

Performances of Virtualization in Design of Fully Collapsed Demilitarized Zone

Suad Kasapovic
Faculty of Electrical
Engineering
Franjevska 2, 75000
Tuzla, Bosnia and
Herzegovina

Esmir Biberkic
Faculty of Electrical
Engineering
Franjevska 2, 75000
Tuzla, Bosnia and
Herzegovina

Lejla Banjanovic-
Mehmedovic
Faculty of Electrical
Engineering
Franjevska 2
Tuzla, Bosnia and
Herzegovina

ABSTRACT

In this article are presented the different ways of virtualization computing resources and advantages and disadvantages of using the virtualization technology. Different designs of the demilitarized zone that can be applied by using the VMware ESX hypervisor are being explained. Different ways to ensure high availability for IT services, using VMware ESX hypervisor are presented and evaluated the virtualized server models. Special focus was on measuring the impact that virtualization has on data center design. This article evaluates performance of virtualized versus physical servers. In the article have presented evaluation based on workloads to compare several key parameters. Results of evaluation confirm that server virtualization technique has good performance and proposed model can save the investment and increasing service performance.

Keywords

Virtualization, fully collapsed demilitarized zone design, VMware ESXi.

1. INTRODUCTION

The business of midsize and the large companies are increasingly linked to several geographic locations (e.g. separate offices or multiple data centers). Maintenance and management of ICT infrastructure, in such companies, is becoming more complex, more expensive and less effective. The rapid development of technology forces companies to follow the trends in ICT. Following the trends, in many cases, produces accumulation of equipment and this produces that each application gets a separate physical server for which it is necessary to provide space, power, network connectivity, licenses, backups, staff for its maintenance, etc. Increased number of devices, increases the operating costs of the company (growing space requirements in the data centers, the electricity demand grows, increases the number of staff to maintain the whole system). Dynamics of business makes companies to have their services available to clients 24/7. In addition to this requirement, it is necessary to provide the ability to create data backups and control of resources, protection of data from unauthorized access, implemented business continuity and disaster recovery solutions. Managers of data centers have a responsibility to select right technology for IT infrastructure to meet all business and economic requirements. Therefore, the problems that exist in terms of ICT infrastructure are problems of ensuring high availability service (24/7), the ability to create a backup, the possibility of centralized management and control of ICT resources, the possibility of implementing business continuity and disaster recovery solutions. In addition to the technical requirements there are business requirements related to the reduction of

costs related to the management of the entire system, power consumption, space requirements and so on. In this paper is shown one way to respond to the business requirements that are being presented to the ICT. Technologies of server virtualization in data centers have experienced a huge improvement in the last ten years. Managers of data centers use virtualization technology to improve utilization of physical servers and increased flexibility in terms of developing applications. Server virtualization technologies enable efficient use of server resources, increase application availability and simplify management of resources and the infrastructure [1]. The term "Fully Collapsed" was created and it represents a way of organizing the delivery of ICT services by using virtualization of servers and computer networks. The physical servers are converted in to the virtual machines and they run as virtual machines on physical servers. This allows for better use of resources, it is possible to use less physical servers, needs for space are reduced and power supply, it is possible to implement business continuity and disaster recovery solutions and all of this is done to reach the goal of reaching 24/7 availability of services. The average utilization of an x86 server is generally around 10% to 15% of its capacity [2].

After introduction, in the Section 2 is shown review of use virtualization technology. The difference between the various hypervisors and fully collapsed design demilitarized zone with VMware ESXi hypervisor is presented in the Section 3. The performance of virtual and physical machines in some variety test scenarios are shown in the Section 4.

2. VIRTUALIZATION

Virtualization is the pooling and sharing of technological resources, including servers, storage and networking. With the help of virtualization, resources can be dynamically arranged within the organization. Within the virtualization environment, the logical functions of servers, data storage systems and network equipment, separate from their physical location. This allows the allocation of elements of such a system (manual or automatic) to be carried out exactly according to the needs of the environment in which the system operates. This operation contributes to the large savings, environmental awareness, and provides a fully adaptable work infrastructure. Another advantage of this mode is multiple utilization of shared resources and a focusing of resources according to current tasks of the system [2]. Server virtualization creates a virtual environment that allows multiple applications or servers to run on a single physical device such that each application or server has a special physical condition [3]. There are many different virtualization technologies that are available today and the choice of technology depends on the goals of the system. The main

difference between the virtualization technologies are in the degree of flexibility and performance. The flexibility of virtualization is reflected in the independence of the operating system and hardware. Flexibility is the result of how really a virtual machine is separate from the hardware [1]. As shown in Figure 1., various technologies allow various levels of flexibility and performance.

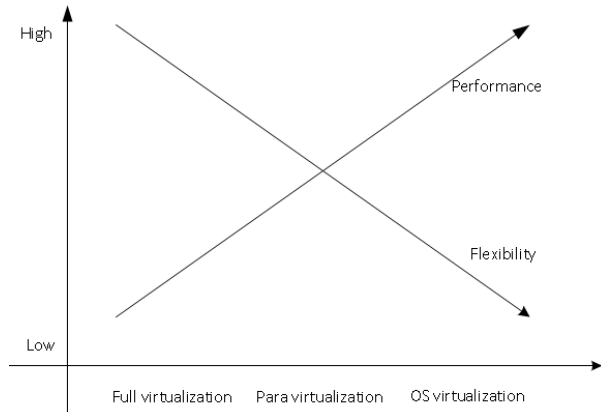


Figure 1. Review the performance due to the use of different virtualization technologies

The concept of virtualization has several strengths that can be used in high availability clusters. Some of the benefits of using virtualization are flexibility, availability, scalability, security. The disadvantages of using the virtualization are performance, single point of failure and administration (requires advanced knowledge to administer the entire system). Using virtualization is difficult to guarantee QoS for services that run on the virtual machines. This is one reason why data center managers do not decide to virtualize certain services and run them on the physical servers. The differences in performance between physical and virtual servers are not negligible.

3. FULLY COLLAPSED DESIGN WITH VMWARE ESXI HYPERVISOR

In the market of virtualization hypervisors, there are several companies producing software that enables server virtualization. These are companies like Microsoft, VMware, Citrix, Parallels, Red Hat, etc. The choice of platform on which server virtualization will be based is not simple, and it includes an analysis of the prices of licenses, number of hours to be spent in the administration of the system, enabling them to perform various operating systems, the use of different virtualization technologies, compatibility with other hardware manufacturers, the resulting performance of the entire system and the customer support from the hypervisor manufacturer. About 70% of total number of servers installed today is being virtualized, which speaks about the importance of choice for virtualization hypervisor [3], [9]. According to analysis of Gartner, Hyper-V and VMware ESXi are leaders in the x86 server virtualization. In terms of supported operating systems (in recent versions of the hypervisor), VMware supports 95 different operating systems, while Microsoft supports 29 different operating systems. From May 2012 to April 2013 Microsoft released 27 security patches for the Hyper-V, while

VMware has not released any patch. In terms of system administration (for example, adding a new host) it is possible to see the difference between how much time is required to perform such operations with VMware and Microsoft solution. By analyzing the data in Table 1., it can be seen that using the VMware requires 78% less time to add a new host to the cluster than using the Microsoft's hypervisor solution

Table 1. Times, in hours: minutes: seconds, to complete the tasks relating to provisioning new hosts

Microsoft Windows Server 2008 R2 SP1 Hyper-V solution		VMware vSphere 5 solution	
Task	Time	Task	Time
Enter license and log into the domain.	0:00:45	Click Apply Host Profile.	0:00:05
Connect LUNs via iSCSI Initiator.	0:01:44	Answer profile questions.	0:01:03
Bring disks online via Disk management.	0:00:36	Waiting until host is configured and ready.	0:01:45
Create four new virtual networks for Hyper-V	0:02:12		
Join host to the cluster	0:02:04		
Total	0:07:21	Total	0:02:53

It can be said that the hypervisor is the "brain" of each virtualization environment [4]. VMware vSphere ESXi 6 (at time of writing) is the latest version of the virtualization software. Figure 2. shows the difference between the classical Intel architecture and VMware vSphere ESXi Server hypervisor installed on Intel architecture. The figure shows that VMware presents individual virtual hardware to each virtual machine. In this way, the operating system and applications installed on a virtual machine, do not know the background of virtual hardware. VMware vSphere includes components such as VMware vSphere Fault Tolerance, VMware vSphere vMotion, VMware vSphere High Availability, vSphere Replication etc. These components can be used to ensure high availability of services, to implement a business continuity and disaster recovery solutions. Fault tolerance solutions in the past were based on redundancy. For physical servers it meant to have redundant hardware. Fault Tolerance protection is done at the level of the hypervisor and it provides continuous availability and protection of virtual machines from the errors on the host. In the event that an error occurs at the host, there will be no need to restart the virtual machines (which are protected with Fault Tolerance) that are located on the host. With the help of Fault Tolerance technology, virtual machines will continue to run in the cluster on the host which has sufficient resources. VMware vMotion technology is developed by VMware and it allows the virtual machines to migrate from one host to another without interruption of service availability. This technology makes it possible to achieve a balance in the work environment and prevents the occurrence of disasters.

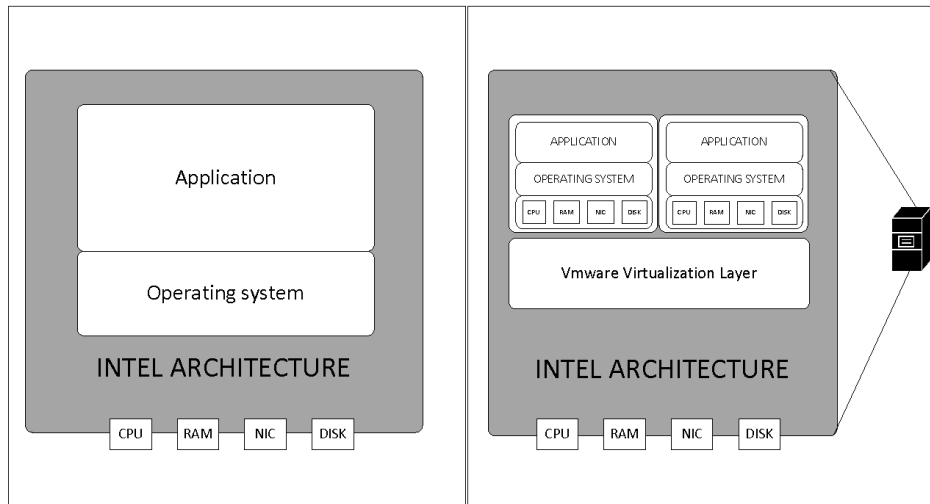


Figure 2. A comparison between the traditional architecture of Intel and VMware vSphere ESXi Server

In the event that an error occurs at the host VMware vSphere High Availability technology will restart the virtual machine (for machines where High Availability is turned on) on another physical server that has sufficient resources. This technology helps to prevent the disaster [5]. In order to take advantage of virtualization it is necessary to choose the appropriate design of server and network infrastructure. With the use of virtualization technologies, the design of the entire computer system (including the DMZ (Demilitarized Zone))

as a part of it, needs not to be significantly changed. For example, design of a computer system which has the DMZ and that does not include virtualization techniques is given in the Figure 3. This is an example where all devices are physical devices. Virtualization technology makes it possible to do server consolidation and replace the physical servers with the virtual ones. In doing so, their functionality is not changed and process of their configuration is not being more complicated.

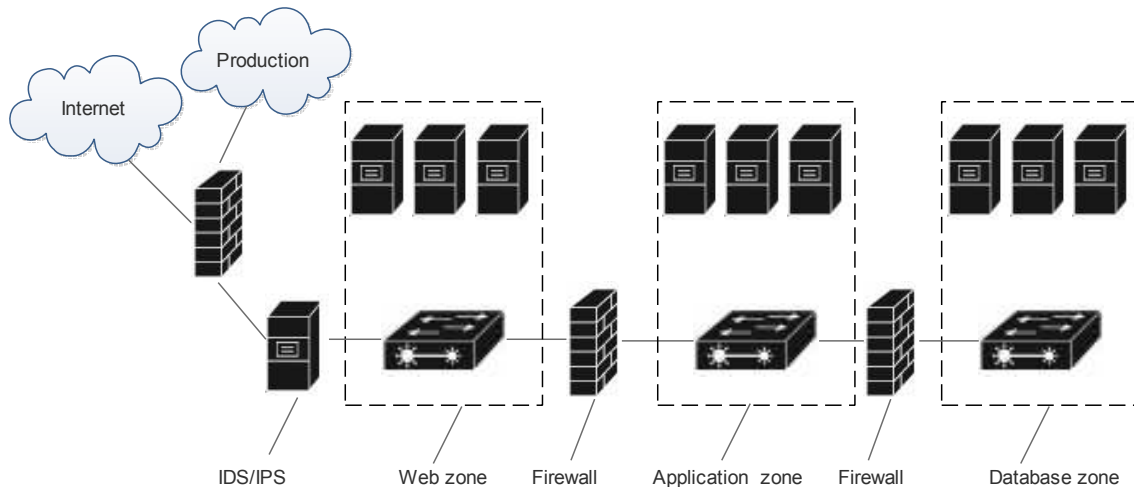


Figure 3. The typical DMZ configuration with the physical equipment

Consolidation of servers in the DMZ can be made (and in all other security zones) using virtualization technology (relying on existing security infrastructure) [6]. Three Typical Virtualized DMZ Configurations: partially collapsed DMZ with separate physical trust zones, partially collapsed DMZ with virtual separation of trust zones and fully collapsed DMZ. Approach shown in Figure 4. includes all the benefits

of virtualization and VMware technologies. This way virtualization of the entire DMZ is done (and all other security zones), including network and security devices. Sometimes, this design is described as "DMZ in a box". This approach enables the maximization of server consolidation and it is possible to achieve significant savings (reducing the number of physical devices, requirements for space, power

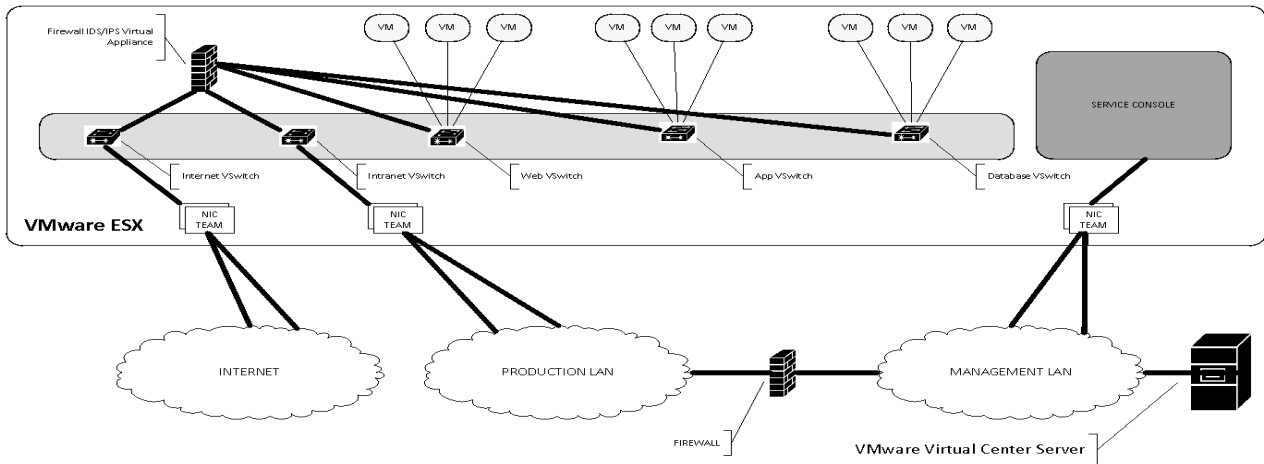


Figure 4. Fully Collapsed DMZ

consumption, enables centralized resources management) [6]. This design of DMZ relies entirely on the benefits of consolidation. All servers and devices that are used for network security are virtualized. Isolation of virtual servers and networks, and their communication is accomplished using the virtual devices. It is possible that security devices cannot fully exploit the possibilities of VMware technology such as VMware VMotion and VMware Distributed Resource Scheduler because of limitations in these devices. VMware VMsafe technology will remove these limitations in future. This completely virtual infrastructure can fully implement isolation and security between the DMZ security zones. It is possible to have virtual servers, which are located on one physical server, in different security zones [6]. This design does not exclude the potential risks that exist when using only physical devices. With the following the best practices for the configuration of applications and the equipment these risks can be reduced. Compared to other approaches of DMZ design, this design is the most complex and for its implementation and maintenance are required advanced knowledge related to virtualization technology. The risks associated with the misconfiguration in configuring the equipment are the higher in the “Fully collapsed” design of the demilitarized zone. It is important to design a virtual network in such manner so that there is isolation between them, and communication between the networks can be achieved only through firewalls or other devices that can filter traffic [7]. It is important to properly configure virtual firewalls and virtual switches. These devices are responsible for implementing security policies in the network. It is possible to use 802.1 VLANs in this configuration, but they are not required as is the case in the use of partially collapsed design of DMZ. In case of using a fully collapsed designs DMZ host must have a minimum three network cards - one is connected to the Internet, a second to the internal network and the third for the ESXi management console. VMware strongly recommends that you use several network cards (NIC teaming) in order to obtain redundancy [8], [9], [10]. Benefits: fully utilization of resources, replace the physical devices with virtual, lower cost of implementation and management of the entire system from one management console. Disadvantages: complexity, risk of misconfiguration, it is necessary to do frequent reviews of configuration and loss of functionality such as VMotion if current virtual security appliances are not properly configured and audited. Fully collapsed design allows reducing the number of physical servers and other network devices (switches, firewalls, routers). The physical switches are replaced with the virtual switches in hypervisor.

Virtual switches don't have all mechanisms implemented that physical switches have (e.g., port mirroring, multicast, virtual switches have limited security mechanisms to protect the network) [5]. Fully collapsed design allows meeting the targets set for the ICT infrastructure (high availability of services, possibility of implementing business continuity and disaster recovery solutions, control and centralized management of resources). It is possible to achieve savings in physical space, consumed energy and the amount of physical equipment. This design involves the use of five different virtual switches for different security zones (Database zone, Application zone, Web zone, Intranet zone and Internet zone). Physical server network cards would be terminated in three different security zones on the physical switch: Internet, Production and Management. Communication between virtual servers that are located in different security zones is achieved with the help of virtual firewalls. This approach increases the level of safety for the services.

4. PERFORMANCE OF VIRTUALIZATION

The difference in performance can be seen best by running various tests on physical and virtual servers. To test the performance of various installations we used software tools SiSoftware Sandra 2014 Lite and Iperf. Tests are made with the VMware ESXi 5.1 hypervisor. Each individual test is run three times. Results presented in this paper are mean value of three launched test. The first test was carried out on a physical machine that has the characteristics shown in Table 2. On this physical machine was installed Microsoft Windows Server 2012 R2. For this measurement diagrams shown with the label "Microsoft Windows Server 2012 R2, physical".

Table 2. The physical characteristics of the server

Processor	Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz (4C 2.68GHz, 2x 3MB L2)
RAM	4GB DIMM DDR2
Hard Drive	WDC WD1600AAJS-00B4A0 (160GB,SATA150, 3.5", 7200rpm, 8MB Cache)
Network Card	Realtek PCIe GBE Family Controller

The second performance measurement included performance measurement when Microsoft Windows Server 2012 R2 is installed on the VMware ESXi 5.1 hypervisor. The hypervisor is installed on an identical machine as in the first scenario. For

this measurement diagram is shown with the "Microsoft Windows Server 2012 R2, virtual, single". The characteristics of virtual machines are shown in Table 3.

Table 3. Characteristics of Microsoft server 2012 R2 virtual machine

Processor	Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz (4C 2.68GHz, 3MB L2)
RAM	4GB DIMM DDR2
Hard Drive	40GB (NTFS) @ VMware Virtual disk (43GB, SASCSI, SCSI-2, 7200rpm)
Network Card	Intel(R) 82574L Gigabit Network Connection (Ethernet, 1Gbps)

The third measurement is done when a hypervisor executed two virtual machines. Second machine was running only Microsoft Windows 7 Service Pack 1 x86-based operating system that had only basic services running (clean installation). On the charts, that measurement is shown with the "Microsoft Windows Server 2012 R2, virtual, 2vms". Characteristics of Windows 7 virtual machines are shown in Table 4.

Table 4. Characteristics of Microsoft Windows 7 virtual machine

Processor	Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz (2C 2.68GHz, 3MB L2)
RAM	4GB DIMM DDR2
Hard Drive	34GB (NTFS) @ VMware Virtual disk (79.9GB, SASCSI, SCSI-2, 7200rpm)
Network Card	Intel(R) 82574L Gigabit Network Connection (Ethernet, 1Gbps)

The fourth test shows a performance of Windows Server 2012 R2 operating system when it is executed in parallel with Microsoft Windows 7 Service Pack 1 x86-based operating system that is also loaded (running performance tests on both virtual machines at the same time). For this test, there is a diagram shown with the "Microsoft Windows Server 2012 R2, virtual, 2vms @ 100%".

Fifth test shows performance of virtual machines when virtual machine has lower performance (characteristics are shown in Table 5.) In this case the amount of memory is reduced, instead of 4 GB, 1 GB of RAM is allocated, and number of processor cores is reduced from four to two. The diagram of this measurement is shown with the "Microsoft Windows Server2012 R2, virtual, 2CPU, 1 GB."

Table 5. Characteristics of virtual machine

Processor	Intel(R) Core(TM)2 Quad CPU Q9400 @ 2.66GHz (2C 2.68GHz, 3MB L2)
RAM	1GB DIMM DDR2
Hard Drive	40GB (NTFS) @ VMware Virtual disk (43GB, SASCSI, SCSI-2, 7200rpm)
Network Card	Intel(R) 82574L Gigabit Network Connection (Ethernet, 1Gbps)

4.1 Processor multi-core efficiency

This test is designed to measure the effectiveness of various multi-core processors, with different architectures. This test does not measure the computing performance of different multi-core processors, but only shows how well connected are different cores. As shown in Figure 5., this test showed that much more bandwidth between the processor cores is achieved when there is no virtualization.

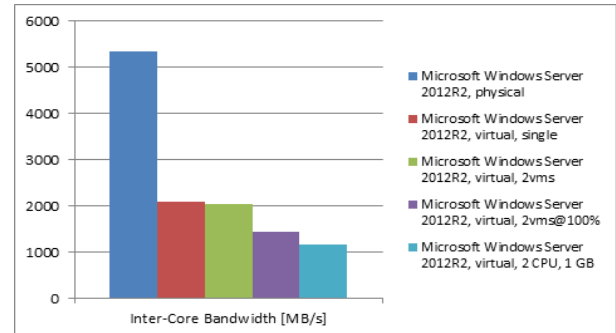


Figure 5. Processor multi-core efficiency

Much better results are for the case when Windows Server when it is not loaded with multiple virtual machines. 2012 R2 is installed directly on the physical machine. It is possible to see the difference in performance in the case where the hypervisor is loaded and

4.2 Processor multi-media test

This benchmark generates a picture (640x480) of the well-known Mandelbrot fractal, using 255 iterations for each data pixel, in 32 colours. It is a real-life benchmark rather than a synthetic benchmark, designed to show the improvements that MMX/Enhanced, 3DNow!/Enhanced, SSE(2) bring to such algorithm[13].

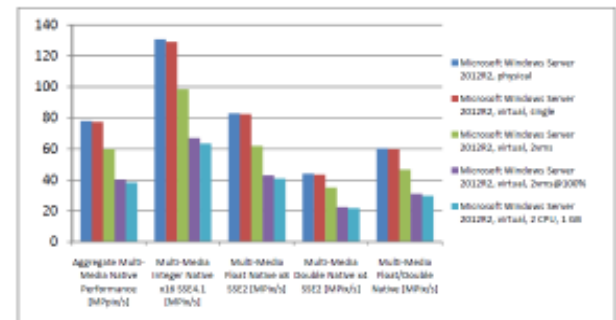


Figure 6. Overview of multimedia performance in various scenarios testing

For the multimedia content processing, there is minimal difference between Windows Server 2012 R2 operating system installed directly on a physical machine and the hypervisor (in the case of the hypervisor, there is only one virtual machine running). In this example it is possible to see how the allocation of an appropriate number of processor cores to the virtual machine may affect performance. As shown in Figure 6., when the hypervisor is loaded, performance of virtual machines are significantly reduced.

4.3 CPU Arithmetic Performance Benchmark

The Whetstone benchmark is widely used in the computer industry as a measure of FPU or Co-Processor performance. Floating-point arithmetic is most significant in programs that require a Co-Processor. These are mostly scientific, engineering, statistical and computer-aided design programs. The Whetstone benchmark used here is a multi-threaded, 32/64-bit variant of the original one which runs under UNIX. Up to 64 CPUs in SMP systems are supported. The result is determined by measuring the time it takes to perform some sequences of floating-point instructions. Due to various changes, the result is not directly comparable with other Whetstone benchmarks. However, the MFLOPS (Million

Floating Operations per Second) should be the same for the same system (+5-10% variation) between benchmarks [13]. As shown in Figure 7., for the execution of various calculations there is a minimal difference between installing Windows Server 2012 R2 operating system directly on a physical machine and the hypervisor. Also, there is a possibility to see how the assignment of an adequate number of cores to virtual machine can affect performance. It is important to note that the performance of virtual machine may vary depending on the load of ESXi server. Quality of service (QoS) is very difficult to provide in the virtual environment. Due to this fact the services that require a high quality of service are not advisable to run in a virtual environment.

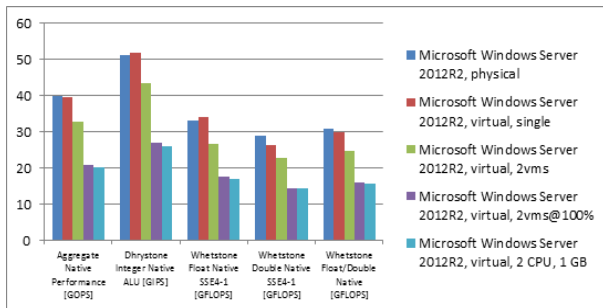


Figure 7. Arithmetic Performance

4.4 Network performance

To check network performance, we have used Iperf tool. Measurements included network performance between physical machines and virtual machines, between two different physical machines and two different virtual machines on the same server. As a network switch was used HP 2520-8-PoE Switch (J9137A). Based on these results (shown in Figure 8.) we can conclude that virtualization does not reduce the network performance (there is no lower bandwidth between different entities in virtual environment). In this case, a much greater bandwidth is possible to have between virtual machines stored on a same server, than between two physical machines. Therefore, you need to plan where you will locate the virtual machines. Otherwise, there is unnecessary load of other network equipment.

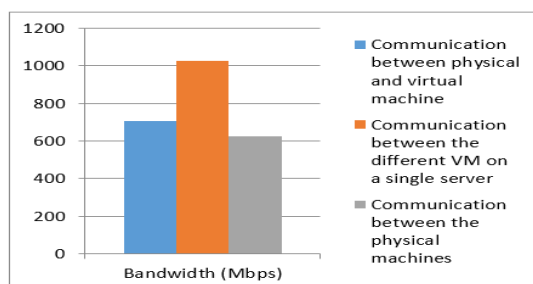


Figure 8. Network performance

5. CONCLUSIONS

Based on the theoretical analysis of the data center, different ways of design of the data center and various performance

tests for medium and large companies “Fully Collapsed” design is the most cost-effective and allows the use of all the benefits of using virtualization technologies. With a “Fully Collapsed” design of the data center it is possible to have a smaller number of physical switches and physical servers than any other design. System security is achieved by separation of security zones with the help of physical switches, or in the case of using a “Fully Collapsed” design, with the help of virtual switches on the server and Virtual local area networks on the physical switch. Performance in case of choosing “Fully Collapsed” design can be lower in the relation to the design with the physical servers. In case that the operation of applications performance is very important, and predictability of performance is important, this application should not be placed on virtualized servers.

6. REFERENCES

- [1] Espen Braastad, “Management of high availability services using virtualization”, University of Oslo, Department of Informatics, 2006.
- [2] Will Schmied, Damiano Imperatore, Dr. Thomas W. Shinder, Robert J. Shimonski, Victor Chang, Drew Simonis, "The Business Value of Virtualization", Syngress Publishing, Inc., 2003.
- [3] “Magic Quadrant for x86 Server Virtualization Infrastructure” <http://www.gartner.com/technology/reprints.do?id=1-1WR7CAC&ct=140703&st=sb>, May, 2015.
- [4] Vjekoslav Dalic, “Analiza uvođenja virtualne infrastrukture te studija isplativosti implementacije unutar obrazovnih ustanova”, Sveučilišta u Zagrebu, Fakulteta organizacije Informatike u Varaždinu, 2009.
- [5] “VMware vSphere® High Availability 5.0 Deployment Best Practices”, Technical MarketinDocumentation, Updated January 2013.
- [6] Michael A. Bell, „Use Best Practices to Design Data Center Facilities“, Gartner, 2005.
- [7] Marshall, Beaver, McCarty: "VMware ESX: Essentials in the Virtual Dana Center", CRCPress, 2009.
- [8] Marian Friedman Michele Girola Mark Lewis Alessio M. Tarenzio “IBM Data Center Networking Planning for Virtualization and Cloud Computing”, IBM International TechnicalSupport Organization, 2011.
- [9] Richard Kelley, Scheila Rossana Rinaldo Maliska, Leandro Torolho, Michael Voigt, Jon Tate”, IBM SAN Solution DesignBest Practices for VMware vSphere ESXi” IBM International Technical Support Organization, 2013.
- [10] “VMware Virtual Networking Concepts”, http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf, May, 2015