Benchmarking Comparison of VMware Workstation and Sun VirtualBox OSE

Mark Revels PhD
Western Kentucky University
mark.revels@wku.edu

Mark Ciampa PhD
Western Kentucky University
mark.ciampa@wku.edu

Abstract

Virtualization is becoming increasingly popular, both for servers as well as desktop systems. Several studies have been undertaken to examine the impact that virtualization has on system performance. This study is a benchmarking comparison of desktop application performance between VMware Workstation and Sun VirtualBox OSE using WorldBench 6 benchmark stress testing, which utilizes application-based tests to gauge real-world system performance. As was expected, both virtual machines imposed a performance impact upon the systems. However, an unexpected result was that the open source Virtualbox OSE performed in an almost identical level to the commercially available and more expensive VMware Workstation product.

Introduction

Virtualization is a means of managing and presenting technology resources by function without regard to their physical layout or location. According to the International Data Corporation approximately18 percent of all new servers shipped in the fourth quarter of 2009 were virtualized. This represents an increase from 15 percent compared to the previous year (IDC), and the server virtualization market is expected to grow at a rate of 30 percent per year through 2013 (Huber, von Quast and Brosig, p. 1).

Virtualization dates back 50 years to the early 1960's (Goldberg, p. 37). This technology was initiated by IBM (Creasy, p. 485) with the development of the IBM 360/67 and was designed to take full advantage of the processing capabilities of expensive mainframe systems, which were partitioned into separate virtual machines. This configuration permitted multiple jobs to be executed concurrently as a means of leveraging the expense of the hardware. In 1974, Popek and Goldberg defined three characteristics of how virtual machines should behave. These characteristics were an equivalence property (code executed on a virtual machine must execute in an identical manner to code executing on hardware), a resource control property (the virtual machine should manage and protect all hardware resources), and an efficiency property (safe instructions should be executed without intervention of the virtual machine) (Popek and Goldberg, p. 415).

In the mid-1990's the use of inexpensive Intel x86 processors spawned a rapid proliferation of servers supporting internal as well as external or Web-based applications. In many instances a single hardware server was installed to support a single application, providing users with a continual on-demand availability of applications and IT personnel with the ability to granularly manage the server to meet demand. However, this resulted in several issues (Ciampa, p. 60):

- Wasted server utilization. Although many servers and their applications were used only during business hours the servers still ran 24/7. These servers typically only utilized about 10 percent of their capacity.
- Increased energy consumption. The proliferation of servers resulted in significant amounts of energy consumed. The cost of electricity to run servers in data centers as well as keep server rooms cool doubled between 2000 and 2006, to $4.5 billion per year (the equivalent of the electric bills for 5.8 million U.S. households). For every $1 spent on computing equipment in data centers, an additional $0.50 is spent to power and cool them (Efficiency).
- Increased data center space. The need to expand data centers to accommodate the increasing number of servers, along with the associated infrastructure requirements, forced many organizations to build out existing centers or create new data centers to accommodate the increase. This resulted in significant capital expenditures.
- Disaster recovery needs. The need to provide sufficient disaster recovery, such as asymmetric server clusters or stockpiling hard drives as spare parts, drove costs significantly higher.

To help address these issues, the virtualization of server operating systems was first made available by VMware in 1999. Using server operating system virtualization an entire operating system environment is simulated in hardware. With operating system virtualization a virtual machine (VM) is simulated as a self-contained software environment by the host system (the native operating system to the hardware) but appears as a guest system (a foreign virtual operating system). For example, a computer that normally boots to Windows 7 (the host) could run a virtual machine of Linux (the guest). Server operating system virtualization typically relies on the hypervisor, which is software that runs on a physical computer to manage one or more virtual machine operating systems.

There are several advantages to virtualizing server operating systems. Instead of purchasing one physical server to run one network operating system and its applications, a single physical server can run multiple virtual operating systems, reducing hardware costs, energy consumption, data center space, and disaster recovery expenses. Another advantage of server virtualization is that it can be beneficial in providing uninterrupted server access to users. Data centers need to have the ability to schedule planned "downtime" for servers to perform maintenance on the hardware or software. However, with the mobility and almost unlimited access needed for users, it is often difficult to find a time when users will not be inconvenienced by the downtime. This can be addressed by virtualization that supports live migration: this technology enables a virtual machine to be moved to a different physical computer with no impact to the users. The virtual machine stores its current state onto a shared storage device immediately before the migration occurs. The virtual machine is then reinstalled on another physical computer and accesses its storage with no noticeable interruption to users. Live migration can also be used for load balancing; if the demand for a service or application increases, then network managers can quickly move this high-demand virtual machine to another physical server with more RAM or CPU resources.

The major types of operating system virtualizations are summarized in Table 1.

Table 1 Operating system virtualization

Type of Virtualization	***Explanation***	***Example***
Emulation	Virtual machine simulates the complete hardware of a computer and allows an unmodified operating system version to be executed.	Microsoft Virtual PC
Paravirtualization	The virtual machine does not simulate the hardware but instead has special “hooks” that requires operating system modifications.	Xen
Full virtualization	The virtual machine partially simulates enough hardware to allow an unmodified operating system to run, but the guest operating system must be designed for the same type of central processing unit.	VMWare
Operating system-level virtualization	The host operating system kernel is used to implement the guest operating systems, so that the host can only support the same operating systems as the guest.	Linux-VServer

Today virtualization has expanded beyond servers and is significantly different from the early implementations (Rosenblum, p. 35). The major uses of virtualization besides server virtualization (multiple virtual servers running on a single physical server) are application virtualization (applications run independently of the underlying host operating system), network virtualization (combines resources on a network so they can be managed as a single entity), storage virtualization (multiple storage devices to be combined as one large storage resource), and desktop virtualization (which allows virtual desktops to be centrally managed on a server and run by the end user on a thin client computer).

Application virtualization targets the local desktop computer. Like server virtualization, local virtualizing applications can provide value in ease of management yet it can also give increased flexibility and employee mobility. Local application virtualization makes it possible to run different operating systems on a single system in order to meet the needs of different types of computing environments. As an example, an application developer may run a separate development environment on a laptop without interfering with or putting at risk personal applications such as e-mail or office software. Application virtualization can help keep the two environments separate (Open Virtualization: More Innovation Without Vendor Lock In Open Virtualization).

Local application virtualization also offers benefits to information systems educators and students. According to Lunsford by using virtualization technologies students may work with systems in ways that would otherwise be undesirable because of the threat to the stability and availability of computers in shared laboratories. As an added benefit, local application virtualization can enable a student’s changes to remain persistent between sessions so that the student can engage in extended projects and projects that build upon successive projects. This allows faculty to extend the range of topics covered in information systems courses, as well as integrate more risky, hands-on activities while allowing the host computer to remain unaffected (Lunsford).

Because security is a key element in today’s IT environment, virtualization is often examined within the lens of security. There are several security advantages to hosts running virtualization:

- The latest patches can be downloaded and run in a virtual machine to determine the impact on other software or even hardware, instead of installing the patch on a production computer and then being forced to “roll back” to the previous configuration if it does not work properly.
- Penetration testing can be performed using a simulated network environment on a computer using multiple virtual machines. One virtual machine can virtually attack another virtual machine on the same host system to determine vulnerabilities and security settings. This is possible because all of the virtual machines can be connected through a virtual network.
- Host operating system virtualization can be used for training purposes. Instead of the expense of installing an actual network for setting up defenses and creating attacks, it can be done through a virtual network.

Yet security for virtualized environments can be a concern:

- Physical security appliances are not always designed to protect virtual systems. For example, a physical firewall may not be able to inspect and filter the amount of traffic that comes from a hypervisor running multiple virtualized servers.
- Because live migration allows a virtualized server to be moved from one hypervisor to another with only one click of the mouse, the security must be in place to accommodate this transfer. Unless there is careful planning, moving virtual machines to other physical computers through live migration can leave these virtual servers unprotected.
- Not all hypervisors have the necessary security controls to keep out determined attackers. If a single hypervisor is compromised, then multiple virtual servers are at risk.
- Existing security tools, such as anti-virus, anti-spam, and IDS, were designed for single physical servers and do not always adapt well to multiple virtual machines.
- Some security tools are external physical appliances designed to protect one or more physical machines and not multiple virtual servers.
- Virtual machines must be protected from both outside networks and also from other virtual machines on the same physical computer. In a network without virtual machines, external devices such as firewalls and IDS that reside between physical servers can help prevent one physical server from infecting another physical server, yet no such physical devices exist between virtual machines.

In response to the need for protecting virtualized desktops and servers, a growing number of virtualization security tools are becoming available. Table 2 lists features found in these tools.

Table 2 Virtualization security tool features

Feature	***Description***
Basic protection	Anti-virus, firewall, and IDS features protect virtualized servers.
Restrict changes	Users cannot stop or change the configuration of a virtual machine.
Auditing	Logs can automatically be scanned to determine if any changes were made.
Compliance	Selecting a specific set of guidelines can generate 30 or more automatic hardening procedures, such as securing SNMP access and enforcing minimum password requirements.
Customization	Different security zones can be created for different virtualized servers.
Reporting	Visual maps of which guests are running on which hosts along with network traffic patterns and the amount of disk storage attached can be generated.

Several studies have undertaken to examine the impact that virtualization has on system performance. Kloster, Kristensen, and Mejlholm (Kloster, Kristensen and Mejlholm) compared hardware virtual machines with native performance in Xen. Their research indicated that processor intensive workloads yielded "near to native" performance that is often indistinguishable, yet other workloads exhibited significant overhead, such as those that exercised the shadowed page related structures and emulation of I/O devices. Wang et al. also examined Xen performance on a Linux system (Wang, Zang and Wang). Laadan and Nieh used seven "micro-benchmarks" in which each Linux process (pid, getsid, getpgid, fork, execve, shmget, and shmat) ran a system call in a loop and measured its average execution time as well as applying five different workload applications (make, hackbench, mysql, volano, and httperf) (Laadan and Nieh). Huber et al. used the Passmark PerformanceTest v7.0 1 and SPEC CPU2006 2, an industry standard CPU benchmark, in their analysis (Huber, von Quast and Brosig). Marojevic examined VMware using the SiSoftware Sandra Benchmarks (Marojevic) while Barnett and Irwin looked at VMware performance using dbench and Netperf (Barnett and Irwin). Li outlined experiences with VMware and Sun's VirtualBox yet did not perform any benchmarking (Li).

Tickoo, Iyer, Illikkah, and Newell note the challenges when benchmarking the performance of virtual machines. These challenges can be summarized in three areas: VM performance is not only dependent on its own characteristics but also dependent on any "interference" caused by the other virtual machines running on the same platform; this interference can affect the use of shared resources (core, memory capacity) that are visible to the operating system/VM and those (cache space, memory bandwidth, etc.) that are invisible because they are transparent resources managed by the hardware; and the scheduling disciplines adopted by the virtual machine monitor (Tickoo, Iyer and Illikkah, p. 1).

Design Methodology

The purpose of this study was to examine local application virtualization in a system with a relatively low amount of random access memory (RAM). Virtualized server environments typically are configured with very large amounts of RAM to accommodate virtualized environments. This large amount of memory may mask limitations imposed by the virtualized environment. In contrast, local application virtualization is typically installed on systems that are not optimized for a virtualized environment; rather, they are implemented on standardized desktop environments that may be limited in the amount of memory available. Any negative impacts of the virtualized system may then be more apparent.

This study is a benchmarking comparison of VMware Workstation and Sun VirtualBox OSE on a desktop. To determine the performance of the host machine and the virtual machines (VM), each was subjected to benchmark stress testing using WorldBench 6, which purports to use application-based tests to gauge real-world system performance. Other benchmark tools were considered including VMmark, PassMark, and others.

However, these tools were rejected for a variety of reasons: they were written by one of the VM software manufacturers, they measured low-level performance variables, or they were not considered accurate when used on VM software. In addition, as this research was used to evaluate virtual desktop software, not virtual server software, desktop application performance was of paramount importance.

The study procedure was to install and run the benchmark software on the test system and record the results of three sequential benchmark tests. Each test resulted in a Worldbench 6 performance index. These were then averaged for a final performance index for that particular test system.

The systems tested included the host hardware, Virtualbox OSE, Virtualbox CSE, and VMware Workstation, all running Windows 7. All virtual machines were installed on the same host machine, which was running Ubuntu v9.1. The host configuration for VM testing is outlined in Appendix A. Ubuntu 64-bit (v9.1) w/Gnome (2.28.1) was installed to a newly formatted hard drive. The disk was checked disk for defects and no errors were detected. Defaults were accepted during installation.

VMware Workstation Installation and Configuration

VMware 7.1.1 (build-282343) was installed on the previously described Ubuntu installation. The No Updates option was selected. The Send Anonymous System Data was set to "no". The Eclipse Directory was not used, and Eclipse C/C++ debugging set to "no". File descriptors were set at 4096, and the installation was successful.

The test VM was installed with the following options:

- Guest Operating System: Microsoft Windows 7 x86
- VM Name/Location: Default
- Disk Size: 40GB (stored as a single file)
- Hardware: Defaults
- VMware Tools installed
- No Direct 3d

Next, a copy of Windows 7 Professional (32-bit) was installed with the following options:

- Windows 7 Ver 6.1 Build 7600
- Selected "Home Network"
- No updates were applied

The resulting virtual machine Windows configuration for VMware Workstation is provided in Appendix B

Virtualbox CSE Installation and Configuration

For the installation of Virtualbox CSE, Ubuntu 64-bit (v9.1) with Gnome (2.28.1) was installed to a newly formatted hard drive. The disk was checked disk for defects and no errors were. Defaults were taken during installation, which was successful.

The Virtualbox CSE software (Version 3.0.8_OSE r53138) was successfully installed through the Ubuntu Software Center. Next, a Windows VM was created with the following characteristics:

- Operating System: Microsoft Windows
- Version: Windows 7 32-bit
- Base Memory Size: 1023MB
- Boot hard disk: Create new hard disk
- Storage Type: Fixed-size storage (40GB)
- CD/DVD Mounted
- Installed Guest Additions
- No Direct 3d

Then a copy of Windows 7 Professional (32-bit) was installed with the following options:

- Windows 7 Ver 6.1 Build 7600
- Selected Home Network
- No updates were applied

The resulting virtual machine Windows configuration for Virtualbox CSE is provided in Appendix C.

Virtualbox OSE Installation and Configuration

For the installation of Virtualbox OSE, the same process was used as for Virtualbox CSE

Results

The summary performance results are shown in Tables 3 and 4. Note that higher scores indicate better performance. The detailed performance results are listed in Appendices D and E.

Table 3 Performance Results Host Only and Linux with Virtual Box OSE

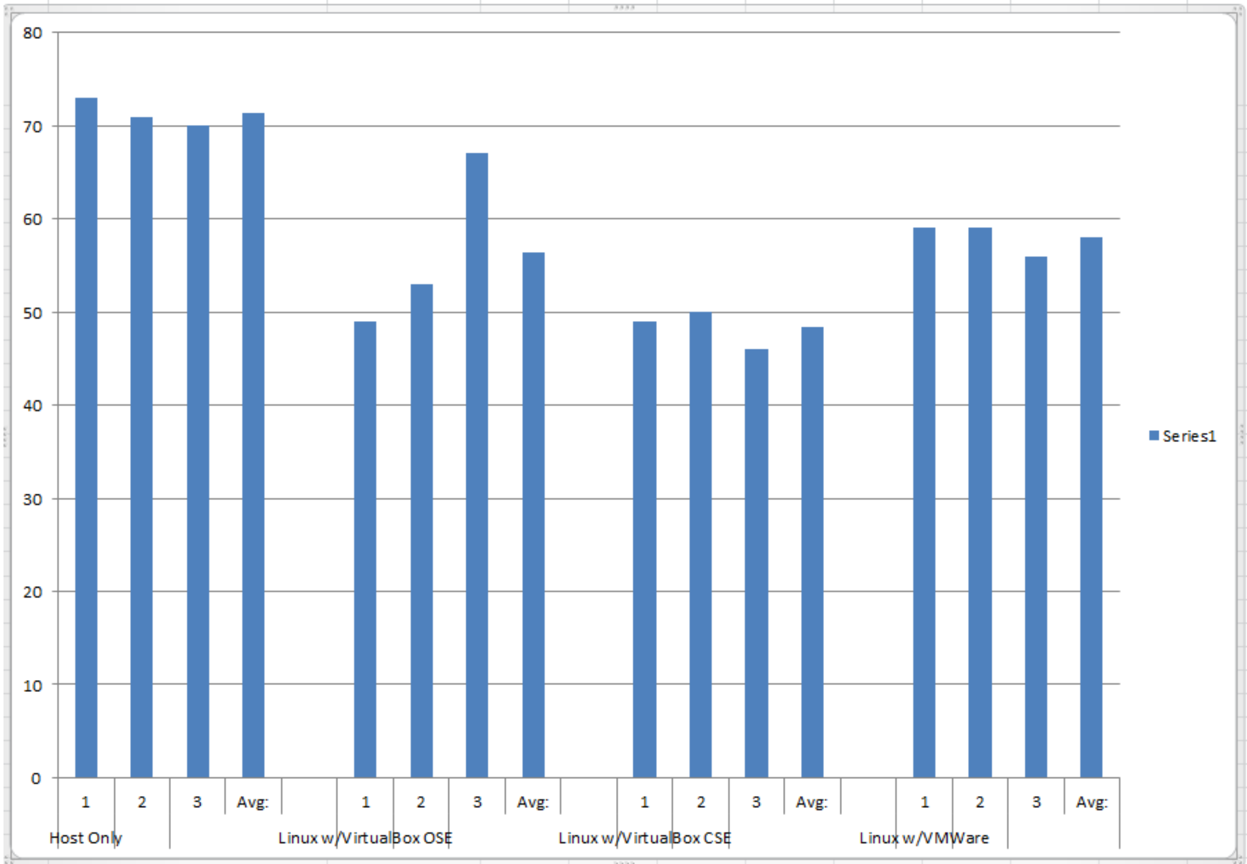
	Host Only (Test 1)	***Host Only (Test 2)***	***Host Only (Test 3)***	***Linux w/Virtual Box OSE (Test 1)***	***Linux w/Virtual Box OSE (Test 2)***	***Linux w/Virtual Box OSE (Test 3)***
WB Score	73	71	70	49	53	67

Table 4 Performance Results Linux with Virtual Box CSE and Linux with VMware

	Linux w/Virtual Box CSE (Test 1)	***Linux w/Virtual Box CSE (Test 2)***	***Linux w/Virtual Box CSE (Test 3)***	***Linux w/VMware (Test 1)***	***Linux w/VMware (Test 2)***	***Linux w/VMware (Test 3)***
WB Score	49	50	46	59	59	56

The WorkBench scores and averages are illustrated in Figure 1.

Figure 1 WorkBench scores and averages



It was anticipated that the performance of all virtual machines would be inferior to using native hardware. This expectation was validated since the average score of all VMs was 54 while the average score of the native hardware was 71. It was also anticipated that a commercial product would perform significantly better than an open source product; however, this was not the case. VMware Workstation and Virtualbox OSE performed in a similar fashion at 58 and 56, respectively. In addition, it was anticipated that Virtualbox CSE would perform better than Virtualbox OSE. Again, this was not the case as the scores were 48 and 56, respectively. However, it should be noted that for unknown reasons Worldbench 6 was not able to complete the Nero 7 Ultra Edition test on any instance of the Virtualbox CSE tests. This is likely the result of the included video driver, which caused a significant drop in performance for this test.

It should also be noted that just as the application performance between VMware Workstation and Virtualbox were similar, likewise their features are similar as well. Table 5 compares the features between the three VM versions.

Table 5 Feature Comparison

VM Version	*Feature*	*Comments*
VMware Workstation	Paravirtualization	Called ‘VMware Tools,’ allows for better mouse, video, and other I/O performance in a

		virtual environment
	Shared folders	Allows for simple file transfer between VM and host
	USB support	Supports USB 1.1 and 2.0
	Sound support	Emulates Intel AC’97 or SoundBlaster 16
	Hardware virtualization	Supports VT-X and AMD-V
	Multiple CPUs	8 CPU’s and 32gb RAM per VM
	Graphics support	Supports 3D graphics and Aero
	Desktop virtualization	‘Unity’ allows for virtualization of individual applications
	Encryption	VMs can be encrypted with 256-bit AES encryption
	Remote control	Remote control using VNC client
	Host printer	Driverless printing
Virtualbox OSE	Paravirtualization	Called ‘Guest Additions,’ allows for better mouse, video, and other I/O performance in a virtual environment
	Shared folders	Allows for simple file transfer between VM and host
	Sound support	Emulates Intel AC’97 or SoundBlaster 16
	Hardware virtualization	Supports VT-X and AMD-V
	Multiple CPUs	16 CPU’s and 16gb RAM per VM
	Graphics support	Supports 2D and 3D graphics (“experimentally”)
	Desktop virtualization	Allows for virtualization of individual applications
	Remote control	Remote control using VNC client
Virtualbox CSE	Same as OSE, but adds the following:	
	Remote Display Protocol (RDP) Server	Remote display using RDP client
	USB support	Supports USB 1.1 and 2.0
	USB over RDP	Supports remote USB using RDP

Core features such as paravirtualization, shared folders, USB support, sound support, hardware virtualization, multiple CPUs, graphics support, desktop virtualization, and remote control are similar between VMware Workstation and Virtualbox CSE. However, VMware Workstation’s addition of encryption and native printer support may be important to some users. Moreover, Virtualbox OSE lacks USB support.

Practical Implications

Generally speaking users who require desktop portability and the ability to run multiple applications on various operating systems will find all of the tested systems performed in a satisfactory fashion. While we were somewhat surprised that a commercial package did not perform significantly better in terms of speed, we also note that VMware Workstation is the most mature product, has an excellent reputation, and simply feels more ‘polished.’ However, for users with limited financial support, Virtualbox is an excellent option.

Works Cited

Barnett, R. and B. Irwin. *Performance effects of running concurrent virtual machines in VMware workstation*. Grahamstown, South Africa: Rhodes University, 2007.

Ciampa, M. *Security+ Guide to Network Security Fundamentals, 3ed*. Boston: Course Technology, 2009. Print.

Creasy, R. "The origin of the VM/370 time-sharing system." *IBM Journal of Research and Development* 25.5 (1981): 483-490.

Efficiency, IBM Energy. *IBM Systems*. n.d. Web site. 15 November 2011.

Goldberg, R. "Survey of virtual machine research." *IEEE Computer Magazine* (1974): 34-45.

Huber, N., et al. *Analysis of the performance-influencing factors of virtualization platforms*. Karlsruhe, Germany: Karlsruhe Institute of Technology, 2008.

IDC. "Virtualization market accelerates out of the recession as users adopt 'virtual first' mentality." 2010.

Kloster, J., J. Kristensen and A. Mejlholm. *A comparison of hardware virtual machines versus native performance in Zen*. Aalborg, Denmark: Department of Computer Science, Aalborg University, 2007.

Laadan, O. and J. Nieh. "Operating system virtualization: practice and experience." *SYSTOR*. Haifa, Israel: ACM, 2010. 12-24.

Li, P. "Selecting and using virtualization solutions: our experiences with VMware and VirtualBox." *Journal of Computing Sciences in Colleges* 25.3 (2010): 11-17.

Lunsford, Dale. "Virtualization technologies in information systems education." *Journal of Information Systems Education* (2009): 339-348. Document.

Marojevic, V. *Evaluating hyperthreading and VMware*. Catalonia: Polytechnic University of Catalonia, 2004.

"Open Virtualization: More Innovation Without Vendor Lock In Open Virtualization." White Paper. 2009.

Popek, G and R. Goldberg. "Formal requirements for virtualizable third generation architectures." *Communications of ACM* 17.7 (1974): 412-421.

Rosenblum, M. "The reincarnation of virtual machines." *Queue* 2.5 (2004): 34-40.

Tickoo, O., et al. *Modeling virtual machine performance: challenges and approaches*. Santa Cruz, CA: Intel, 2010.

Wang, X., et al. "Selective hardware/software memory virtualization." *VEE*. Newport Beach, CA: ACM, 2011. 30-40.

Appendix A - Host Configuration for VM Testing

The host hardware was a Dell Optiplex 745, and was configured as follows:

- CPU Manufacturer: GenuineIntel
- Number of CPU: 1
- Cores per CPU: 1 (Note that one core was disabled for consistent comparison with the single core VMs)
- CPU Type: Intel Core2 6400 @ 2.13GHz
- CPU Speed: 2130.9 MHz
- Cache size: 2048KB
- O/S: Windows 7 (32-bit)
- Total RAM: 1013 MB
- Available RAM: 661 MB
- Video settings: 1024x768x32
- Video driver: Standard VGA Graphics Adapter

Appendix B – Virtual Machine Windows Configuration for VMware Workstation

- CPU Manufacturer: GenuineIntel
- Number of CPU: 1
- Cores per CPU: 1
- CPU Type: Intel Core2 6400 @ 2.13GHz
- CPU Speed: 2545.5 MHz
- Cache size: 2048KB
- O/S: Windows 7 (32-bit)
- Total RAM: 1023.5MB
- Available RAM: 542.8MB
- Video settings: 1024x768x32
- Video: Standard VGA Graphics Adapter
- BIOS: 2.0
- Total Disk Space: 39.9GB
- Cluster Size: 4.0 KB
- File system: NTFS

Appendix C – Virtual Machine Windows Configuration for Virtualbox CSE

- System information: This Computer
- CPU Manufacturer: GenuineIntel
- Number of CPU: 1
- Cores per CPU: 1
- CPU Type: Intel Core2 6400 @ 2.13GHz
- CPU Speed: 3470.3 MHz
- Cache size: Unknown
- O/S: Windows 7 (32-bit)
- Total RAM: 1022.6MB
- Available RAM: 686.0MB
- Video settings: 1024x768x32
- Video driver: VirtualBox Graphics Adapter
- Total Disk Space: 39.9 GB
- Cluster Size: 4.0 KB
- File system: NTFS

Appendix D - Performance Results Host Only and Linux with Virtual Box OSE

	Host Only (Test 1)	***Host Only (Test 2)***	***Host Only (Test 3)***	***Linux w/Virtual Box OSE (Test 1)***	***Linux w/Virtual Box OSE (Test 2)***	***Linux w/Virtual Box OSE (Test 3)***
WB Score	73	71	70	49	53	67
Adobe Photoshop CS2	602	599	609	873	885	939
Autodesk 3ds max 8.0 SP-3 (Direct X)	477	401	778	512	586	508
Autodesk 3ds max 8.0 SP-3 (Rendering)	1487	1702	1502	1701	1846	2176
Firefox 2	361	387	380	744	527	585
Microsoft Office 2003 SP1	356	389	370	557	470	477
Microsoft Windows Media Encoder 9.0	363	361	364	429	432	429
Multitasking: Firefox & Windows Media Encoder	666	669	665	1090	849	903
Nero 7 Ultra	463	464	459	988	971	1028
Roxio VideoWave Movie Creator	309	307	307	350	347	348
WinZip Computing 10.0	349	347	344	583	583	639

Appendix E - Performance Results Linux with Virtual Box CSE and Linux with VMware

	Linux w/Virtual Box CSE (Test 1)	***Linux w/Virtual Box CSE (Test 2)***	***Linux w/Virtual Box CSE (Test 3)***	***Linux w/VMware (Test 1)***	***Linux w/VMware (Test 2)***	***Linux w/VMware (Test 3)***
WB Score	49	50	46	59	59	56
Adobe Photoshop CS2	731	735	747	667	666	684
Autodesk 3ds max 8.0 SP-3 (Direct X)	1359	622	2740	557	423	700
Autodesk 3ds max 8.0 SP-3 (Rendering)	1555	1781	1505	1517	1783	1529
Firefox 2	573	577	577	635	610	628
Microsoft Office 2003 SP1	772	459	436	469	471	492
Microsoft Windows Media Encoder 9.0	438	437	436	379	439	397
Multitasking: Firefox & Windows Media Encoder	946	953	947	744	769	757
Nero 7 Ultra	0	0	0	596	646	652
Roxio VideoWave Movie Creator	356	346	360	354	349	370
WinZip Computing 10.0	509	505	503	428	405	419