Making Data Center using VMware tools: vSphere ESXi and vCenter

Submitted in the partial fulfilment of Bachelor of Technology in

Computer Science and Engineering

Submitted By:

Name	Aarushi Sharma	Jannat Miglani	Shivang Seth
Class Roll No.	101/19	128/19	156/19
Univ. Reg. No.	1903575	1903600	1903627

Department of Computer Science & Engineering
DAV Institute of Engineering & Technology
Jalandhar, India

CERTIFICATE

We hereby declare that the work which is being presented in the report entitled "**Making Data Center using VMware tools: vSphere ESXi and vCenter"** by our team in partial fulfilment of requirements for the award of degree of Bachelor of Computer Science and Engineering submitted in the Department of Computer Science and Engineering at DAVIET, Jalandhar is an authentic record of our own work under the supervision of Dr. Parveen Kakkar. The matter presented in this report has not been submitted by using any other University/Institute for the award of Degree/Diploma.

Aarushi Sharma **[**1903575**]**

Jannat Miglani **[**1903600**]**

Shivang Seth [1903627]

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Dr. Parveen Kakkar

The Viva Examination is held at Department of Computer Science and Engineering, DAV Institute of Engineering &Technology, Jalandhar.

Signature of the EXTERNAL EXAMINER

Signature of the HEAD

Department of Computer Science and Engineering

ABSTRACT

Virtualization is a technique of how to separate a service from the underlying physical delivery of that service. It is the process of creating a virtual version of something like computer hardware. It was initially developed during the mainframe era. It involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource. With the help of Virtualization, multiple operating systems and applications can run on same machine and its same hardware at the same time, increasing the utilization and flexibility of hardware.

In other words, one of the main cost effective, hardware reducing, and energy saving techniques used by cloud providers is virtualization. Virtualization allows to share a single physical instance of a resource or an application among multiple customers and organizations at one time. Virtualization allows to share a single physical instance of a resource or an application among multiple customers and organizations at one time. It does this by assigning a logical name to a physical storage and providing a pointer to that physical resource on demand. The term virtualization is often synonymous with hardware virtualization, which plays a fundamental role in efficiently delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing.

VMware has a better approach to cloud security than other virtualization and cloud vendors with a new set of virtualization-aware security products that work with existing solutions to enable adaptive and cost-effective security and compliance within a single management framework.

- It occupies the highest market in virtual servers i.e., about 80%
- It not only provides virtual servers but also a lot many types of services like vCenter, vSphere.
- Cost efficient

ACKNOWLEDGEMENT

The constant guidance and encouragement received from Dr. Harpreet Bajaj, Head of Department of Computer Science and Engineering, DAVIET Jalandhar has been of great help in carrying out the project work and is acknowledged with reverential thanks.

We would like to express our gratitude to Dr. Parveen Kakkar, Assistant Professor, Department of Computer Science and Engineering, DAVIET, Jalandhar for his stimulating guidance, continuous encouragement and supervision throughout the course of present work.

We express our gratitude to other faculty members of Computer Science and Engineering department of DAVIET for their intellectual support throughout the course of this work.

LIST OF FIGURES

LIST OF TABLES

CHAPTER - 1

INTRODUCTION

1.1 INTRODUCTION TO PROJECT

The project aims at administering VMWare, vSphere ESXi and vCenter. Starting with the installation and configuration of VMWare and ESXi server. The further tasks include setting up virtual machines and their management, reviewing and modification of resources. With the help of vSphere, the following functionality such as creating and managing multiple VMs with ease, performing live migration of the workloads and maintenance of datacenters without downtime etc. will be achieved.

vCenter Server will allow for centralized management of the virtual infrastructure. The hosts and VMs can be controlled from a single console, which will enhance visibility and help with error prevention. The next step would be creating cluster which is a group of hosts. This will be followed by migrating VM with the help of vMotion.

The project also aims on using features like cloning, templates, export, import and organizing VMs. The feature of high availability then helps in load balancing between multiple hosts. The storage and networking facilities are optimized.

1.2 OBJECTIVES

- To set up a data center using virtualization tools in which IaaS services will be lent to the users connected to it. Our data center would facilitate the new VMs by providing networking capabilities and storage. This makes the data center highly scalable. The resources of two ESXi's will be clubbed together.
- To understand different type of tools provided by VMWare software according to the needs of the project.
- To run multiple virtual machines on a same physical server, each VM can have its own Operating system, which means multiple OS can run on one physical server sharing resources which is provide by the ESXi physical Bare metal hypervisor tool.
- To provide centralized and extensible platform vCenter server performs a few tasks, including resource provisioning and allocation, performance monitoring, workflow automation and user privilege management. It enables a vSphere administrator to manage multiple ESXi and ESXi servers and virtual machines (VMs) through a single console.
- To implement resource allocation that takes a vital role in Virtual machines, if the resources are improperly allocated then some machines may have high load and other have low load which may guide for extra utilization so resource allocations is must in VMs so resources allocations major issue as the VM can be scaled starting from only two VM's to thousand no. of VM's which is impossible to test. Thus, the simulation occurs for testing the VM's as per the requirement which can consume less time, cost and energy.

1.3 PROBLEM FORMULATION

Growing your business is hard. Scaling up operations, infrastructure, and people is not only challenging, but also daunting. Virtualization offers one way to build in flexibility, agility, and support into your rapidly expanding business. It does this by allowing you to run multiple instances of software in parallel, without investing in new hardware. Traditionally, software runs on a particular piece of hardware. Your operating system and applications are installed on *your* computer. A shared-enterprise application is installed on *a* server computer. It's a one-to-one relationship that has its benefits but offers little flexibility and can be inefficient. Enterprise applications run on servers with at least one dedicated server for their application — a fairly common setup, but one that leaves the majority of each server's capacity unused. All of those servers require lots of power to run and — because they generate heat — to cool. They also take up space, which is becoming a scarce commodity.

Maintenance, repair, and upgrading of internal servers, results in productivity-sapping downtime and periods of slow system performance. Often, identifying a problem can involve troubleshooting that has negative ripple effects throughout your IT infrastructure. **Slow fulfilment of IT requests-**Overburdened IT staff often cannot respond with sufficient promptness to service requests. Server virtualization facilitates the reduction of response times. **Data vulnerability-** With physical servers, it's usually a costly and complex process to back up and store data offsite for disaster recovery. Virtual servers eliminate the need to duplicate your production infrastructure. **Captive, underused, and aging servers-** Using virtual servers frees IT from the responsibility of managing these machines and allows old servers to be repurposed.

1.4 EXISTING SYSTEM

On- premises

On premises refer to the software technology that has physical confines for the enterprises and the data is stored within the organization itself. The software and hardware are installed and run within the premises of the company and the staff has physical access to the stored data. The staff of the company can also manage the security and the stored data. The solutions are installed in the computer system through USB drive or CD devices. Hence, it limits the employees to access data organization and it doesn't follow the approach of 'anytime, anywhere'. The data stored in on-premises technology can be operated within the data center only and it uses computer and hardware. The vendors are not responsible for the security or management but they only offer sales and technical support in the enterprise. It is extremely expensive and requires huge investment at every step. Traditional and outdated model of on-premises is behind virtualized environment for a number of reasons including security, data management, etc. In an on-premise system:

- Moving your physical server environment to another location is a more resource-intensive task. In this case, you will need to copy all data stored on the server to a removable media, transport the media as well as all hardware resources that you have to a new location, and then re-install all of the system components on a new server. Essentially, you will have to re-build a server from scratch.
- To expand a physical server environment, you need to buy additional hardware components, which can be very expensive, and go through a long process of installation and configuration.
- Physical servers do not use their hardware and software capabilities to maximum levels, with their average production capacity being at 25%. Thus, a lot of computing resources are left unused, which isn't cost-effective.
- If the production site was hit by disaster, it is essential to quickly restore mission-critical data and operations so as to reduce system downtime and minimize its negative impact on business. It can take several hours or days to restore business operations running on a physical server. In this case, the disaster recovery (DR) process entails setting up a new physical server, installing an OS, setting up applications, and restoring critical data from backups.
- If a disaster has affected or destroyed your physical server infrastructure, the damage, in most cases, is irreversible.
- With physical servers, you have to build a system of protection for each individual server, depending on its computing capabilities and resources and the sensitivity of data that it stores. This can be a resource-intensive task if your IT infrastructure is built upon 10 or more physical servers.
- Building and maintaining a physical server environment can be quite expensive. This is due to constant hardware and software upgrades, frequent system failures, and breakdown of computer components and equipment, which are difficult or even impossible to repair.

1.5 PROPOSED SYSTEM

Virtualized Environment (VMware vSphere)

Virtualization relies on software to simulate hardware functionality and create a virtual computer system. This enables IT organizations to run more than one virtual system – and multiple operating systems and applications – on a single server. The resulting benefits include economies of scale and greater efficiency. A virtual computer system is known as a "virtual machine" (VM): a tightly isolated software container with an operating system and application inside. Each self-contained VM is completely independent. Putting multiple VMs on a single computer enables several operating systems and applications to run on just one physical server, or "host."

A thin layer of software called a "hypervisor" decouples the virtual machines from the host and dynamically allocates computing resources to each virtual machine as needed. Partitioning, Isolation, Encapsulation and Hardware Independence are its key features.

- Portability-You can easily move VMs across the virtual environment and even from one physical server to another, with minimal input on your part. This is due to the fact that VMs are isolated from one another and have their own virtual hardware, which makes a VM hardware-independent.

- Scalability- A virtual server environment provides the option of on-demand scalability. A single virtual server can host multiple VMs at the same time, which can be added or removed with the click of a mouse. Your virtual environment can be scaled up or down depending on the growth of your business needs. In this case, you don't need to buy additional hardware to ensure VM deployment. This is due to the fact that VMs running on the host share the same computing resources, which can be evenly distributed among all VMs. Thus, you can design an easily configurable environment which can carry out operations of any complexity levels.

- Capacity management- A server hosting multiple VMs takes care of underutilized resources by distributing them among other VMs which need it most. This way, optimum capacity management is achieved.

- System recovery-The DR process in a virtual environment is much simpler. You can restore the entire VM at a DR site with the help of previously created VM backups, resulting in almost zero downtime.

- Business continuity-Currently, businesses are expected to operate on an always-on basis, meaning that even a minor interruption in business operations can lead to major repercussions. Therefore, ensuring business continuity, especially in case of disaster, should be one of the main priorities of any organization. When comparing physical servers and VMs, it becomes evident that VMs are more fault-tolerant. In case of disaster, the workload of your virtual environment can be transferred in a few clicks to

another site, so as to ensure the minimum downtime. After the effects of the disaster have been mitigated and the production center has been restored, you can move the workload from the DR site back to the primary site.

- Security-Security management is more easily configurable in a virtual server environment than in a physical one. On the other hand, a virtual server environment can be protected on the basis of a universal security model. Thus, security policies and procedures can be developed, documented, and implemented from a single pane of glass - that is, through the hypervisor dashboard.
- Costs- Virtualization is considered a perfect option for enterprises which contain a large number of servers. A virtual server environment allows you to evenly distribute computing resources among all running VMs, thus ensuring capacity optimization for a minimal price.

1.6 UNIQUE FEATURES OF THE SYSTEM

1. Increased Security: It increases the hosts ability to control the execution of guest programs in a transparent manner which helps open up new possibilities to allow the delivery of a secure and controlled execution environment.

2. Sharing: It is a key feature of virtualization as through this process one can create a separate computing environment within the same host. This allows them to reduce the number of active serves and minimizes power consumption.

3. Aggregation: A group of separate hosts can be tied together and represented to guests as a single virtual host. This functionality is implemented with cluster management software, which harnesses the physical resources of a homogeneous group of machines and represents them as a single resource.

4. Emulation: Guest programs are executed within an environment that is controlled by the virtualization layer, which ultimately is a program. Also, a completely different environment with respect to the host can be emulated, thus allowing the execution of guest programs requiring specific characteristics that are not present in the physical host.

5. VMware vSphere High Availability (HA)- A clustering feature that is designed to restart a virtual machine (VM) automatically in case of failure. VMware vSphere High Availability allows organizations to ensure high availability for VMs and applications running on the VMs in a vSphere cluster (independent of running applications). VMware HA can provide protection against the failure of an ESXi host – the failed VM is restarted on a healthy host. As a result, you can significantly reduce downtime

6. Fault Tolerance-VMware provides a feature for a vSphere HA cluster that allows you to achieve zero downtime in case of an ESXi host failure. This feature is called Fault Tolerance. While the standard configuration of vSphere High Availability requires a VM restart in case of failure, Fault Tolerance allows VMs to continue running if the primary ESXi host on which the VMs are registered fails. Fault Tolerance can be used for mission-critical VMs running critical applications.

7. Distributed Resource Scheduler (DRS)- A VMware vSphere clustering feature that allows you to load balance VMs running in the cluster. DRS checks the VM load and a load of ESXi servers within a vSphere cluster. If DRS detects that there is an overloaded host or VM, DRS migrates the VM to an ESXi host with enough free hardware resources to ensure the quality of service (QoS). DRS can select the optimum ESXi host for a VM when you create a new VM in the cluster.

8. vMotion- Migrate VMs from one ESXi host to another with vMotion, which we mentioned when explaining how Fault Tolerance works. With VMware vMotion, VM migration (CPU, memory, network state) occurs without interrupting running VMs (there is no downtime). VMware vMotion is the key feature for the proper work of DRS.

CHAPTER - 2

REQUIREMENT ANALYSIS AND SYSTEM SPECIFICATION

2.1 FEASIBILITY STUDY (TECHNICAL, ECONOMICAL, OPERATIONAL)

2.2 SOFTWARE REQUIREMENT SPECIFICATION DOCUMENT

which must include the following:

Functional Requirement:

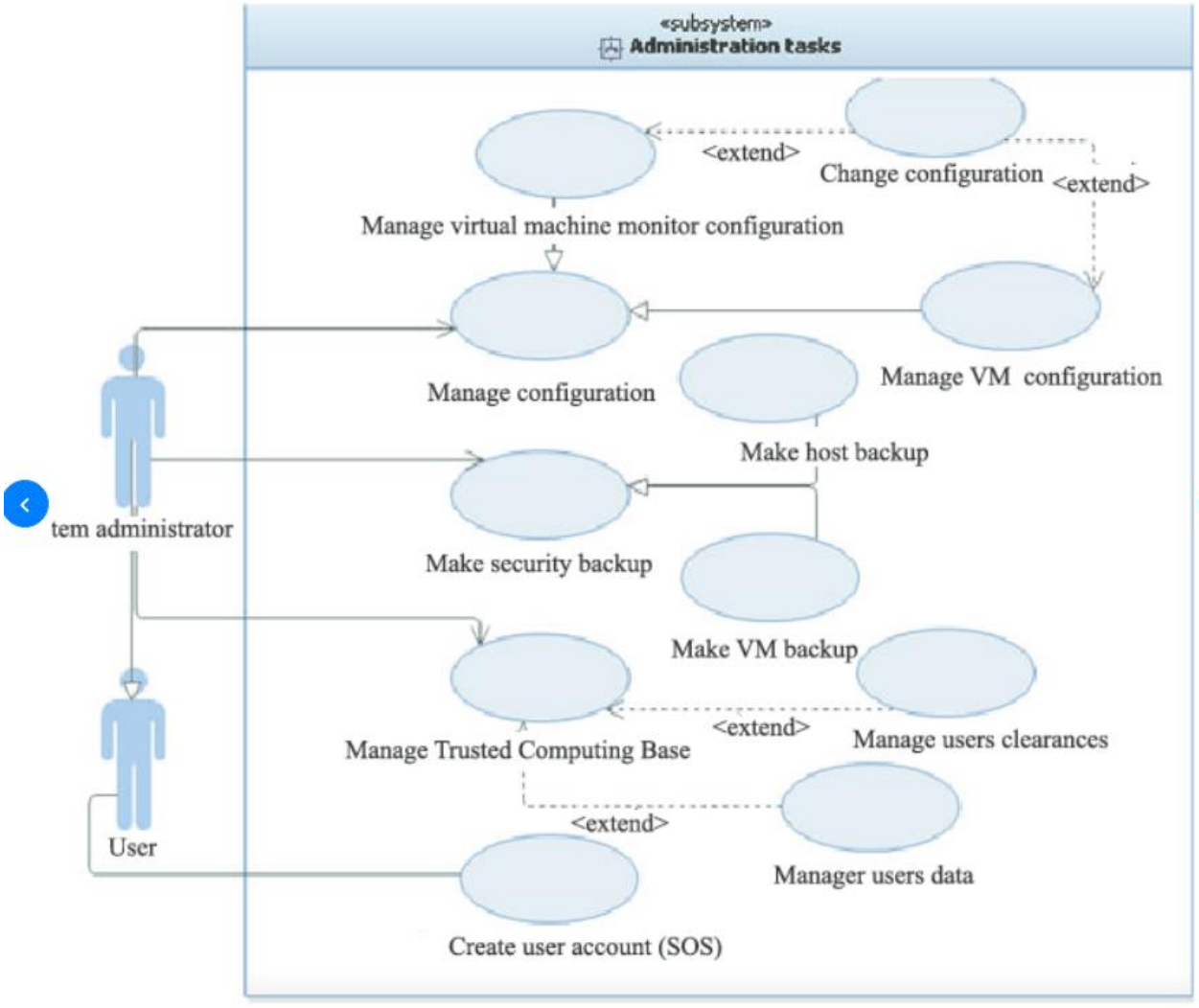


Figure 2.1: Functional requirement

Functional Requirement (FR) is a description of the service that the software must offer. It describes a software system or its component. A function is nothing but inputs to the software system, its behaviour, and outputs. Functional requirements include VM workstation, ESXi Thick client, Linux and windows ISO images, vSphere Thick client, PUTTY.

This is the software that you need when using a VM.

- VMware vSphere Hypervisor (ESXi) version 6 or higher, installed onto bare-metal hardware.
- VMware vCenter Server, required to install the AWS Elemental OVA.
- VMware vSphere web client or desktop client.

System requirement:

The resources that you have available impact your performance. The resources determine the speed for encoding assets and the number of streams, bitrate, and type of encoding that's possible. We recommend the following hardware specifications for optimum performance.

- RAM: 32 GB
- Disk space: 1 TB
- CPU cores: 32
- Processor speed: 2.0 GHz or more (Comparable to an Intel Xeon processor E5-2650)
- IP= 192.168.19.6
- Subnets: 255. 255.255.0
- DNS = 192.168.19.2

Requirement	Details
2 VMs (per stage)	• Hardware Requirements: ◦ vCPU - 8 ◦ RAM - 16 GB ◦ OS Disk - 100 GB ◦ HDD - 500 GB (Thin provisioned) • Software Requirements: ◦ Guest OS. CentOS 7 and above. ◦ Software Packages. You must install specific software packages on the VMs used in Stage-1 and Stage-2 testing. See the relevant sections for more information. • Connectivity Requirements: ◦ Network Connectivity to manage VLANs of ESX hosts. ◦ Internet Connectivity is required to access VMware repository and to install additional software. ◦ SSH enabled for root user. ◦ Access to the ESXi Management VLAN and the Management VM VLAN.

Figure 2.2: Hardware requirement

To secure your virtual machines, keep the guest operating systems patched and protect your environment just as you protect your physical machine. Consider disabling unnecessary functionality, minimize the use of the virtual machine console, and follow other best practices.

Protect the guest operating system

To protect your guest operating system, make sure that it uses the most recent patches and, if appropriate, anti-spyware and anti-malware applications. See the documentation from your guest operating system vendor and, potentially, other information available in books or on the Internet for that operating system.

Disable unnecessary functionality

Check that unnecessary functionality is disabled to minimize potential points of attack. Many of the features that are used infrequently are disabled by default. Remove unnecessary hardware and disable certain features such as host-guest filesystem (HGFS) or copy and paste between the virtual machine and a remote console.

See Disable Unnecessary Functions Inside Virtual Machines.

Use templates and scripted management

Virtual machine templates enable you to set up the operating system so that it meets your requirements, and to create other VMs with the same settings.

If you want to change virtual machine settings after initial deployment, consider using scripts, for example, PowerCLI. This documentation explains how to perform tasks using the GUI. Consider using scripts instead of the GUI to keep your environment consistent. In large environments, you can group virtual machines into folders to optimize scripting.

For information on templates, see Use Templates to Deploy Virtual Machines and the *vSphere Virtual Machine Administration* documentation. For information on PowerCLI, see the VMware PowerCLI documentation.

Minimize use of the virtual machine console

The virtual machine console provides the same function for a virtual machine that a monitor on a physical server provides. Users with access to a virtual machine console have access to virtual machine power management and to removable device connectivity controls. As a result, virtual machine console access might allow a malicious attack on a virtual machine.

Consider UEFI secure boot

You can configure your virtual machine to use UEFI boot. If the operating system supports secure UEFI boot, you can select that option for your VMs for additional security. See Enable or Disable UEFI Secure Boot for a Virtual Machine.

2.3 EXPECTED HURDLES

1. Resource distribution

The way virtualization partitions systems can result in varied ways — some might function really well, and others might not provide users access to enough resources to meet their needs. Resource distribution problems often occur in the shift to virtualization and can be fixed by working on capacity planning with your service provider.

2. VM Sprawl

VM sprawl, the unchecked growth of virtual machines in a virtual environment, as any virtualization admin knows, can cripple an otherwise healthy environment. It is problematic because its underlying cause often stays hidden until it manifests in resource shortages.

You should look at how virtual machines will be managed, who will be doing what, and what systems you're going to use. One of the optimal times to develop an overall management plan is when you're in a testing phase, before migration.

3. Backward compatibility

Using legacy systems can cause problems with newer virtualized software programs. Compatibility issues can be time-consuming and difficult to solve. A good provider may be able to suggest upgrades and workarounds to ensure that everything functions the way they should.

4. Performance monitoring

Virtualized systems don't lend themselves to the same kind of performance monitoring as hardware like mainframes and hardware drives do. Try tools like VMmark to create benchmarks that measure performance on virtual networks and to monitor resource usage as well.

5. Backup

In a virtualized environment, there is no actual hard drive on which data and systems can be backed up. This means frequent software updates can make it difficult to access backup at times. Software programs like Windows Server Backup tools can make this process easier and allow backups to be stored in one place for easier tracking and access

CHAPTER – 3

SYSTEM DESIGN

3.1 DESIGN APPROACH

Virtualization is the modern way to maximize IT resources. Virtualization can apply to applications, servers, storage, and networks and is the single most effective way to reduce IT expenses while providing users better access to systems from wherever they are working.

With virtualization, applications are contained in virtual machines (VMs) which are isolated from each other but share a pool of resources managed by a hypervisor. But without the proper planning your virtualization project could be destined to fail.

It All Starts with the Architecture. There are many virtualization hypervisors in the marketplace today, from the big players such as VMware and Microsoft, to the open-source Linux built systems.

All these platforms were created to allow the end user to create and run virtual machines within the user's environment.

An important factor to consider when selecting which hypervisor to deploy comes down to price versus dependability/reliability, where the goal of the virtualization design should be to provide high availability for mission critical applications.

The first step in any virtualization architectural project is to understand what the cost of downtime would mean to the business.

The higher the cost of downtime, the more robust the design should be. All projects must begin with a thorough understanding of the company’s current environment and the expectations or vision of the company's leaders.

3.2 DESIGNING A VIRTUALIZATION APPROACH:

There are many details to consider when designing a virtualization infrastructure.

1. Physical Equipment
   - Computing servers
   - Storage networks and storage devices
   - IP networks
   - Management servers
   - Networking

2. Production network
   - DR/backup network
   - Storage network
   - DMZ network

3. Backups
   - Host system
   - Storage system

4. Virtual Environment
   - Hosts
   - Clusters
   - Resource pools
   - Network
   - Virtual machines
   - vMotion
   - DRS
   - HA
   - Licensing

5. Windows licenses
   - VMware licenses
   - Backup licenses

3.3 USER INTERFACE DESIGN:

First, we download and install the VMware Workstation Player. We use the version 16 of the VMware player. The version of the player does not make any difference as long as it is compatible with your operating system.

Figure 3.1: VMware Workstation Player website

After the installation is completed, The VMware Workstation Player is ready to use.

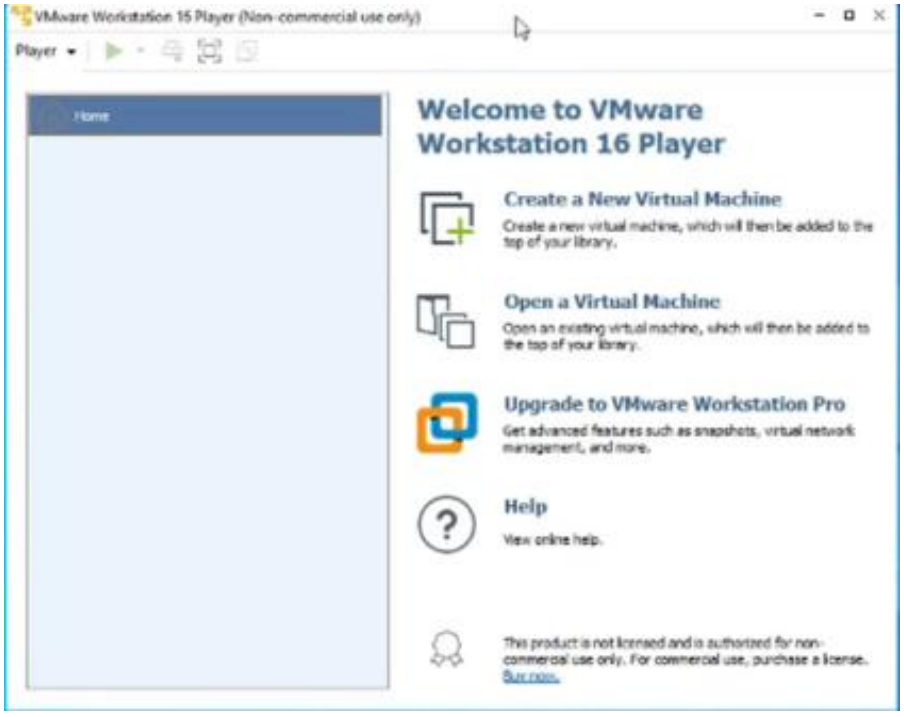


Figure 3.2: VMware Workstation 16 Player

Next, we download and install an ESXi server on our VMware Workstation Player. We choose ESXi version 6.5 because most of the companies use the versions 6.0 or 6.5.

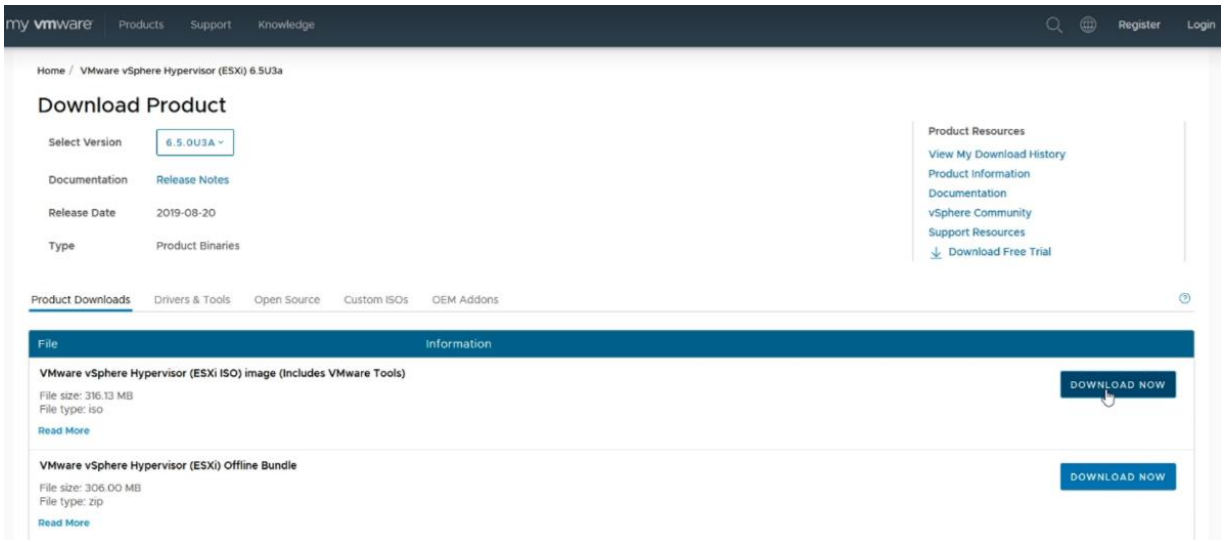


Figure 3.3: VMware vSphere Hypervisor ESXi

After downloading, the VMware Player detects the disc file of ESXi and the installation takes place on VM which in turn shows the ESXi server's interface in a yellow and black screen.

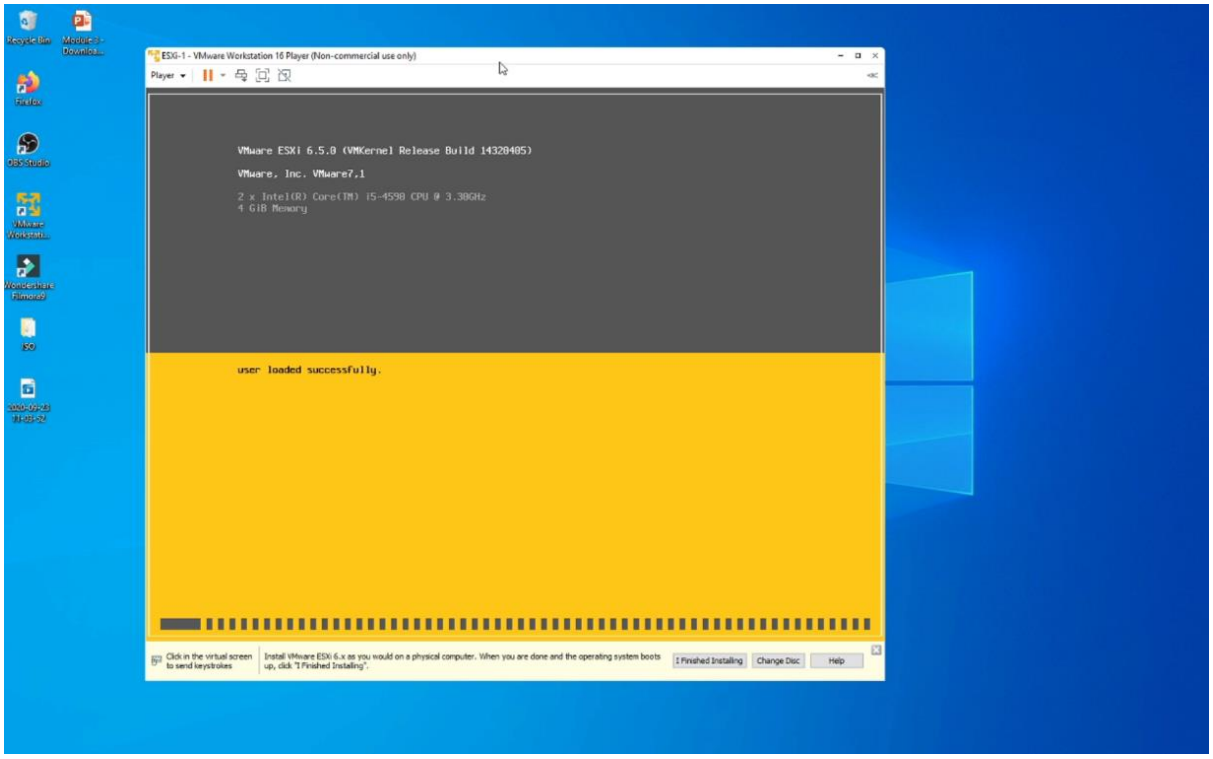


Figure 3.4: ESXi-1 server

The next step includes creating the first Virtual Machine (VM) on the VMware Player. We install Linux operating system with CentOS version 7 on our ESXi server.

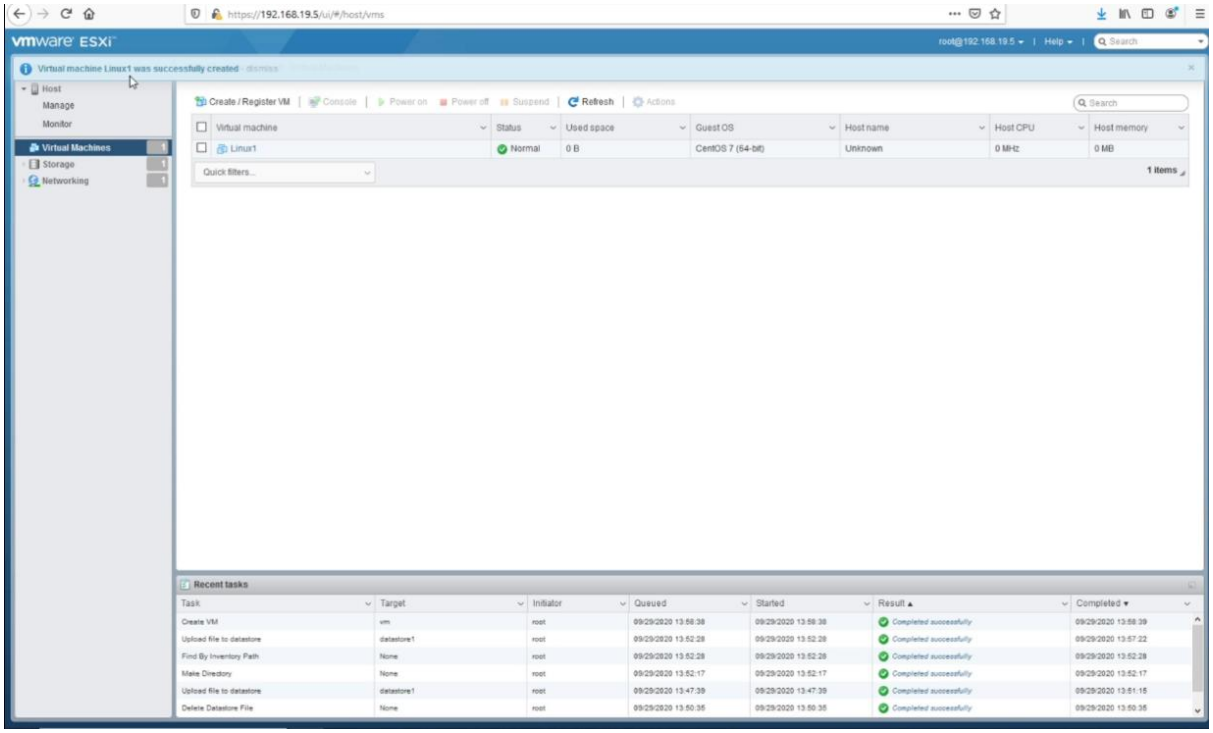


Figure 3.5: Virtual Machine (Linux)

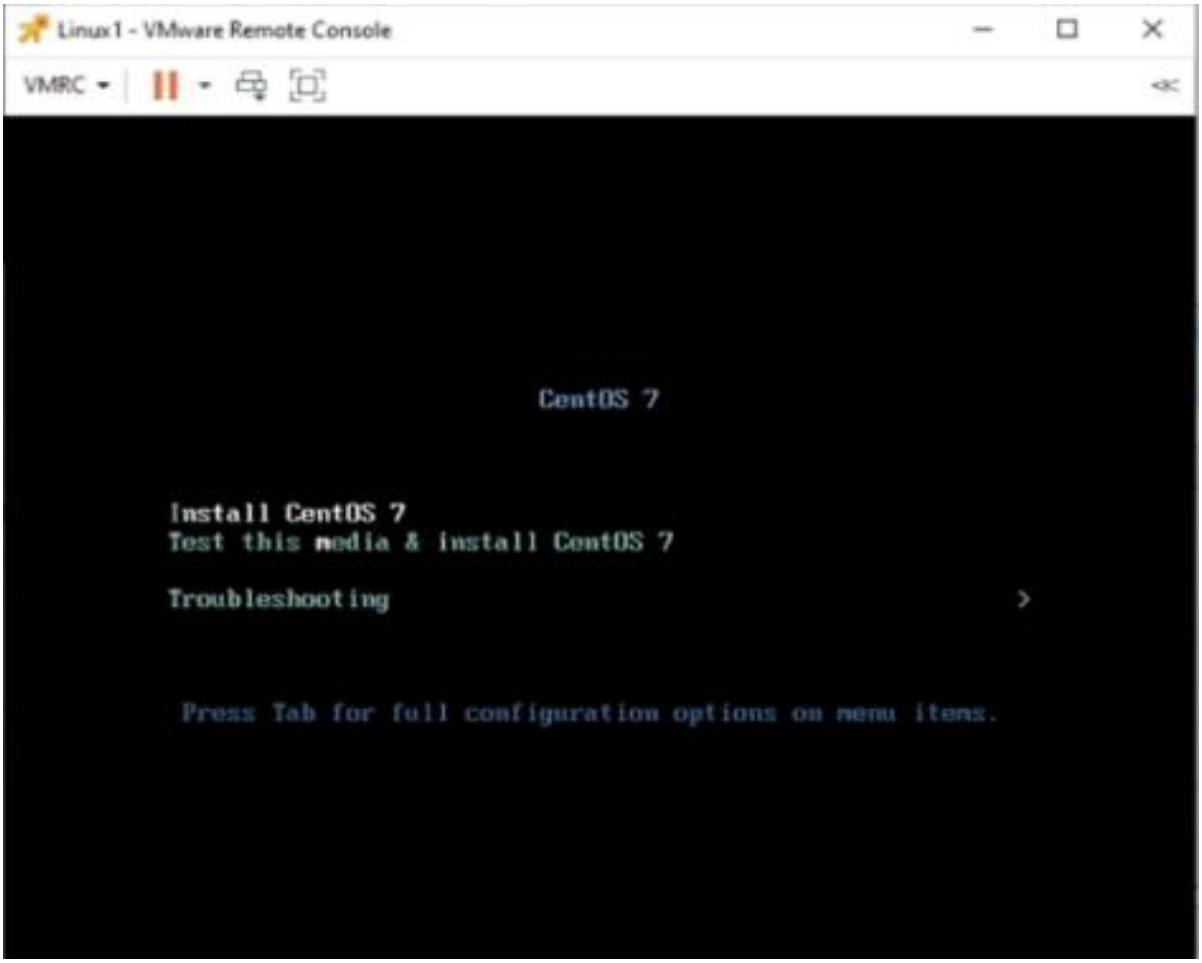


Figure 3.6 : CentOS 7 installation

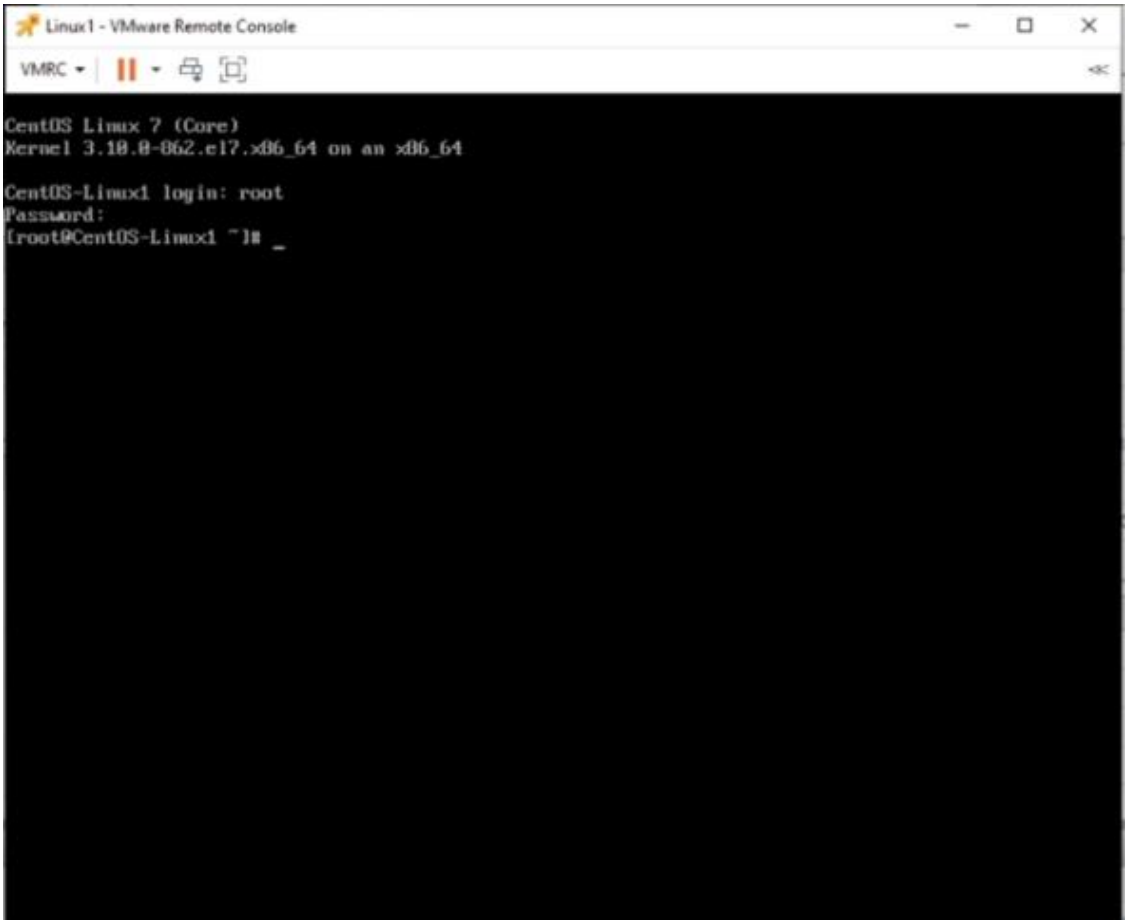


Figure 3.7: Linux CentOS 7

Next, we create another Virtual Machine on which we install Windows with help of an ISO file by attaching it to the ESXi server which later detects it and proceeds further.

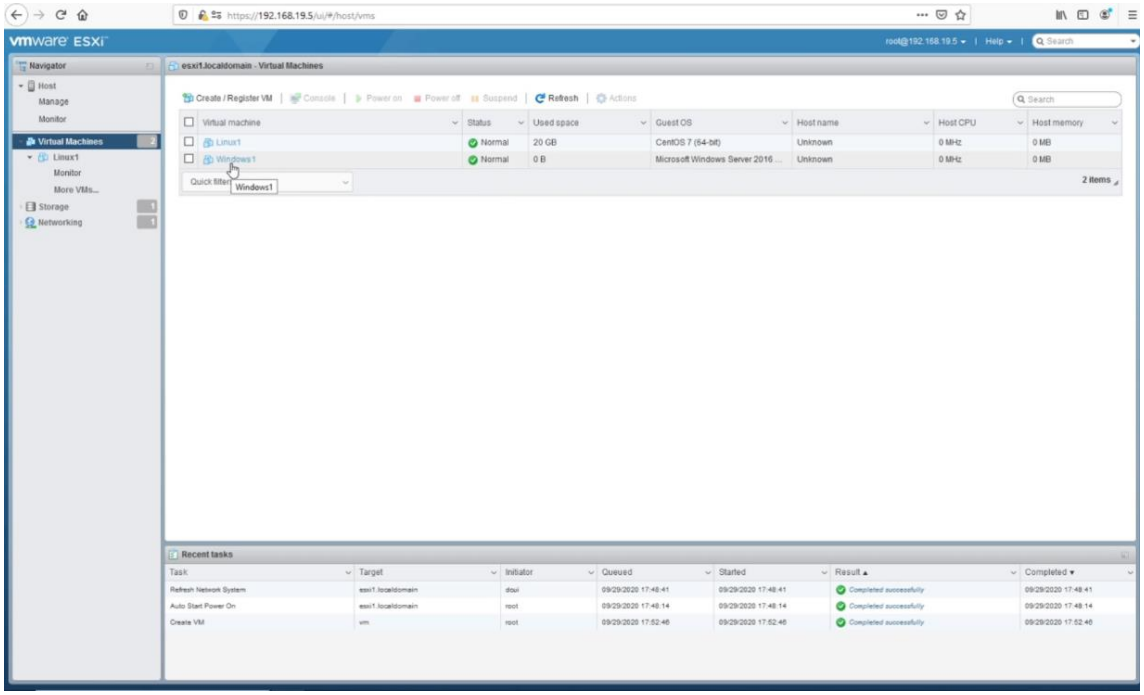


Figure 3.8: Virtual Machine (Windows)

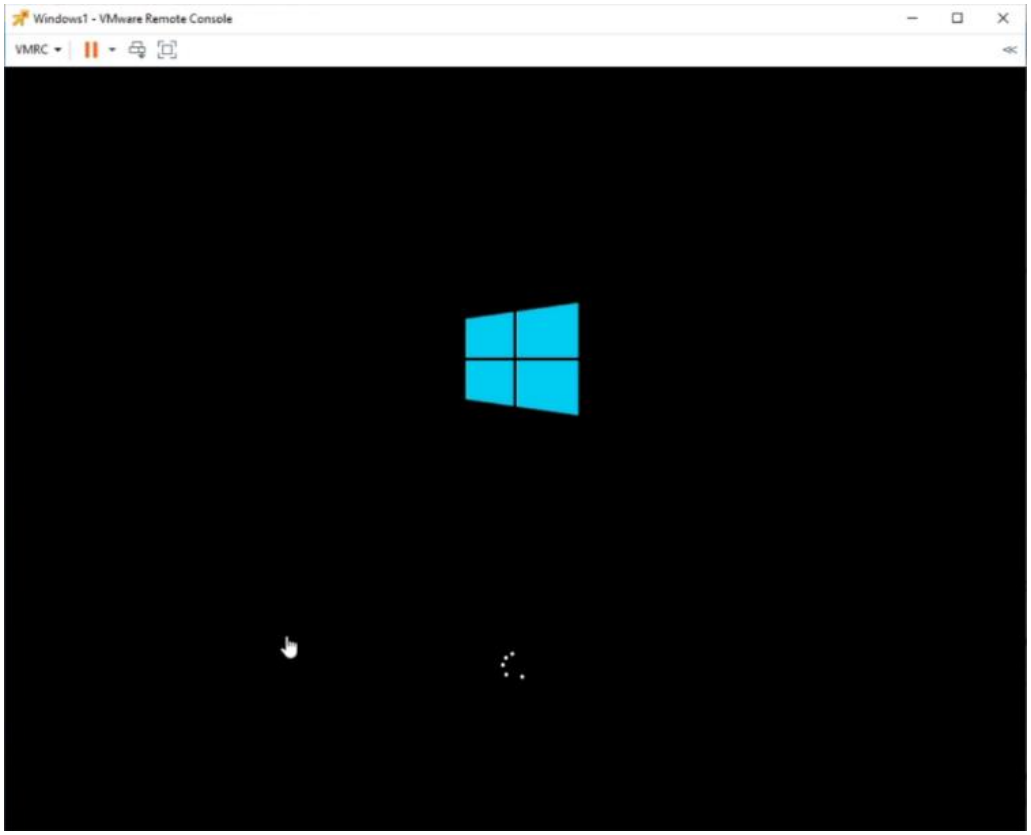


Figure 3.9: Windows installation

After the installation is completed, the welcome screen of Windows appears.

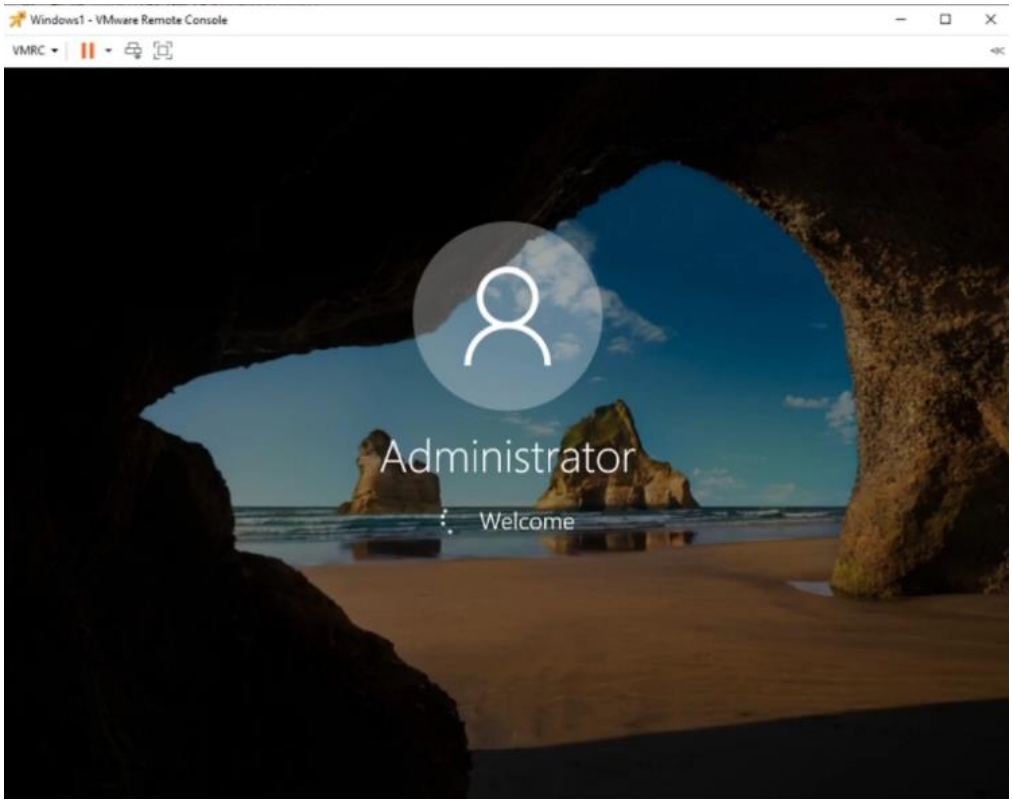


Figure 3.10: Windows welcome screen

Now, we install another ESXi server to organize vCenter on it.

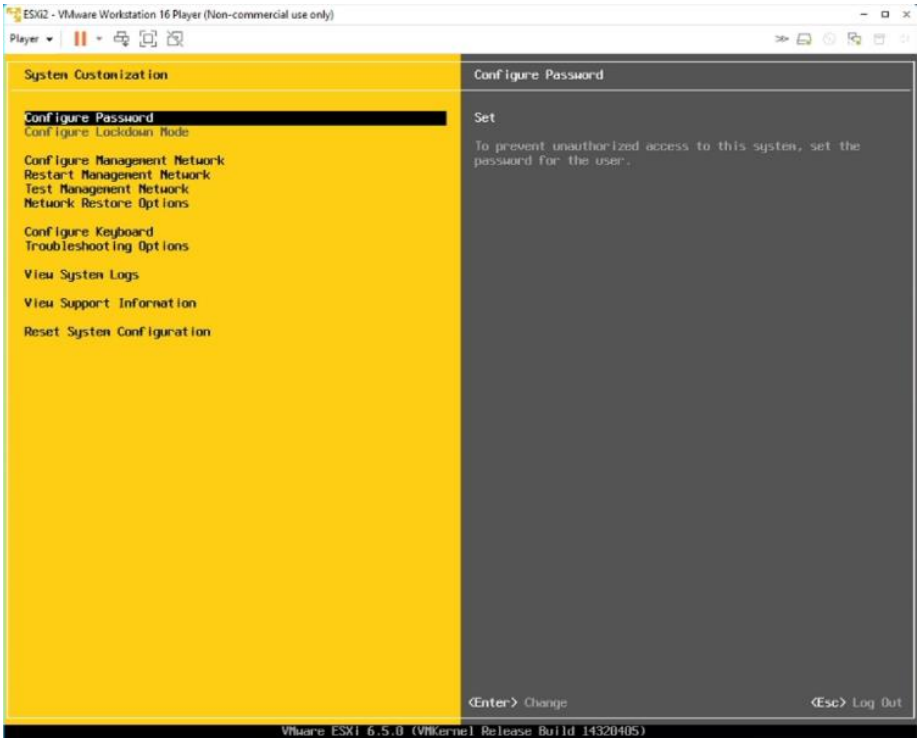


Figure 3.11: ESXi-2 server

After installing the second ESXi server, we download and install vCenter which helps to manage two or more virtual machines, their operating systems and applications, and provides a smooth and hassle-free work experience to the user.

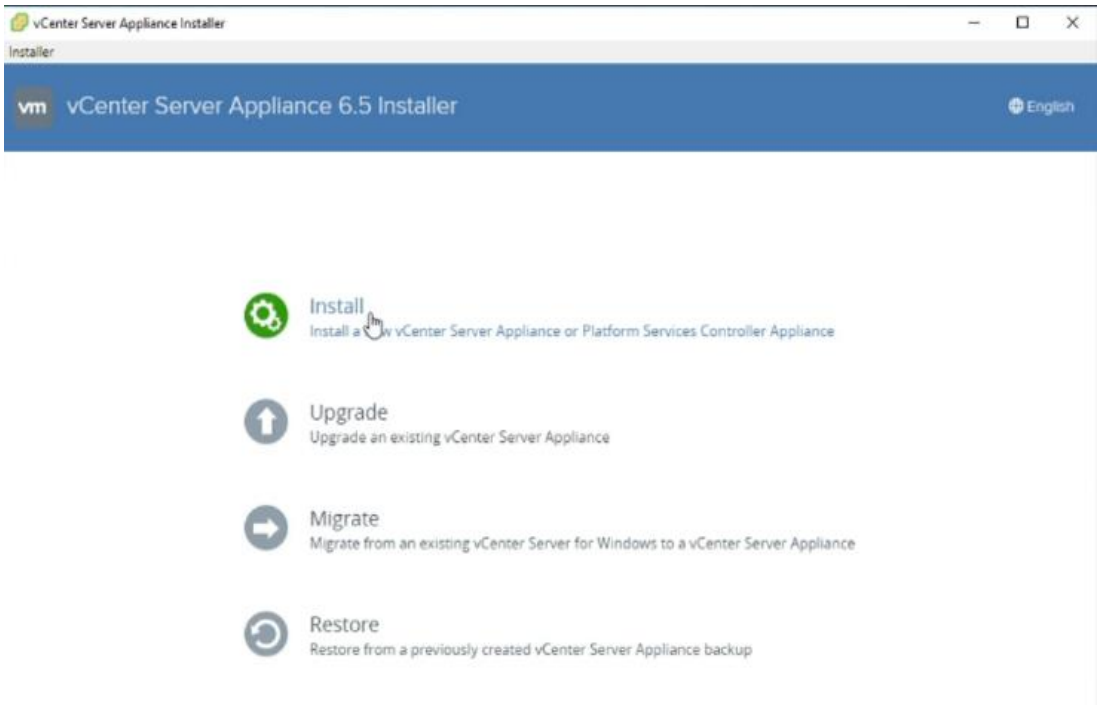


Figure 3.12: vCenter installer

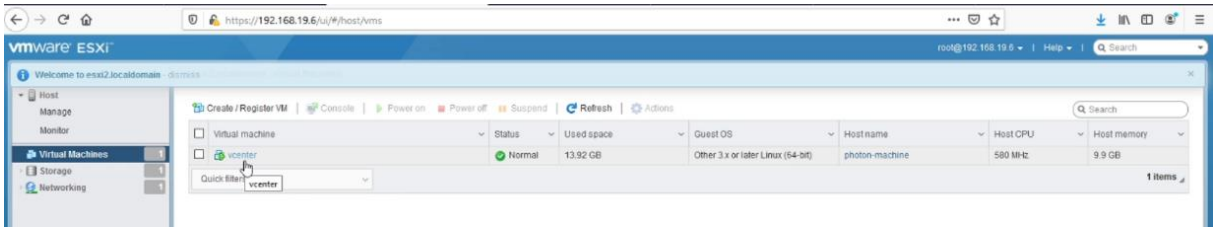


Figure 3.13: Virtual Machine (vCenter)

3.4 METHODOLOGY OF SYSTEM:

This section includes the downloading, installing, configuring, and setting up our system where we implement our virtualization, i.e., VMware lab. Setting up VMware lab with all most of the components of Vmware is not very straightforward. There are so many pieces of VMware that has to be installed and configured.

A regular VMware virtualization design consists of a physical server with a hypervisor on top of it. We can install this hypervisor on any machine which does not have any operating system. Then we spin up all different kinds of operating systems and then we run all different kinds of applications. The hypervisor can be managed by accessing it through the vSphere Web Client. But if the physical server dies in any case, then all the operating systems and all the applications running on that physical server die with it.

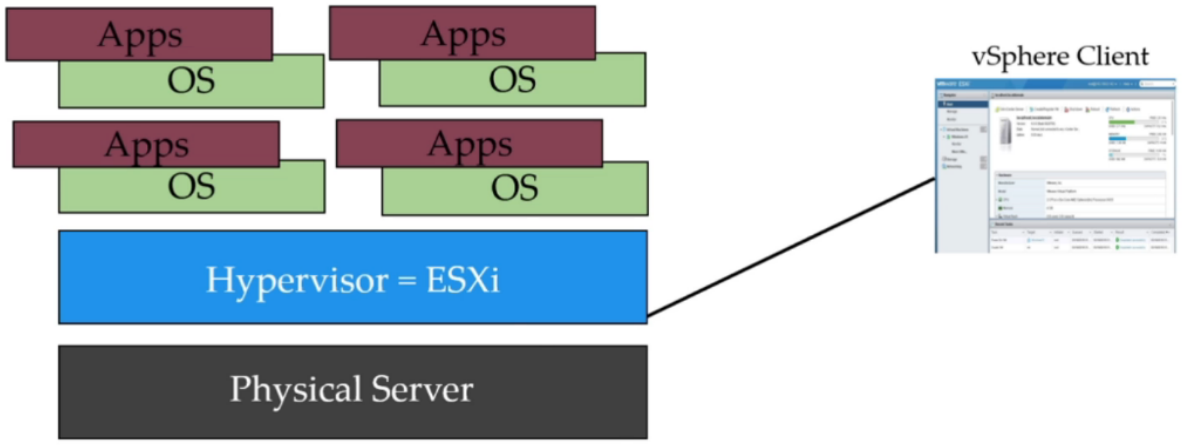


Figure 3.14: vSphere Client

With VMware server virtualization, a hypervisor is installed on the physical server to allow for multiple virtual machines (VMs) to run on the same physical server. Each VM can run its own operating system (OS), which means multiple operating systems can run on one physical server. All the VMs on the same physical server share resources, such as networking and RAM.

The lab is designed with redundancy, i.e., we have one physical server on which we organize virtualization (ESXi) and then we run operating systems and applications. Then we put a second and a third physical server, all of which will become hypervisors which will be managed through vCenter. So, if one physical server goes down, it can move its operating system to the second one, or to the third one depending on where the resources are. A software is needed to manage this kind of cluster, and hence we use vCenter here. This vCenter server can be installed on ESXi server itself to manage all the ESXi servers. All of these are put under one software, i.e., VMware Workstation Player.

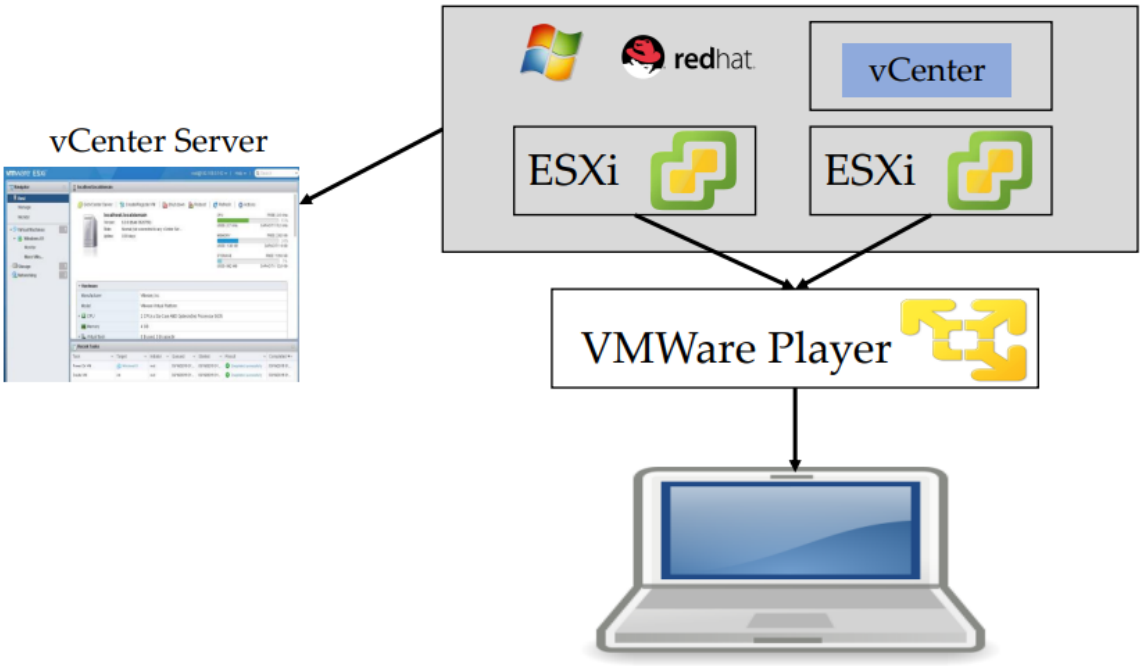
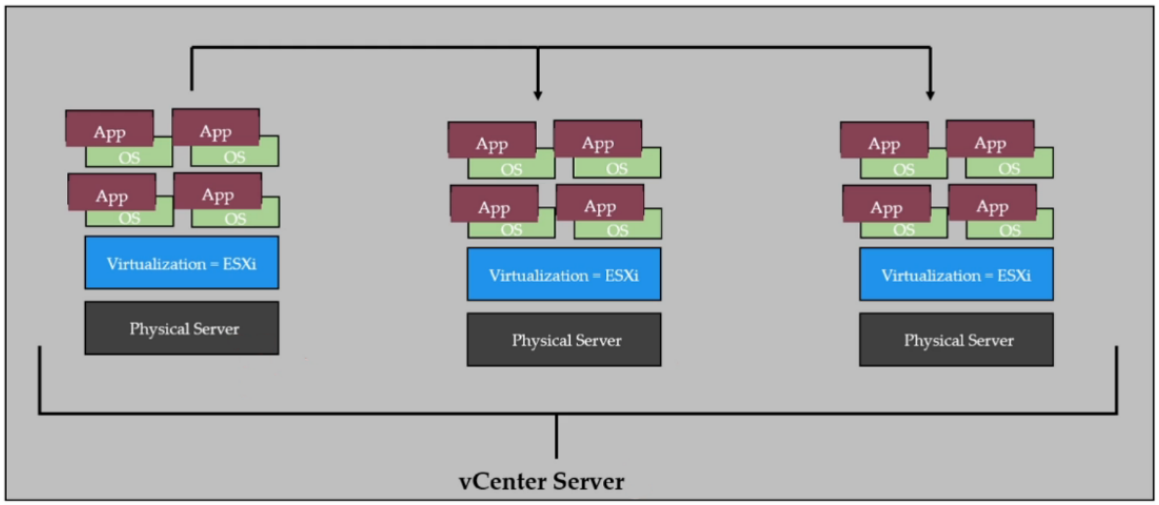


Figure 3.15: vCenter Server

Basically, on our desktop computer or laptop, we install VMware Workstation player on it. Then we create a virtual machine and install ESXi server (with 4GB of memory) on it. Then we install another ESXi server on which we will run vCenter, which will control and access this system through vCenter Client Portal.



VMWare Workstation Player

Figure 3.16: VMware Workstation Player

The first step is to install VMware Workstation Player on our system, and then we create a virtual machine on which ESXi server will be installed. It is like creating a virtual machine within a virtual machine.

We create one ESXi with 4 GB of RAM and we can have Windows or Linus or both. Then for redundancy, we install another ESXi with 12 GB of RAM on which we run vCenter and vCenter requires 10 GB of RAM and at least 250 GB of hard disk.

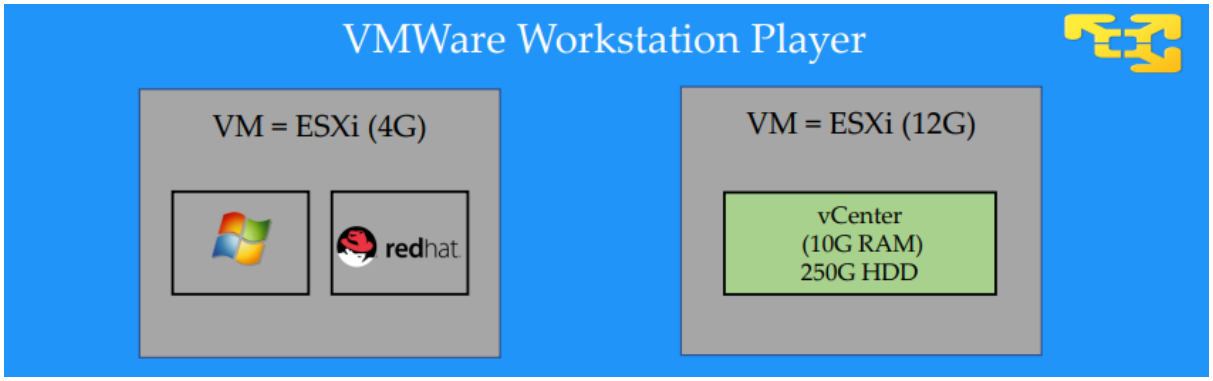


Figure 3.17: ESXi hosting on VMware Player

CHAPTER – 4

IMPLEMENTATION, TESTING AND MAINTENANCE

4.1 TOOLS AND TECHNOLOGIES USED FOR IMPLEMENTATION

VMWare:

VMWare, Inc. is an American publicly traded software company from California, USA. It provides cloud computing and virtualization software and services. It was one of the first commercially successful companies to virtualize the x86 architecture in 1998.

VMWare has approximately 80% of the virtualization market share.

The company came up with the name **V M Ware** which means **Virtual Machine Ware**, implying to the combination of the terms: software (which we cannot touch) that runs on top of the hardware (which we can touch physically).

There are two main virtualization software:

1. VMWare Player: Runs over an operating system
2. VMWare hypervisor: Bare-metal hypervisor runs over a hardware without having any operating system

Importance of VMWare:

- System administration
  - Linux, Windows, Solaris, or any OS
- Network/Storage administration
  - Switches, routers, firewall
  - Fiber switches, storage array etc.
- Programming or development
  - Automation or testing
- Database or application administration
  - DB or apps run on OS and OS runs on VMs
- Cloud
  - Approx. 90% of the cloud infrastructure run on virtual environment
- Any IT Job
  - QA, IT Technician, System or Network Architecture, Data Science, Security

Fig.4.1: VMware

Products of VMWare:

- **VMWare Workstation Player**

VMWare Workstation Player (formerly known as Player Pro) is a free desktop application from VMWare. It is a much simpler virtualization application that allows you to easily and quickly create and run virtual machines using a user interface that is designed to be as simple as possible.

VMWare Workstation Player is an ideal utility for running virtual machines on Windows, Linux, or MAC computers. Organizations use Workstation Player to deliver managed corporate desktops, while students and educators use it for learning and training. The free version is available for non-commercial, personal, and home use.

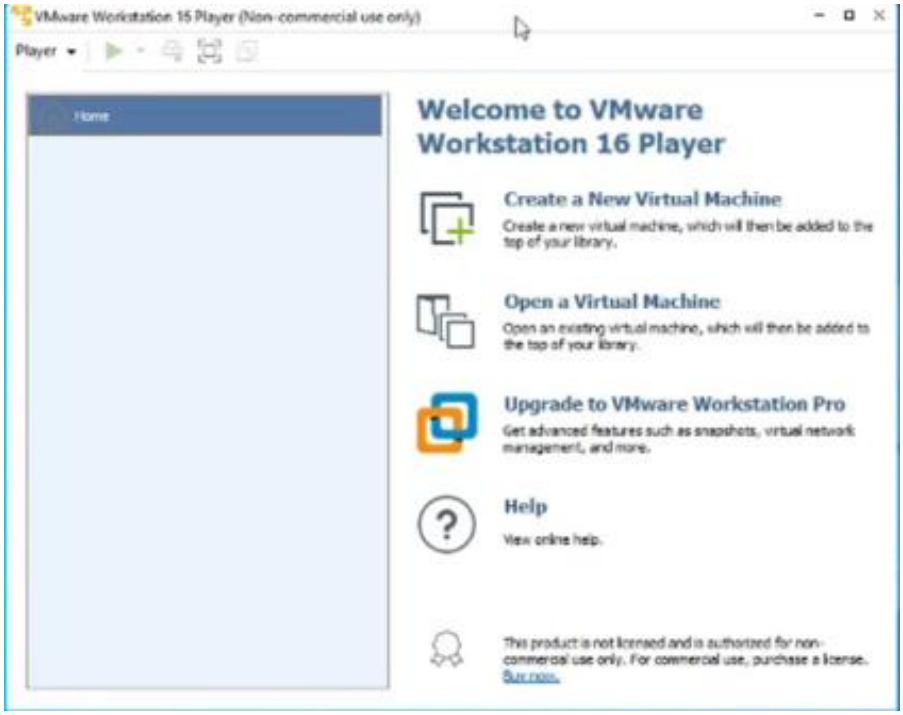


Fig.4.2: VMware Workstation 16 Player

- **VMWare vSphere Hypervisor (ESXi)**

VMware ESXi Server is a bare metal (Type-1) hypervisor that was developed for vSphere, VMware's server virtualization and container-based application development software. A hypervisor can be thought of as an operating system that allows multiple virtual machines, virtual appliances, and containers to run efficiently on the same physical server.

ESXi is one of the two core components of vSphere, VMware's popular management system for containers and virtual machines (VMs). ESXi servers are managed by a VMkernel (based on the Linux kernel) and installed directly on a local disk in the host machine. Whenever a VMkernel receives a request for resources, the kernel presents the request to the host's physical hardware for fulfilment.

VMware Inc. developed ESXi as a bare-metal embedded hypervisor, which means it runs directly on server hardware and does not require the installation of an additional underlying operating system. The virtualization software creates and runs its own kernel, which is run after a Linux kernel bootstraps the hardware. The resulting service is a microkernel, which has three interfaces: Hardware, Guest system and Console operating system (service console).

VMware ESXi Server features include:

- Remote management tools.
- Application programming interface (API) integration that eliminates the need for administrators to install and control third-party management agents.
- A lightweight architecture and small code base.
- Command line scripting environments.
- Quick installation from a USB flash drive.
- Simple security configurations.

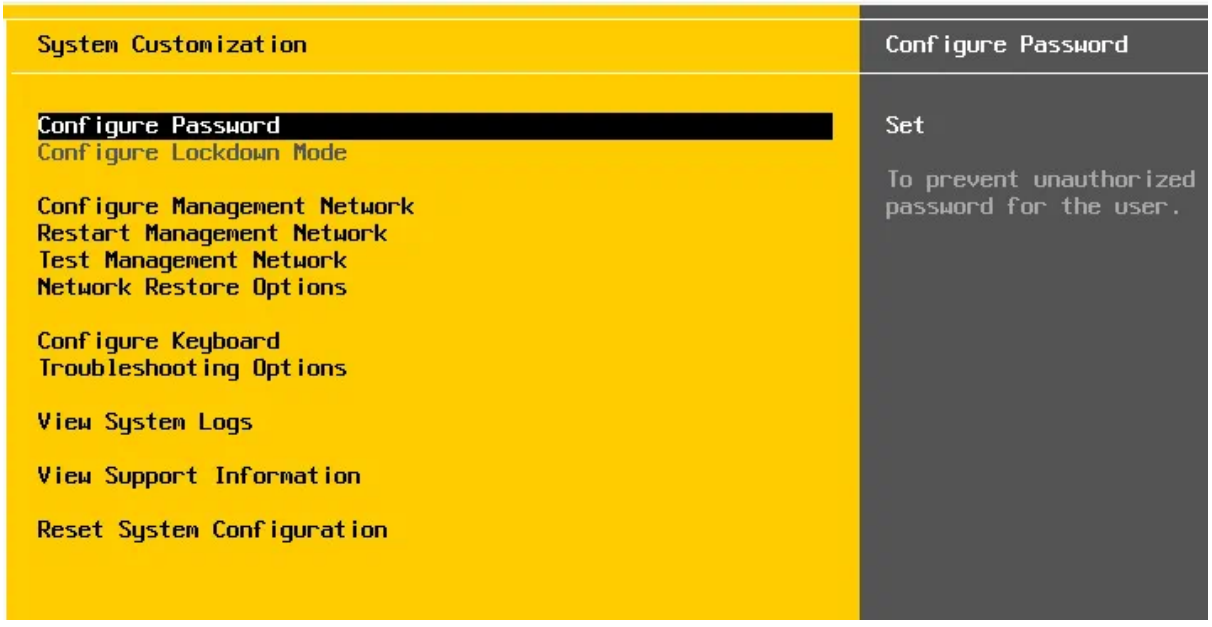
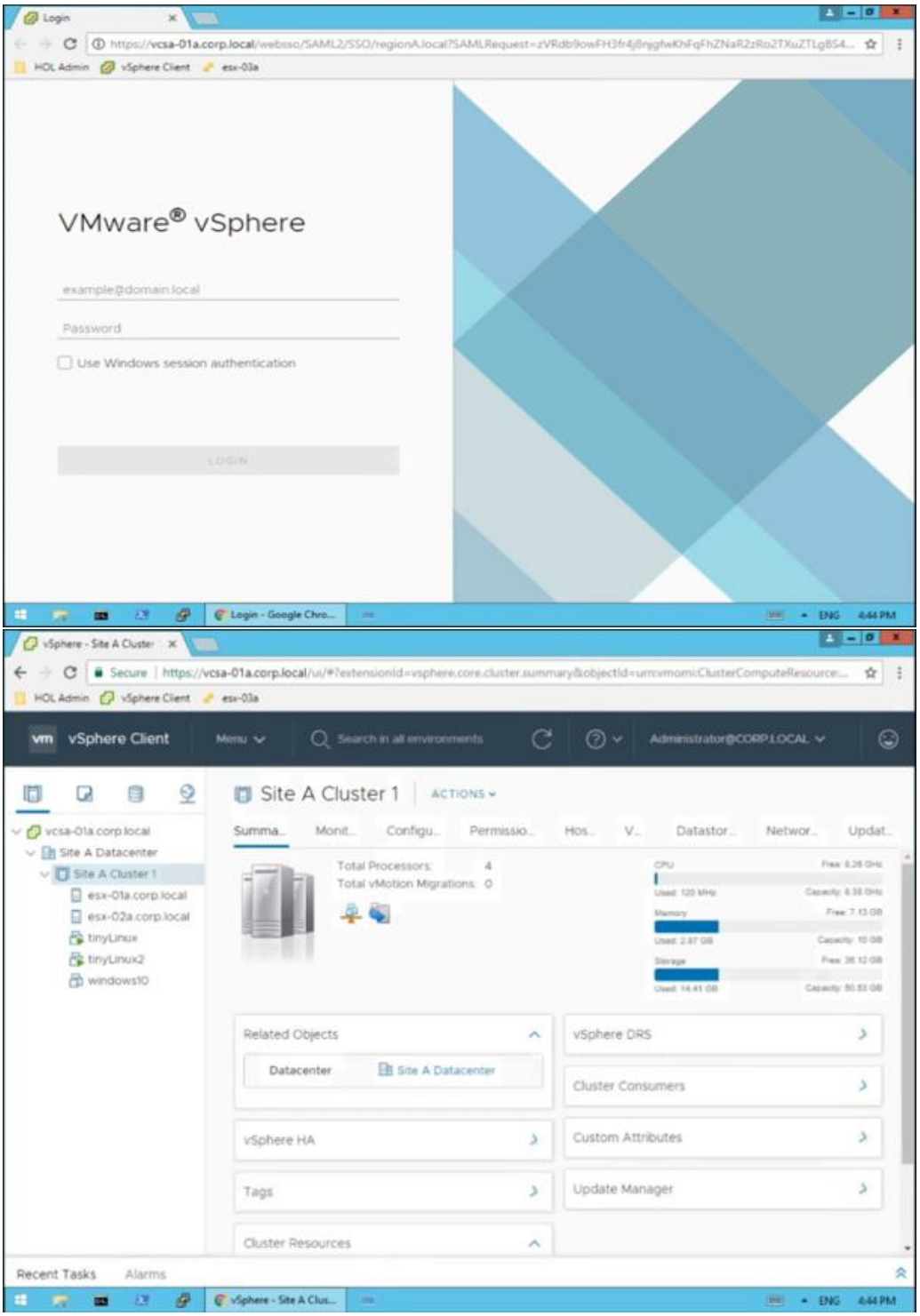


Fig.4.3: System Customization

- **VMWare vSphere Client**

vSphere is a cloud computing virtualization platform delivered by VMware. VMware vSphere is not a particular software, but rather a software package that has several sub-components. vSphere encompasses several individual products and technologies to provide a complete infrastructure for virtualization. It is an interface that allows you to connect to a hypervisor. It is a client just like RDP for Windows and Putty for Linux servers. It is now web-based client. The older version was thick client.



- **VMWare vCenter**

vCenter Server is an application that enables you to manage your vSphere infrastructure from a centralized location. It acts as a central administration point for ESXi hosts and their respective virtual machines. It is a management tool to manage multiple hypervisors. The interface is same as vSphere Client with added functionality.

vCenter Server can be installed on a supported version of Windows or you can use a preconfigured Linux version known as vCenter Server Appliance. vCenter Server is required for some advanced vSphere features, such as vSphere High Availability (HA), vSphere Fault Tolerance (FT), vSphere Distributed Resource Scheduler (DRS), and VMWare vSphere vMotion.

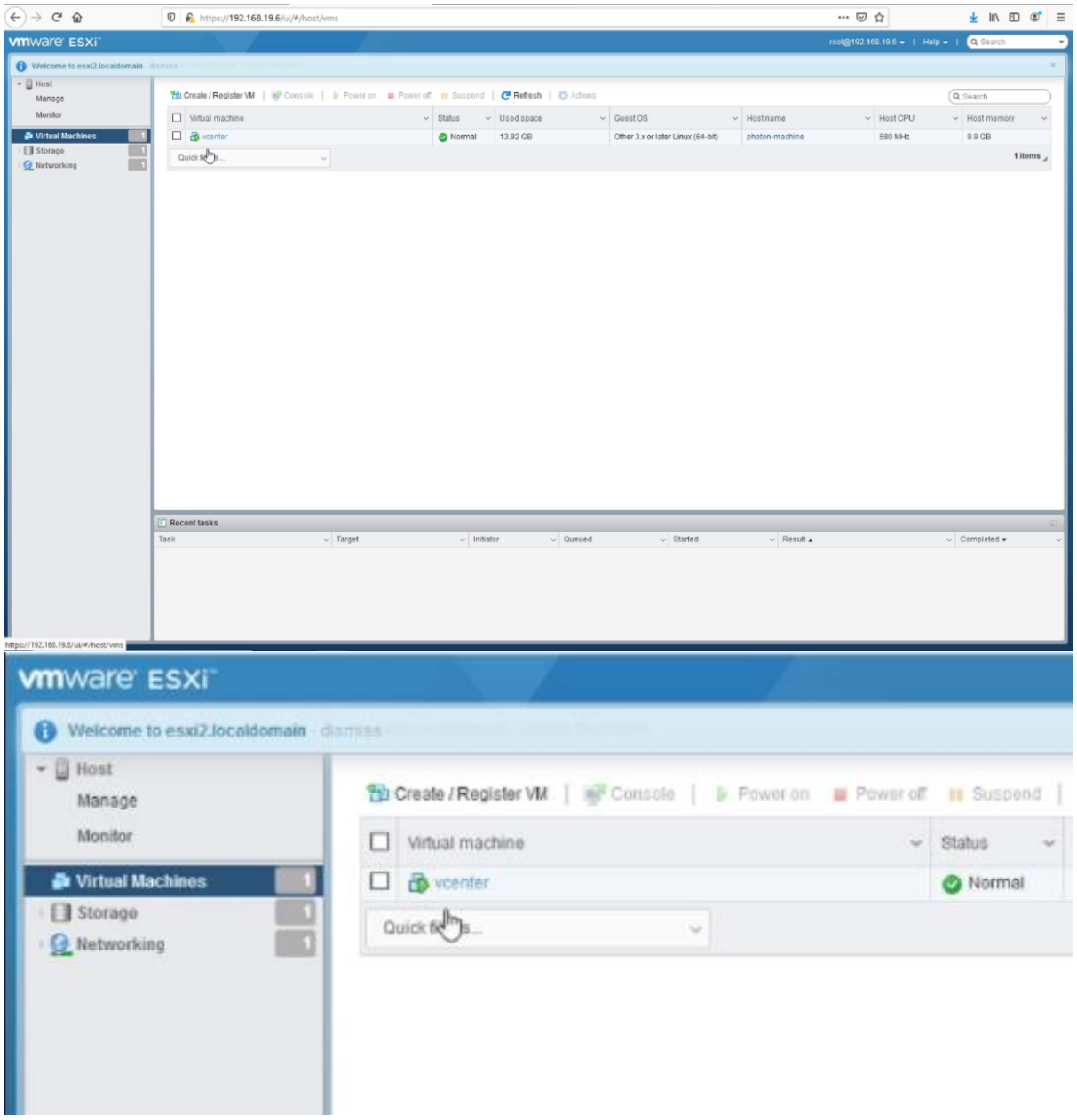


Fig.4.4: VMware ESXi

4.2 PLANNING A VIRTUALIZATION APPROACH:

1. Information Gathering

The best way to gather the required information about the existing environment is with a scanning tool such as SysTrack Virtual Machine Planner, Microsoft Assessment and Planning Toolkit, or VMware's Capacity Planner. These tools will capture information such as server host names, operating systems, the number and type of CPUs, and storage devices deployed, as well as provide CPU, memory, and network load metrics.

The goal here is to gather accurate metrics about the current environment that will help determine the proper design/configuration of a virtual implementation.

Equally as important as this technical information, you need to determine what is the vision, or end goal, from the perspective of the company's leadership team. You need to discuss costs, interview users, and pinpoint the project requirements.

2. Acceptable Risk Versus Budget

Often the acceptable risk and the budget are at odds with one another. Most businesses are not willing to incur the cost associated with their vision of a robust and scalable computing environment.

There is often no easy answer to this issue and compromises must be made. Companies must factor in the myriad costs associated with licensing, hardware/infrastructure upgrades, monitoring software, and staff retraining.

CHAPTER – 5

RESULTS AND DISCUSSIONS

5.1 USER INTERFACE REPRESENTATION

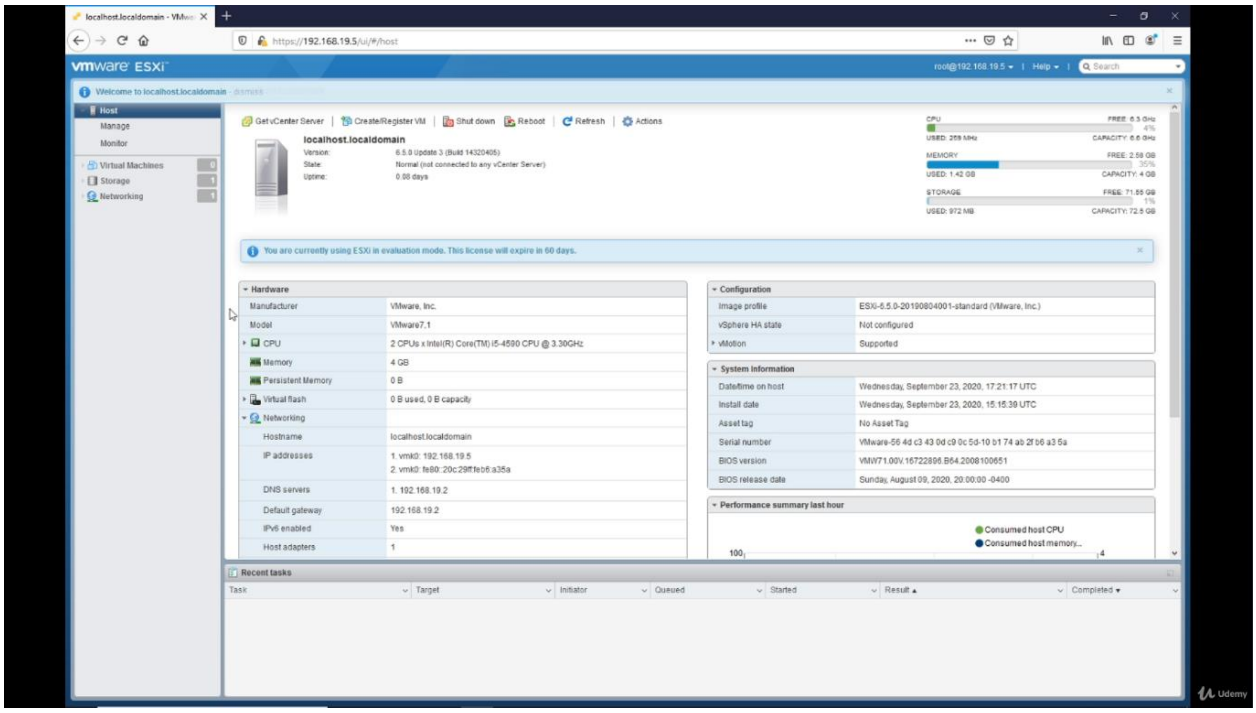


Fig. 5.1: VMware ESXi web console

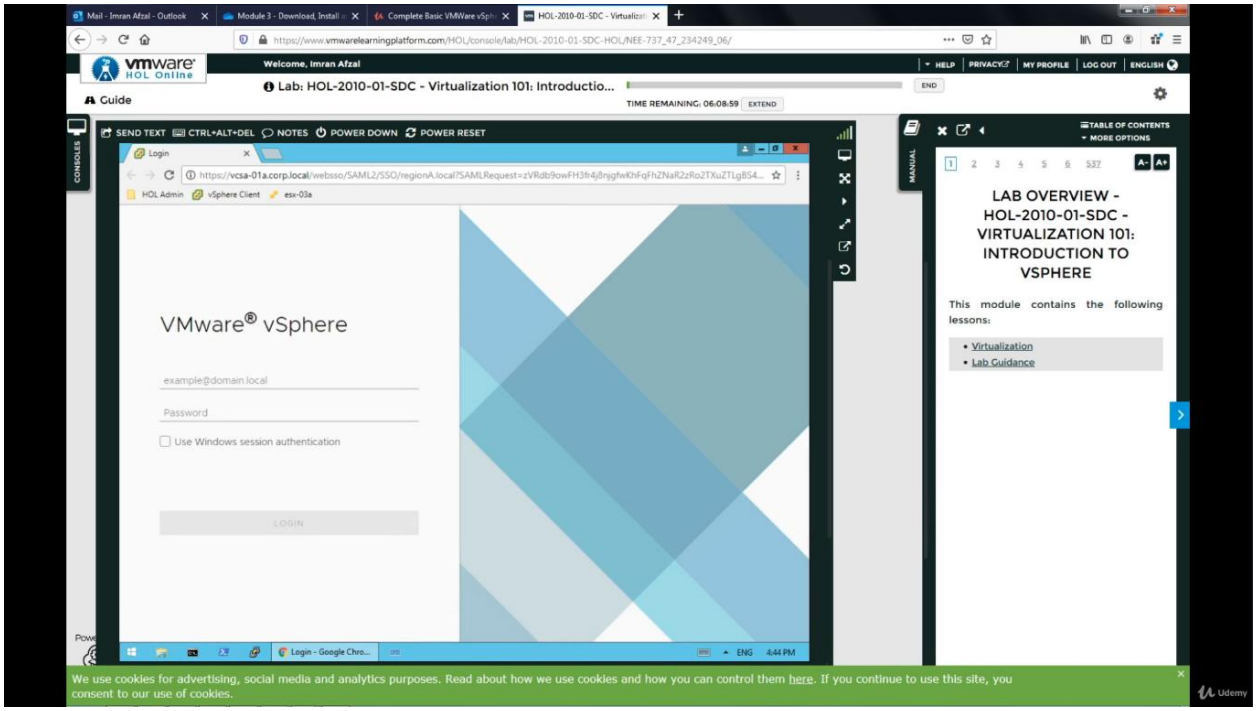


Fig 5.2: VMware vSphere web console

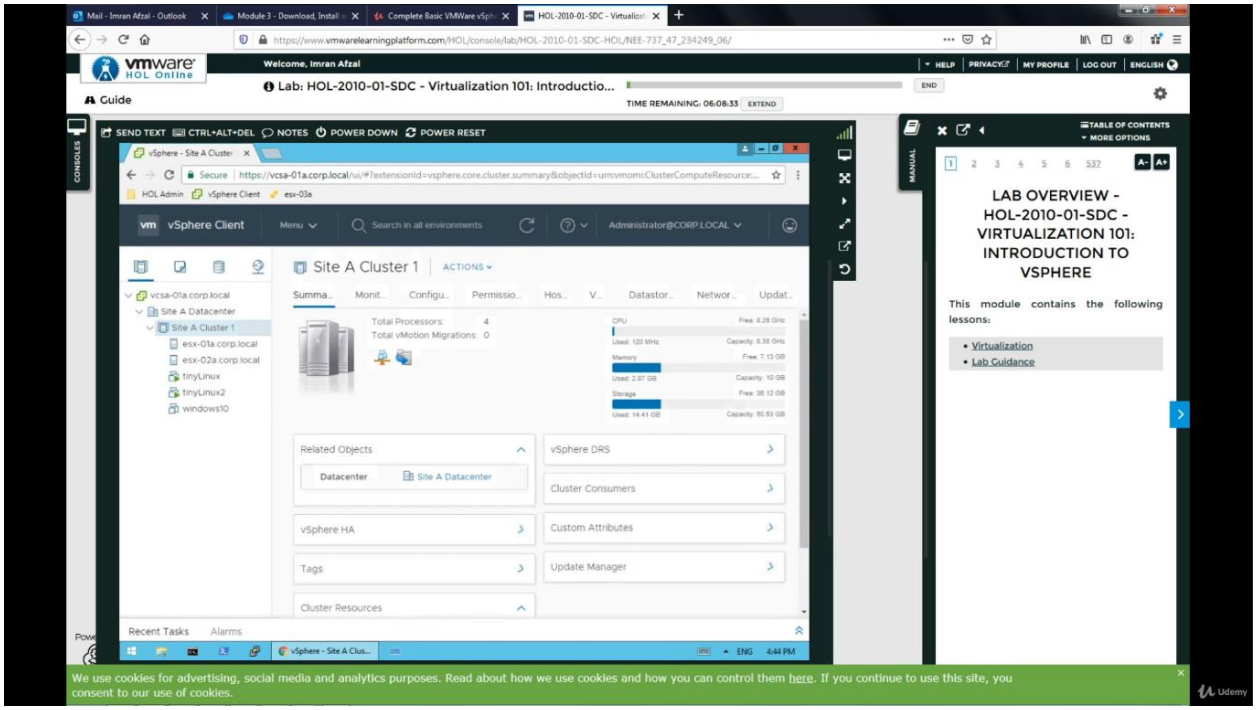


Fig. 5.3: VM vSphere Client

5.2 BRIEF DESCRIPTION OF VARIOUS MODULES OF THE SYSTEM AND SNAPSHOTS OF SYSTEM WITH BRIEF DETAIL OF EACH

• What is Virtualization?

Virtualization is the creation of a virtual -- rather than actual -- version of something, such as an operating system (OS), a server, a storage device or network resources.

Virtualization uses software that simulates hardware functionality to create a virtual system.

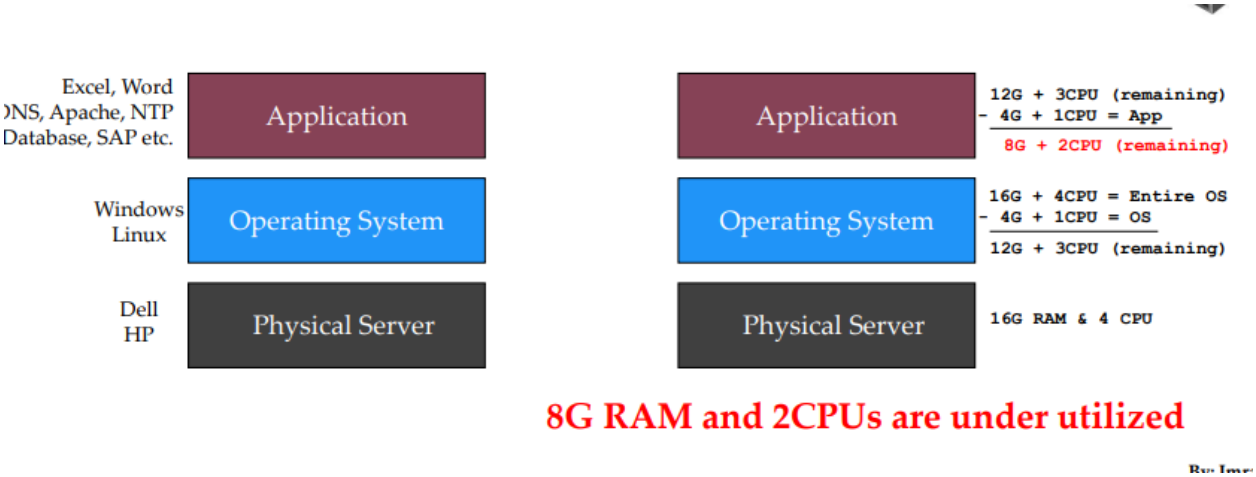


Fig. 5.4: Virtualization

• **How Virtualization Works?**

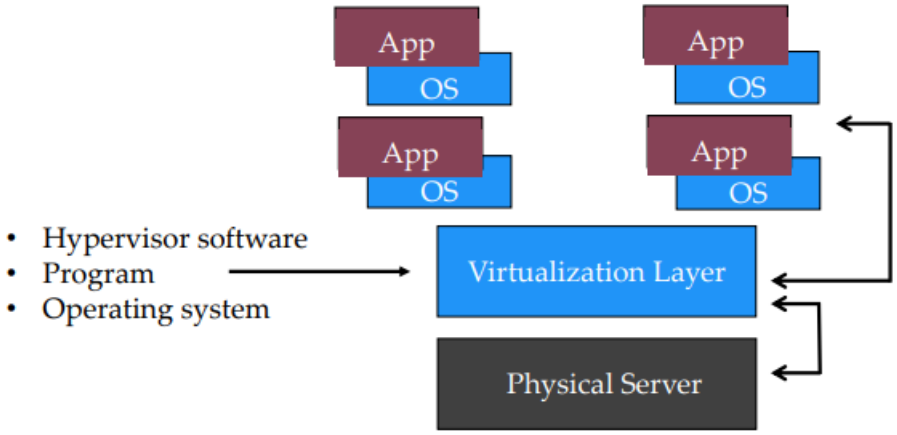


Fig. 5.5: Virtualization Working

• **Basic Virtualization Terms**

1. Bare-metal server = Physical server with NO OS
2. Hypervisor = Host or Virtual server
3. Virtual Machine = VM, Guest, Instance
4. Virtualization Manager = vCenter, OVM manager etc.
5. Virtual Desktop = VDI • P2V = Physical to virtual
6. V2V = Virtual to virtual
7. VM template
8. Snapshot
9. Clone or cloning

• **Benefits of Virtualization**

1. Cost $$$
2. Real estate
3. Electricity
4. Ease of management
5. Redundancy (lesser downtime)
6. Faster deployment of machines
7. Resource availability
8. Better testing and performance
9. Licensing

• **Virtualization Technology Companies**

Companies that host hypervisor are:

Company name	**Hypervisor**	**Cloud Technologies**
Vmware • Vmplayer	ESXi	Vcloud
Oracle • oracle virtualbox	OVM or OLNM	OCI
Microsoft	Hyper-v	Azure
Citrix	Xenser	Citric cloud
Red hat	KVM	Red hat cloud suite

Table 5.1: Companies that host hypervisor

• **Difference Between Virtualization and Cloud**

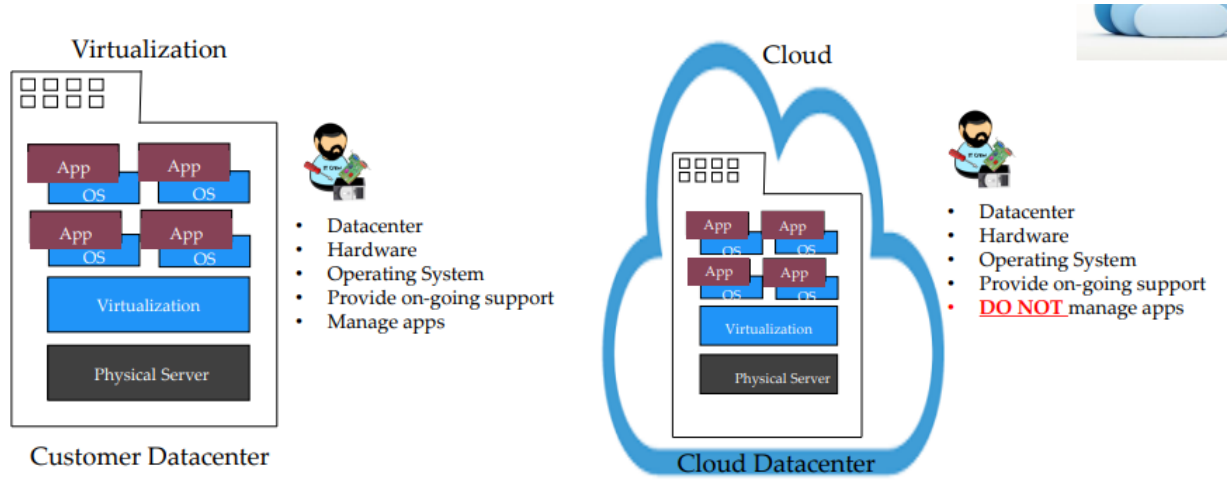


Fig. 5.6: Difference between virtualization and cloud

• **Lab Design**

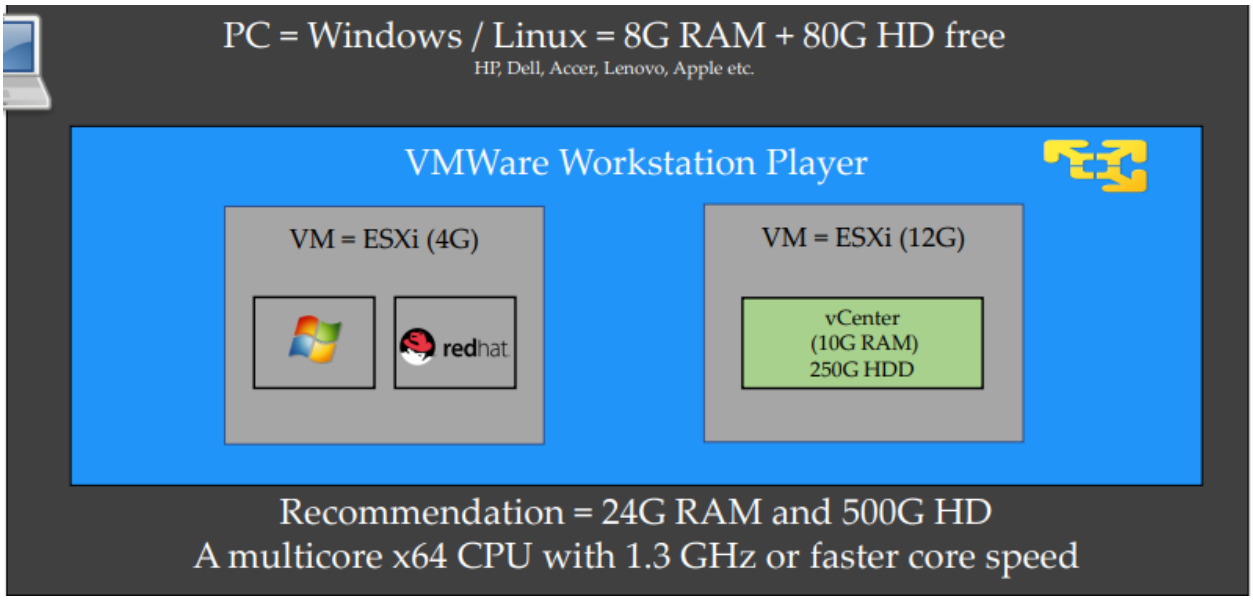


Fig. 5.7: Lab design

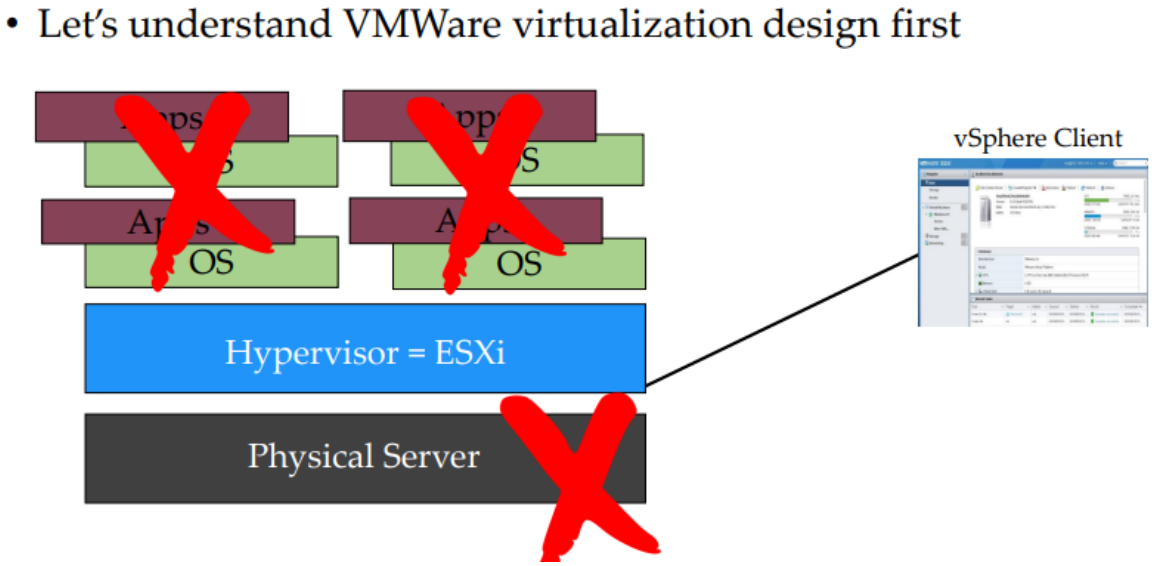


Fig. 5.8: Lab design to understand virtualization.

• **VMWare Online Lab - Virtualization 101**

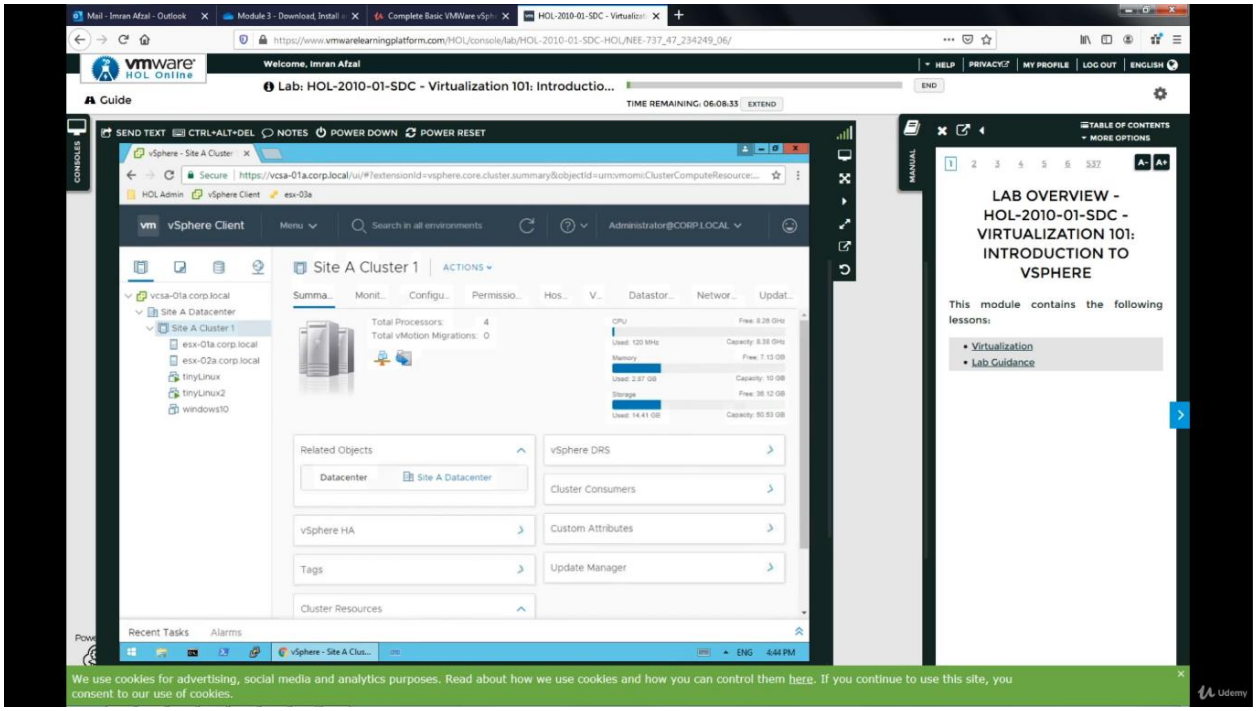


Fig. 5.9: HOL online VMware lab

• **Download and Install VMWare Player**

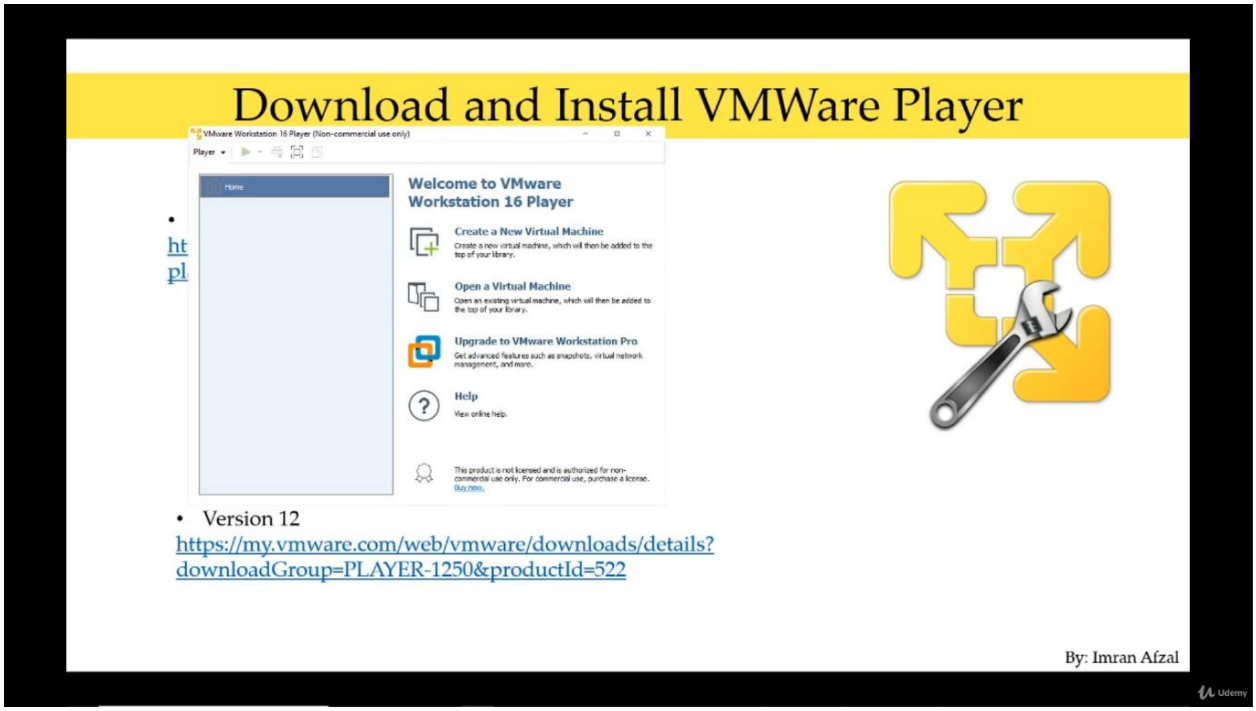


Fig. 5.10: VMware Player Download

• **First VM on VMWare Player (Linux)**

Fig. 5.11: Installing Linux

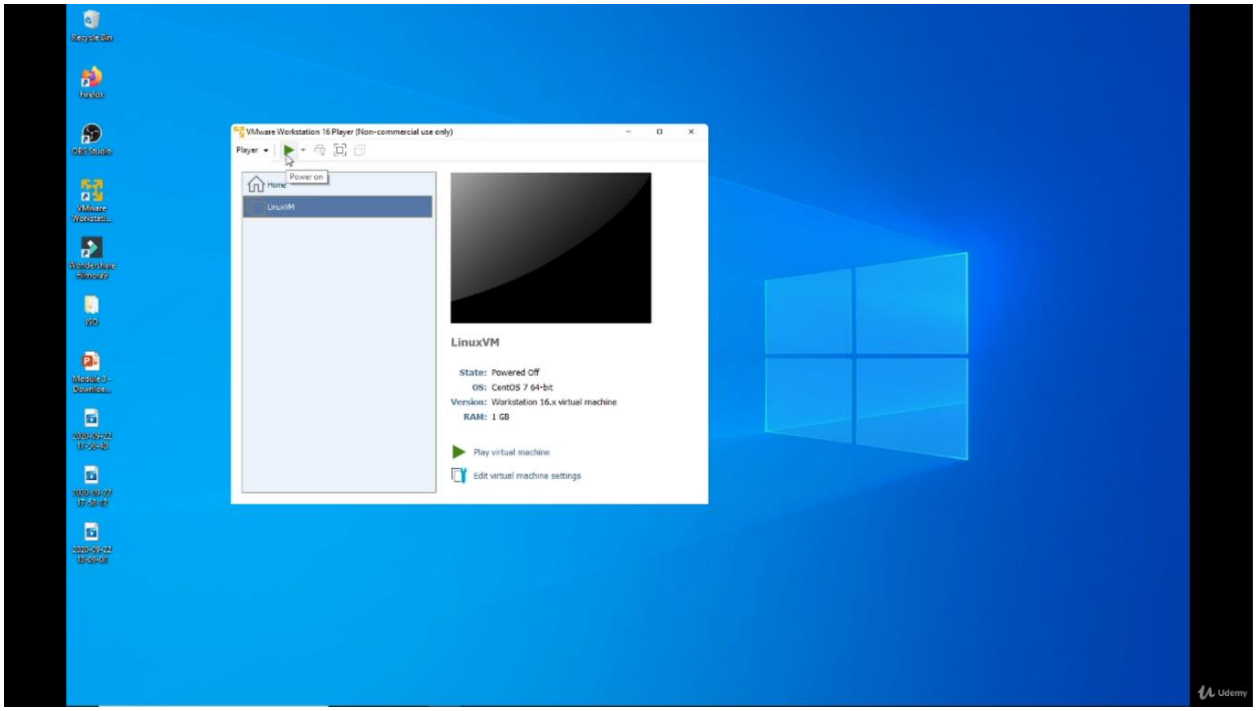


Fig. 5.12: Linux installation

• **Download and Install ESXi Server (Hypervisor)**

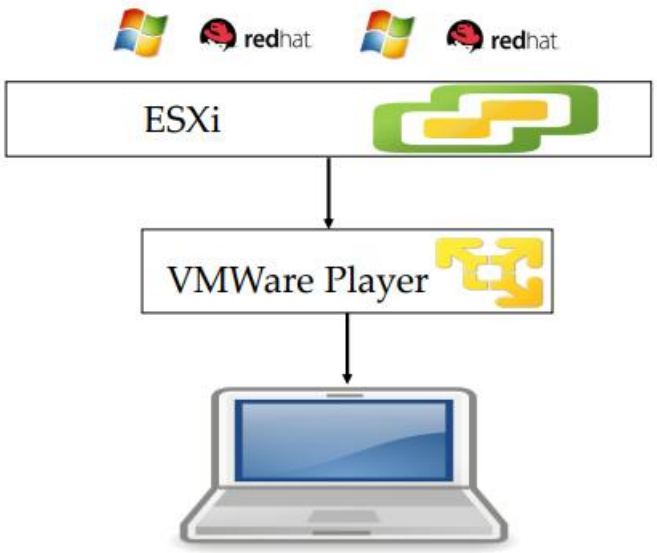


Fig 5.13: Installing ESXi Server

• **Configure ESXi Server**

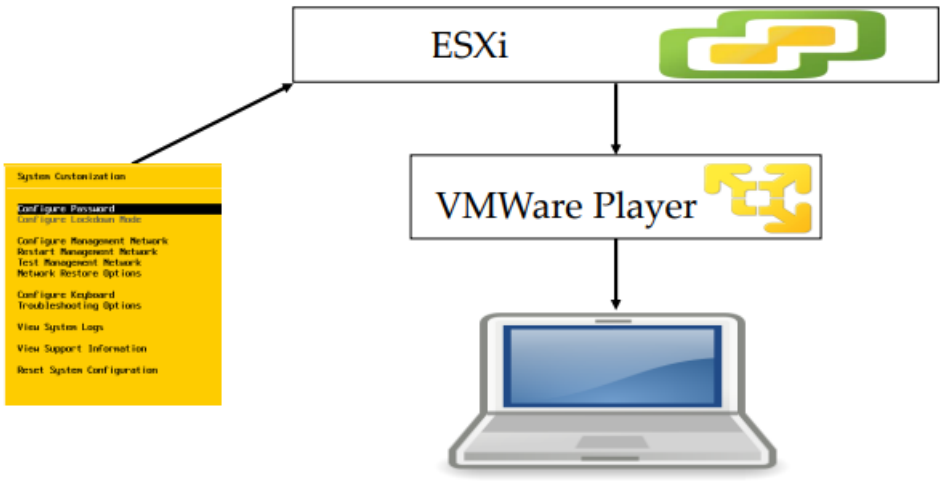


Fig. 5.14: Configure Server

• **Connect to ESXi and Explore vSphere Dashboard**

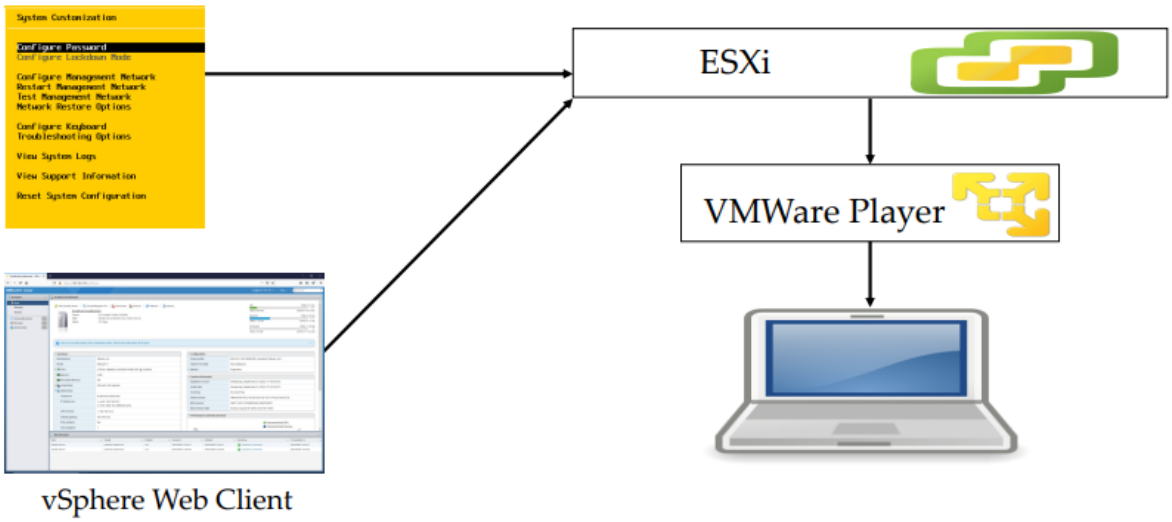


Fig. 5.15: ESXi and vSphere Dashboard

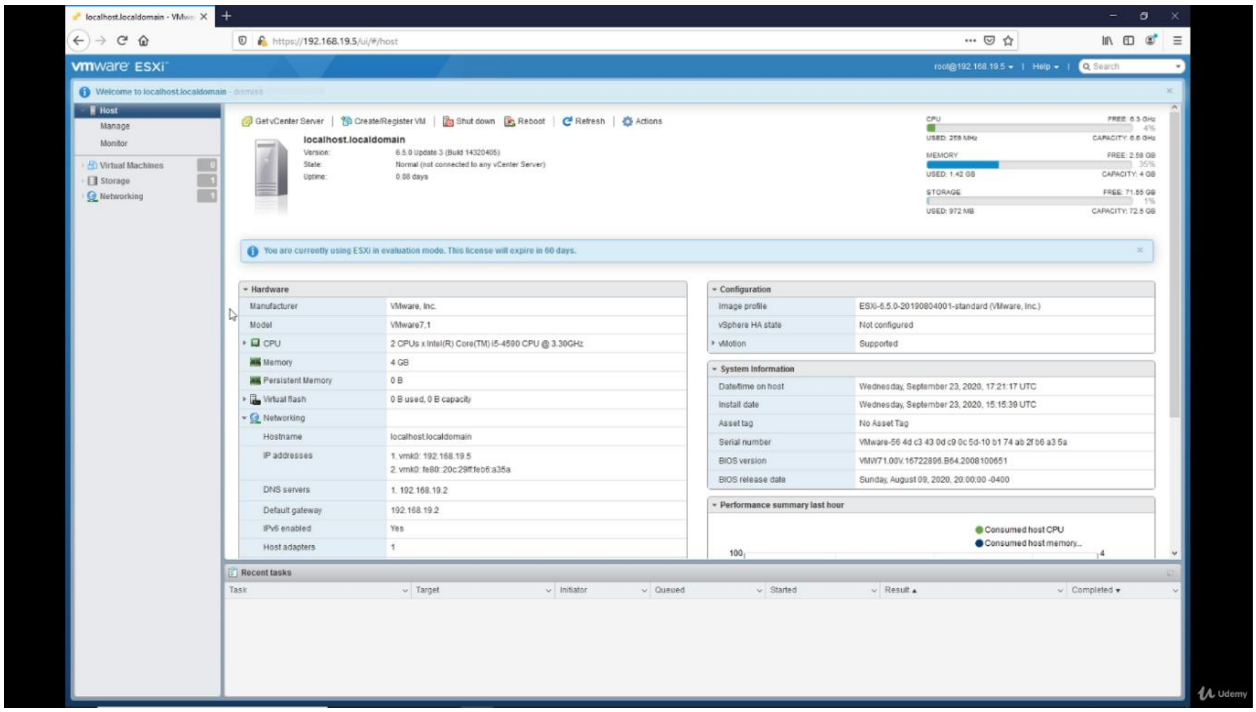


Fig. 5.16: ESXi Web Console

• **First VM on ESXi**

a. Gather the IP address of ESXi server
b. Create a new a virtual machine
c.

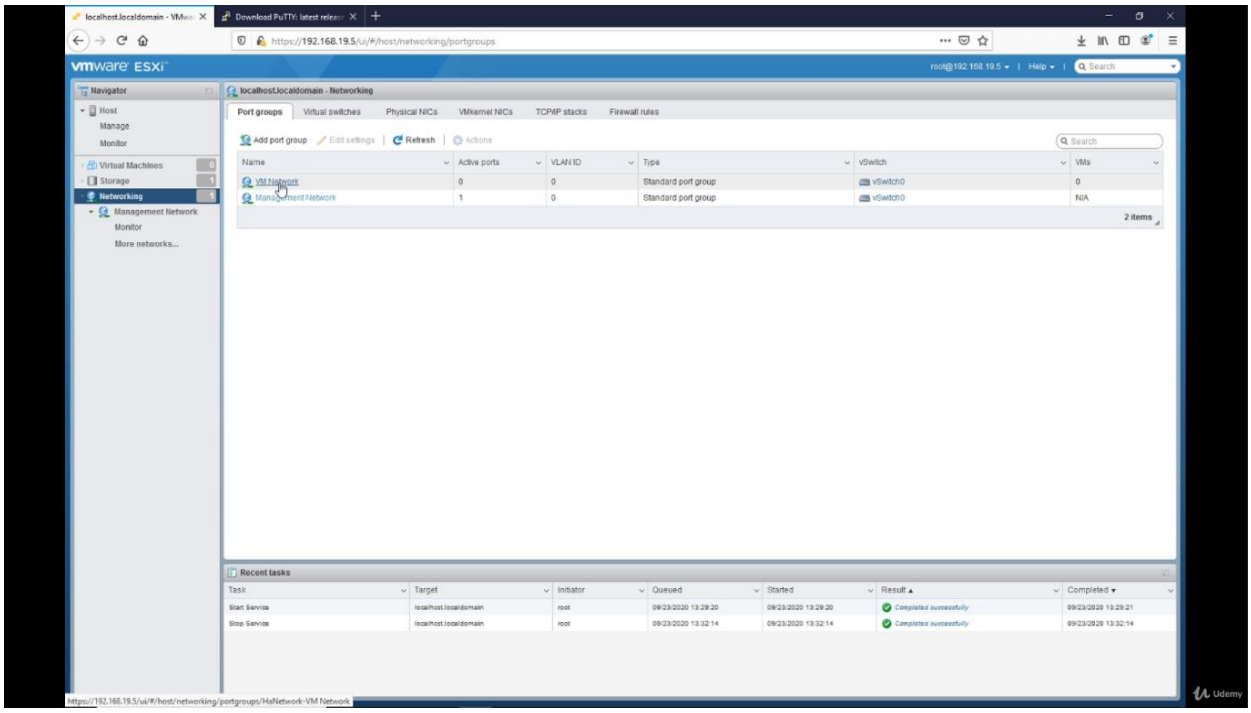


Fig. 5.17: Creating Linux VM

d. Customized and configure your VM

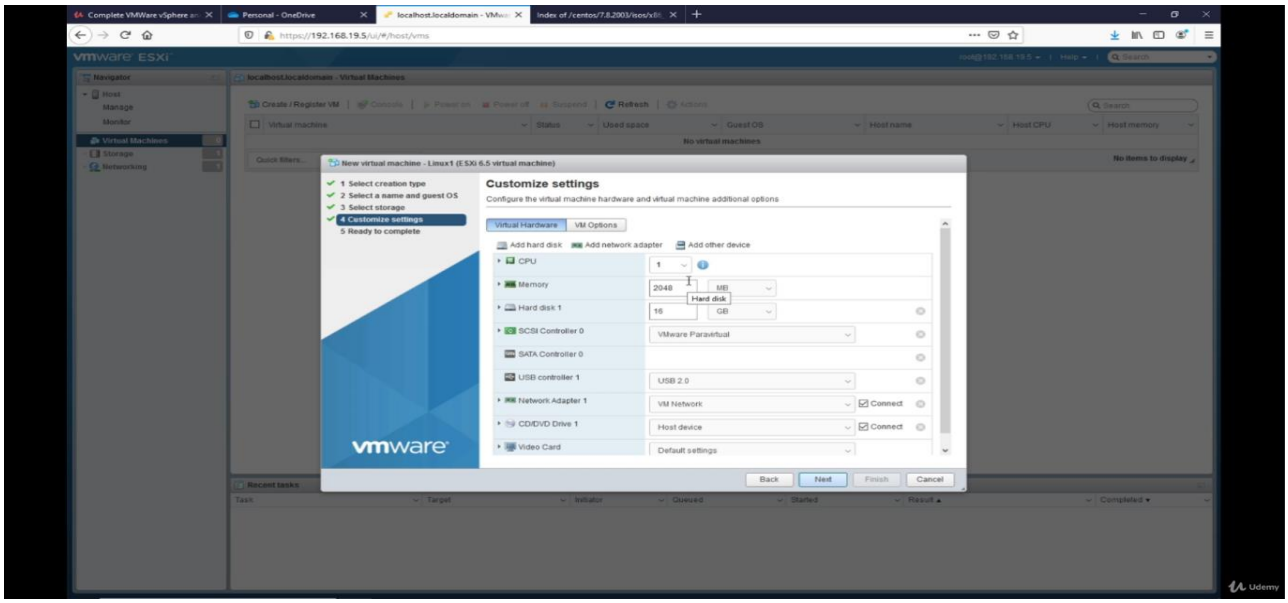


Fig. 5.18: Customizing VM Settings

• **Upload the ISO file**

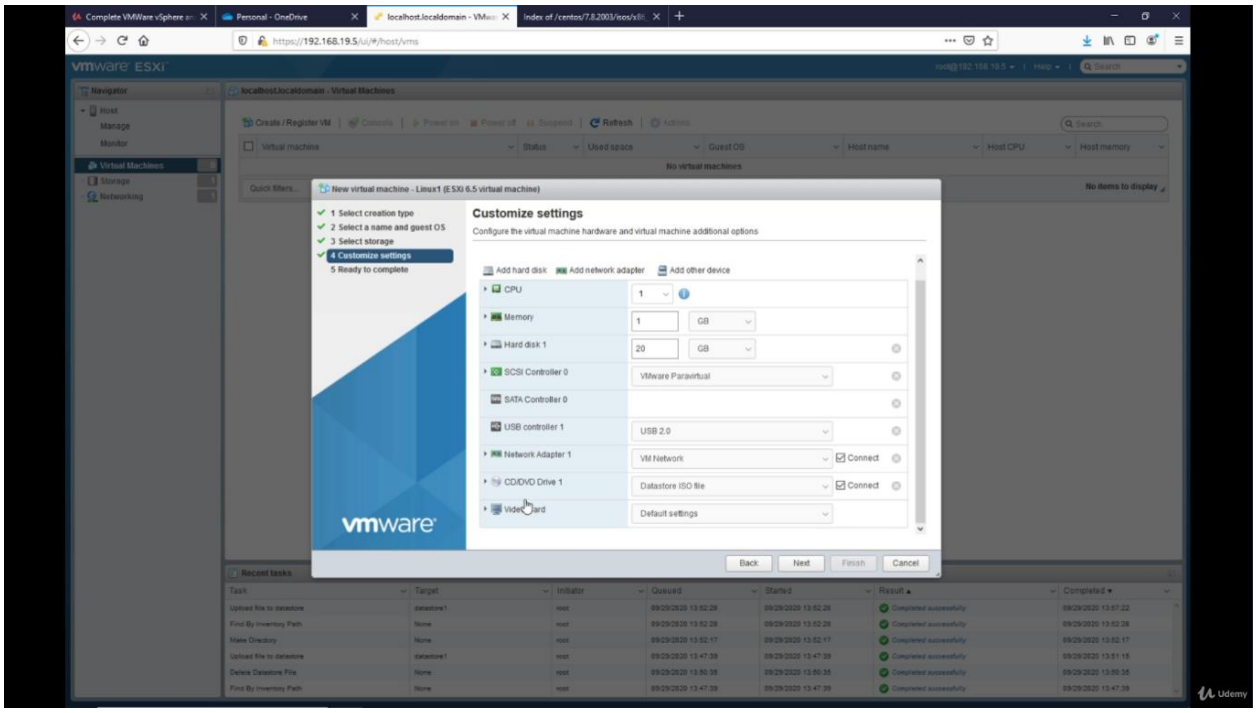


Fig. 5.19: Attaching ISO file

• **Install Linux OS**

Creating first VM by installing a Linux Operating system on top of the vSphere ESXi server

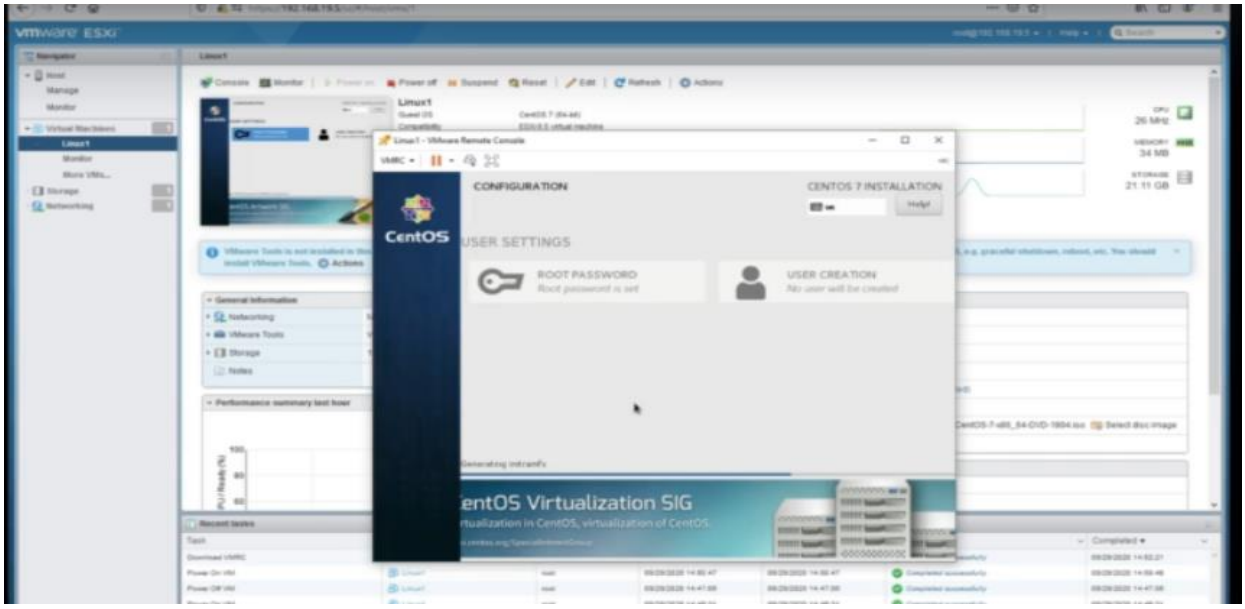


Fig. 5.20: Web console Linux installation

• **VM Management**

It's important for not only the administrator but the user to understand the management of the system so to work on it, thus the user can access the ESXi server from the console and manage it and add specifications to make it more friendly.

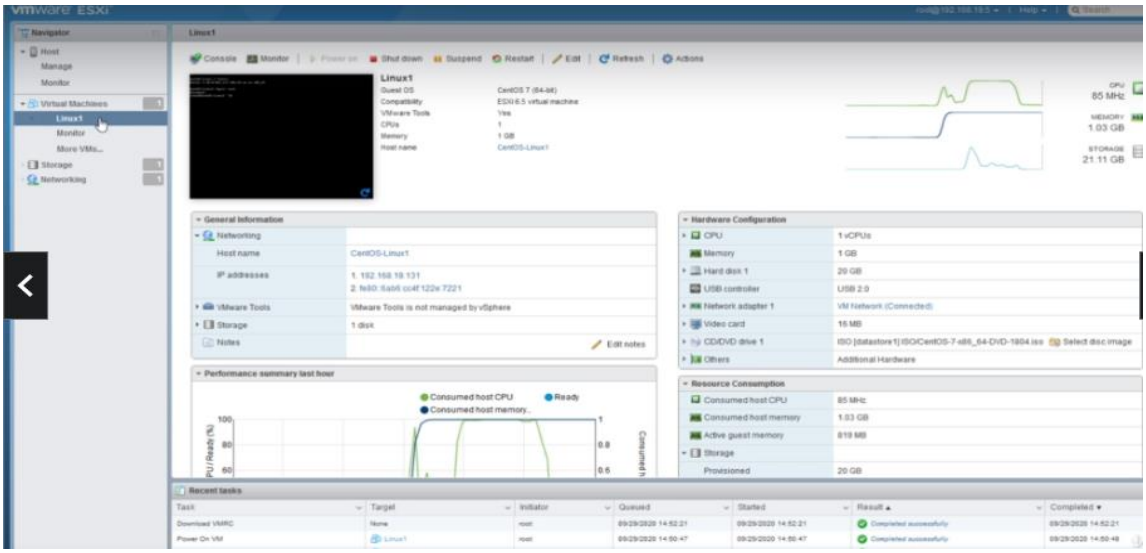


Fig. 5.21: Linux VM1 is created

• **Update ESXi hostname**

• **Install Windows on a VM**

Now on top of the ESXi layer we are ready to create another VM with a Windows operating system, increasing the VM count to 2.

This can be done by using an ISO image of the Windows operating system, create a new VM and attach the image you it.

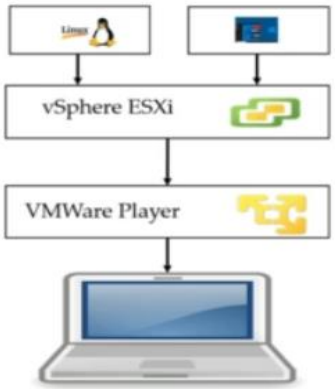


Fig. 5.22: Flowchart

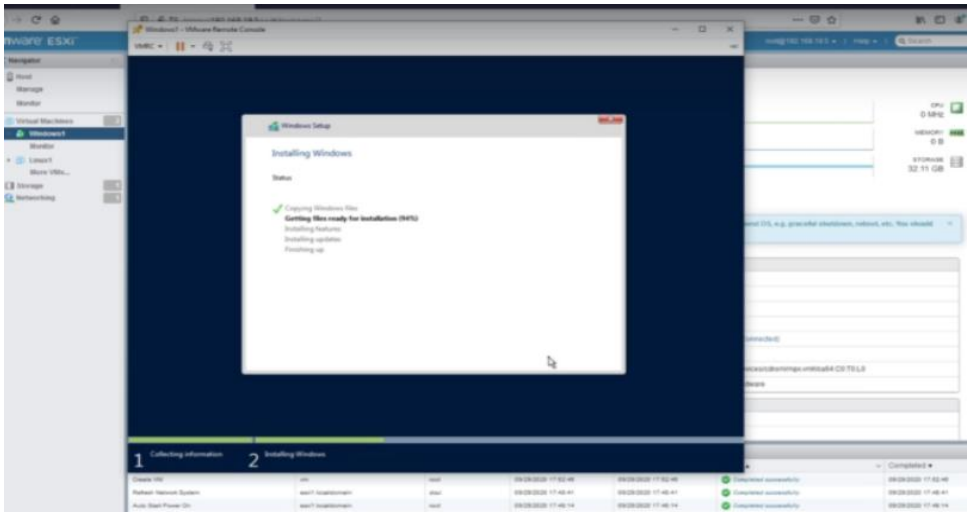


Fig. 5.23: Downloading Windows

• **Install VMWare Tools – installing VMware tools like vSphere**

We install other tools to manage these VMs. These tools are vSphere.

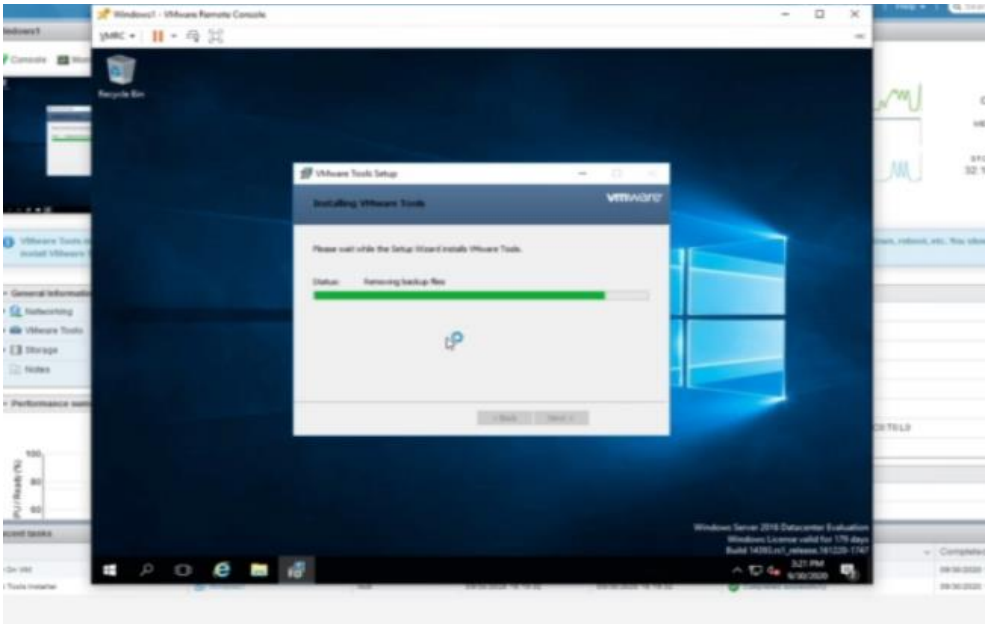
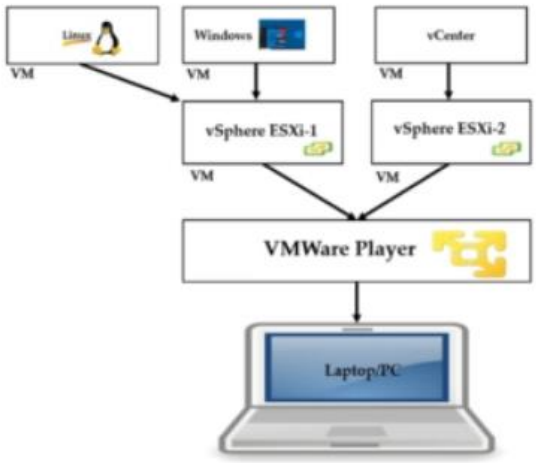


Fig. 5.24: VMware tools

• **Install 2nd ESXi Server**



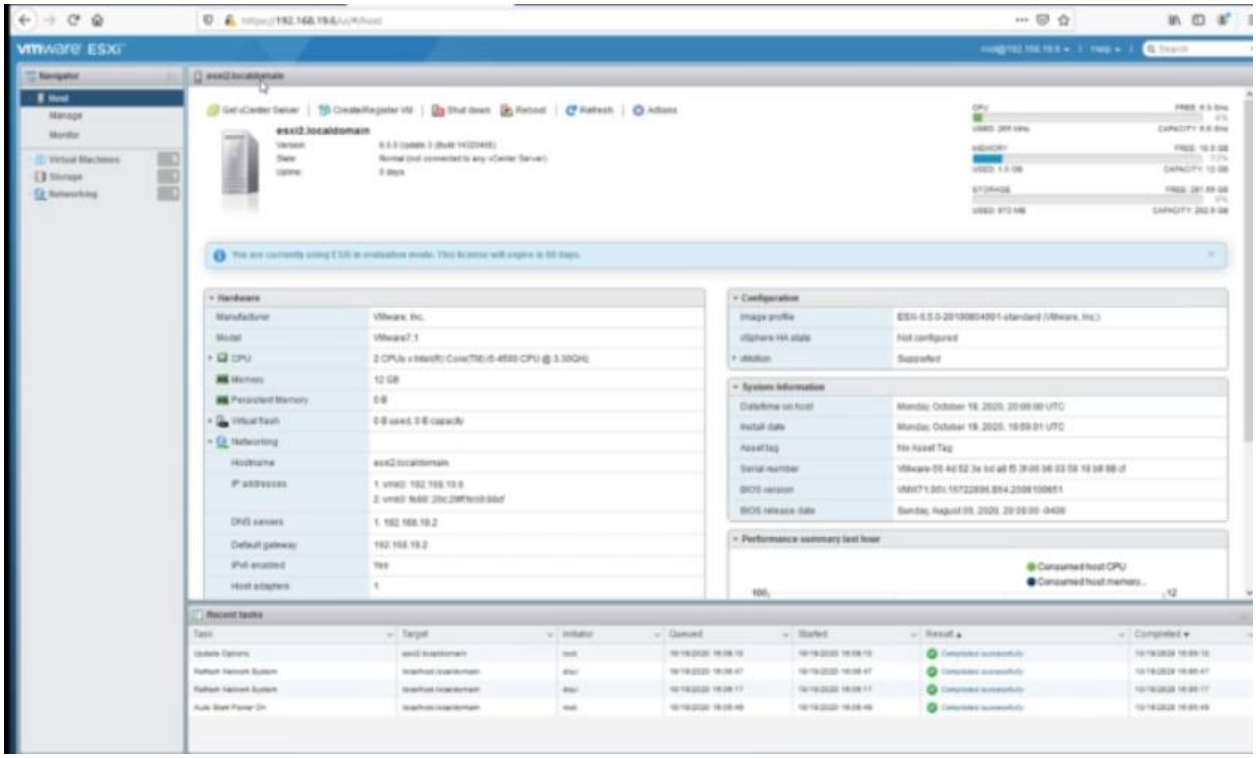


Fig. 5.25: ESXi second host

• What is vCenter?

We need vCenter as a single glass pane, as one dashboard where we can manage all our multiple ESXi and all the virtual machines that are within those ESXi are managed from one central location.

vCenter supports functions like:

1. **HA - High Availability** -
2. **DRS - Distributer Resource Scheduler**.
3. **vMotion-**is a feature that allows you to migrate washing machine from one host to another.
4. **vDS** distributed switches, which allows you to set your networking of servers all at the same time.
5. **vSAN** is virtual storage. It has everything that you commercialize on the storage side.
6. SSO which has single sign on, meaning you could sign on to your web center and all that is accessible from one active directory if you have it, or any kind of a directory services that you have.

• Downloading vCenter and Installation Options (Win32 UI or OVA)

3 ways to download vCenter

1. ISO File image
2. OVA – Open Virtualization Format
3. From VMware site download

• Install vCenter

Resources = 12GB, 2CPU and 300GB of Disk

IP = 192.168.19.6

Subnet = 255.255.255.0

Gateway = 192.168.19.2

DNS = 192.168

Hostname = ESXi2

Domain Name = localhost

- **Accessing vCenter (Flash/HTML, SSH, Console, Admin Portal)**

  a. **Browser**

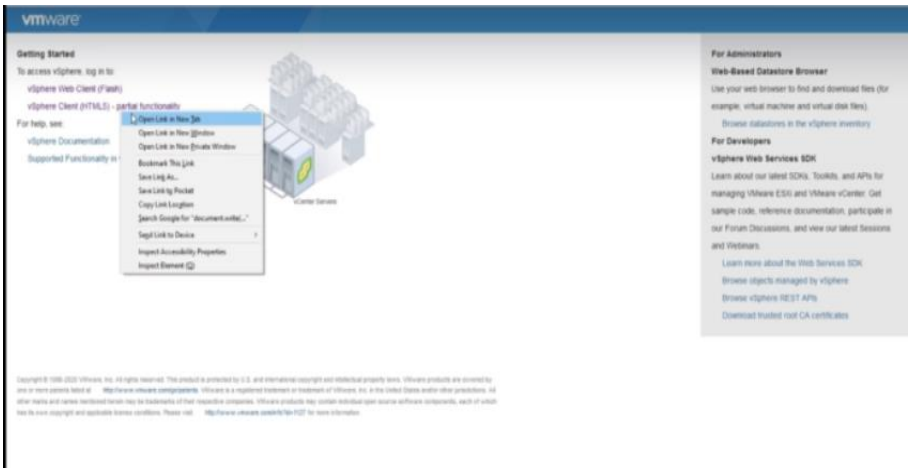


Fig. 5.26: Using web browser to access vCenter

  b. **Flash**

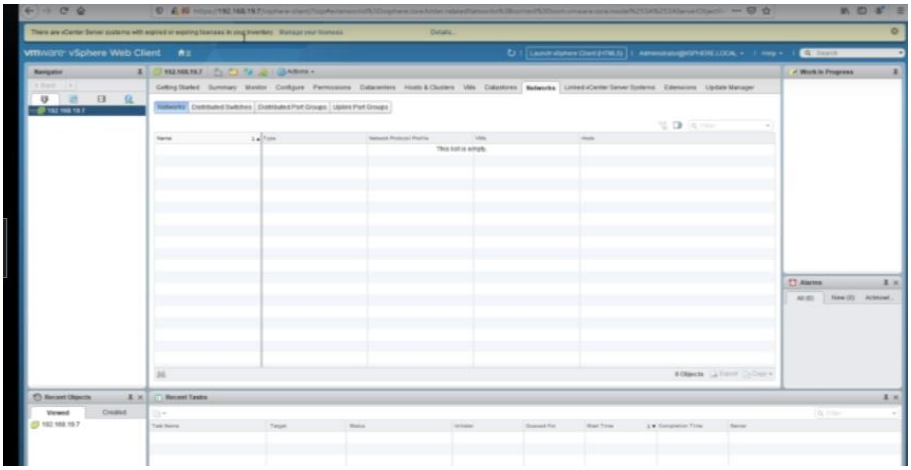


Fig. 5.27: Flash to access vCenter

c. HTML

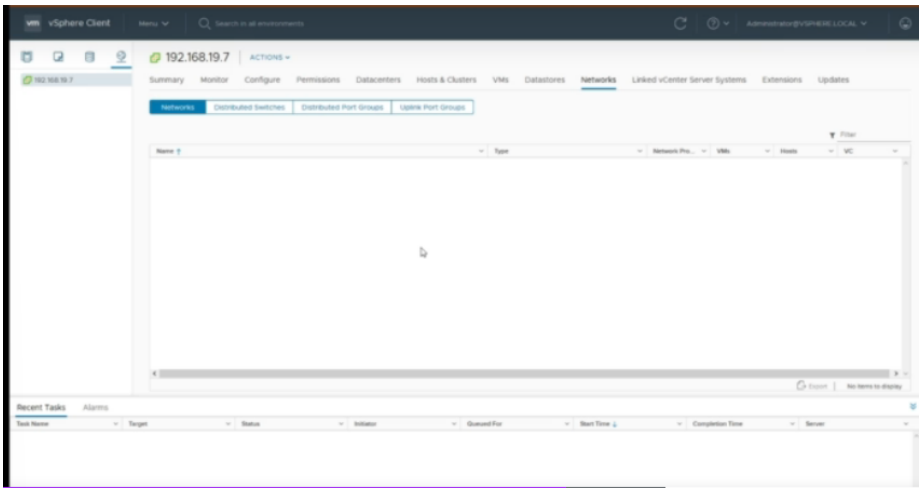


Fig. 5.28: HTML access vCenter

Console (within web client)

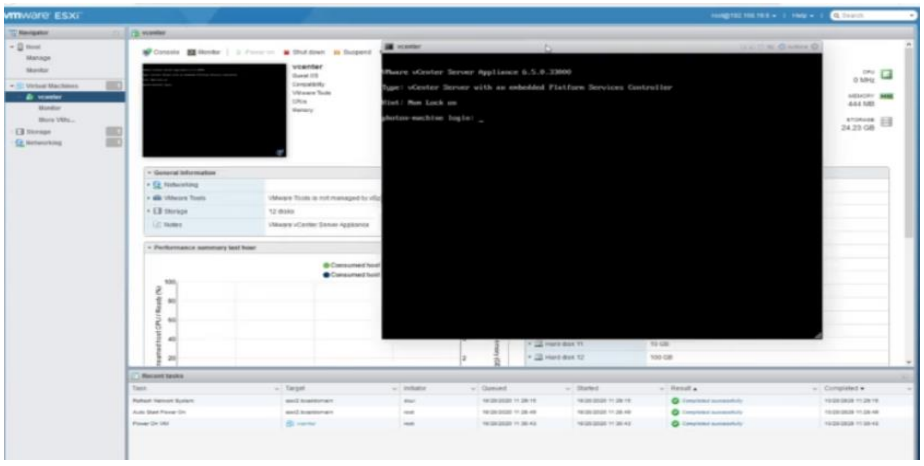


Fig. 5.29: Console (within web client)

vCenter Management Interface

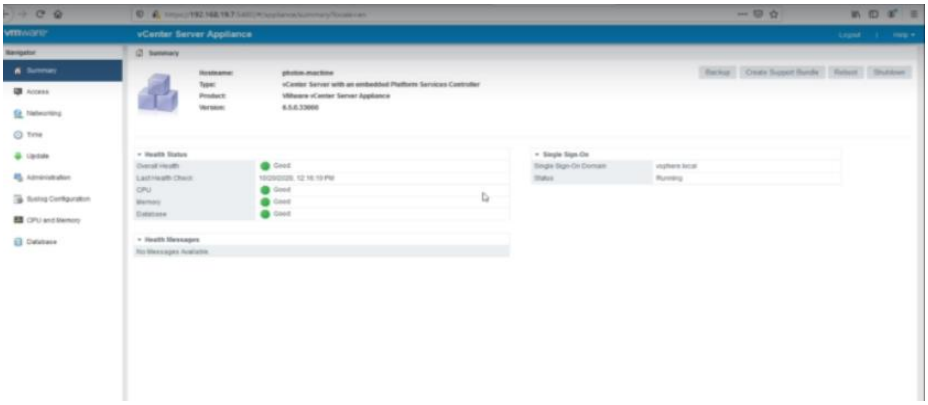


Fig. 5.30: Using IP Address

• Create a Data Center and Add ESXi Servers

How to add ESXi server to vCenter so they can be managed by vCenter

1. Login to vCenter
2. Create a data center
3. Add ESXi 1
4. Add ESXi 2

This can be done by opening the vSphere and clicking on add host to add the ESXi server and type in the IP address of the ESXI, customize the options and add the second ESXi server as well.

Check the Various VM you Created

So, the vCenter can now manage the ESXi servers from a single point rather that going to each one and managing from there.

• Managing hosts on vCenter

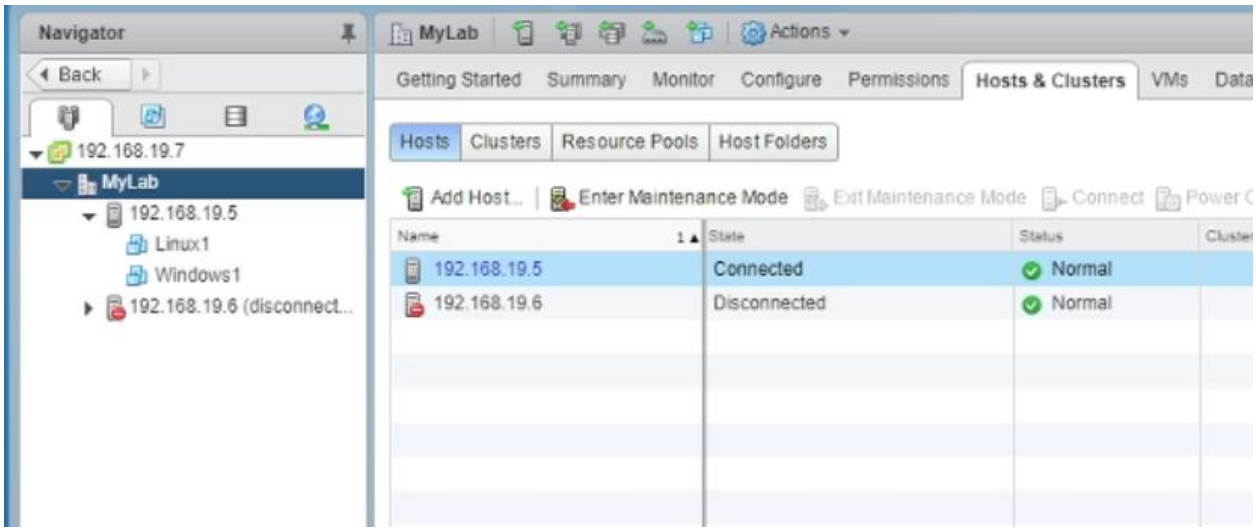


Fig. 5.31: ESXi servers on the vSphere

• vCenter Homepage

Different categories at the vCenter home page inventory are:

1. Hosts and Clusters
2. VMs and templates
3. Storage
4. Networking
5. Content lib
6. Global inventory

• Operations and policy

1. Task console
2. Event console
3. VM storage policy

4. Customization specification manager
5. Update manager
6. Host profile

• **Administration**

1. System config
2. Licensing
3. Customer experience
4. Operation manager

• **Plug in for installation**

Hybrid cloud manger

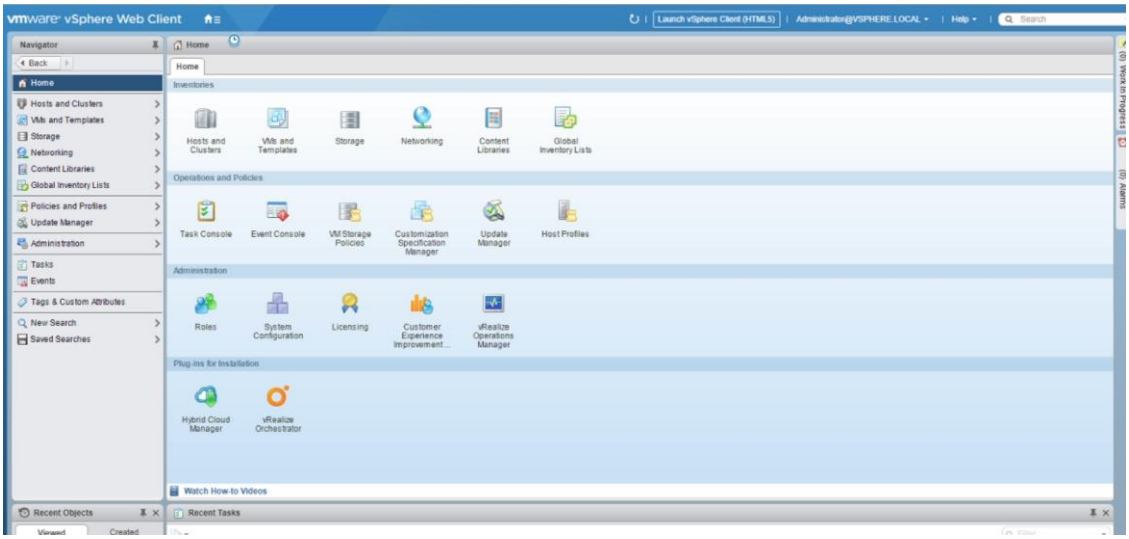


Fig. 5.32: vCenter Homepage

Other than these options we also have drop down menu these are

• Monitors menu
• Configure, Permissions and Data centers (Menu)
• Hosts & Clusters and VMs
• Other Menu Options

CHAPTER - 6
CONCLUSION AND FUTURE SCOPE

6.1 CONCLUSION

The introduction of virtualization has completely changed the way businesses conduct their operations. Creating a virtual server environment provides a greater quantity and array of benefits and opportunities for your organization. The security is served through firewalls that prevent from any unreliable access and preserve the data safe and confidential. With the deployment of virtualization, users can work efficiently as the working process is very streamlined and agile. With this technique companies can manage additional expenditure on physical devices and servers. Being active with a virtual environment, data can be gathered on virtual servers. It also reduces the rigorous use of electricity (that has been a concern if several physical devices and services are being used at the same time), lowering bills while executing the numerous components of an operating system and applications over the users and company's network. The data can be transferred to virtual servers anytime and also be retrieved due to this users or provider need not to waste time in finding out hard drives to discover data. This system failure can be protected with virtualization as users could perform the same task simultaneously over multiple devices, and the accumulated data can also be retrieved anytime with any device. Enhance development productivity. i.e., if one VM is not working, it will not affect other VM's, remote access, rapid scalability, multiple platforms on single system, optimal storage, framework, HA, DRS etc. are some unique features that VMware virtualization offers.

6.2 FUTURE SCOPE

Virtualization is a foundational element of cloud computing and helps deliver on the value of cloud computing. Virtualization and cloud computing work together to provide various services. The cloud can – and most often does – include virtualization products to deliver the computer service. We view cloud computing as an evolution of virtualization. Customers who virtualize their hardware servers may adopt cloud computing over time for increased self-service, scale, service delivery levels and agility. By definition, cloud computing is an impressive combination of both on-premises and cloud architectures. It accommodates the creation of a hybrid platform that helps businesses expand, without worrying about investments and the right environment. The latest cloud technologies are more versatile and flexible than ever. It helps businesses of all sizes and domains meet their infrastructure, software, and hardware requirements.

In line with the recent trends in cloud computing, the technology has become more flexible and scalable than ever. This helps industries have more control over their data. Also, it helps in providing better levels of security at each data center. The most integral components of the latest technology in cloud computing are heavily organized.

Finally, we need to focus on the future of virtualization and cloud computing. This is an interesting bond that has plenty of scope for research and development. To begin with, when

cloud computing and virtualization are brought together, a unique architecture is required. This could be a development that maps to the qualities of the Computing Cell. And the computing cells is known for its consistent need for finer and sophisticated software infrastructure, which is paired with intricate features like encryption, third party authentication, efficient and reliable network segmentation, and data management.

All these improvements need to be provided across all channels in the cloud. And it is important for the service providers to ensure that their cloud technology meets these standards. Virtualization and cloud can bring to light a hybrid IT system, which is a challenge and a big problem today. Another important reason why virtualization and cloud computing is crucial would be budgeting. When hardware expenses are limited and cut down to the services offered by the cloud, there will be more cost-cutting and savings. In fact, the way data needs to be stored can be controlled using algorithms. It will no longer need the support of humans.

REFERENCES/BIBLIOGRAPHY

- https://www.vmware.com/content/vmware/vmware-published-sites/it/company/why-choose-vmware.html
- https://www.vmware.com/in.html
- https://labs.hol.vmware.com/HOL/catalogs/
- https://www.simplilearn.com/merits-demerits-of-vmware-vsphere-hosted-virtual-environment-article
- https://www.nakivo.com/blog/vmware-esxi-vs-vsphere-vs-vcenter-key-differences/
- https://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_intro_vi.pdf
- https://www.gacbe.ac.in/pdf/ematerial/18MCS35E-U3.pdf
- https://www.businessnewsdaily.com/5791-virtualization-vs-cloud-computing.html
- https://www.jigsawacademy.com/blogs/cloud-computing/future-of-cloud-computing/
- https://www.nakivo.com/blog/physical-servers-vs-virtual-machines-key-differences-similarities/
- https://www.nakivo.com/blog/vmware-vsphere-ha-and-drs-compared-and-explained/