A MINI PROJECT REPORT
on

Application Performance Isolation in Cloud

Submitted by

Varun Khandelwal (161500609)
Kartik Sharma (161500259)
Shivam Arora(161500516)
Muqeet Zama Khan (161500333)

To
Mr. Ambrish Gangal

Department of Computer Engineering & Applications
Institute of Engineering & Technology

GLA University
Mathura- 281406, INDIA
April, 2019

Department of Computer Engineering and Applications
GLA University, Mathura
17 km. Stone NH#2, Mathura-Delhi Road, P.O. – Chaumuha,
Mathura – 281406

DECLARATION

We hereby declare that the work which is being presented in the Mini Project **"Application Performance Isolation In Cloud",** in partial fulfillment of the requirements for Mini-Project LAB, is an authentic record of our own work carried under the supervision of **Mr. Ambrish Gangal, Assistant Professor, GLA University, Mathura**.

Varun Khandelwal

Kartik Sharma

Shivam Arora

Muqeet Zama Khan

Department of Computer Engineering and Applications
GLA University, Mathura
17 km. Stone NH#2, Mathura-Delhi Road, P.O. – Chaumuha,
Mathura – 281406

CERTIFICATE

This is to certify that the project entitled **"Application Performance Isolation In Cloud"** carried out in Mini Project – II Lab is a bona fide work done by **Varun Khandelwal (161500609), Kartik Sharma (161500259), Shivam Arora (161500516), Muqeet Zama Khan(161500333)** and is submitted in partial fulfillment of the requirements for the award of the degree Bachelor of Technology (Computer Science & Engineering).

_____

Signature of Supervisor:

Name of Supervisor: Mr. Ambrish Gangal

Date:

Department of Computer Engineering and Applications
GLA University, Mathura
17 km. Stone NH#2, Mathura-Delhi Road, P.O. – Chaumuha,
Mathura – 281406

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the report of the B. Tech Mini Project undertaken during B. Tech. Third Year. This project in itself is an acknowledgement to the inspiration, drive and technical assistance contributed to it by many individuals. This project would never have seen the light of the day without the help and guidance that we have received.

Our heartiest thanks to **Dr. (Prof). Anand Singh Jalal,** Head of Dept., Department of CEA for providing us with an encouraging platform to develop this project, which thus helped us in shaping our abilities towards a constructive goal.

We owe special debt of gratitude to **Mr. Amrish Gangal,** Assistant Professor Department of CEA, for his constant support and guidance throughout the course of our work. His sincerity, thoroughness and perseverance have been a constant source of inspiration for us. He has showered us with all his extensively experienced ideas and insightful comments at virtually all stages of the project & has also taught us about the latest industry-oriented technologies.

We also do not like to miss the opportunity to acknowledge the contribution of all faculty members of the department for their kind guidance and cooperation during the development of our project. Last but not the least, we acknowledge our friends for their contribution in the completion of the project.

Varun Khandelwal

Kartik Sharma

Shivam Arora

Muqeet Zama Khan

Department of Computer Engineering and Applications
GLA University, Mathura
17 km. Stone NH#2, Mathura-Delhi Road, P.O. – Chaumuha,
Mathura – 281406

ABSTRACT

Performance isolation is the desirable thing in virtual machine based infrastructure to meet Service Level Objectives. Many experiments in this area measure the performance of applications while running the applications in different domains, which gives an insight into the problem of isolation. we run different

kind of benchmarks simultaneously in virtual environment to evaluate the isolation strategy provided by the hypervisor.

Application Type:
Cloud Computing
Virtualization

Targeted Hypervisor used:
VmWare Workstation

Table of Contents

Chapter 1. Introduction

1.1 Motivation and Overview

Analyzing the performance of applications running in different domains using several benchmarking parameters and evaluating the isolation strategy provided by hypervisor.

Modern data centers use virtual machine based implementation for numerous advantages like resource isolation, hardware utilization, security and easy management. Applications are generally hosted on different virtual machines on a same physical machine. Virtual machine monitor like VmWare is a popular tool to manage virtual machines by scheduling them to use resources such as CPU, memory and network. Performance isolation is the desirable thing in virtual machine based infrastructure to meet Service Level Objectives.

1.2 Objective

Benchmark the performance of the different applications running in different domains using standard benchmarking tools considering the different parameters like CPU, Network and Disk Utilization. We use hypervisor and compare the performance of applications how they behave differently for above mentioned parameters.

Our targeted Hypervisors are:-

- VmWare Workstation (Free Version).

Chapter 2: Software Requirement Analysis

2.1 Problem Statement

Virtualization is nowadays very hot topic. Most of the big market service providers are already enjoying the benefits of this technology. While the other are thinking to use it. As there are number of vendors available in the market and therefore, it needs to make detailed study about which technology is better than the other for a specific setting that suit to an organization.

Modern data centers use virtual machine based implementation for numerous advantages like resource isolation, hardware utilization, security and easy management. Applications are generally hosted on different virtual machines on a same physical machine. Virtual machine monitor like Xen is a popular tool to manage virtual machines by scheduling them to use resources such as CPU, memory and network. Performance isolation is the desirable thing in virtual machine based infrastructure to meet Service Level Objectives. Many experiments in this area measure the performance of applications while running the applications in different domains, which gives an insight into the problem of isolation.

Data centers which host these virtual machines on their physical machines follow Service Level Agreements (SLAs), which specifies the service requirements with different constraints and parameters to be fulfilled by service provider or cloud provider . These constraints and parameters include total uptime and downtime, requirement of CPUs, network bandwidth and disk space. While running more than one virtual machine on a single physical server, virtual machine scheduler is responsible for allocating resources as defined by SLAs. This allocation also includes a most demanding and inherent property which is referred as isolation among virtual machines. Isolation is meant for securing and providing the resources to a virtual machine which is co-hosted with other virtual machines on a single physical server. These resources are CPU share, network share, memory share and disk share to each virtual machine. Thus isolation property is forbidding a misbehaving virtual machine to consume other virtual machine resources and providing fairness according to their shares.

2.2 System Hardware and Software Specifications

Hardware Specifications:

A PC with following configurations was used for benchmarking purpose:

CPU

1. Ram : 16 GB
2. No of cores : 4
3. No of threads : 8
4. Clock Speed : 2.13 GHz
5. Instruction Set : 64 bit

Hard Disk

1. One HDD with 1024 GB

Software Specifications:

1. Linux Distribution-Ubuntu 18.04
2. Windows 7
3. Windows 10
4. VmWare Workstation Pro 15
5. ESXi service 6.5
6. Goolge Chrome
7. VmWare Client

Chapter 3. Background and Literature

3.1 Virtualization

Virtualization means to create a virtual version of a device or resource such as sever, storage device, network or even an operating system where the framework divides the resource into one or more execution environments.

Virtualization provides isolated environment over the hardware for application of operating system as the user want to get maximum utilization of the hardware, so this virtualization technique provide s the opportunity for optimum benefits from hardware resources that a close to real machine.

The system virtualization provides the usual hardware like Ethernet controllers, CPU's or hard disk drives to an operating system which runs inside of it. Such a system that has attach physical hardware is capable of running many virtual machine at a time that is known as virtualization host whereas the virtual machine running on it are called guest. The operating system running on each virtual machine is known as guest operating system

Every virtual machine have a set of following requirements:-

• **Equivalence**: The application that is running in virtual machine is just like same as it is running on the hardware without any additional plugin requirement. It must be identical in behavior while running in two different case.

• **Control**: The abstraction layer in between hardware and virtual machines must be controlled and synchronized access of virtual machines to hardware resources.

• **Isolation**: Virtualization technology was developed to ensure the isolation in between virtual machines. The purpose is to ensure stability of crashing one virtual machine should not affect others. Security from compromised virtual machine should not grant access to other virtual machines and data consistency.

• **Performance**: The virtualization overhead that is due to abstraction layer should be minimal, almost close to "Bare Metal" performance.

• **Encapsulation**: Cloning of the virtual machines are easy when they exist in the form of directory of file that also allow easy migration of the virtual machines.

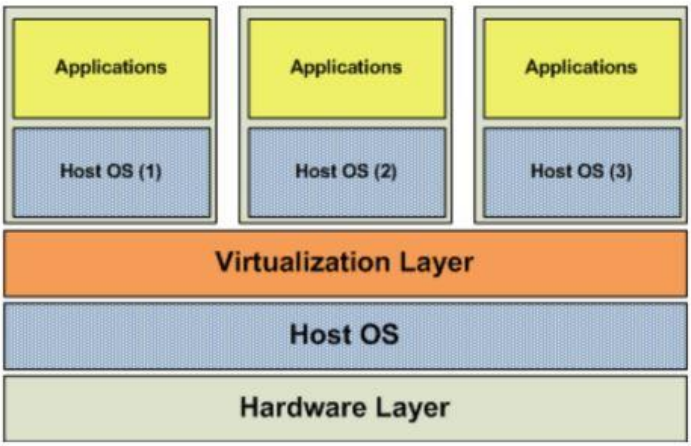

Figure 3.1: Virtualization

3.2 Virtualization Usage Benefits

Virtualization technology has plenty of benefits for using. Some main advantages are listed below.

• Workload consolidation can be possible with the help of virtual machines to use the fewer machines, even on single server can be used. Virtualization for workload consolidation having benefits of saving on hardware, environmental costs, management, and administration of the server infrastructure.

• Untrusted applications that are vulnerable for the system can be isolated by using separate virtual machines which are an important concept in building secure computing platforms.

• Execution environments with resource limited operating system can be created for a specific purpose. For example if an operating system that don't needed graphical environment or other resources like NIC etc can be created that might be able to increase the quality of service enabled operating system.

• System backup, recovery, or migration is quite easy and manageable by using virtualization.

3.3 Hypervisor

A hypervisor is a hardware virtualization technique that allows multiple guest operating systems (OS) to run on a single host system at the same time. The guest OS shares the hardware of the host computer, such that each OS appears to have its own processor, memory and other hardware resources. A hypervisor is also known as a virtual machine manager (VMM).

The hypervisor installed on the server hardware controls the guest operating system running on the host machine. Its main job is to cater to the needs of the guest operating system and effectively manage it such that the instances of multiple operating systems do not interrupt one another.

Hypervisors can be divided into **two** types:

Type 1: Also known as native or bare-metal hypervisors, these run directly on the host computer's hardware to control the hardware resources and to manage guest operating systems. Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer and Microsoft Hyper-V hypervisor.

Type 2: Also known as hosted hypervisors, these run within a formal operating system environment. In this type, the hypervisor runs as a distinct second layer while the operating system runs as a third layer above the hardware.

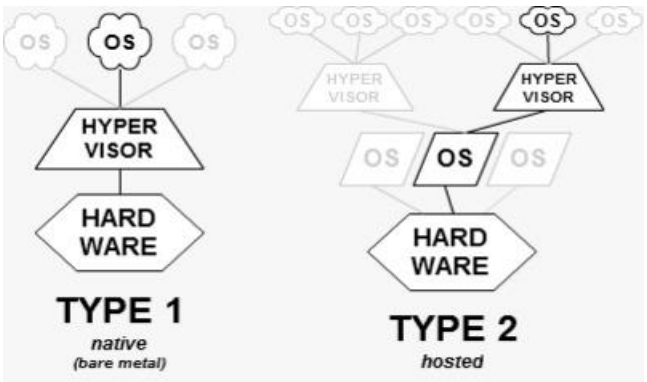

Figure 3.2: Types of Hypervisors

Targeted Hypervisor is:-

VMware Workstation: VMware Workstation is a hosted hypervisor that runs on x64 versions of Windows and Linux operating systems (an x86 version of earlier releases was available); it enables users to set up virtual machines (VMs) on a single physical machine, and use them simultaneously along with the actual machine. Each virtual machine can execute its own operating system, including versions of Microsoft Windows, Linux, BSD, and MS-DOS. VMware Workstation is developed and sold by VMware, Inc., a division of Dell Technologies. There is a free-of-charge version, VMware Workstation Player, for non-commercial use. An operating systems license is needed to use proprietary ones such as Windows. Ready-made Linux VMs set up for different purposes are available from several sources.

Figure 3.4: VMware

Advantages of VMware

I. Cost effective use of hardware.

II. Large portions of your production environment can be replicated on few servers.

III. Lower cost of hardware for the entire test environment.

IV. Faster rollback during testing.

V. Faster deployment of a new test platform.

VI. Test VMs can be decommissioned and even deleted after they are not needed.

Disadvantages of VMware

I. Requires that your staff have (or learn) some basic VMware skills.

II. VMs are not good for load testing if your production environment is completely physical.

III. Very low transfer rate to and from USB 2.0 devices

VMware ESXi Server : VMware ESXi (formerly ESX) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers. As a type-1 hypervisor, ESXi is not a software application that is installed on an operating system (OS); instead, it includes and integrates vital OS components, such as a kernel. ESX runs on bare metal (without running an operating system) unlike other VMware products.It includes its own kernel: A Linux kernel is started first, and is then used to load a variety of specialized virtualization components, including ESX, which is otherwise known as the vmkernel component. The Linux kernel is the primary virtual machine; it is invoked by the service console. At normal run-time, the vmkernel is running on the bare computer, and the Linux-based service console runs as the first virtual machine. VMware dropped development of ESX at version 4.1, and now uses ESXi, which does not include a Linux kernel.

3.4 Isolation Strategy

Virtual machines are the containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance.

Even a user with system administrator privileges on a virtual machine's guest operating system cannot breach this layer of isolation to access another virtual machine without privileges explicitly granted by the ESX system administrator. As a result of virtual machine isolation, if a guest operating system running in a virtual machine fails, other virtual machines on the same host continue to run. The guest operating system failure has no effect on : The ability of users to access the other

virtual machines, The ability of the operational virtual machines to access the resources they need and performance of the other virtual machines

Each virtual machine is isolated from other virtual machines running on the same hardware. Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine cannot detect any device other than the virtual devices made available to it, as shown in Virtual Machine Isolation.

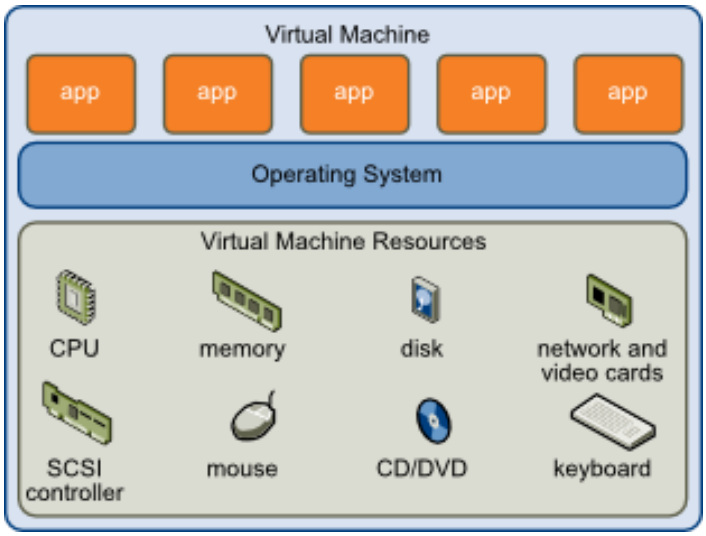

Figure 3.5: Virtual Machine Isolation

Because the VM kernel mediates the physical resources and all physical hardware access takes place through the VMkernel, virtual machines cannot circumvent this level of isolation. Just as a physical machine communicates with other machines in a network through a network card, a virtual machine communicates with other virtual machines running in the same host through a virtual switch. Further, a virtual machine communicates with the physical network, including virtual machines on other ESX hosts, through a physical network adapter, as shown in Virtual Networking Through Virtual Switches.

You can further protect virtual machines by setting up resource reservations and limits on the host. For example, through the detailed resource controls available in ESX, you can configure a virtual machine so that it always receives at least 10 percent of the host's CPU resources, but never more than 20 percent. Resource reservations and

limits protect virtual machines from performance degradation that would result if another virtual machine consumed excessive shared hardware resources. For example, if one of the virtual machines on a host is incapacitated by a denial-of-service (DoS) attack, a resource limit on that machine prevents the attack from taking up so much of the hardware resources that the other virtual machines are also affected. Similarly, a resource reservation on each of the virtual machines ensures that, in the event of high resource demands by the virtual machine targeted by the DoS attack, all the other virtual machines still have enough resources to operate.

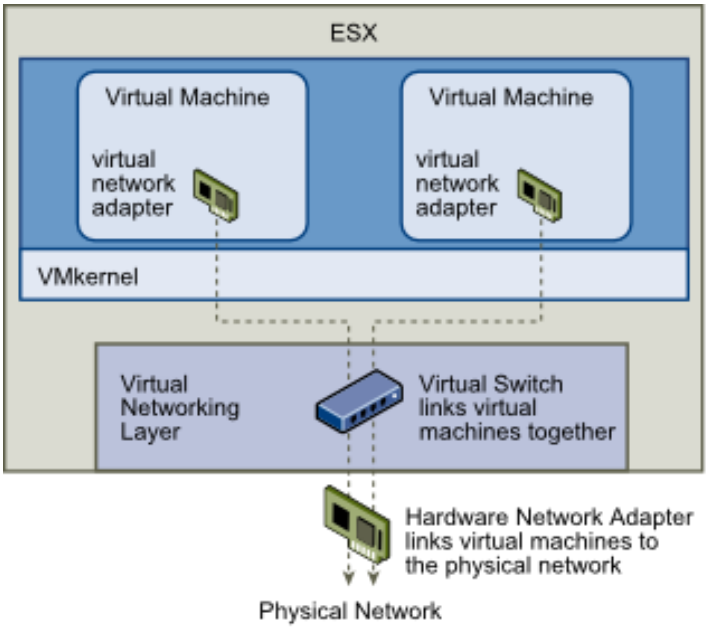

Figure 3.6: Virtual Networking Through Virtual Switches

By default, ESX imposes a form of resource reservation by applying a distribution algorithm that divides the available host resources equally among the virtual machines while keeping a certain percentage of resources for use by other system components. This default behavior provides a degree of natural protection from DoS and distributed denial-of-service (DDoS) attacks. You set specific resource reservations and limits on an individual basis to customize the default behavior so that the distribution is not equal across the virtual machine configuration.

3.5 Domains

These are the Operating Systems that are used to run different network, Disk and CPU intensive applications and further perform benchmarking based on several parameters.

Domains Used are:-

Windows 7 Professional - Windows 7 is a personal computer operating system that was produced by Microsoft as part of the Windows NT family of operating systems. It was released to manufacturing on July 22, 2009 and became generally available on October 22, 2009, less than three years after the release of its predecessor, Windows Vista. Windows 7's server counterpart, Windows Server 2008 R2, was released at the same time. Windows 7 was primarily intended to be an incremental upgrade to Microsoft Windows, intended to address Windows Vista's poor critical reception while maintaining hardware and software compatibility. Windows 7 continued improvements on Windows Aero (the user interface introduced in Windows Vista) with the addition of a redesigned taskbar that allows applications to be "pinned" to it, new window management features. Other new features were added to the operating system, including libraries, the new file sharing system Home Group, and support for multi-touch input. A new "Action Center" interface was also added to provide an overview of system security and maintenance information, and tweaks were made to the User Account Control system to make it less intrusive. Windows 7 also shipped with updated versions of several stock applications, including Internet Explorer 8, Windows Media Player, and Windows Media Center.

Ubuntu v18 - Ubuntu is a free and open-source Linux distribution based on Debian. Ubuntu is officially released in three editions: Desktop, Server, and Core (for internet of things devices and robots). Ubuntu is a popular operating system for cloud computing, with support for OpenStack. Ubuntu is released every six months, with long-term support (LTS) releases every two years. The latest release is 19.04 ("Disco Dingo"), and the most recent long-term support release is 18.04 LTS ("Bionic Beaver"), which is supported until 2028.Ubuntu is developed by Canonical and the community under a meritocratic governance model. Canonical provides security updates and support for each Ubuntu release, starting from the release date and until the release reaches its designated end-of-life (EOL) date. Canonical generates revenue through the sale of premium services related to Ubuntu. Ubuntu is named after the

African philosophy of Ubuntu, which Canonical translates as "humanity to others" or "I am what I am because of who we all are"

3.6 Some Similar Tools

Xen Server- Citirix XenServer is a hypervisor platform that enables the creation and management of virtualized server infrastructure. It is developed by Citrix Systems and is built over the Xen virtual machine hypervisor. XenServer provides server virtualization and monitoring services. It is available in a 64-bit hypervisor platform and can be executed on the entire x86 series of processors. Citirix XenServer is a hypervisor platform that enables the creation and management of virtualized server infrastructure. It is developed by Citrix Systems and is built over the Xen virtual machine hypervisor. XenServer provides server virtualization and monitoring services. It is available in a 64-bit hypervisor platform and can be executed on the entire x86 series of processors.

Solaris Winds- SolarWinds Virtualization Manager is an infrastructure monitoring tool that offers a robust Hyper-V monitoring system. With SolarWinds Virtualization Manager you can track storage I/O performance. Tracking storage I/O performance allows you to address storage I/O contention, which is one of the most common issues with managing Hyper-V environments. The main dashboard is fully customizable and can be used to view current alerts and warning messages so that you keep up-to-speed with developments in infrastructure performance. There is also a VM Sprawl dashboard which allows you to keep track of key metrics like CPU, memory, and storage. You can see how much total storage space you've used. Alerts are one of the main ways that SolarWinds Virtualization Manager helps you to track Hyper-V performance. For instance, you configure the program to send you an alert when CPU utilization is too high. This ensures that you don't miss anything important and risk your VM going down.

Logic Monitor- LogicMonitor is a network management system, but it integrates the monitoring of virtual environments. So, you can use it as a system-wide monitor or just limit it to monitoring your virtual machine implementations. The LogicMonitor system offers VMware vCenter monitoring, ESX/i hosts monitoring, and also covers

individual VMs, including ESX and ESXi. LogicMonitor performs Microsoft Hyper-V performance tracking at both the hypervisor and individual VM levels. This system can also interact with Citrix XenServer technology. The software for this monitor is accessed in the cloud. It is platform-neutral and can monitor cloud-provided VM services as well as on-site systems. However, it's not a completely off-site implementation because you need to install collectors on your servers and network devices. These collectors route through your gateway up to the central Logic Monitor server. All communications over the internet are encrypted, as is stored data on the Logic Monitor server. Information is decrypted in real time when accessed through a valid user account, which requires access credentials.

Chapter 4. Benchmarking Overview and Tools

4.1 Benchmarking

A computerized test for measuring the properties of the particular technology is called benchmarking. The properties might include speed, performance, transfer rate, etc.

Benchmarking is important before making decision to select an equipment. The equipment that is going to buy, must be tested before in the same environment and workload as in real working situation. Besides the working situation, it should also has to be tested in worst case situation. It might not always be possible due to non-availability of replicated surrounding environment. This includes the actual data system that is working with. Because of privacy issues of data or huge amount of data replication of the systems data might not be possible. So the artificial workloads are needed for execution and monitoring the benchmark program.

For testing the characteristics of the technology for academic or research purpose, it is difficult to provide the real system configuration. In such cases benchmarks could serve the purpose to provide with close to real application systems for better results.

While implementing a system should have to consider the potential performance and cost of the system. Benchmarking provides the results that can help. Many factors are considered when benchmarking for comparison of different vendors products. Results from the benchmarking that are a reasonable match for the application and system size that you are considering.

Benchmarks are categorized as follows:

• **Performance focused** these benchmarks aim for the highest performance regardless of system cost.

• **Price or performance focused** these benchmarks aim for the lowest cost regardless of the system performance.

Following can also be considered while benchmarking:

• **System Architecture** 32-bit or 64-bit.

• **System size** the number of CPUs in the system under test

• **System configuration** Multiple clustered systems, or a single non-clustered system. Benchmarks for multi-tier applications may use different architectures and operating systems for different tiers.

4.2 Benchmarking Parameters

CPU: CPU performance measurement is very important for large scale infrastructure like cloud data centers. In Large scale systems CPU Computing power is allocated/ shared in between to run multi-tenant environments. It includes the percentage of CPU used for carried out the task given by the stress. The CPU is stressed using four processes. Figure 4 shows CPU utilization for the hypervisors.

RAM: It includes the percentage of RAM used. RAM will be stressed using 2 processes (each sizing around 256MB).

DISK Read and Write speed: It gives the write and read speed of the disk, the DISK will be stressed with a process that is about 1GB in size.

N/W Read and Write speed: Network transmission and receiving speed is checked. Network latency is more important for data intensive applications in the cloud computing data centers.

4.3 Benchmarking Tool -

VMware ESXi Server - VMware ESXi Server is computer virtualization software developed by VMware Inc. The ESXi Server is an advanced, smaller-footprint version of the VMware ESX Server, VMware's enterprise-level computer virtualization software product. Implemented within the VMware Infrastructure, ESXi can be used to facilitate centralized management for enterprise desktops and data center application.

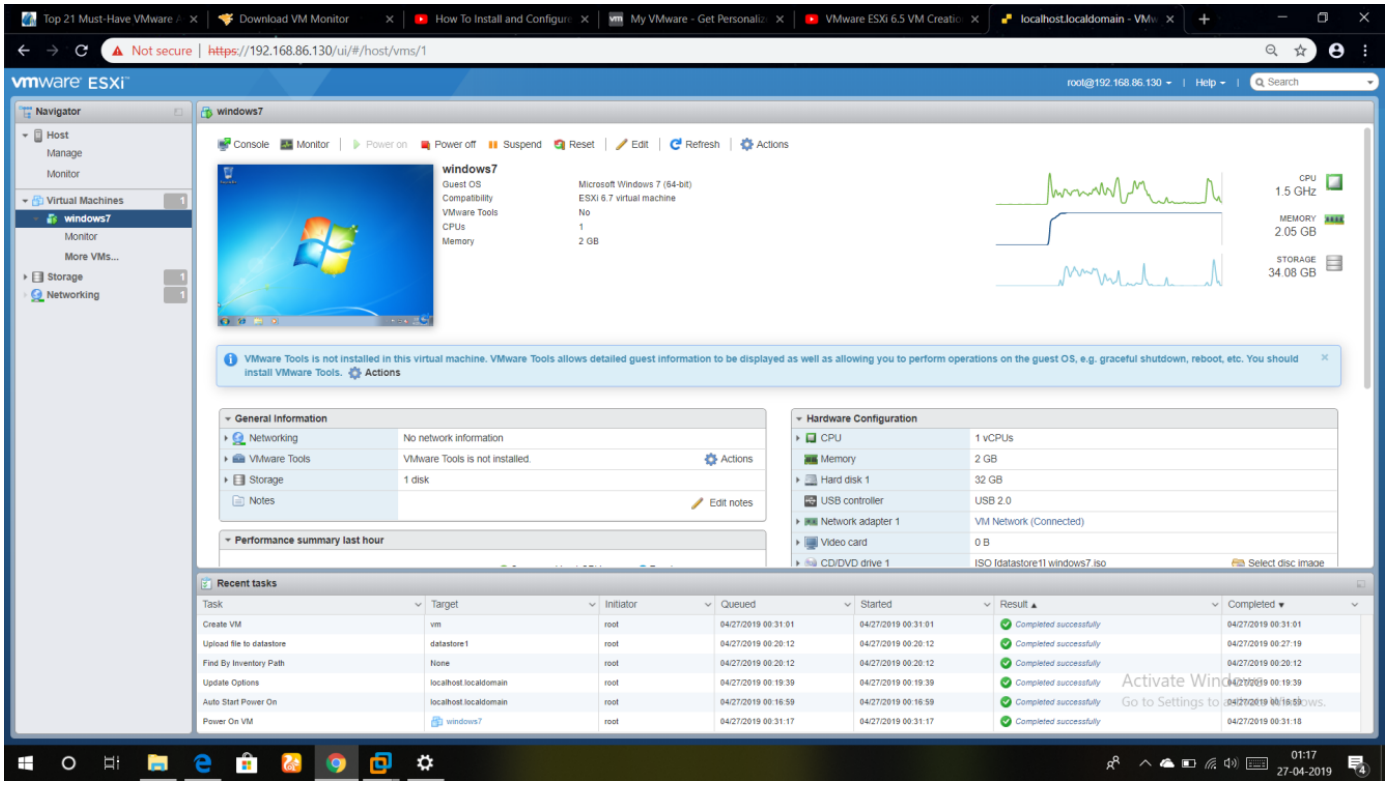

Figure 4.3.1: VMware ESXi Console

Chapter 5. Approach

5.1 Methods for Conducting the Tests

Experiment setup consists of two different guest operating system environments.

Windows 7 and Ubuntu-Linux 18.04 which are mounted on the top of the ESXi server and the ESXi server is mounted on the top of the Vmware Workstation and all the different VMs are basically on the top of the workstation itself.

Firstly, on our host machine which is running a windows 10 operating system we installed VmWare workstation pro 15.

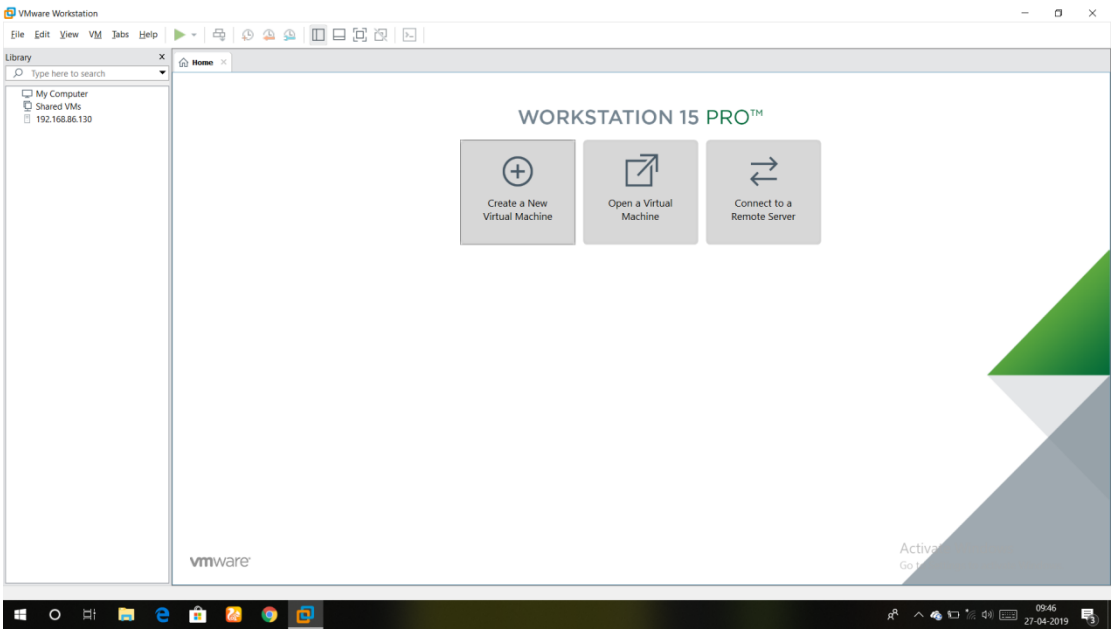

Figure 5.2.1: VMware Workstation Pro Console

After that, we download the ESXi server from the VmWare website and created a VM on the VmWare Workstation with the help of that ESXi server ISO image.

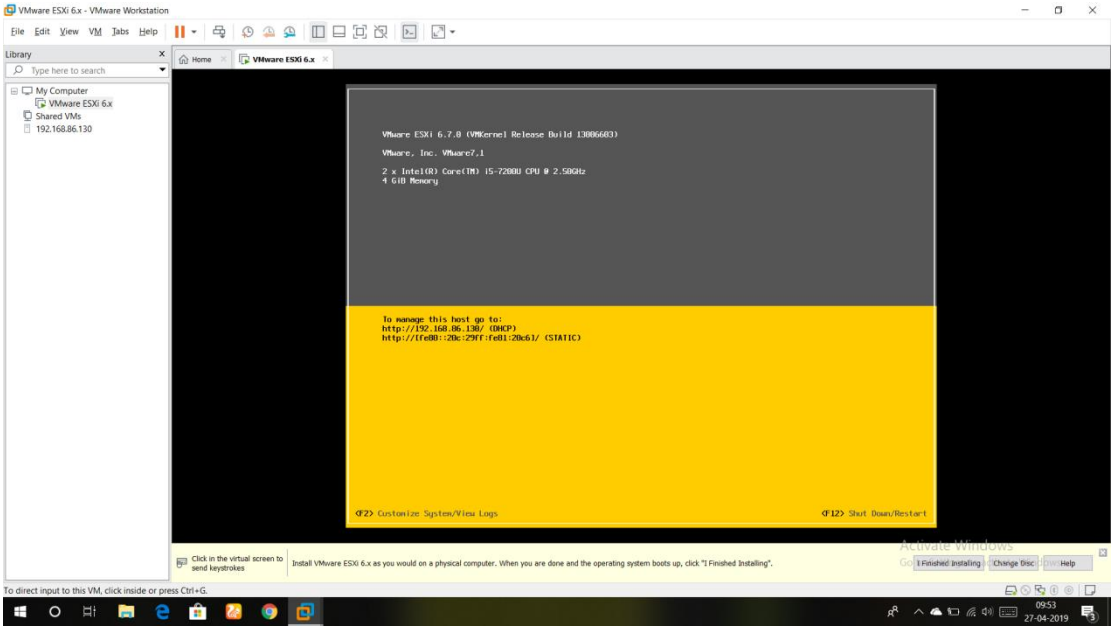

Figure 5.2.2: Installation Of VMware ESXi

After creating the VM of the server on the top of the workstation we have to manage the server and need a monitoring and management tool and console for the server. By default the server provide a local host console for the management and monitoring of the server. This local host console can be operated either by a tool called Vmware Client or we can also use the console by going to the ip address provided by the sever on any browser. In this we used Google Chrome as the browser to open the ip address.

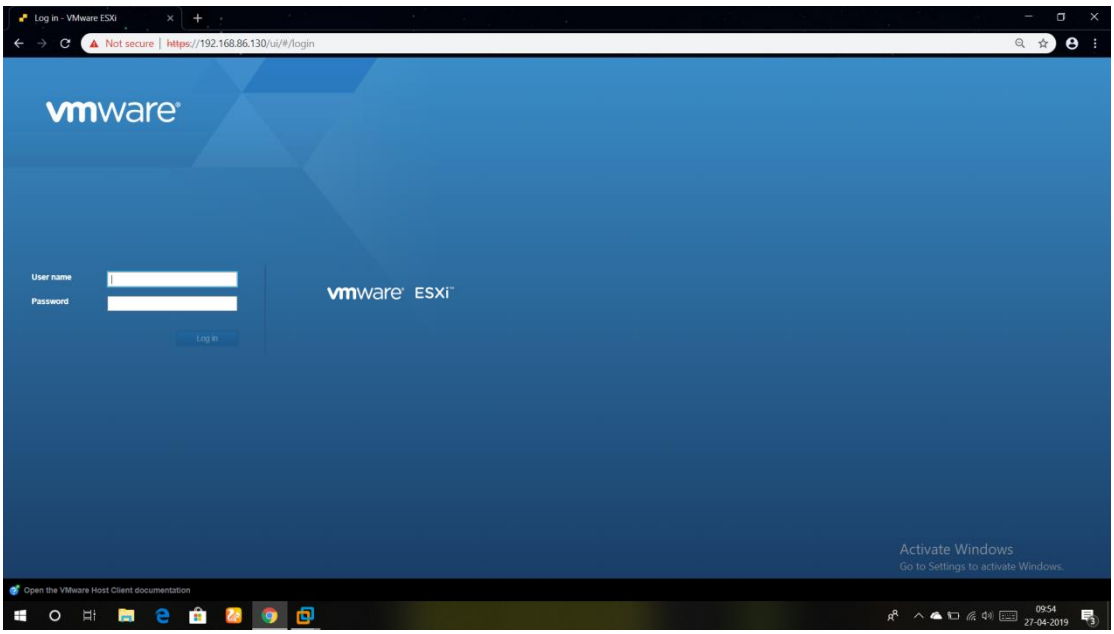

Figure 5.2.3: VMware ESXi Login Page

After opening the management console of the server, we now have to create the VMs on that server.

First we create the virtual machine of Windows 7

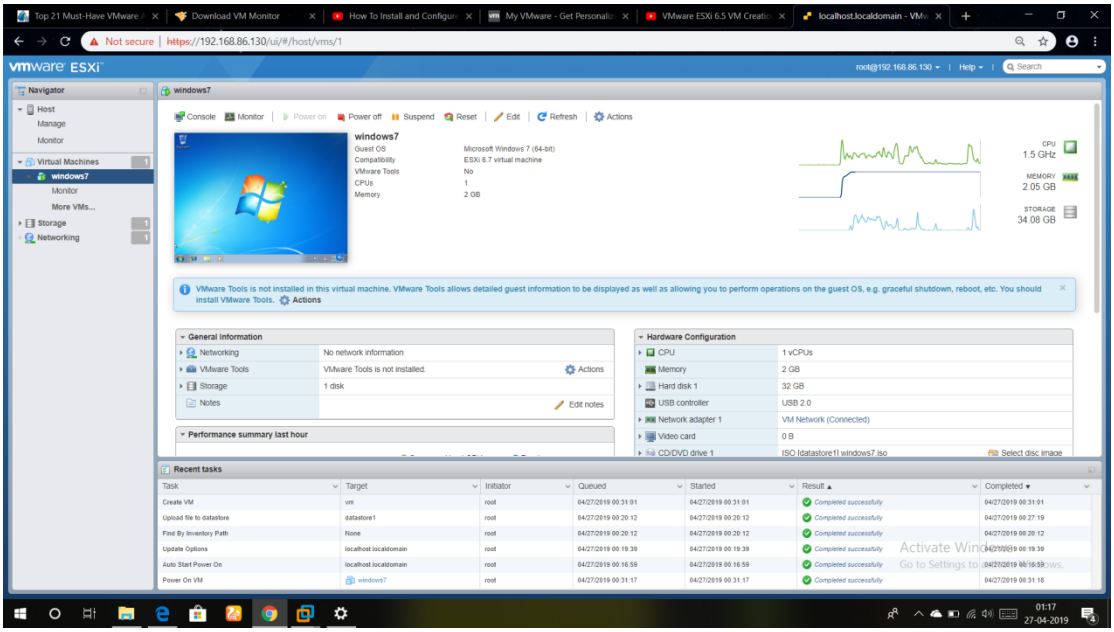

Figure 5.2.4: Windows 7 Dashboard In VMware ESXi Server

Figure shows the CPU utilization statistics in the installation process of the Windows 7 operating system in the isolated virtual environment.

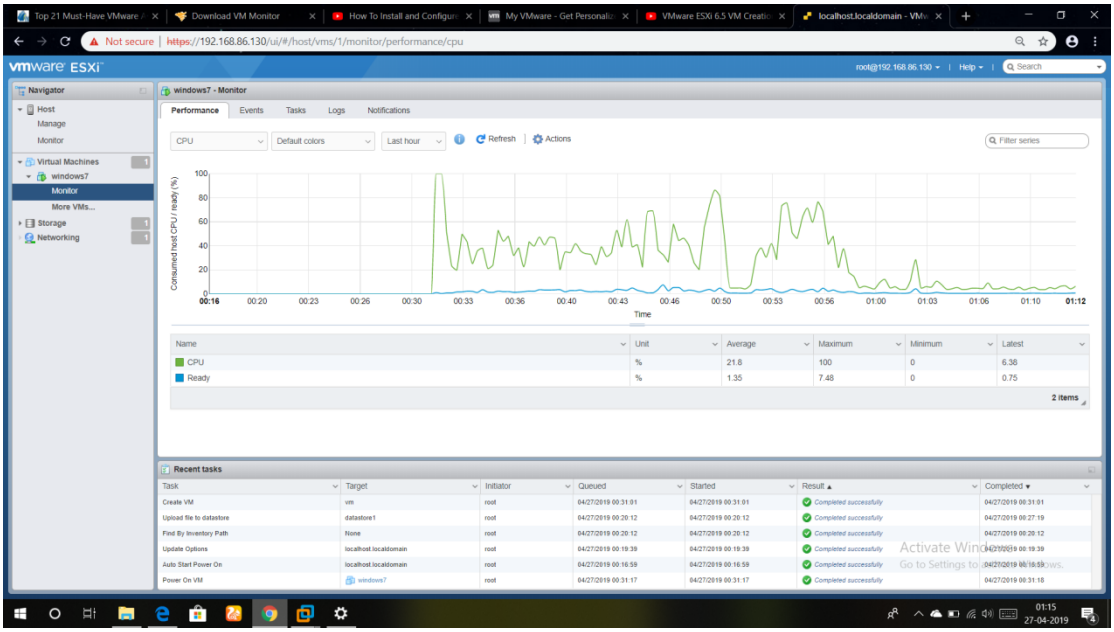

Figure 5.2.5: CPU Utilization During Installation Of Win 7

Now we have created a virtual machine of Windows 7 on our server and next we create a virtual machine of Ubuntu 18.04 on the server by using an Ubuntu 18.04 ISO image.

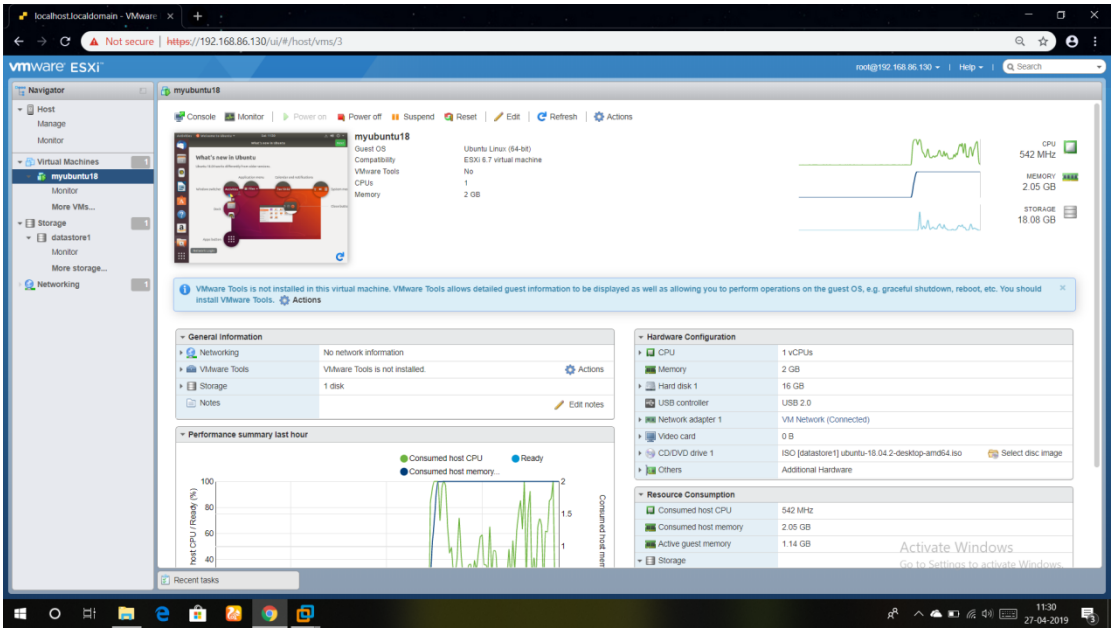

Figure 5.2.6: Ubuntu Dashboard In VMware ESXi Server

Figure shows the CPU utilization statistics in the installation process of the Ubuntu 18.04 operating system in the isolated virtual environment.

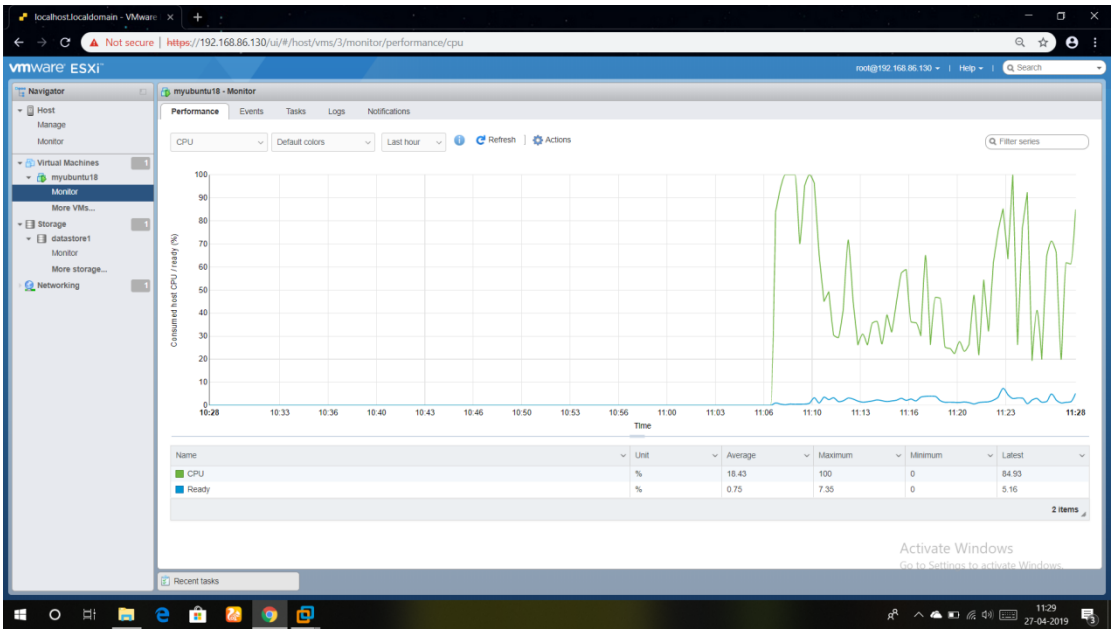

Figure 5.2.7: CPU Utilization During Installation Of Win 7

Now after creating the two virtual machines on the server we have to do benchmarking of an application in these two different isolated virtual environments.

And for doing the benchmarking we have installed Google Chrome on both virtual machines and now we benchmark this application by opening 3 tabs simultaneously which are running Youtube.com online streaming on them.

By doing so we are putting some extra amount of load on the application and can extract the statistics of the application in two different isolated virtual environments.

6. Results and Outcome

After completing pervious steps, we have done benchmarking on 3 different parameters which are as follows:

1. CPU Utilization
2. Disc Read/Writes
3. Network Usage

Benchmarking is done for 10 minutes time frame after opening Goolge Chrome on the different isolated environments and 3 Youtube tabs on Google Chrome.

1. CPU UTILIZATION:-

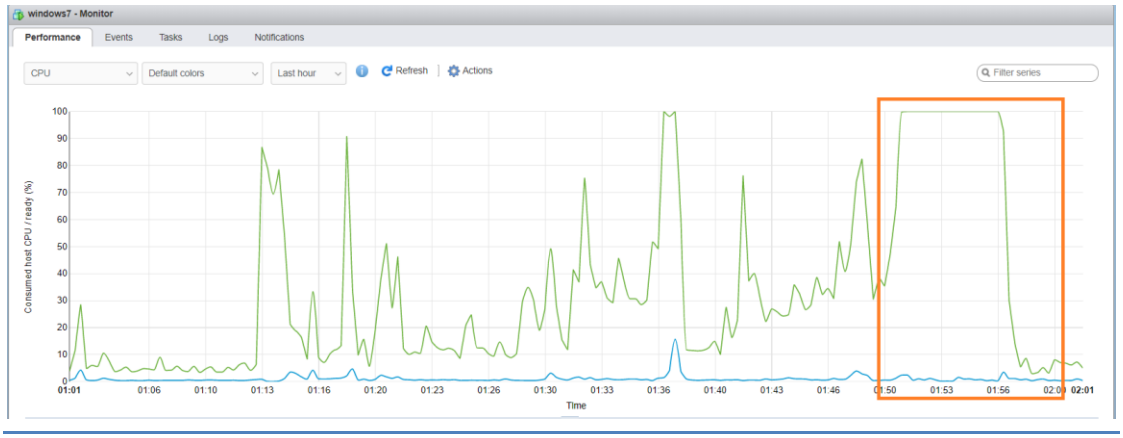

Figure 6.1: CPU Utilization Of Windows 7

Above figure shows the CPU Utilization of Google Chrome application in Windows7 in isolated environment for a given time frame of 10 minutes.

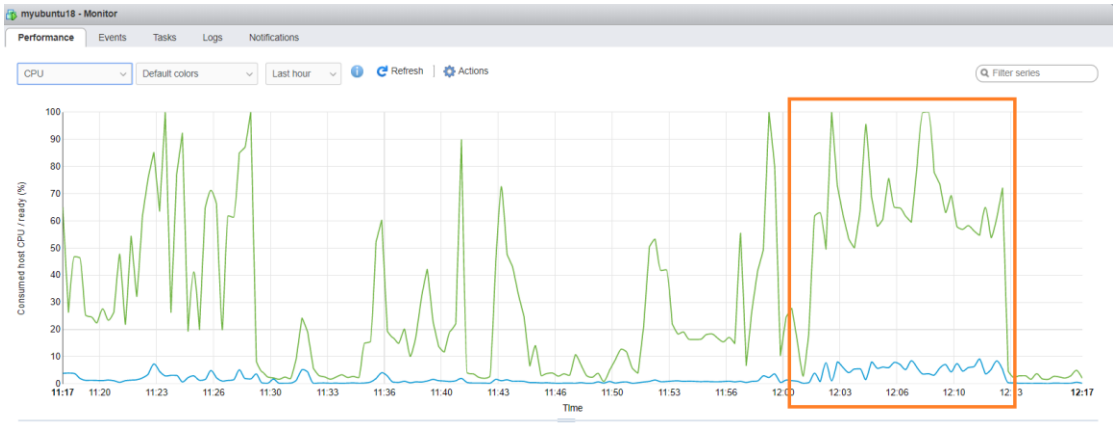

Figure 6.2: CPU Utilization Of Ubuntu 18.04

Above figure shows the CPU Utilization of Google Chrome application in Ubuntu 18.04 in isolated environment for a given time frame of 10 minutes.

2. DISK READ/WRITES:

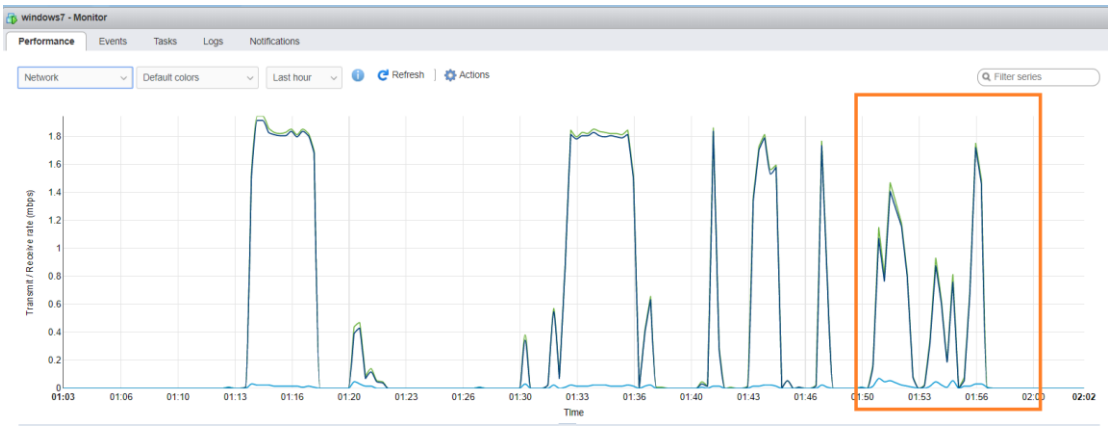

Figure 6.3: Disk read/writes Of Windows 7

Above figure shows the Disk read/writes of Google Chrome application in Windows 7 in isolated environment for a given time frame of 10 minutes.

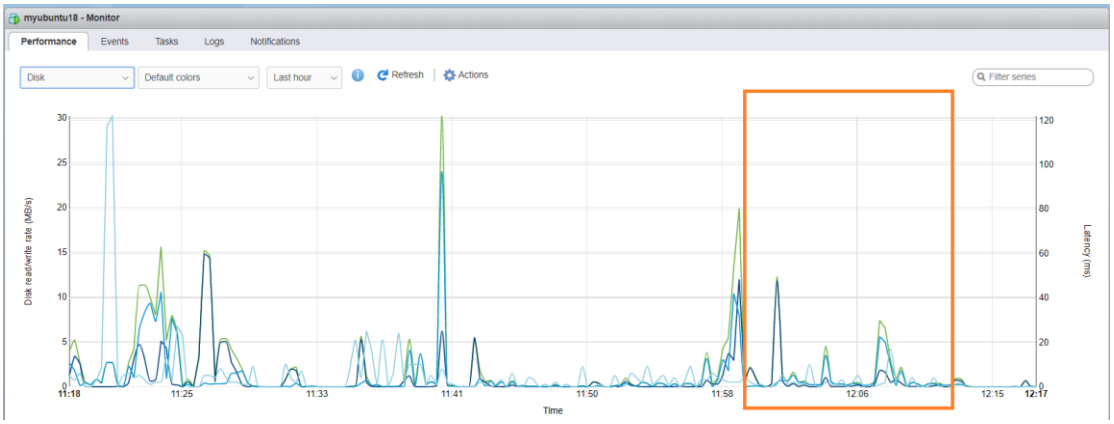

Figure 6.4: Disk read/writes Of Ubuntu 18.04

Above figure shows the Disk read/writes of Google Chrome application in Ubuntu 18.04 in isolated environment for a given time frame of 10 minutes.

3. NETWORK USAGE:

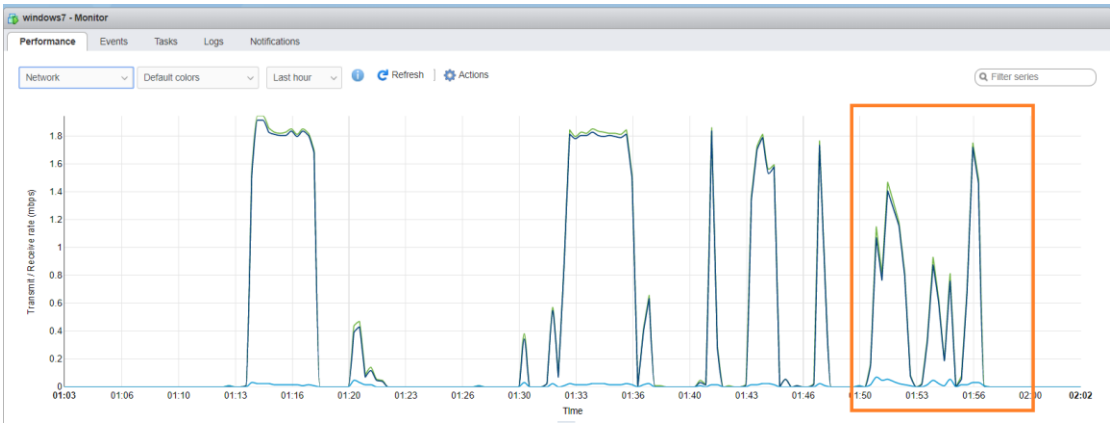

Figure 6.5: Network Usage Of Windows 7

Above figure shows the Network Usage of Google Chrome application in Windows 7 in isolated environment for a given time frame of 10 minutes.

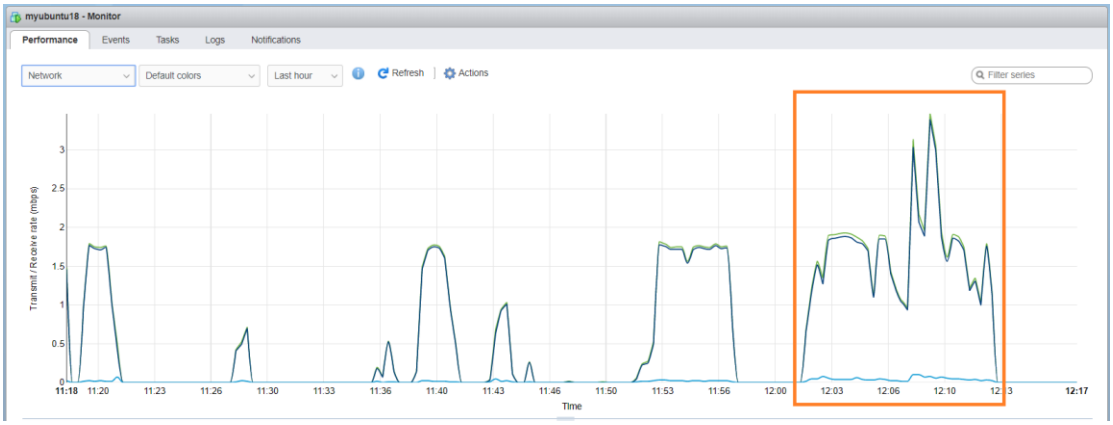

Figure 6.6: Network Usage Of Ubuntu 18.04

Above figure shows the Network Usage of Google Chrome application in Ubuntu 18.04 in isolated environment for a given time frame of 10 minutes.

7. Conclusion

IT managers are increasingly looking at virtualization technology to lower IT costs through increased efficiency, flexibility, and responsiveness. As virtualization becomes more pervasive, it is critical that virtualization infrastructure can address the challenges and issues faced by an enterprise datacenter in the most efficient manner. Resource contention in terms of disk and network bandwidth is the major consideration for finding a place for a virtual machine to physical host. ESXi in many domain environments provide good isolation when running high throughput and non-real time applications with credit scheduler but it becomes difficult to predict the performance and time guarantees when running soft real time applications on it. SEDF has shown relatively good performance than credit scheduler. SEDF requires effective deadline setting and it may have more context switches with smaller slices. In conclusion, high level matrices like time to complete a benchmark test is taken into account while measuring the performance, but more precise and lower level matrices are needed to evaluate scheduler traces for each kind of applications. Work can be continued in the direction while measuring more precise characteristics in ESXi environment. It helps in understanding scheduler behavior for different kind of load they run and their behavior on placement of these applications. Application placement problem is still in its initial phase, it can be seen while running different real time and live benchmarks like for web servers and multimedia applications. Choosing correct parameters and configuring a scheduler is not a trivial task with complex Service level Objectives (SLO). Clear mapping of SLO parameters and scheduler parameter is needed for isolation.

8. References/Bibliography

VMware ESXi Documentation

https://docs.vmware.com/en/VMware-vSphere/index.html

VMware Documentation

https://www.vmware.com/support/pubs/

Performance Benchmarking of Hypervisors - A Case Study

- By Gaurav Somani and Sanjay Chaudhary