Mail server that will host e-mail accounts. It was installed using ubuntu's mail server option during the initial install.

Partition 6 is the apache web server that hosts student websites for classes. By browsing to http://externalIP/~user_name students can access their web pages. Since programming in Java is the primary class using the web server, the site is configured to filter out .Java files so others can't view the source code. Further, students are cautioned about what they put in this folder since world wide access is allowed to this URL and data therein can be accessed and/or downloaded.

Partition 7 is the NFS server that is configured with a second drive image that reads and writes directly to the host's /dev/md2 raid5 drive. It's configured as a second drive within the virtual box and is mounted to

/mnt/raid/. Partition 7 is using NFS to share the home directories across the 10 network.

Partition 8 is the network installation server that is running FAI (Fully Automated Installation) which allows machines to be configured to boot from the network and allows installation of a debian or ubuntu image. It is primarily used in the student lab on machines that get changed from windows to Linux every other semester. This installation option makes it easy to reload images and give students a fresh default setup. It's also used as a quick and easy way to setup new workstations with Linux desktops for end-users. This host also supports apache web services and hosts the Ubuntu/Debian mirror on the network for the domain.

Partition 9 is a virtual machine with Solaris 10 Update 6 installed and is the headnode for the clusters. Solaris HA Cluster Tools is installed which includes sge for resource management and open-mpi for message passing.

A Second machine to serve as a replica to the first physical host is setup the exact same way as the first and features the same exact hardware. The only difference will be that the LDAP and Kerberos will be setup to propagate changes to the second machine and clients will be setup to see the second box as the authentication server if the first one doesn't respond. A remote file synchronization procedure (rsync) or some other form of replication will be setup so that the RAID5 arrays can be synchronized. This process will ensure timely backups, fault tolerance and load balancing capabilities. The plan is to eventually invoke three replica hosts, one in the main equipment room, one in another building on the same campus and one at a remote location 350 miles away. This allows for backup, high availability, load balancing, and disaster recovery.

Table 2 Details of the virtual machines

Host	Vms	CPUs	RAM	Storage	NICs	OS	Description
Host	9	4 core AMD 2.5ghz	8 GB	320mb raid1 & 1.5 TB raid5	3	UBUNTU Server – Standard Install	NTP Server, Virtual Machine host(Virtual Box), Ubuntu/Debian Mirror(apt-mirror)
	Partition 1	1	256 MB	10 GB	2	UBUNTU Server	Main Student Server. SSH login server(Firewall will forward all port22 traffic to)(Sun Java(jre,jdk), TCPDump, Hping3, portmap, dig, trace-route)
	Partition 2	1	256 MB	10 GB	2	UBUNTU Server	Secondary SSH login server as backup if partition 1 locks up (Firewall will forward alternate port to hermes2 port22)
	Partition 3	1	256 MB	10 GB	2	UBUNTU Server	LDAP/Kerberos Server (OpenLDAP/Kerberos5-mit)
	Partition 4	1	256 MB	10 GB	2	UBUNTU Server	DNS/DHCP Server (Bind9/DHCP3-Server-LDAP)
	Partition 5	1	256MB	10 GB	2	UBUNTU Server	E-Mail Server (Ubuntu Mail Server install)
	Partition 6	1	256 MB	10 GB	2	UBUNTU Server	Web Server (Apache Tomcat)
	Partition 7	1	256 MB	10 GB	2	UBUNTU Server	NFS-Kernel-Server for Home folders

	Partition 8	1	256 MB	10 GB	2	UBUNTU Server	Network Installation Server (FAI-Server)
	Partition 9	1	256 MB	16 GB	2	Solaris 10 update 6	Head Node for Clusters (HA Cluster Tools)

DISCUSSION/CONCLUSIONS

With the need to be ever more responsible in an overtaxed environment the concept of virtualization offers enormous benefits in regard to saving resources in IT operations. In this example, the number of computers required to run a production domain are reduced from 9 down to 1. Assuming the average power consumption per box at a conservative 100 watts per hour, this would be a savings of 800 watts per hour or 19.2 kilowatts per day. At 10 cents a kilowatt hour that is over $700 per year. Further, this value could be at least doubled when one considers the heat that does not need to be dissipated by air conditioning.

Further, the reduction in complexity makes it easier for system/network staff to configure and maintain the system thereby reducing personnel cost significantly. Given that personnel is the highest cost within IT this is a most positive development. Also, less hardware needs to be purchased to perform the same tasks, which means less money is needed up front to upgrade existing equipment. Specifically, [7] found that in a case study involving a six host virtualization disaster recovery case study that the virtual architecture could save $39,000 in personnel costs and over $100,000 in hardware cost when compared to a traditional hot disaster recovery model.

While there is a concern as to whether the virtualized model would be able to offer the same performance as the separate physical hosts model. It is expected that the performance will be a function of the workload distribution on each of the virtual machines. If they all are experiencing intense workloads at the same time then of course performance will suffer drastically. However, the analysis of the existing physical hosts model revealed that if intense work load did occur it typically was limited to a single host. In summary, the analysis basically indicated that workload was pretty much evenly distributed which means the 9 partitions should be able to co-exist comfortably from a performance perspective. The observations to date on the live functioning system have supported this assertion. Therefore determining the optimum number of zones that can be safely loaded into a physical host is a function of that hosts processing power and the workload distribution each virtual partition will generate. This requires detailed analysis, but a general observation is that 6-12 zones are typically reasonable. This was especially appropriate in the case study herein because the physical hosts being upgraded were 1.5GHz 32bit processors that were just moderately loaded. These 9 physical computers virtualized well into a 2.5 GHz 64bit host that actually provided even better performance than was observed in their original physical form.

Also the observations to date have verified that the isolation provided by the partitioning strategy have been effective from a security perspective. While the process of converting all physical hosts in the domain to a virtual server solution has not been completed what has been experienced to date has been entirely positive. Over the next five years the plan is to continue utilize and optimize the virtual model. Because the available physical space has been pretty much maxed, virtualization will provide an opportunity to grow without having to request additional physical space, which in today's economic times would be a most difficult request to have fulfilled.

In summary, it appears that virtualization fulfills all the hype associated with it. It definitely can save energy resources which helps the environment. While at the same time reducing IT costs in regard to hardware and personnel. It is definitely a technology worth investigating.

REFERENCES

1. Armitage, G. and Harrop, W. (2005). Teaching IP Networking Fundamentals in Resource Constrained Educational Environments, *Australasian Journal of Educational Technology*, 21(2), 263-283.

2. Barham, P. et al. (2003). Xen and the Art of Virtualization, *Proceedings of the 19th ACM Symposium on Operating Systems Principles*, 164-177. Borden, T., Hennessy, J. and Rymarczyk, J. (1989). Multiple Operating systems on One Processor Complex, *IBM systems Journal*, 28(1), 104-123.

3. Borden, T, Hennessy, J. and Rymarczyk, J. (1989). Multiple Operating Systems on One Processor, IBM Systems Journal, 28(1), 104-122.

4. Boyd, T. and Dasgupta, P. (2002). Process migration: A Generalized Approach Using a Virtual Operating System, *Proceedings of the 22nd International Conference on Distributed Computing Systems*, 385.

5. Guster, D. C., Hall, C., Herath, S., Jansen, B., & Mikluch, L. (2008, April 24). *Analysis of vulnerabilities in a global authentication system in a university based distributed processing laboratory*. Presentation at the 3rd International Conference on Information Warfare and Security, Omaha, NE.

6. Guster, D. C., McCann, B., Krzenski, K., & Lee, O. F. (2008). A cost effective, safe, and simple method to provide a disaster recovery plan to small and medium sized businesses. *Review of Business Research*. 8(4), 63-71.

7. Lee, Olivia F. Dennis C. Guster, Mark B. Schmidt, and Brandon McCann. (2009) 'Applying the scale-free degree distribution algorithm to assess communication complexity and failure points in disaster recovery models', *Journal of Information Technology Management*, In press.

8. Laureano, M., Maziero, C. and Jamhour, E. (2007). Protecting Host-based Intrusion Detectors Through Virtual Machines, *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 51(5), 1275-1283.

9. Lin, Q., et al, (2007). Grid-based Large-scale Web3D Collaborative Virtual Environment, *Proceeding of the 12th International Conference on 3D Web Technology*, 123-132.

10. Lowell, D., Saito, Y. and Samberg, E. (2004). Devirtualizable Virtual Machines Enabling General, Single Node, Online Maintenance, *Proceedings of the 11th International conference on Architectural Support for Programming Languages and Operating Systems*, 211-223.

11. Smith, J. and Nair, R. (2005). The Architecture of Virtual Machines, *Computer*, 38(5), 32-38.