3-2016

Cloud Ready Desktop Virtualization Solution

Siva Prasad Madduri
St. Cloud State University, masi1301@stcloudstate.edu

Cloud Ready Desktop Virtualization Solution

by

Siva Prasad Madduri

A Starred Paper

Submitted to the Graduate Faculty

of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree of

Master of Science in Information Assurance

March, 2016

Starred Paper Committee:
Dr. Dennis Guster, Chairperson
Dr. Susantha Herath
Dr. Sneh Kalia

Abstract

Cloud computing is a relatively new set of technologies that can allow businesses to easily scale their computing resources and improve responsiveness to customer needs. This has held true for application, server, and desktop virtualization. Desktop virtualization in particular provides a means to solve many of the traditional challenges associated with deploying and maintaining large business workstation environments, including centralized data management, rapid deployment of workstations, and centralized updating. VMware, a longtime leader in the virtualization sector, offers a desktop virtualization platform that is widely considered to be the best in class. This paper explores the process of building a desktop virtualization solution using VMware View, a cloud-ready desktop virtualization solution from VMware.

Table of Contents

Chapter Page

Chapter Page

List of Tables

List of Figures

Chapter I

INTRODUCTION

Introduction

A significant consideration for Chief Financial Officers (CFOs) today is decreasing the cost of operating their IT infrastructure and increasing the amount budgeted for research and development. VMware, one of the most prominent companies in the virtualization sector, offers a wide range of products that can allow a company to reduce the total cost of ownership (TCO) of its desktop infrastructure and improve their return on investment (ROI). VMware offers a RCOI calculator at http://roitco.vmware.com. This document talks about the benefits and the methodology of VMware View on top of vSphere hypervisor. A VMware View deployment can help companies rapidly and dynamically scale their IT infrastructure to respond to customer demands and take their services to new markets more rapidly. VMware View helps companies to rapidly provision, centrally manage, and efficiently patch their end-user desktops. This is possible only when they also deploy an ESXi server infrastructure, which is part of VMware vSphere product suite. The vSphere suite allows companies to build and run multiple servers as virtual machines on top of the ESXi hypervisor. This paper explores the many benefits of moving to desktop and server virtualization using VMware virtualization technologies.

Problem Statement

Many companies in today's competitive market risk losing their competitive edge due to not keeping pace with market trends. Customers now want services delivered faster, in more locations, and on a variety of devices. This shift in customer expectations means that companies must be able to rapidly provision computing resources, patch systems transparently, and recover services from any unplanned downtime, all without disrupting the

end-user experience. This paper focuses on how a company can rapidly provision and deliver services and manage and patch them centrally from a single virtual datacenter.

Nature and Significance of the Problem

The issues and challenges explained in the problem statement affect virtually every company throughout the world. Changes in the IT marketplace have increased the demands customers place on the information systems they use, and companies that wish to remain relevant and profitable need to adapt accordingly.

Objective of Research

This research focuses on understanding and solving significant challenges facing IT departments in businesses worldwide. Specifically, it looks at how virtualization solutions like VMware View can help companies decrease their capital and operational costs by centralizing IT system management.

Research Questions and/or Hypotheses

1. How can vSphere High Availability provide an effective and affordable disaster recovery solution?
2. How do vCenter Server, View Composer, and View Connection Server work together to provide seamless desktop virtualization?
3. How does View Composer optimize storage?
4. How many virtual desktops can be run concurrently on a single ESXi server?
5. What is the optimal storage design for VMware View?
6. How many IOPS (Input/output Operations per Second) should a storage LUN (Logical Unit Number) be able to provide?

Acronyms

AD: Active directory

AMD RVI: Rapid virtualization technology

DC: Domain Controller

DCUI: Direct Console User Interface

DMZ: Demilitarized zone

DPM: Distributed power management

DRS: Distributed resource scheduler

DSN: Data source name

EULA: End User license agreement

FQDN: Fully qualified domain name

FT: Fault tolerance

GB: Giga bit

HA: High Availability

HVD: Hosted virtual desktop

IAAS: Infrastructure as a service

Intel VT: Virtualization technology

IOPS: Input output per second

IT: Information Technology

LAN: Local area Network

LUN: Logical unit number

MED-V: Medium Enterprise desktop virtualization

MHZ: Mega hertz

ODBC: Open Database Connectivity

OS: Operating system

OVF: Open virtual machine format

PAAS: Platform as a service

PCOIP: Personal computer over Internet protocol

RDP: Remote desktop protocol

ROI: Return on Investment

SAAS: Software as a service

SLES: SUSE Linux enterprise server

SP1: Service pack 1

SSL: Secure Sockets Layer

SSO: Single Sign on

TCO: Total cost of ownership

TCP: Transmission Control Protocol

UCS: Unified computing system

UDP: User Datagram Protocol

VDI: Virtual desktop infrastructure

VM: Virtual Machine

WAN: Wide area network

Chapter II

BACKGROUND AND REVIEW OF LITERATURE

VMware

VMware is a multinational company founded in 1998, which specializes in virtualization, cloud computing, and implementing software-defined datacenters (VMware, 2015).

Cloud Computing

Cloud computing is a way to access information systems and services over Internet. There are three major delivery models in cloud computing:

- **IAAS** (Infrastructure as a Service): End users are provided with access to the bare metal hardware they need for their business needs. Example IaaS providers include Soft Layer, AWS, and Rackspace.
- **SAAS** (Software as a Service): Software can be rented as a service from a cloud provider. Examples include Office365 from Microsoft, Zimbra Cloud Suite, and Google Apps for Business.
- **PAAS** (Platform as a Service): A development platform with all necessary tools to build an application can be purchased from PAAS providers. Major players in the market include Sales force, Microsoft Azure, and Google App engine.

All the above services operate on a pay-as-you-go billing model. A real-world analogy of cloud services is a taxi. Taxis offer a mode of transportation where customers can have convenient access to transportation without having to worry about vehicle maintenance, paying for fuel, or carrying an auto insurance policy (Cloud Computing, 2015).

Virtualization

Virtualization is a technology that, put simply, allows individual, powerful computers to run multiple operating systems and provide a variety of services to customers at one time. The main goal is to transform traditional computing platforms in order to make them more scalable, robust, and flexible. Virtualization technologies come in many different forms for different use cases (Techopedia, n.d.).

Types of Virtualization

Virtualization Type	VMware	Citrix	Microsoft
Server	vSphere	XenServer	Hyper-V
Desktop	View	XenDesktop	Med-V
Application	ThinApp	XenApp	App-V

(Data Center Knowledge, 2012)

Server Virtualization

Server virtualization involves the emulation of an operating system, which can run enterprise application like SQL Server, Oracle 12c, Lotus Notes, Exchange Server, SharePoint, and web server software. Examples of server virtualization products include VMware vSphere, Citrix XenServer, and Microsoft Hyper-V (Raido, n.d.).

Desktop Virtualization

Desktop virtualization involves the emulation of end-user desktop environments in order to allow them to be managed, patched, and security in a centralized manner. Examples of desktop virtualization products include VMware View, Citrix XenDesktop, and Microsoft Med-V (Desktop Virtualization, 2011).

Application Virtualization

Application virtualization involves abstracting the application layer from the underlying operating system layer, making them run inside a bubble, which controls and mediates interactions between each application and the operating system. Benefits include the ability to run legacy applications on modern operating systems, as well as the ability to securely host numerous different applications on a single platform. Examples of application virtualization products include VMware ThinApp, Citrix XenApp, and Microsoft App-V. (Application Virtualization, 2015).

Physical Server Types and Models

There are three different form factors of physical servers in the market today—tower server, rack server, and blade server.

Tower Server

A tower server is a standalone server that is built in an upright cabinet. Examples of tower server models include Dell PowerEdge, HP ProLiant, and IBM System X M5 tower (Dell, n.d.a; Hewlett-Packard, n.d.a; International Business Machines Corporation [IBM], n.d.; Rouse, 2006).

Figure 1. Tower Server (Valli, n.d.)

Rack Server

A rack server is a server designed to be installed in a standard rackmount enclosure. Models of rack servers include Dell PowerEdge, HP ProLiant, and Cisco UCS Rack servers. (Dell, n,d.b; Cisco Systems, n.d.a; Hewlett-Packard, n.d.b; Rouse, 2011).

Figure 2: Rack Server (3 Benefits Of, n.d.)

Blade Server

A blade server is a server with an integrated and modular design, which consumes less datacenter space and less electricity than traditional server types. Models of blade servers include HP C7000, Cisco UCS Blade, and Dell PowerEdge Blade servers. (Blade Server, 2014; Cisco Systems, n.d.b; Dell, n.d.c; Hewlett-Packard, n.d.c).

Figure 3. Blade Server (Hewlett-Packard, n.d.d)

ESXi

VMware's ESXi is type-1 or bare-metal virtualization software on which multiple operating systems can be installed and run simultaneously. ESXi is built around the VMkernal, the central software component which intelligently shares the server hardware on which it is running to all the virtual machines. This is also called as a virtual machine monitor (VMware, 2009).

ESXi Architecture

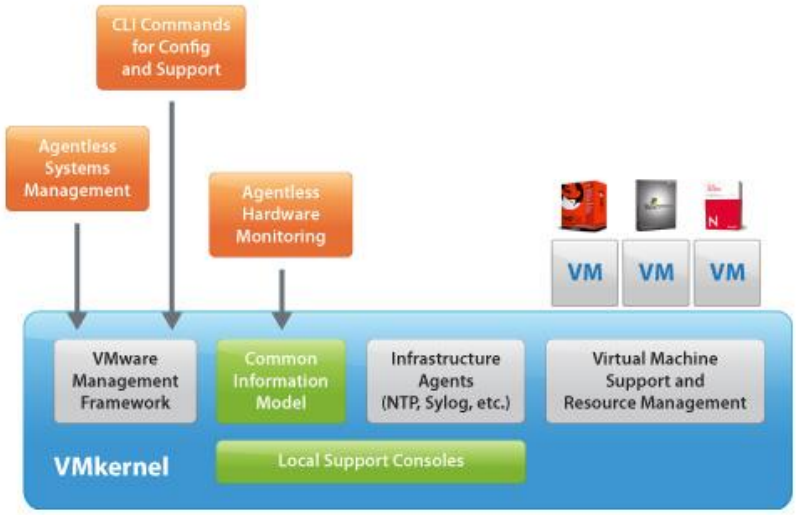


Figure 4. ESXi Architecture (VMware, n.d.m)

ESXi is a very efficient virtualization platform, and has been enhanced over the years of its development. Today, all of the management agents, which used to run on a separate service console on past versions, are now run directly on ESXi without the need for the service console. Third-party agents for hardware monitoring can now run directly on the VMkernel as well. As a result, the disk footprint after removing the service console for ESXi is just 32 MB, making it very efficient and lightweight. ESXi is available in two versions:

- ESXi Installable, which can be installed selecting the hardware-vendor-specific image.
- ESXi Embedded, which comes pre-installed with OEM (original equipment manufacturer) hardware (ESXi, 2013).

Virtual Machine

A virtual machine is essentially a software-defined computer, which is built and run on a virtualization server like ESXi. A virtual machine can offer virtually all of the capabilities of a physical computer, and provide a similar level of performance as well (Virtual Machine, 2009).

vSphere Client

VMware vSphere Client is a secondary piece of software, which is used by administrators to connect to ESXi and vCenter servers. In addition to its core functionality, vSphere Client can be extended with plugins for different solutions, such as Update Manager and Site Recovery Manager (VMware, n.d.a).

Database

A database is software used to maintain data in a structured and tabular format. Some examples of enterprise-class database software include Microsoft SQL Server, Oracle 10g, and PostgreSQL (Database, 2013). Several components in a VMware infrastructure require a database. vCenter Server requires a database to store all the information regarding the ESXi hosts and virtual machines it manages. View Connection Server requires a database to store all the events that happen on a View desktop environment. View Compose also requires a database; this saves the vCenter Server information, linked clone desktop information, replica information of the View Composer, and Active Directory connections (VMware, n.d.b).

Active Directory (Domain Controller)

Active Directory is another key component of a VMware environment. It integrates with vCenter and View to provide centralized authentication and authorization services to all the virtual machines on vSphere and View desktops (Microsoft, n.d.).

vMotion

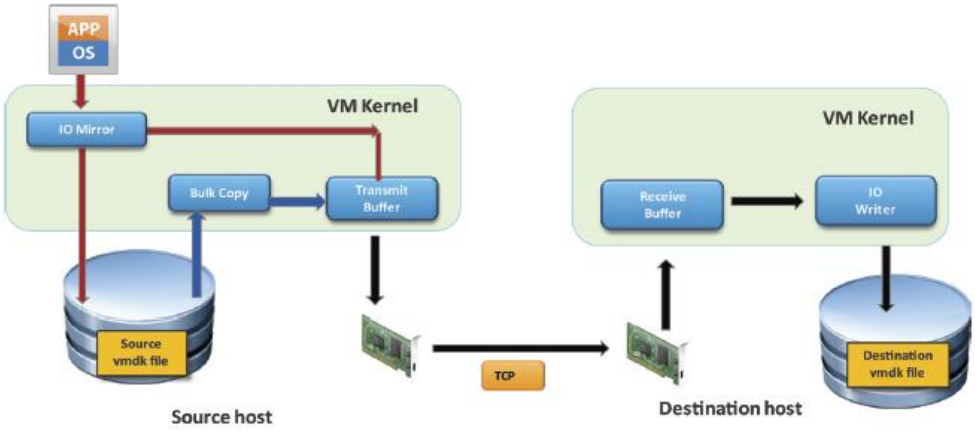


Figure 5. vMotion (VMware, 2012)

vMotion is a feature that allows a running virtual machine to be migrated from one ESXi host to another in the same cluster without powering down the virtual machine. This is otherwise called a "live migration" or "hot migration." Any changes to the virtual machine memory state that occur during the vMotion migration will be captured to the bitmap and, at the end of the migration, the bitmap will be copied to the virtual machine on the destination. vMotion requires shared storage and communication on the VMKernel port enabled on both the source and destination servers. This feature allows for zero-downtime maintenance of the servers in a VMware cluster (VMware, 2012).

Storage vMotion

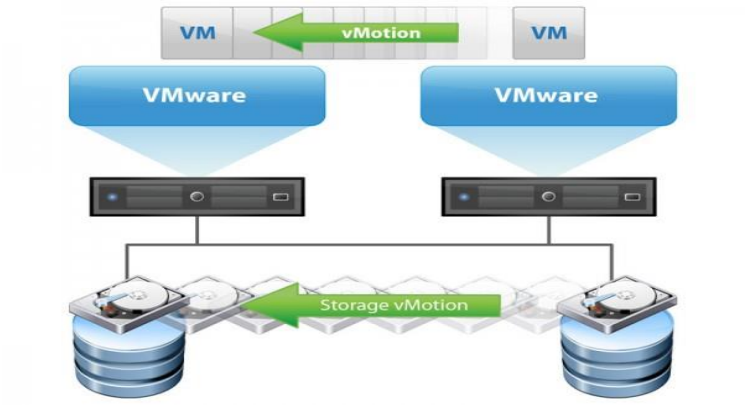


Figure 6. Storage vMotion (VMware, n.d.n)

This feature allows migration of virtual machine disk files from one physical storage location to another without disrupting the virtual machine's operations. This type of "live migration" can help reduce downtime due to storage upgrades and maintenance. This feature requires that the storage LUNs on which the disk files are migrated should be accessible by both ESXi hosts (VMware, n.d.d).

High Availability

High availability is a feature, which can automatically restart virtual machines from a failed server on another server in the cluster. This is a cluster-level feature. A master server will be elected to take care of identifying the failure of a node in the cluster and restarting the virtual machines it hosted on a healthy server. This feature works at the vCenter level (VMware, n.d.e).

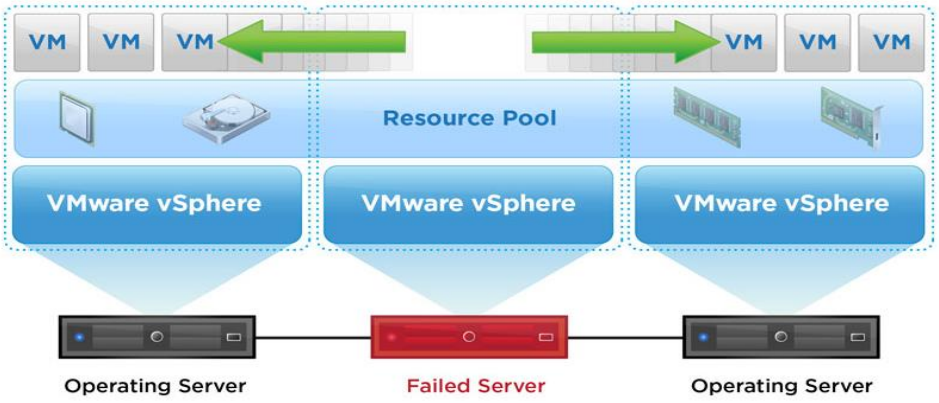


Figure 7. High Availability (VMWare, n.d.e)

vCenter Server

vCenter Server is a centralized management tool, which can be used to manage multiple ESXi servers and the virtual machines running on them. vCenter is necessary in order to use features like vMotion, HA, DRS, FT, Clone, Template (VMware, n.d.f).

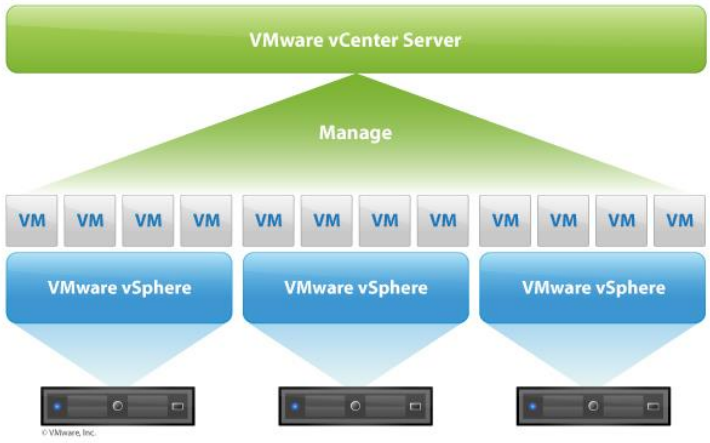


Figure 8. vCenter Server (VMware, n.d.o)

View Connection Server

The View Connection Server is a software component, which acts a broker for clients, allowing for centralized authentication and management of local and remote desktop sessions (von Oven & Coombs, 2015).

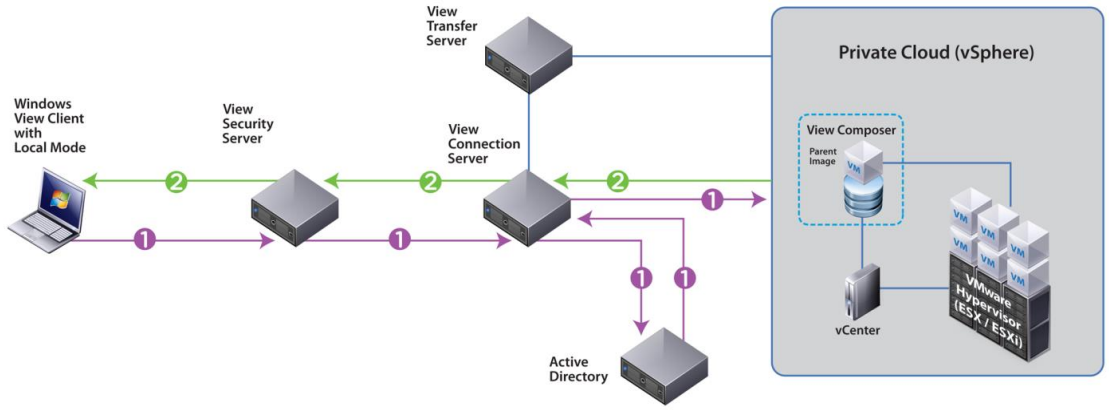


Figure 9. View Connection Server (VMware, n.d.p)

View Composer

View Composer is a component of the View suite, which can conserve storage space by allowing multiple View desktops to share the same virtual disks (VMware, n.d.j).

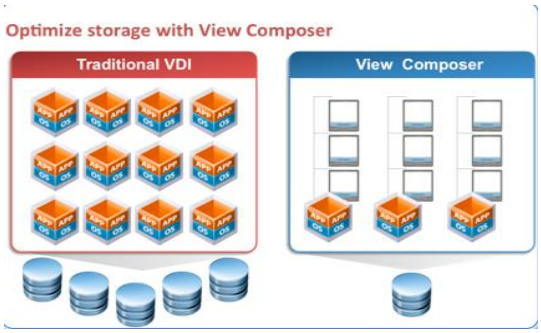


Figure 10. View Composer (Bright-Streams, n.d.)

Chapter III

METHODOLOGY

How It Works

To complete this project, a VMware vSphere datacenter has to be built. The foundation of such a datacenter is one or more ESXi servers with compatible hardware. (VMware. n.d.h). The processor(s) in each server must support either the Intel or AMD virtualization technology (Intel VT and AMD-V, respectively). The high-level steps involved in building a vSphere datacenter are:

1. Install ESXi on two or more servers with compatible hardware.
2. Create LUNs on a supported storage resource and add them as datastores on the ESXi servers.
3. Create one or more virtual networks with standard vSwitches.
4. Create three Windows Server 2008 R2 virtual machines on one of the ESXi servers for vCenter, an Active Directory domain controller, and a SQL Server database server.
5. Install vCenter server to one of the Windows Server virtual machines and configure vCenter to manage the ESXi servers.
6. Configure virtual datacenters and clusters in vCenter.
7. Enable HA & DRS for availability and load balancing, respectively.
8. Check whether the site is fully-functional and troubleshoot any issues that arise.

Once the vSphere datacenter is fully-functional, View must be implemented on top of it, as vSphere handles the compute and network layers for VMware View. Below are the steps to build a View environment on top of vSphere:

1. Install a supported version of Windows Server on two virtual machines, one for the View Connection server and another for the SQL database. If a database is already available, a second Windows server is not necessary.
2. Install a supported version of Windows Server on an additional virtual machine for View Composer. This also requires a database on a new or existing server.
3. Log into View administration portal from a web browser and add vCenter server information and other required parameters.
4. Create a Windows 7 or Windows 8 virtual machine and perform the following tasks: install all the required applications, remove the virtual network interface from the machine, take a snapshot of the VM, and shut it down.
5. Utilize View Composer to build linked clone desktop pools from the Windows 7 or 8 VM snapshot (VMware, n.d.g).

Once these steps have been completed, the architecture will resemble that shown in Figure 11.

vSphere and View Architecture

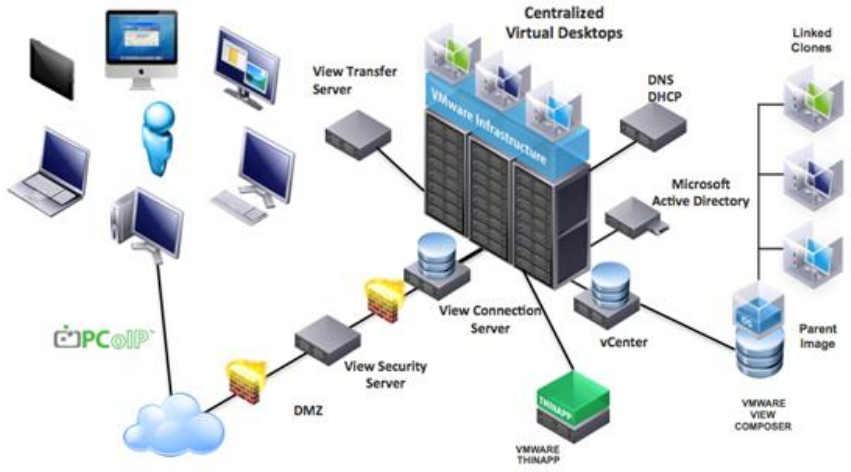


Figure 11. vSphere and View Architecture (Cisco Systems, 2015)

Architecture Explanation

Cloud Based Virtualization

Cloud computing is a service built on top of a virtualized platform. A virtualization platform can be vSphere, Xen server, Hyper-V, Xen, or KVM. The virtualization software acts as a compute layer from which resources are extracted and delivered to organizations over cloud.

vSphere

VMware vSphere is server virtualization platform, which allows organizations to build consolidated datacenters, thereby enabling them to reduce their operating and capital expenses. Some of the technical and financial benefits that vSphere can provide include:

1. Server consolidation
2. Increased server hardware utilization (RAM and CPU)
3. Reduced electricity costs
4. Reduced cooling requirements
5. Reduced datacenter space requirements
6. Zero downtime maintenance of servers
7. High-availability
8. Ability to pool resources from multiple servers

The vSphere product suite also offers a centralized management interface, vCenter Server. A single vCenter Server instance can manage hundreds of ESXi servers and thousands of virtual machines. vCenter offers a wealth of features to an enterprise datacenter, including:

1. Fault tolerance to ensure applications remain available in the case of partial cluster failure.

2. Live migration (vMotion) of virtual machines from one ESXi server to another.
3. Distributed Resource Scheduler (DRS) for dynamic workload balancing on the cluster.
4. Distributed Power Management (DPM), which can automatically place lesser-utilized hosts in standby mode to conserve electricity usage.

VMware Horizon View

VMware Horizon View is the platform to deliver centralized, virtual desktop machines hosted on a server running a hypervisor, and located in a data centre. The end user then connects remotely to their virtual desktop machine from their endpoint device such as a Windows laptop, Apple Mac, or tablet device (Malanco, 2014).

VDI (Virtual Desktop Infrastructure) provides users the freedom to work in a way that suits them, by freeing them from the restrictions of not having to be in the office, but also allowing them the choice of device they use making them more productive, and ultimately your business more agile.

From an IT administrator's perspective, it allows you to centrally manage your desktop environment, from being able to manage desktop images, to the ease of adding and removing user entitlements, all controlled from a single management console.

VMware View VS Traditional Desktops:

Table 1

VMware View vs. Traditional Desktop

Traditional Desktops	VMware Virtual Desktops
Desktops are individual.	Desktops run centrally in the datacenter and are consolidated on to few ESXi hosts.
Less security as the data is stored on the hard disk on each desktop.	Data is stored and accessed centrally from a storage box, which runs in a datacenter.
Hard to maintain security compliance.	Can stay in compliance as the user data disks can be refreshed back to base image states as soon as they log off.
Hard to maintain IT compliance.	Even though if the users install unwanted software, the virtual desktops can be brought to base disk state by just a click.
Desktops provisioning is a big task and time consuming.	Thousands of desktops can be spinned with just a click.
Hardware failures cause downtime.	Hardware failures causes downtime, which is minimal and the environment can be brought up and running ins hardly 10 mins.
Hard disk failures cause data loss.	As data is stored centrally on a storage array, which is robust, and RAID technologies are implemented to make sure data is available even in a event of disk failure.
Have to be physically in front of the desktop to access it.	The virtual desktops can be accessed over internet from a PC or a tablet or a mobile phone.
Less flexibility with ever changing needs.	Multiple desktops types can be provisioned from desktop master images within a few clicks
Patching physical desktops is a nightmare.	Patching all the desktops can be done through a single click from a updated base image snapshot.
Hard to maintain, have to be physically present to troubleshoot issues.	Can be maintained and issues can be fixed centrally.
High Capital and operational costs.	As multiple desktops run on a single ESXI server both capital and operational costs can be reduced.
Storage space on the disk cannot be completely utilized at times.	Storage optimization can be done with desktop virtualization. No chance of disk space wastage.

Virtual Desktop Infrastructure

The desktop operating system is hosted as a virtual machine running on a hypervisor that in turn, is part of the data centre server infrastructure. This is also sometimes referred to as a Hosted Virtual Desktop (HVD).

A user connects to their desktop remotely from a client device (a PC or mobile device) using an optimized delivery protocol (PCoIP) and a connection broker. No data leaves the data centre but screenshot updates are sent over the network.

The virtual desktop typically gets built on-demand, bringing together the different components that make up a full desktop. The operating system, user profile, desktop policies, and applications are all treated as separate components, abstracted from the underlying machine, and are then delivered back together to create a user's desktop experience (Malanco, 2014; Suhr, 2014).

There are three different editions available from VMWare Horizon View: (a) Horizon View Standard Edition, (b) Horizon View Advanced Edition, and (c) Horizon View Enterprise Edition. The key elements of Horizon View are outlined in the following diagram.

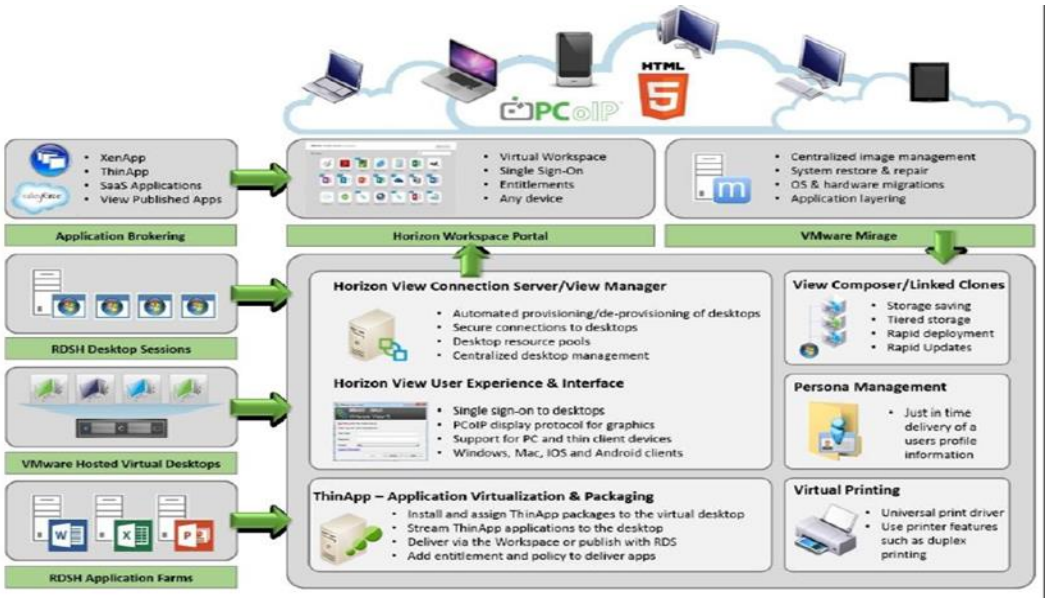


Figure 12. Virtual Desktop Infrastructure (Packt Publishing, n.d.)

VMware View High Level Architecture

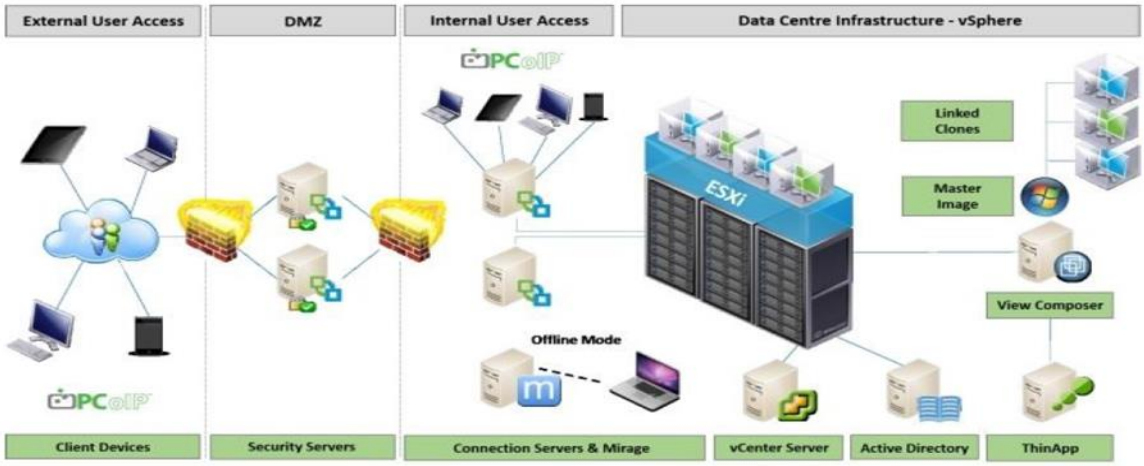


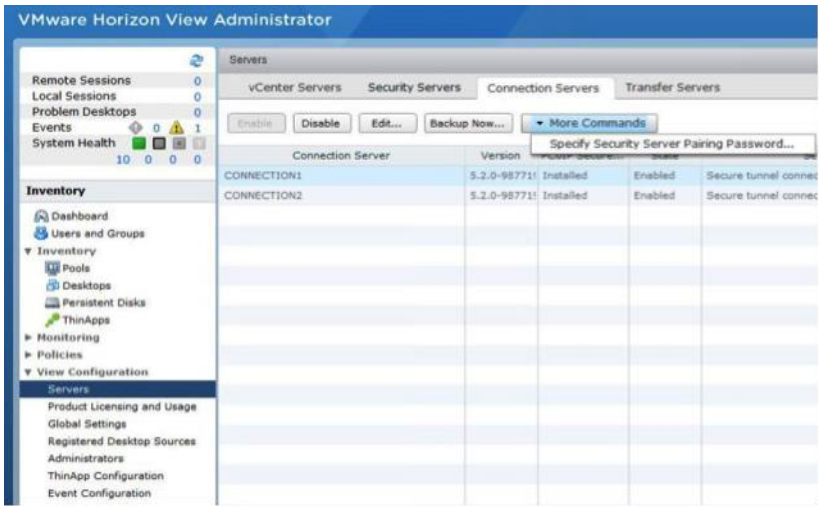
Figure 13. VMware View High Level Architecture (Packt Publishing, n.d.)

The process for connecting to a View virtual desktop is as follows:

1. Install VMware View client on end-user devices.
2. The end user enters the IP address of the connection broker (View Connection server) and his/her logon credentials.
3. The request first hits the load balancer configured to balance the load onto multiple connection servers.
4. The request passes through a firewall and security servers, which help block unwanted access to the View connection servers.
5. Next the request hits the View connection server or the View manager, which authenticates it against Active Directory.
6. Based on the user's credentials, he/she will be presented with desktop pools that he/she is authorized to access.
7. The user can now select a desktop pool from which to activate a virtual desktop.
8. The view connection server will now present a desktop to the user from the desktop pool he/she selected.

9. If there are no virtual desktops available in the pool, View connection server initiates a clone operation on vCenter server.
10. If the user needs to utilize the virtual desktop without a network connection, View transfer server can be used to download the session to the user's device. The user can then upload the desktop back to the View environment once done working on the desktop locally.

Once View connection server is installed, the dashboard looks as below. This is where administrators can actually create and manage desktop pools, add vCenter servers, and troubleshoot problems.



Benefits of Desktop Virtualization

- Centralized administration of desktops
- Centralized data management
- Better IT compliance
- IT security Compliance
- Simplified administration and patching
- Rapid provisioning of virtual desktops
- Access desktops remote and from a variety of devices

Benefits of Desktop Virtualization—Explained

1. **Centralized administration of desktops:** When using traditional, physical desktop workstations, all the desktops must be managed in a decentralized and ad-hoc manner. Desktop support teams work 24/7 to make sure all the desktops are up and running to avoid a loss of employee productivity. In contrast, desktop virtualization all virtual desktops can be managed centrally from a View Connection server console.
2. **Centralized data management:** When using traditional, physical desktop workstations, each employee's data is saved on the hard disk inside his/her workstation. If a hard disk fails or is stolen, it can result in data loss or a major security incident. With desktop virtualization, all the virtual desktops exist on servers owned and secured by the company. This makes data loss and unauthorized access much less likely.
3. **Better IT compliance:** On traditional desktops, it can be difficult and time-consuming to keep track the software that is being installed by end-users. This can result in many employee workstations being out-of-compliance with organizational policies. On virtual desktops, software installation and configuration are managed centrally, and can be more easily tracked by IT staff.
4. **IT security Compliance:** On traditional desktops, security is a challenge as locally-stored data is available to the users and there is a chance for the data being stolen or misused. On virtual desktops, data are centrally stored and secured, making data loss and leakage much less likely.

5. **Easy administration and patching:** View virtual desktops are managed through a centralized management console and View Connection server dashboard. Thanks to this centralized model, virtual desktops can be updated and patched from a single console**.** A new virtual desktop snapshot can be created from the completely patched operating system image, and all the existing desktops can be recomposed to the new snapshot state by using the recompose operation on the View Composer server.
6. **Rapid provisioning of virtual desktops:** Provisioning of physical desktops can take a significant amount of time. When an organization purchases new desktop computers, they must go through a lengthy provision process. With View virtual desktops, administrators can quickly and easily instantiate new virtual desktop instances based on existing operating system images. Linked clones allow for even faster deployment.
7. **Ease and flexibility of access:** Desktops deployed by View Composer are run centrally on the ESXi servers. Virtual desktop sessions can be accessed from a variety of devices, as long as they have network connectivity and the View client software installed on them. If users need to continue their work offline, VMware View can make use of local mode, allowing virtual desktop sessions to be downloaded and utilized in the absence of a network connection. Changes can then be synced with the View servers once the user reconnects.

Security

Desktop virtualization offers several security benefits. As virtual desktop sessions are managed centrally and the data disks of all the desktops are now on shared storage, data is more secure than in a traditional desktop scenario. Users cannot permanently install

unauthorized software on the virtual desktops, as floating desktop pools can regularly refresh desktop sessions to approved images.

Limitations

- Need Perfect design to implement Desktop virtualization without which performance issue can resurface. View implementation makes multiple virtual desktops to run as virtual machines on a single ESXI server. All the desktops running would be sharing the IOPS on the Datastore. Improper design will lead to performance issues on the desktops and also leading to downtime as well. View implementation requires a perfect storage IO design which will eliminate the performance issues mentioned above.
- Initial investment is bit higher. VMware View licensing is costly and company has to purchase high end servers and storage to implement the solution which all leads to end up more on capital expenditure. Considering the benefits of virtualization like less power bills, less cooling cost, view would decrease the operational expenditure (Courtenmanche, 2013).

VMware View Components, Description and Prerequisites

- VMware View Connection server
- VMware View Security server
- VMware View Composer
- VMware View Agent

VMware View Connection Server

VMware View Connection server is a connection broker, which can be managed through a web-based graphical interface. The Horizon View Connection Server, sometimes referred to as Connection Broker or View Manager, is the central component of the View

infrastructure. Its primary role is to authenticate users and deliver the appropriate desktop resources based on the user's profile and user entitlement (Lowe, 2013).

Prerequisites

Table 2

VMware View Connection Server Requirements

Components	Minimum	Recommended
Processor	1cpu (2GHz)	4 CPU
Memory	4 GB	10 GB*
Network	10/100 Mbps NIC cards	1 Gbps

*The RAM 10 GB recommended is to run 50 Virtual Desktops.

OS Requirement

Table 3

VMware View Connection Server OS Requirements

Operating System	Version	Edition
Windows Server 2008 R2	64 Bit	Standard or Enterprise
Windows Server 2008 R2 Sp1	64 Bit	Standard or Enterprise

VMware View Replica Server

View Replica Server is used to provide high availability and load balancing to the connection server. We can have one or more replica servers. For this paper one Replica Server has been installed.

Prerequisites

Table 4

VMware View Replica Server Requirements

Components	Minimum	Recommended
Processor	1CPU (2GHz)	4 CPU
Memory	4 GB	10 GB*
Network	10/100 Mbps NIC cards	1 Gbps

*The recommended 10 GB RAM is to run 50 Virtual Desktops.

Operating System Requirements

Table 5

VMware View Replica Server OS Requirements

Operating System	Version	Edition
Windows Server 2008 R2	64 Bit	Standard or Enterprise
Windows Server 2008 R2 SP1	64 Bit	Standard or Enterprise

In addition to the above requirements, there are few more requirements for installing View Replica Server:

- An administrator account on the View admin portal is required to start the View Replica Server installation.
- The View Replica Server should be connected to the same LAN as the Connection Server, as the database replication cannot be done across a WAN.
- View Replica Server should not be installed on a server that is running any View infrastructure servers.

VMware View Security Server

- Horizon View Security Server is an instance of the View Connection Server which sits within your DMZ so that you can allow end users to securely connect to their virtual desktops from an external network or the Internet.
- Security Server is a component of the View suite, which adds an additional layer of security between the Internet and an organization's internal network.
- The View Security Server should be integrated with Connection Server to get the security benefits it offers.

Pre-Requisites

Table 6

VMware View Security Server Requirements

Components	Minimum	Recommended
Processor	1 CPU	4 CPU
Memory	4 GB	10 GB
Network	10/100 Mbps NIC cards	1 Gbps

OS Requirement

Table 7

VMware View Security Server OS Requirements.

Operating System	Version	Edition
Windows Server 2008 R2	64 Bit	Standard or Enterprise
Windows Server 2008 R2 SP1	64 Bit	Standard or Enterprise

VMware View Composer

VMware View Composer, a key component of VMware vSphere, is tightly integrated with VMware View Manager to provide advanced image management and storage optimization. VMware View Composer reduces storage requirements for virtual desktop machines by up to 90 percent and enables organizations to more effectively manage their desktop images (VMware, n.d.j).

View Composer—Linked Clones

View Composer uses the concept of linked clones to create desktop pools. Linked clones are virtual desktops that share a common base image, thereby greatly reducing the storage requirements for a View desktop pool.

- Step 1: Prepare the master desktop image. In this step the master desktop has to be created on an ESXI server and a snapshot of the desktop has to be taken.

- Step 2: Create the View desktop pool. This step involves creating a desktop pool making use of linked clones. While creating a pool, the following items must be configured: the virtual machine name, number of desktops required in the pool, spare powered-on desktops, and disposable disk settings. A snapshot for the pool creation has to be specified for the wizard.
- Step 3: Enable Provisioning. This is the step where the View Connection Server requests View Composer to create desktop pools.

VMware View Composer Prerequisites

Table 8

VMware View Composer Server Requirements.

Component	Required	Recommended
Processor	1.4 GHz or faster Intel 64 or AMD 64 processor with 2 CPUs	2GHz or faster and 4 CPUs
Networking	One or more 10/100Mbps network interface cards	1 Gbps
Memory	4 GB	8 GB
Disk space	40 GB	60 GB

OS Requirements

Table 9

VMware View Composer Server OS Requirements

Operating System	Version	Edition
Windows Server 2008 R2	64 Bit	Standard or Enterprise
Windows Server 2008 R2 SP1	64 Bit	Standard or Enterprise

Chapter IV

HARDWARE AND SOFTWARE REQUIREMENTS

HP ProLiant DL 360 G8 with Intel Xeon with 96 GB RAM. Dell PowerVault MD3200I storage. A total of six servers and two client machines, one client to serve as a golden image for view desktops and another client used to connect to view environment., where in the view client is installed are created to complete this research paper which include the following:

1. Domain Controller running Windows Server 2008 R2
2. Three SQL Server databases instances to store vCenter configuration, View Connection Server data, and View Composer configuration and inventory data
3. One vCenter Server instance
4. One View Connection Server installed on Windows Server 2008 R2
5. One View Composer Server installed on the same machine where vCenter server is running.
6. Two View Replica Servers
7. Two Windows client operating system instances
8. One Windows 7 Client machine with View Agent installed for Master Image·
9. One Windows Client machine with view client installed to connect to View environment
10. Two VMware ESXi hypervisor (One Bare metal and one Nested)

Product Costing

VMware View licenses are sold in two ways: (a) Named Users: Each desktop is dedicated to a single user and (b) Concurrent Users: A set number of desktops are deployed and used by all staff members.

Table 10

Product Costing

License Type	Horizon View Standard	Horizon View Advanced	Horizon View Enterprise
Named Users	-----	$3025	$4130
Concurrent Users	$3025	$4840	$6800

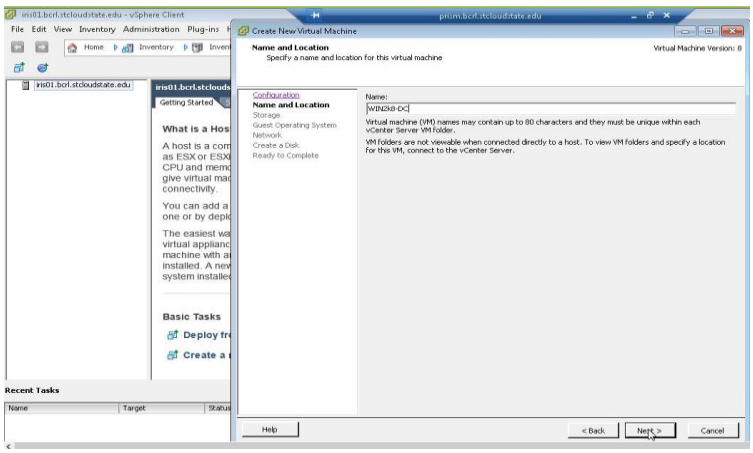
Chapter V

IMPLEMENTATION

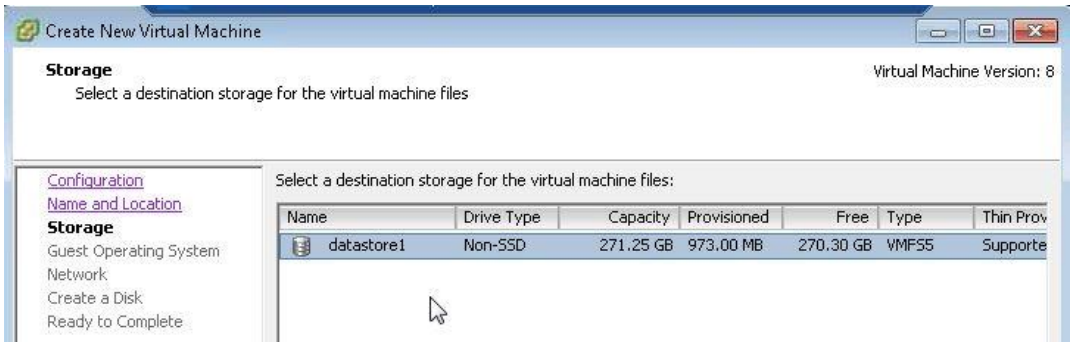
Following are all the screenshots taken while building the VMware View setup. (Beerens, 2013; Courtenmanche, 2013; Lowe, 2013, 2015; Malanco, 2014; Suhr, 2014; VMware, n.d.c, n.d.k, n.d.i, n.d. j, n.d.l).

Domain controller setup:

1. Create a Windows Server 2008 R2 virtual machine on the physical ESXi server. Name used for DC: Win2K8-DC.

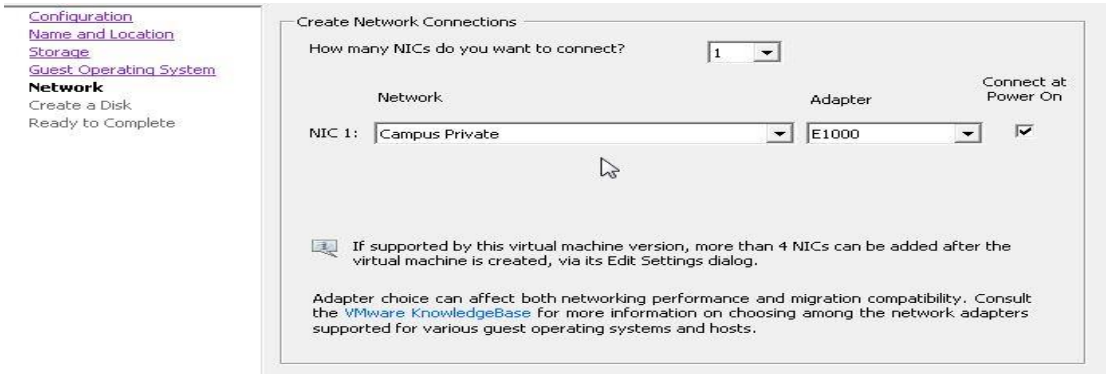


2. Select the datastore for the virtual machine.

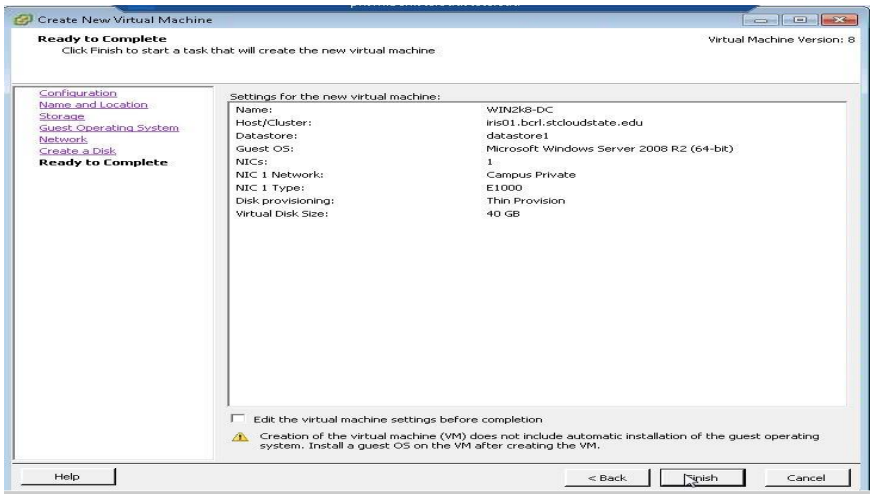


3. Select the OS family and the OS from the list of supported OS.

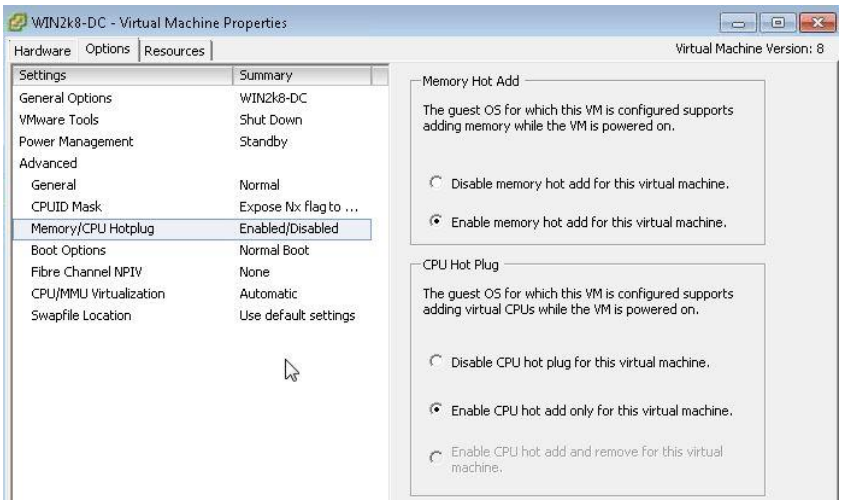
4. Selecting the network card, network label, and adapter type.



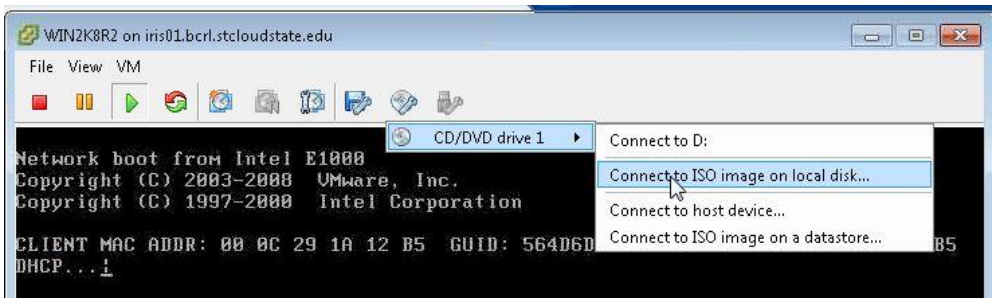
5. Review the selection and click Finish to start creating the VM.



6. Alter the RAM and CPU of the VM as required. Enabling CPU and memory hot plug will allow a user to increase the RAM and CPU of a virtual machine even while it is powered on.



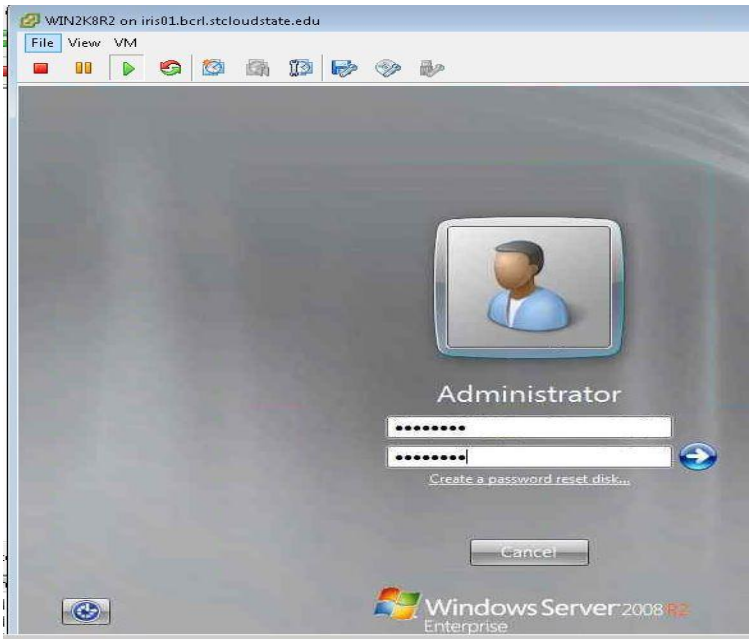
7. Power on the VM and configure the CD/DVD drive to map the ISO image for Windows Server 2008 R2.



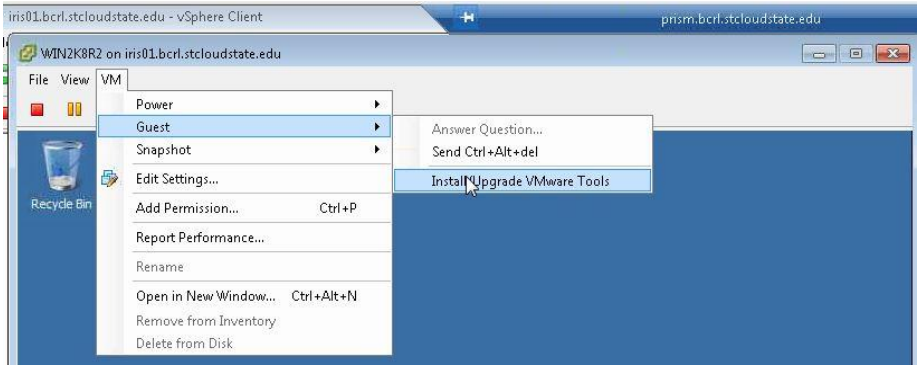
8. Select the language preferences, time, and keyboard layout.

9. Click on Install now.

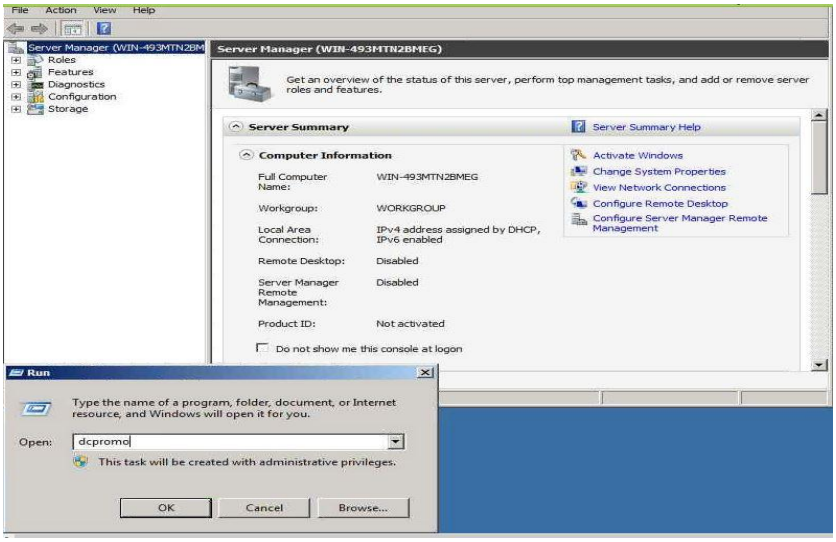
10. Set the password for the administrator user and log into the machine.



11. Install VMware Tools on the VM to enhance the mouse, keyboard, and screen performance. Reboot the VM to ensure the changes take effect.

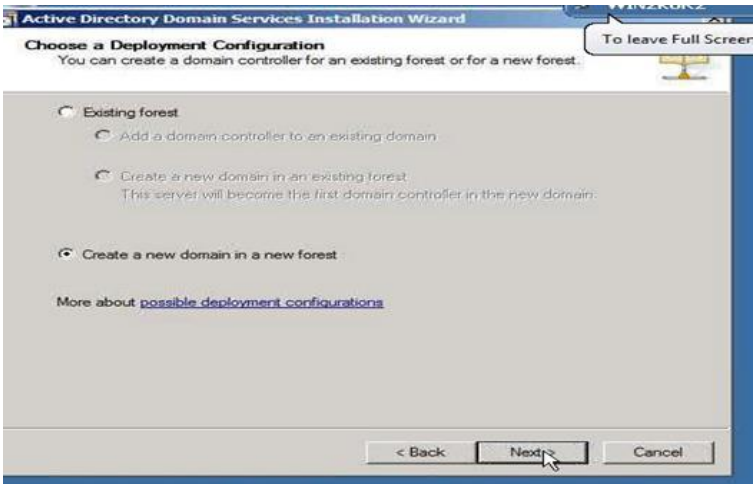


12. Promote the Windows Server instance to a domain controller by running the "dcpromo" command at an administrative command prompt.

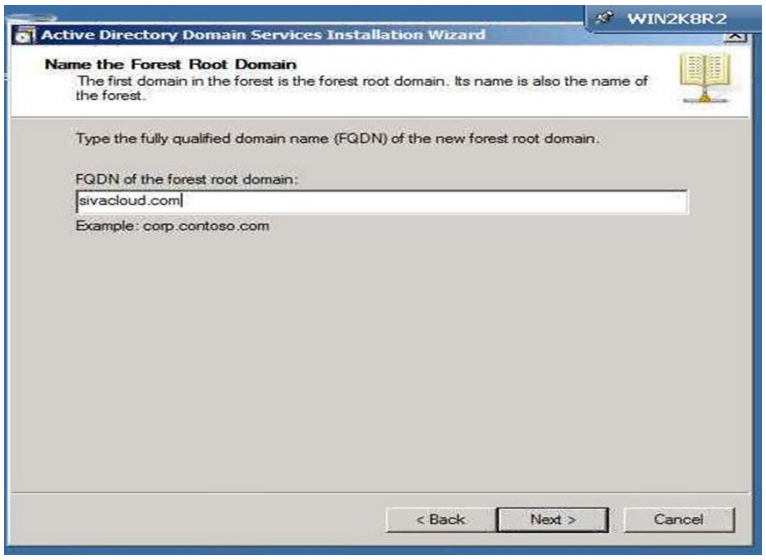


13. DCPROMO will start the AD installation.

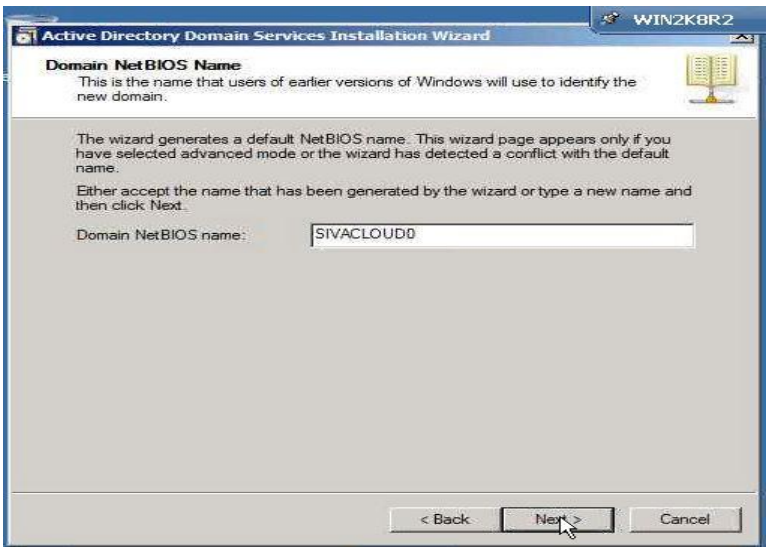
14. Indicate that a new domain in a new forest should be created.



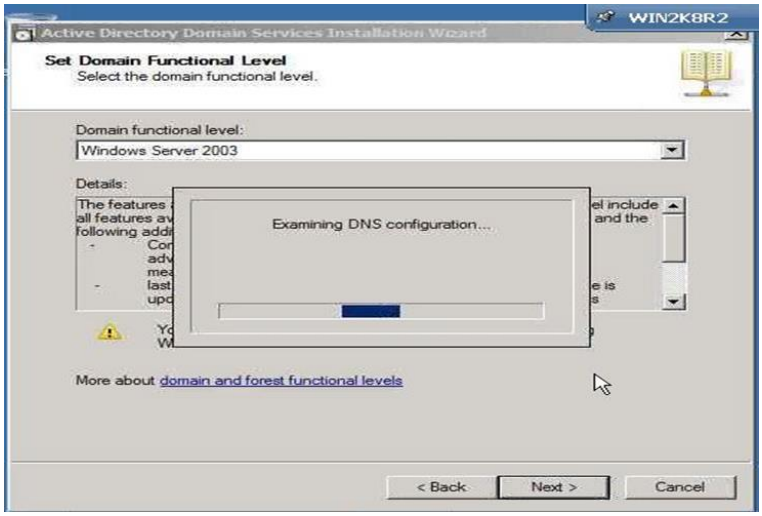
15. Name the FQDN of the forest root domain.



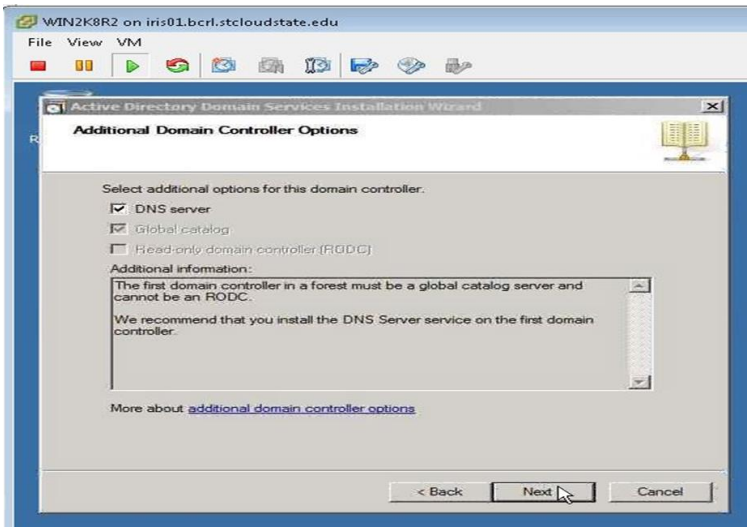
16. Provide a NetBIOS name for the server.



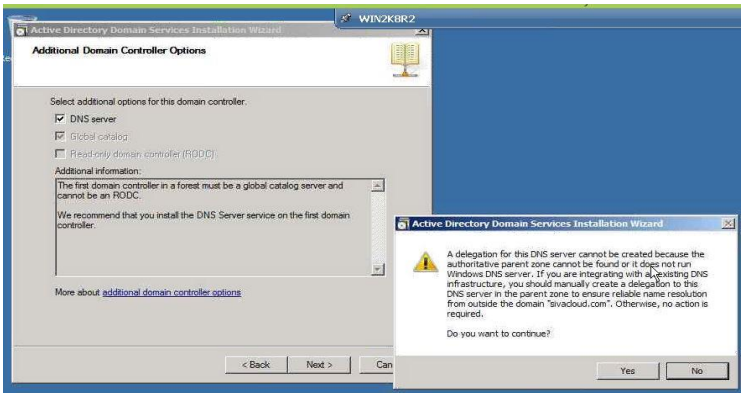
17. Select the domain functional level. Here I have selected the Windows Server 2003 level for backwards compatibility.



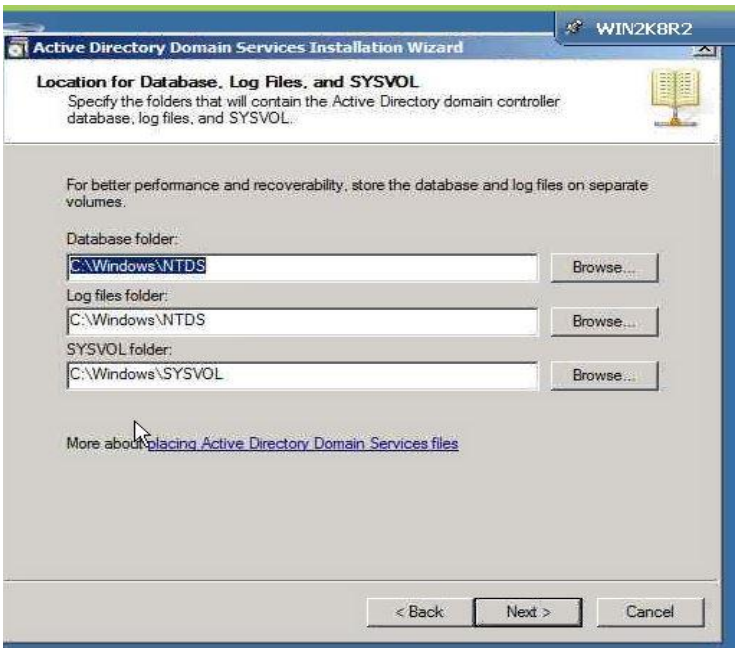
18. Install the DNS server role.



19. Ignore the error message and click Yes to continue.

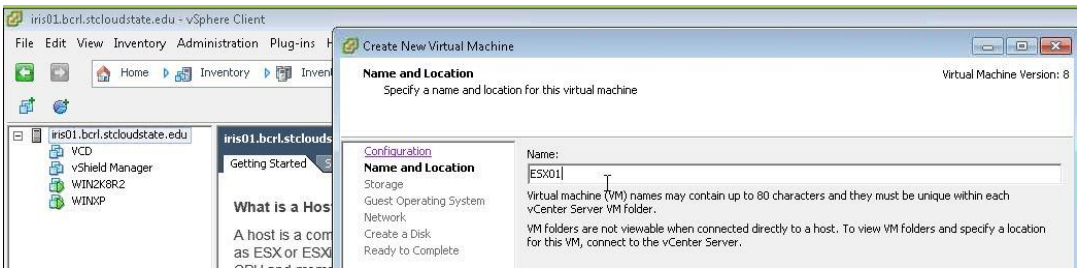


20. Specify the database, log files, and sysvol locations.

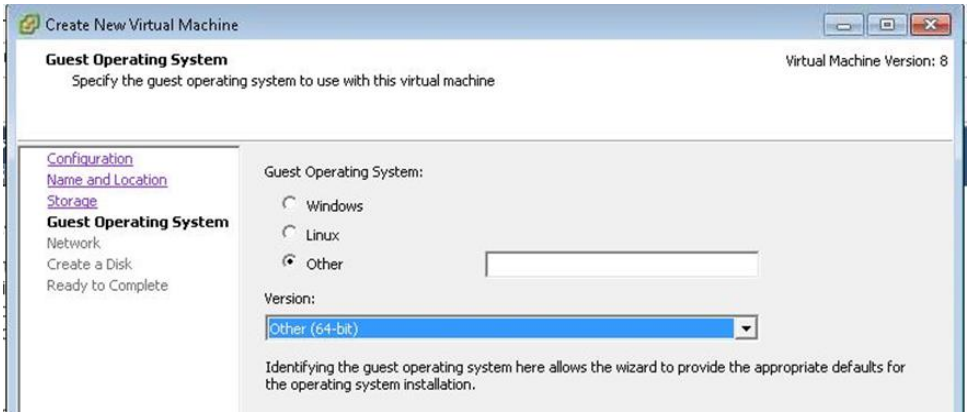


21. Review all the options and click Next.

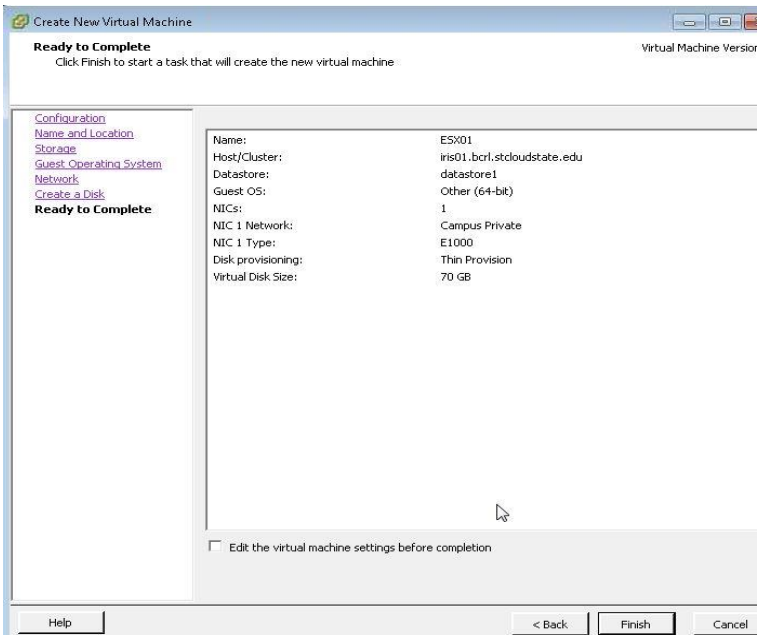
22. Now as we are done with the domain controller installation, we next need to install a virtual ESXi server instance on our physical ESXi server. The steps to complete this process are as follows:



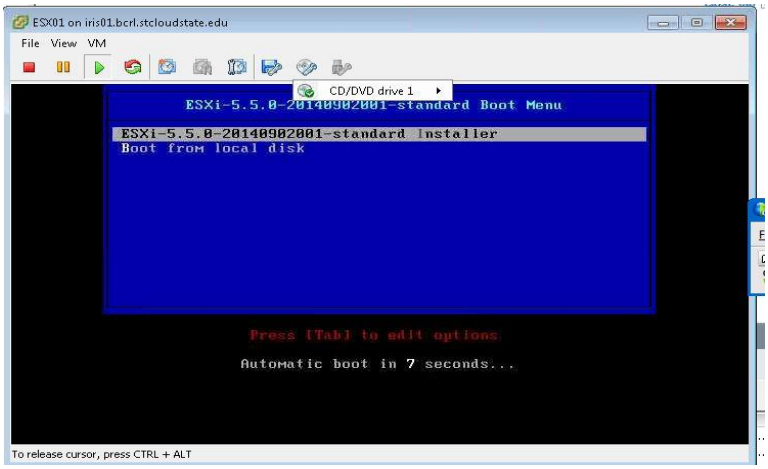
23. In OS type, select Other (64-bit), as ESXi is neither Windows nor Linux.

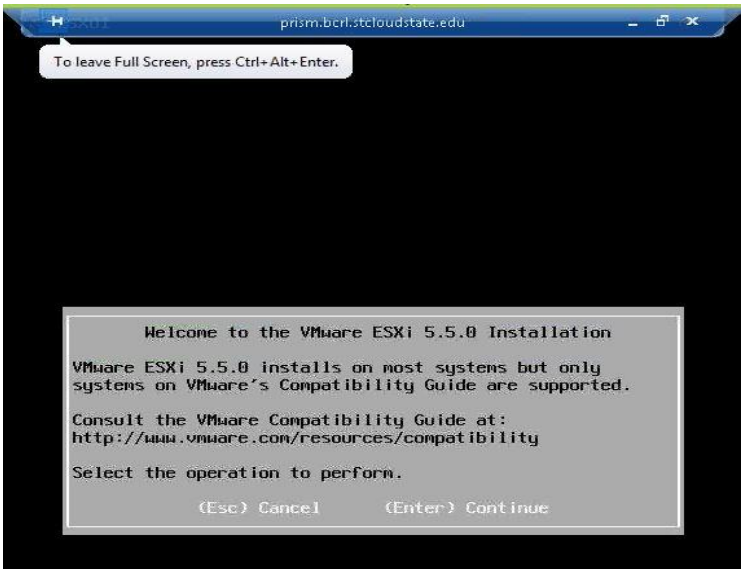


24. Review all the selections and click on Finish to create the virtual machine.

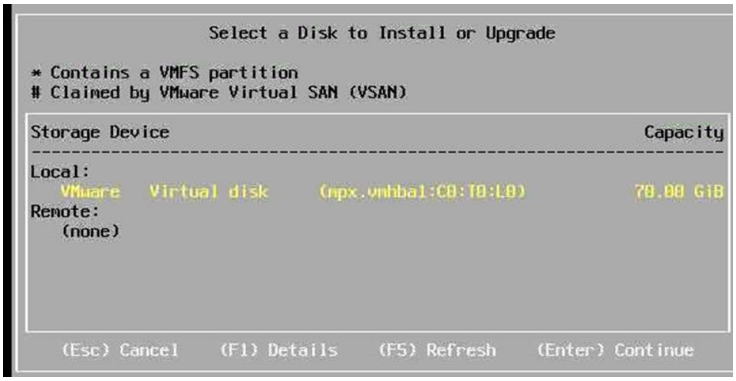


25. Map the installation ISO to the CD/DVD drive and click CTRL+ALT+ INSERT to begin the installation.





26. During the installation ESXi will scan for all the hardware attached.

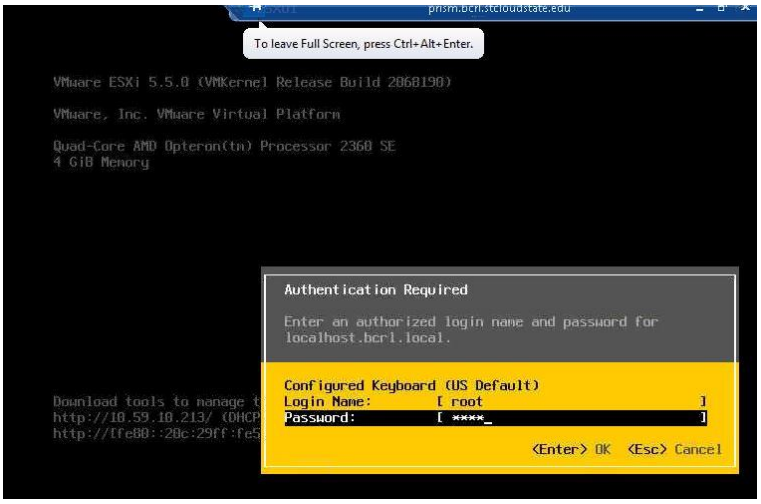


27. Enter a root password. The root account will be used for administering the ESXi server.

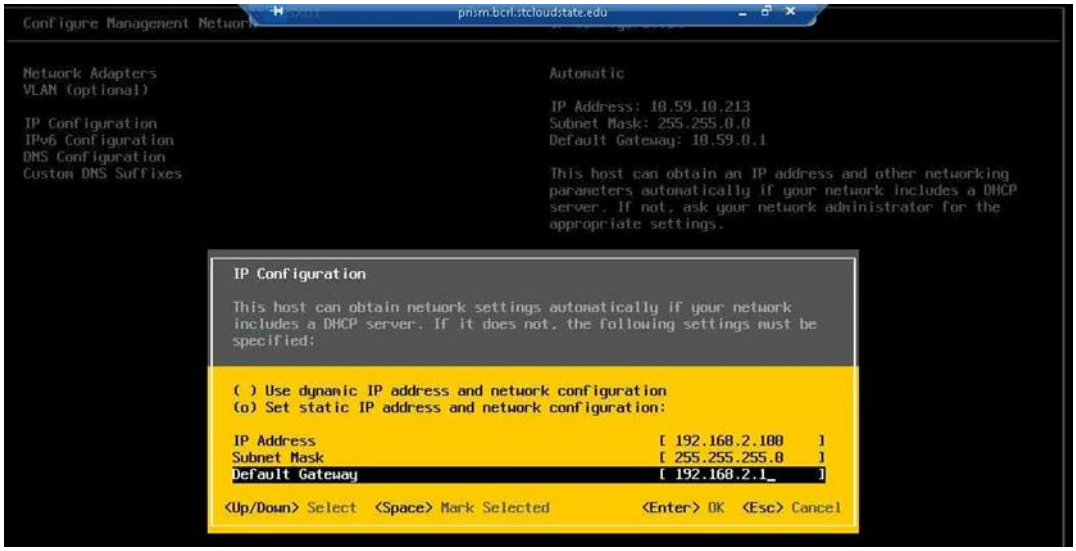
28. Click F11 to start the installation.

29. Enter to reboot after the installation.

30. Login to the ESXi Server with the root account to start the configuration.



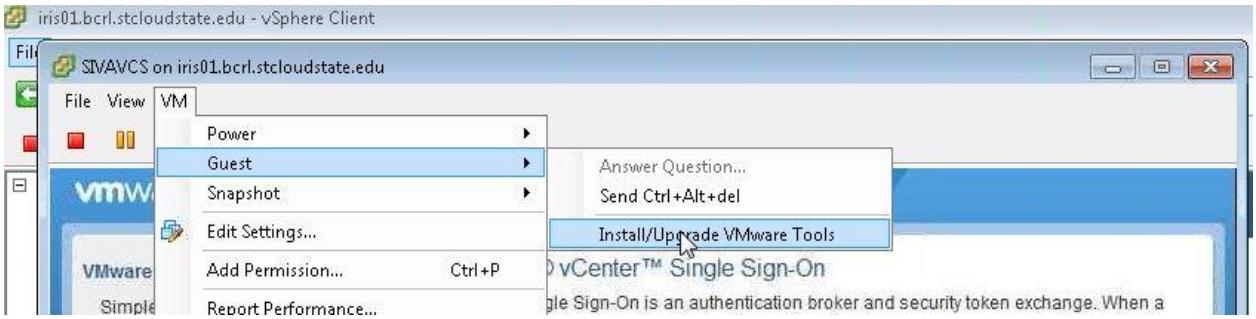
31. Once logged in, the user is shown the Direct Console User Interface (DCUI) of the ESXi server. The DCUI allows the user to configure the IP network settings, root password, and hostname. The user can also view system log files and enable/disable system services.



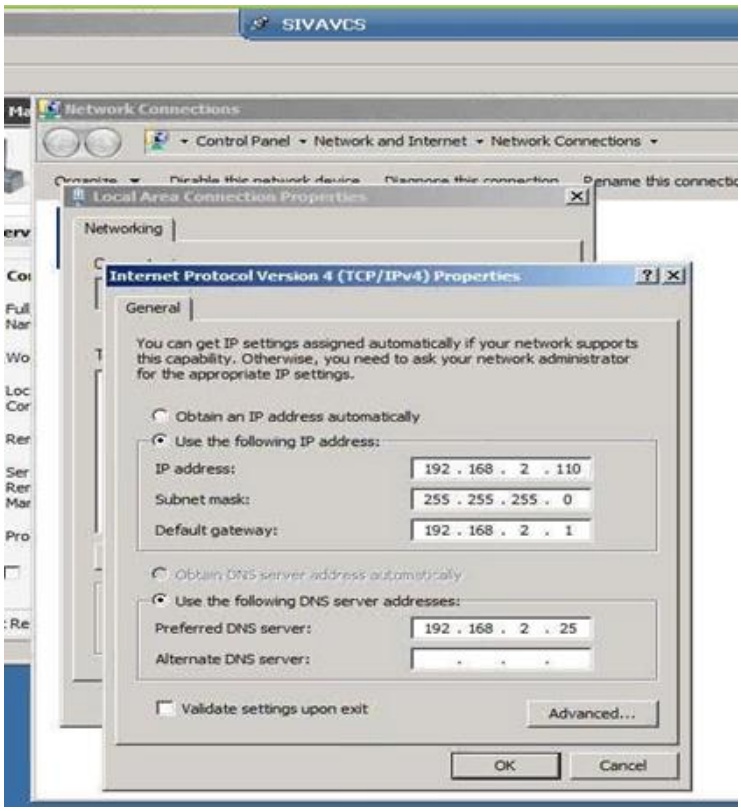
32. Once we have a virtual instance of ESXi installed, the next step is to create a vCenter Server instance on a Windows Server VM. I installed vCenter on a Windows Server 2008 R2 VM and joined the machine to the domain created for this lab.

33. Before installing the vCenter Server software, there are a few preliminary steps that must be taken:

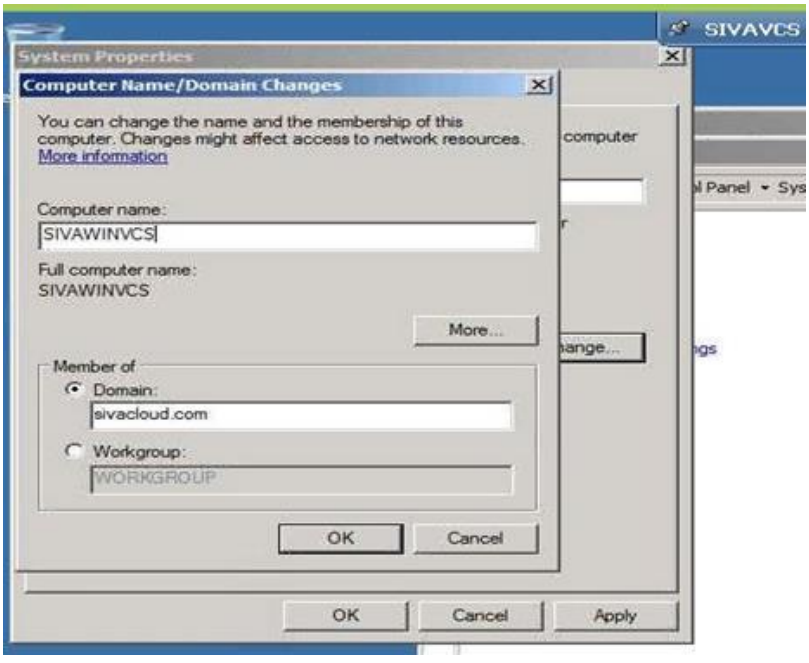
34. Install VMware Tools. VM tools can be mounted from the VM option on the virtual machine console. From the VM option navigate to guest and click on Install/Upgrade the VM tools.



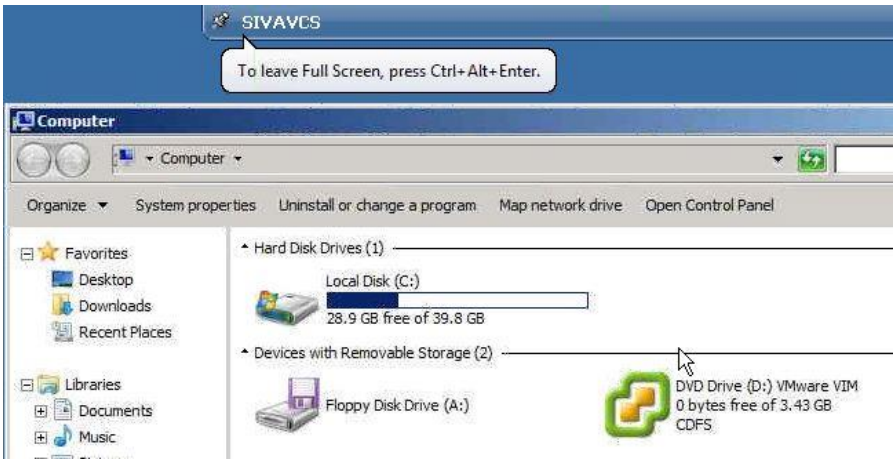
35. Assign the static IP address to the Windows Server instance. Like the ESXi servers it manages, vCenter should always be assigned a static IP address.



36. Change the computer name and join it to the domain created earlier.



37. To begin the vCenter installation, the vCenter ISO image must be mounted onto the virtual machine. The steps to complete the installation are as follows:



38. Either choose the simple install to have the wizard install all necessary components, or choose the custom, component-based installation, where each component is installed separately.

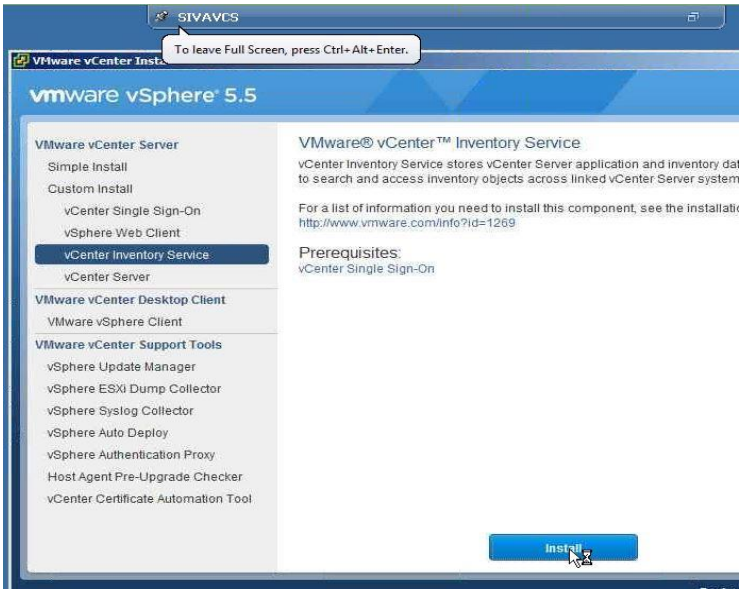
The custom installation option allows the administrator to install vCenter components on different servers, if desired, and configure important features like high availability.

Single Sign On (SSO) is a vCenter component, which allows users to login into all of vCenter components with a single user name and password.

Install the vCenter Web Client. Web Client is used to connect to vCenter Server, offering an alternative to the traditional vSphere Client application. Web client uses a web

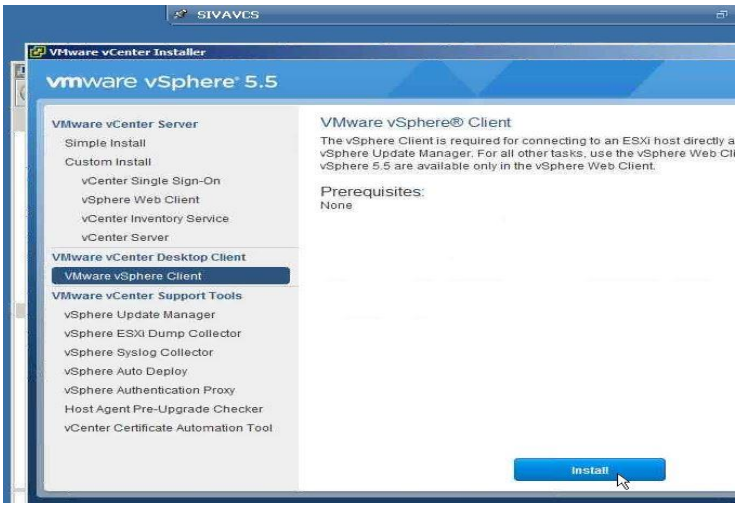
browser like Google Chrome, Mozilla Firefox, or Internet Explorer to administer the vCenter infrastructure without having to use vSphere Client.

1. The next step in the wizard is to install the vCenter Inventory Service.

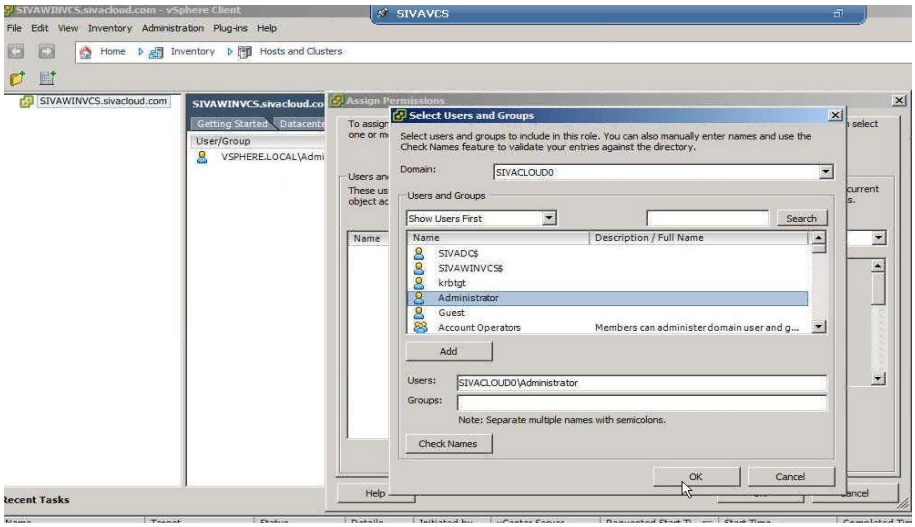


2. Finally, the core vCenter software is installed.

3. We also need to install the vSphere Client application on the same machine.

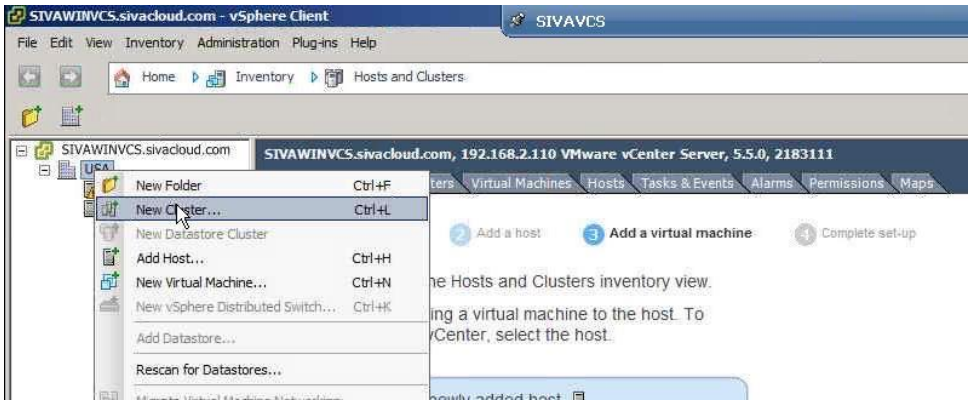


4. Once the vCenter installation completes, we next need to delegate permissions to the administrator user on the same machine so that the user can log in. In vSphere 5.5, a default domain, vsphere.local will be created automatically. By default, only the vsphere.local\administrator account will have access to the vCenter server.

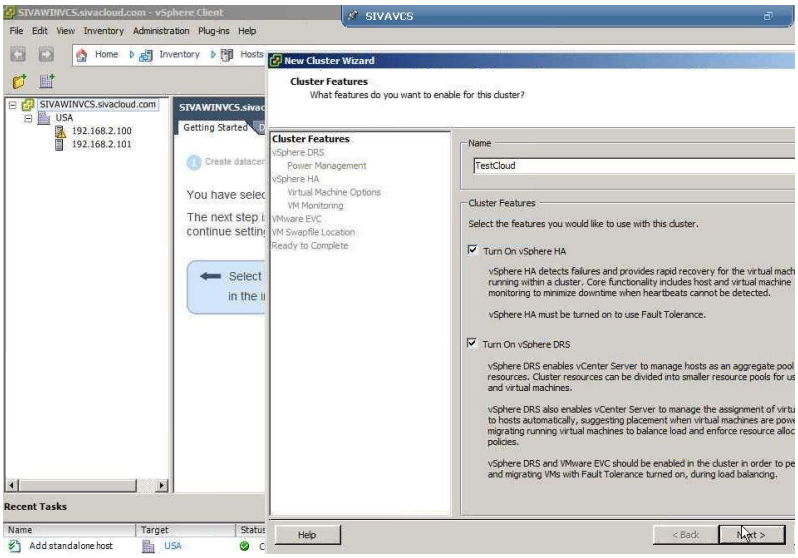


5. The next step is to add the ESXi server to the vCenter server, which was just created. However, before ESXi servers can be managed by vCenter, we must create a virtual datacenter and a server cluster on the vCenter server. A cluster is a group of ESXi servers which will be used to enable HA and DRS for business continuity and load balancing.

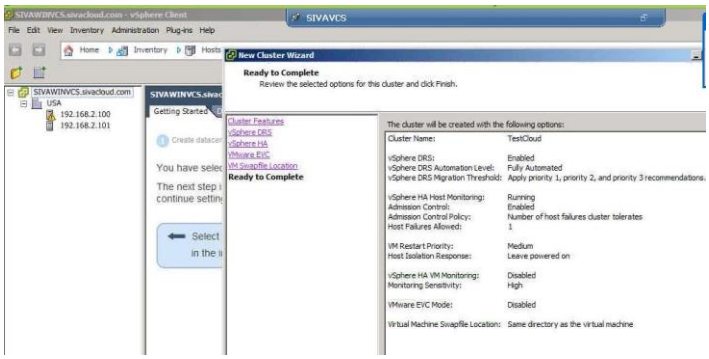
6. Now create a cluster and add both ESXi servers to the cluster.



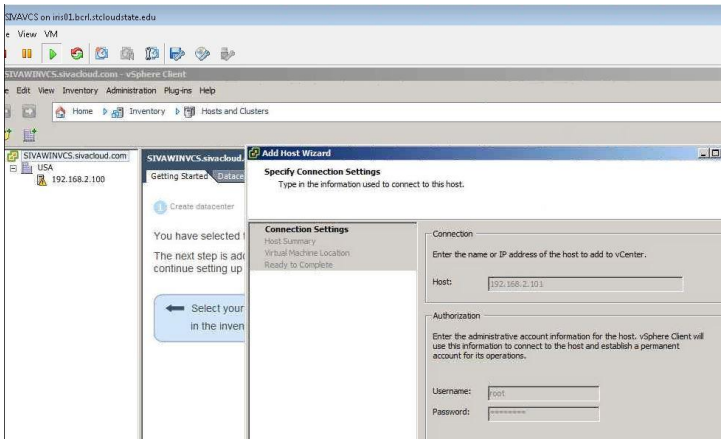
7. Name the cluster. Enable both vSphere HA and DRS, so as to provide high availability using HA and initial placement and load balancing using DRS.



8. Check all the options and finish the cluster creation.



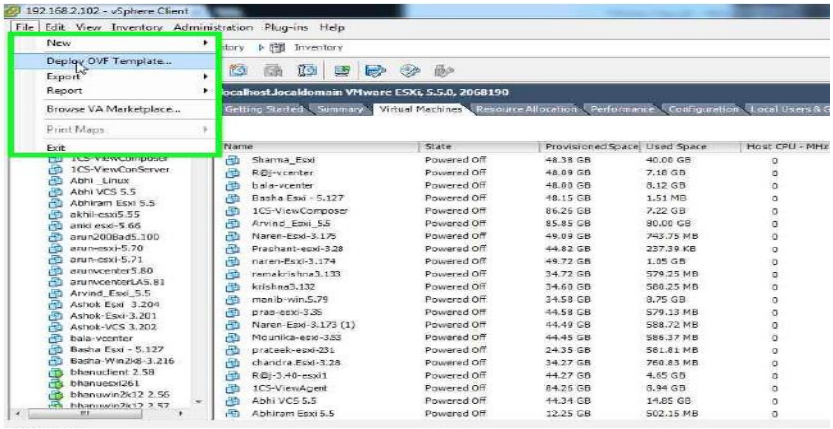
9. While adding the ESXi Server, give the root credentials for authentication. Lockdown mode for the ESXI host can be enabled while adding a ESXI server to vCenter server. This option prevents users from logging in to the ESXi server remotely.



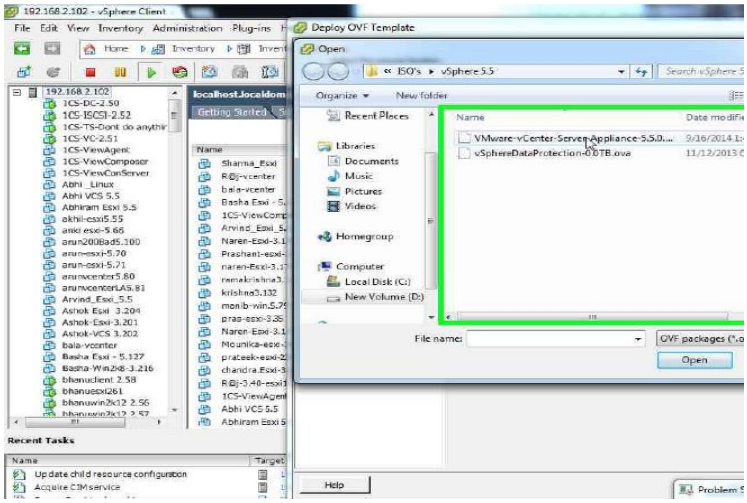
vCenter Server Appliance Installation

In addition to installing the vCenter Server software on a Windows Server instance, a second option exists for deploying vCenter. The vCenter virtual appliance is a prepackaged Linux VM containing all vCenter components. The appliance comes as an open virtualization format (OVF) template that can be downloaded directly from the VMware website. The steps to deploy the vCenter appliance are as follows:

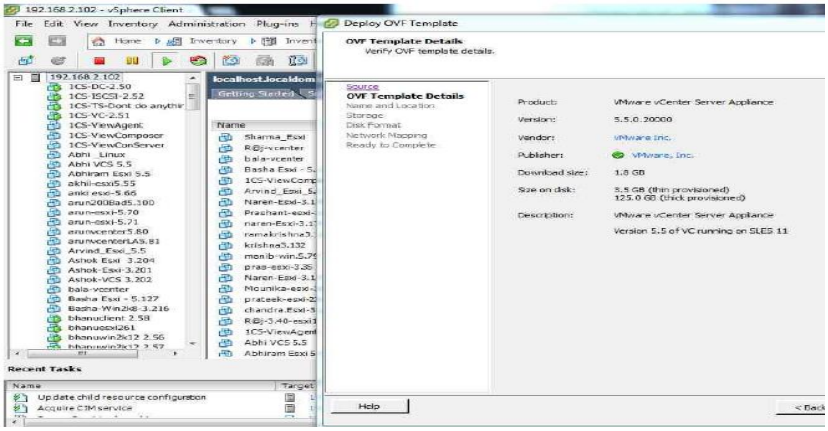
1. Connect to ESXi server from vSphere Client and select File > Deploy OVF Template from the menu bar. The wizard will open as shown below.



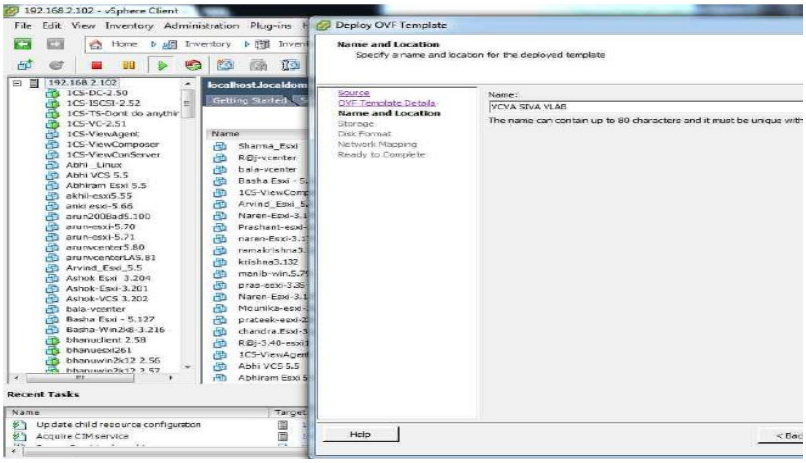
2. Browse to the downloaded OVF file and click Next.



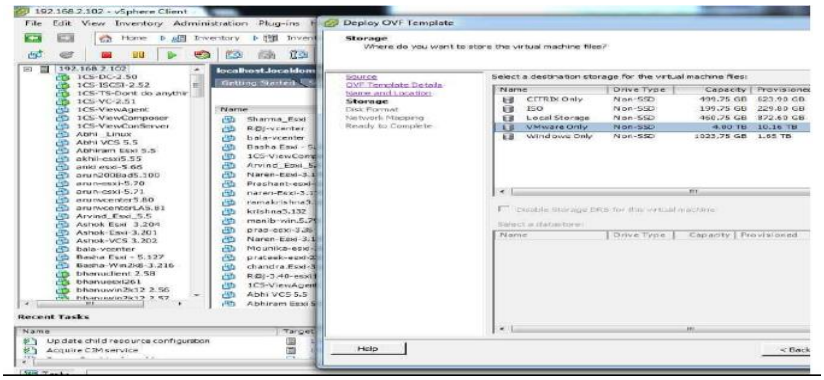
3. On the next screen it shows the description of the product. It is vCenter Server Appliance version 5.5 running on SUSE Linux Enterprise Server 11.



4. Name the vCenter Virtual appliance and click Next.



5. Select a datastore on which to deploy the appliance and Click next.

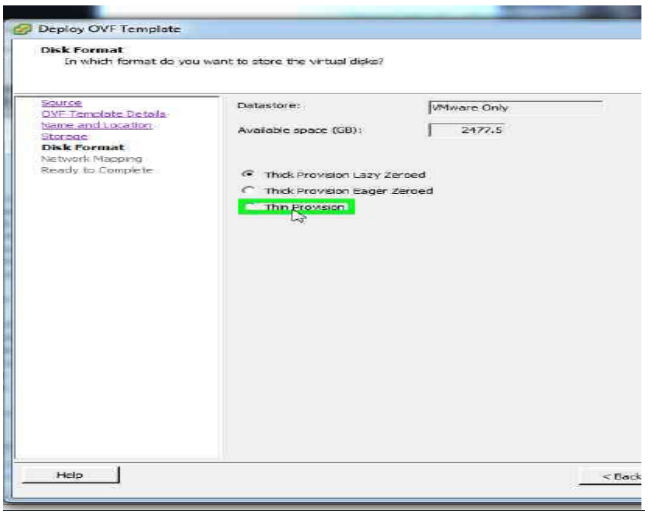


6. Select the provisioning type for the appliance. VMware vSphere offers three provisioning types:

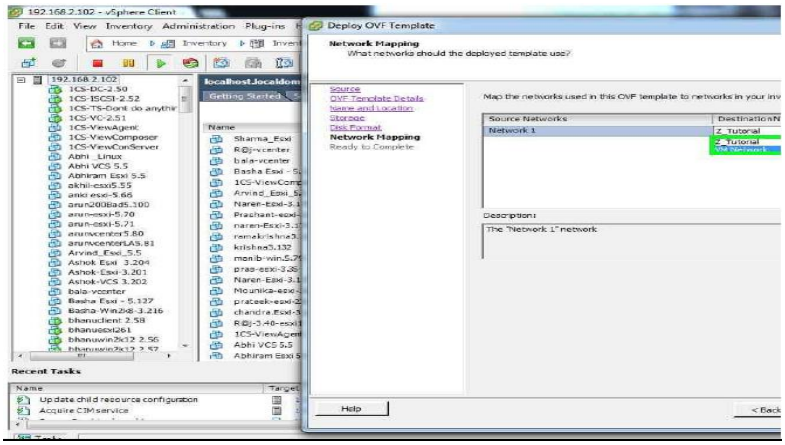
    - Lazy Zeroed (upfront allocation and on-demand formatting). Hard disk space will be allocated to the virtual machine upfront and the formatting of

the disk space will happen on demand when the virtual machine needs it. This is not recommended for mission-critical applications, as the VM must wait for disk formatting to complete.

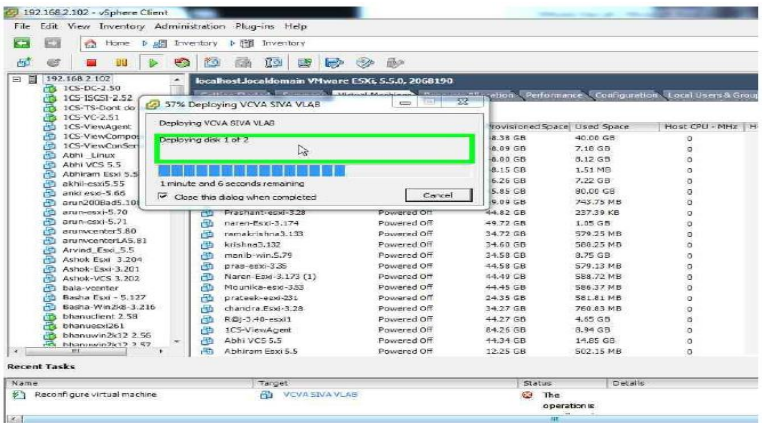
- Thick provision Eager Zeroed (upfront allocation and upfront formatting). In this provisioning type, the hard disk space is provisioned upfront and the formatting of the disk also happens upfront. All disk space is available to the VM immediately. This provisioning type is best for business-critical applications as the app can utilize all disk space immediately.
- Thin provision (on-demand allocation and on-demand formatting). In this provisioning type, the ESXi server owns the disk space and allocates the space to the virtual machine as needed. This provisioning method optimizes storage utilization, as VM will only consume the amount of disk space actually used by the guest operating system. However, it is not recommended for mission-critical applications, as both provisioning and formatting must be done dynamically.



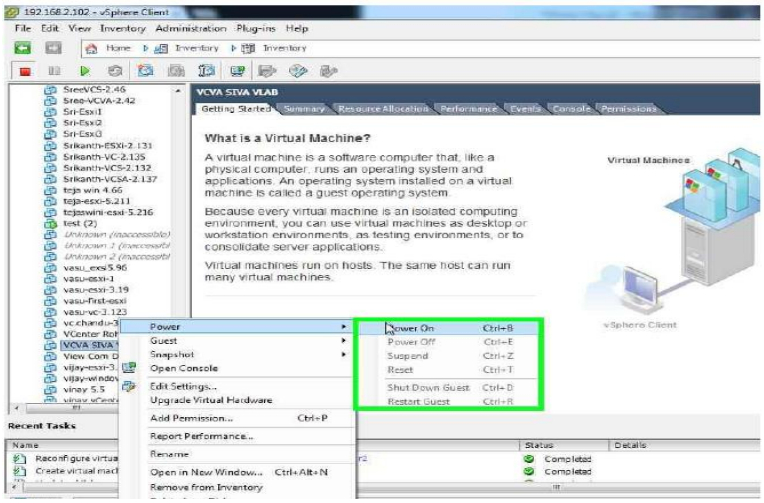
7. Map the network for the virtual machine and click next.



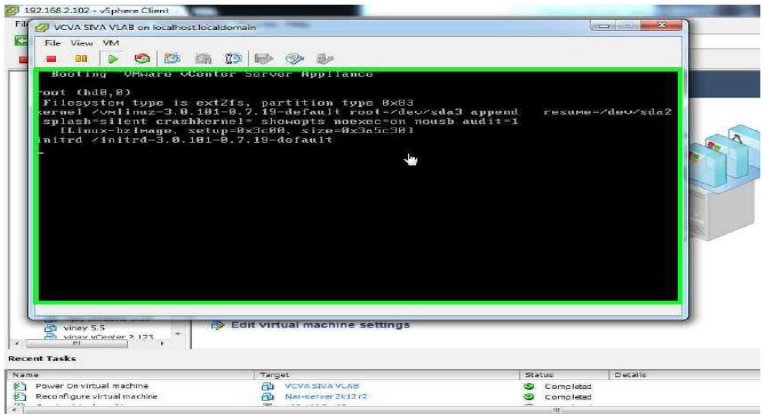
8. Once the above steps have been completed, the appliance deployment will commence.



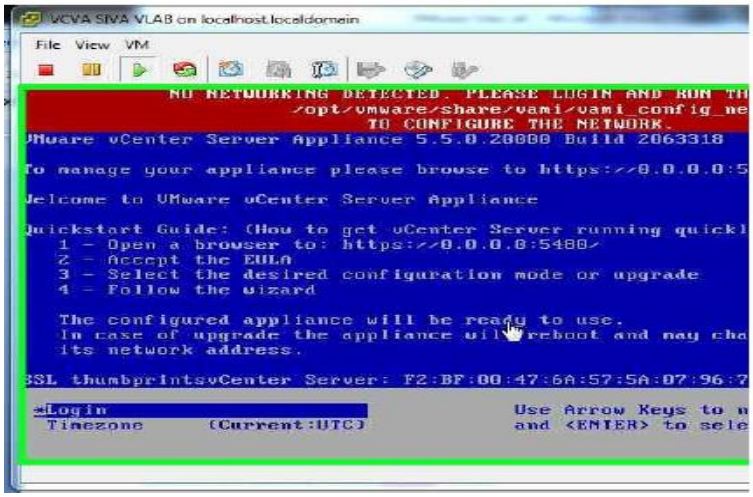
9. Once the deployment is complete, select the virtual machine and power it on.



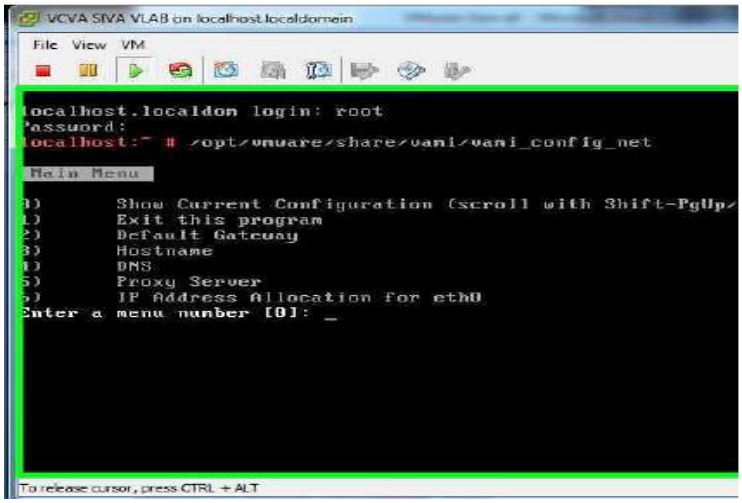
10. The below screenshot shows the boot process of SUSE Linux 11.



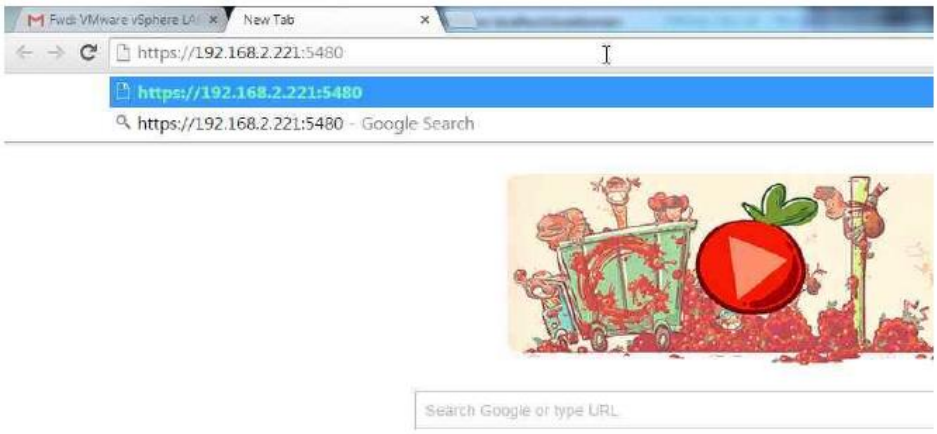
11. Once the appliance is completely booted, log in using the default root user and a password of "vmware". At the Linux command line, run the command "/opt/vmware/share/vami/vami_config_net" to start configuring the virtual appliance.



12. Using the text-based interface, configuring the network settings and hostname for the vCenter server.



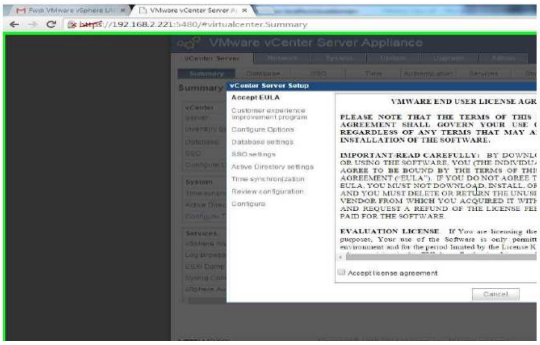
13. Once the appliance is configured, open a web browser and point it to https://hostname:5480.



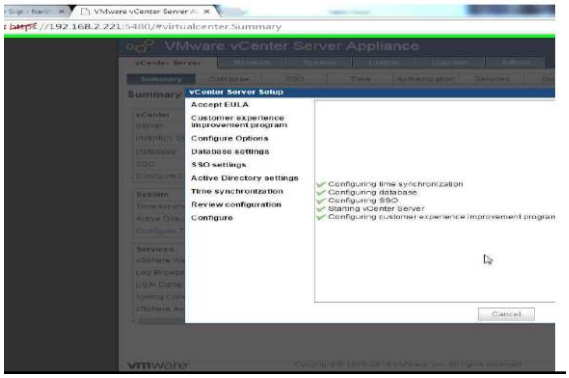
14. A setup wizard will be automatically opened within the web browser. Accept EULA and click Next. The remainder of the configuration can be done in one of four ways:

    - Configure with default settings. This option sets SSO as embedded, database as embedded, and will skip the Active Directory and time sync configurations.
    - Upgrade from a previous version. This option allows the user to upgrade the appliance from an older version to the latest version.

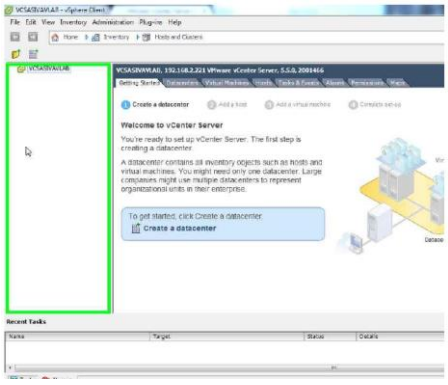
- Upload a configuration file. This option allows the admin to use a configuration file to configure the new appliance. This is possible if the company has existing vCenter instances and wants to replicate the existing configuration onto the new server.
- Configure with custom configuration. This option can be used to configure the appliance with external database.



15. Once the configuration is complete it looks as in the screenshot below.

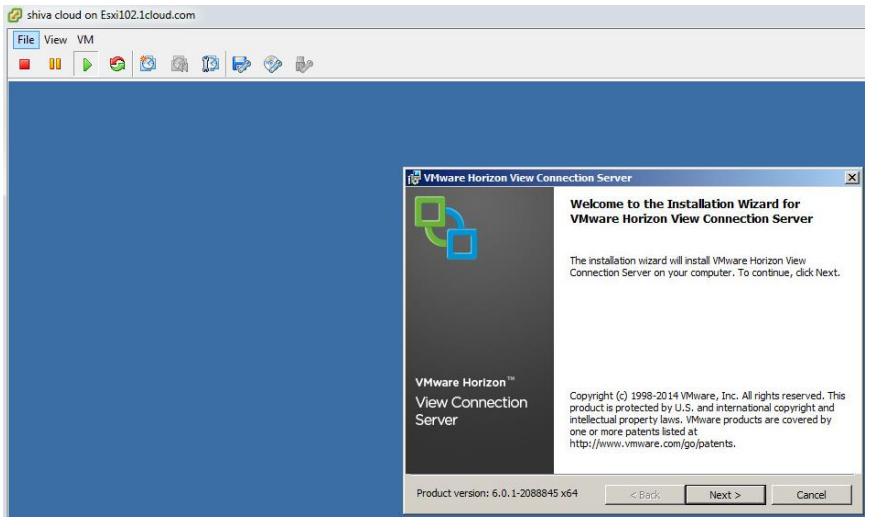


16. You can now log into the vCenter Server instance using the vSphere client.

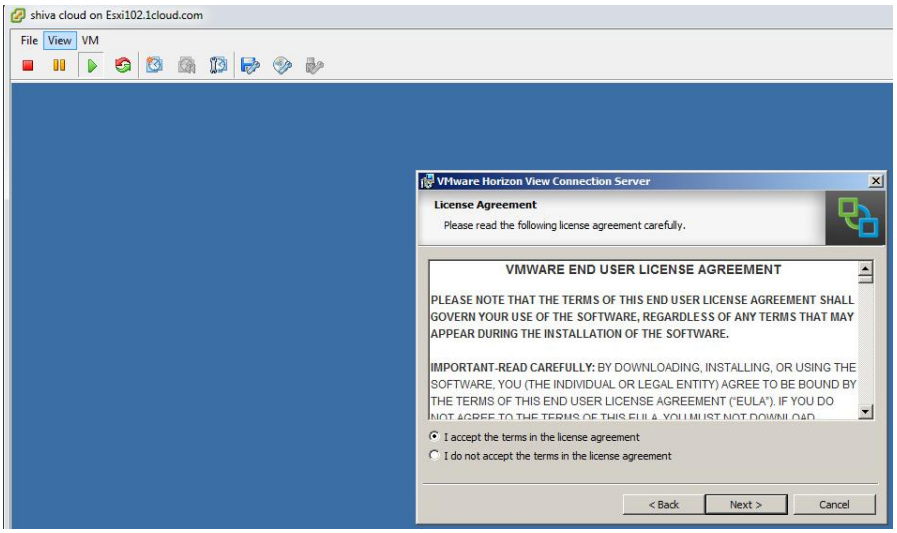


VMware View Connection Server Installation

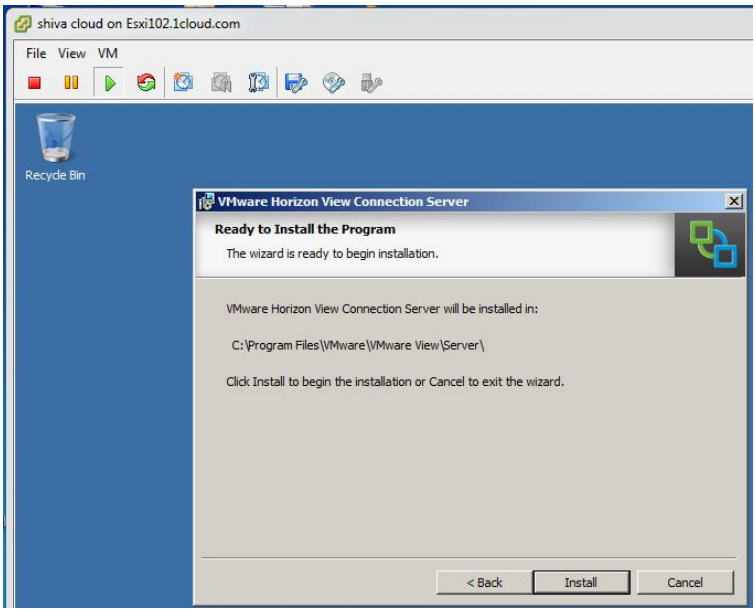
Installing VMware View Connection Server is similar to installing vCenter Server. To start the View Connection Server installation, we first need an instance of Windows Server installed in a virtual machine on an ESXi server. Once the Windows VM is ready, download the View Connection Server installer file and run it to begin the installation. The steps to complete the installation are described below:



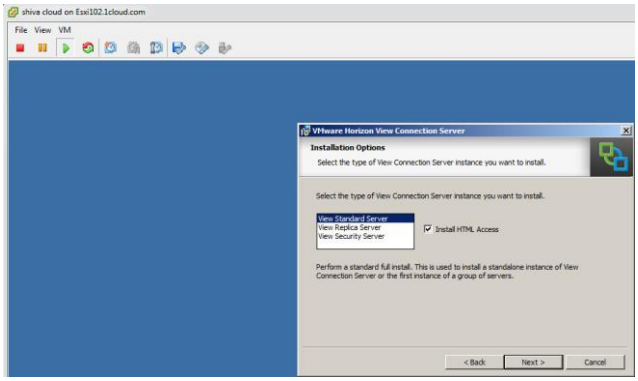
1. Accept the EULA to proceed.



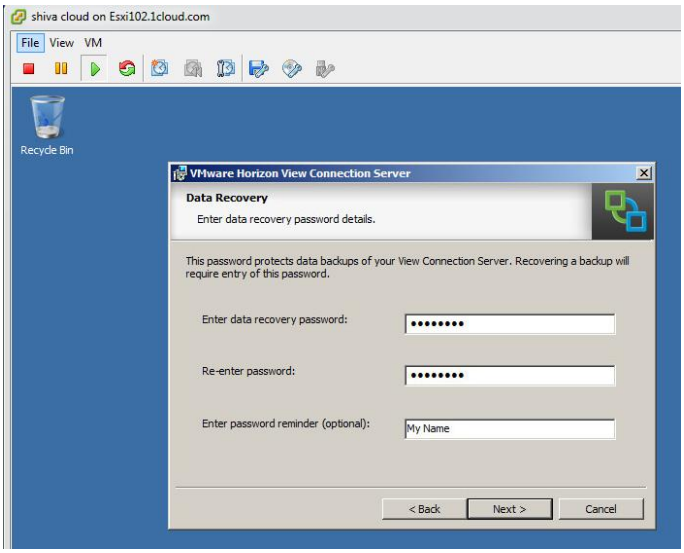
2. Select the installation location and click Next to proceed.



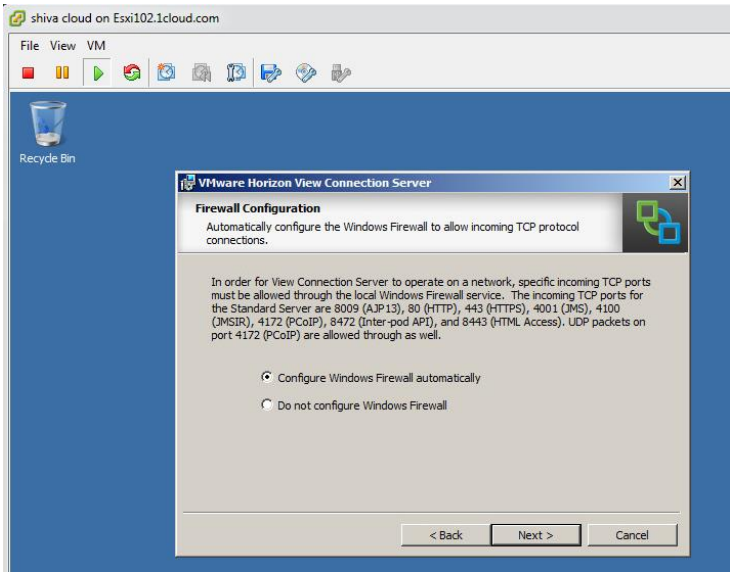
3. Select the type of View installation from the list and click Next to proceed.



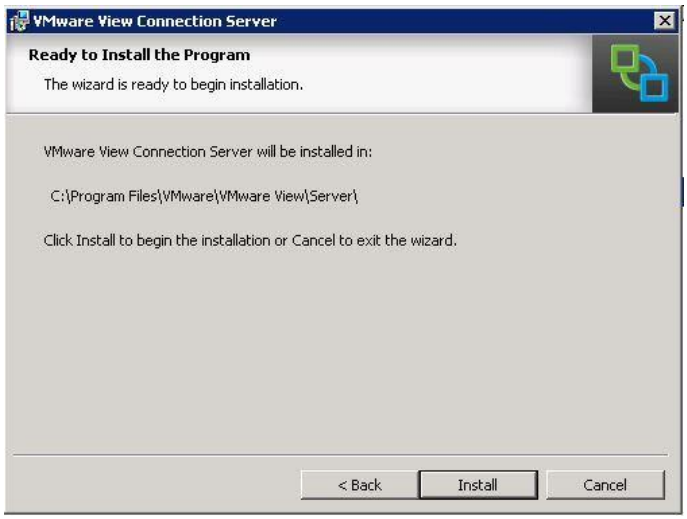
4. Now set a data recovery password, which will be used by Connection Server to protect the regular backups that it makes. This password will be used to recover the View Connection Server from a system crash.

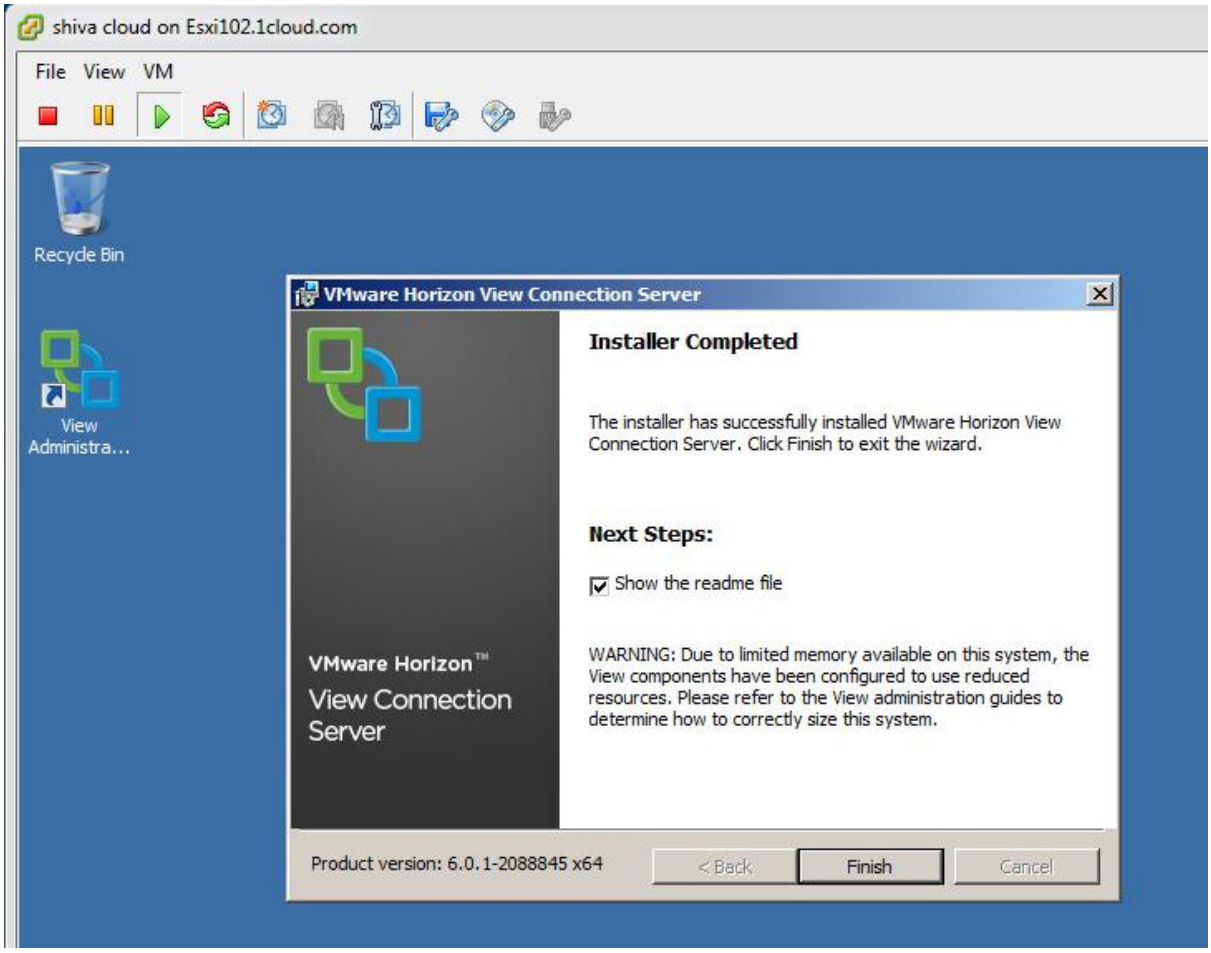


5. The next step is to configure the Windows Firewall to allow the ports needed by the View Connection Sever.



6. Click the Install button to complete the installation.



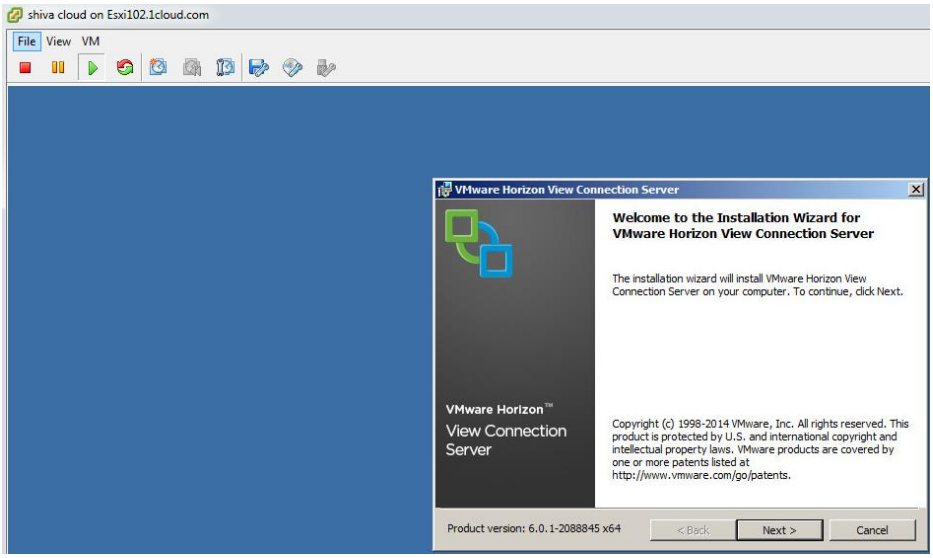


7. Once the installation is complete, open a web browser and browse to the Connection Server web portal.

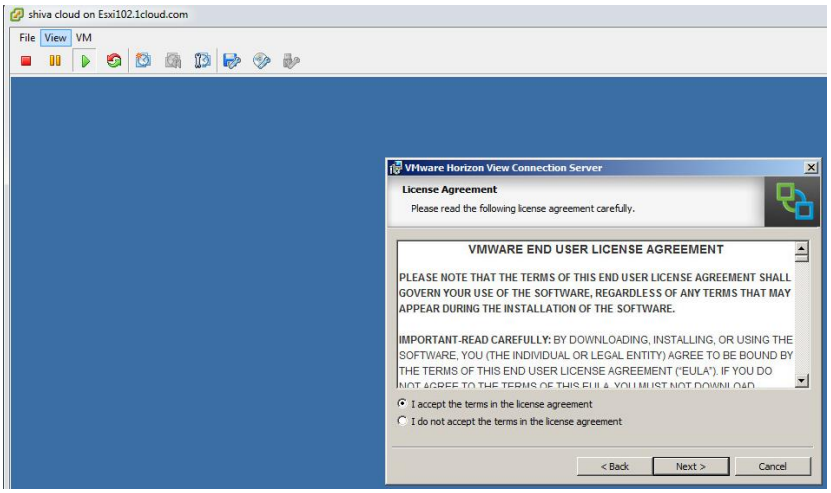
View Replica Server Installation

Once the Windows Server machine is ready, log into the machine using the administrator account and copy the View Connection Server installation media onto the VM. The steps for installing the View Replica server are as follows:

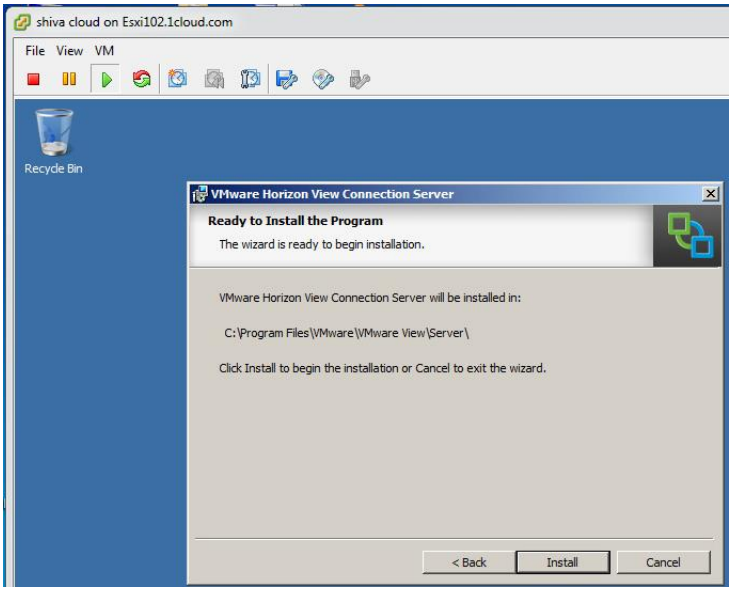
1. Once the installer is launched, a welcome screen appears as below step. Click Next to continue.



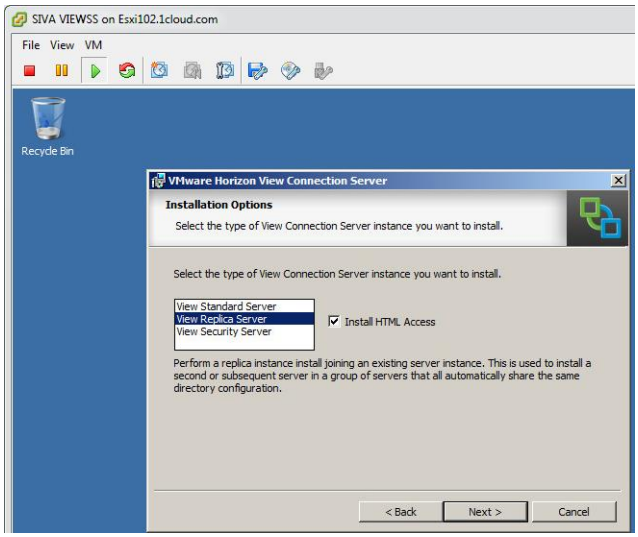
2. Accept the EULA and click Next to continue.



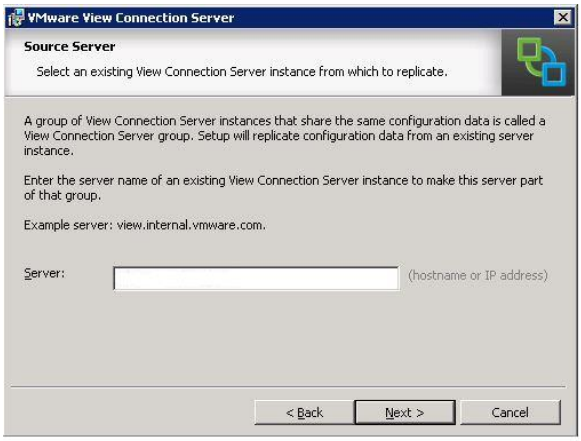
3. Select a location to install the View Replica Server to.



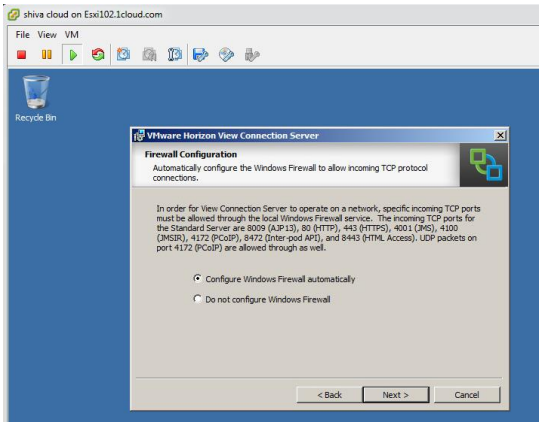
4. Select View Replica Server from the list of installation options.



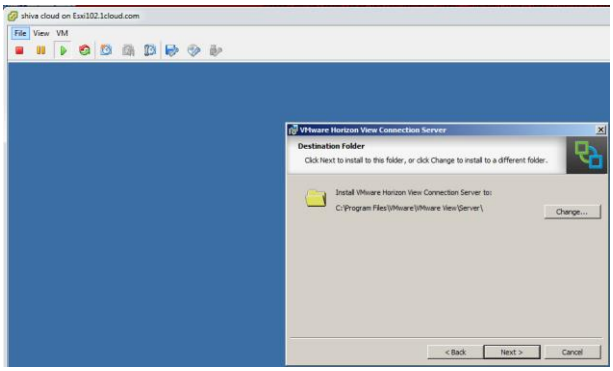
5. Join the Replica Server to the existing View Connection Server group by entering the fully-qualified name of the existing View Server.

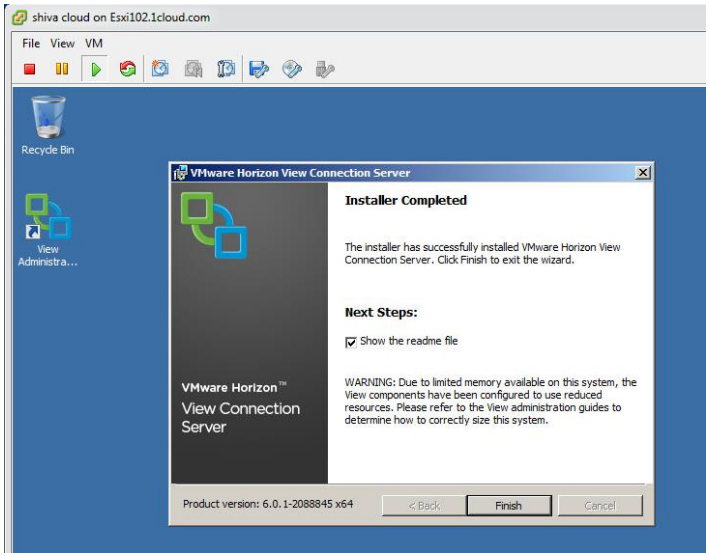


6. Allow the installation wizard to automatically configure the necessary Windows Firewall settings.



7. Click Install to complete the installation.





View Security Server Installation

An additional Windows Server virtual machine is required for installation of the View Security Server. Like the other View components, the Security Server should have VMware Tools installation, be assigned a static IP address, and be joined to a common Active Directory domain.

View Security Server

View Security Server acts as a mediator between the end users and the Internal LAN. This server is typically deployed in a company's DMZ network, which is a high-security zone separated from both the Internet and organizational LAN by firewalls. Users who try to

connect to the View Connection Server first hit the Security Server, which in turn facilitates secured connections to the View Composer Server.

As the Security Server resides between firewalls, there are certain things that have to be carefully considered before implementing it. Most importantly, there is a set of ports, which must be opened on the firewalls.

Important points about View Security Server include:

1. Security Server should be deployed in a DMZ zone.
2. Unlike the other components of VMware View, Security Server should not be a part of an Active Directory domain.
3. A separate SSL certificate has to be created or purchased from a valid certificate authority.
4. As users connect to their virtual desktops using the RDP or PCoIP protocol, the corresponding network ports should be allowed through the perimeter firewall protecting the DMZ. These ports include the following.
5. Ports required between clients and Security Server:
6. TCP destination port 4172 from Client to Security Server
7. UDP destination port 4172 from Client to Security Server
8. UDP source port 4172 from Security Server to Client.
9. Ports required between Security Server and View Servers on internal network:
10. TCP destination port 4172 from Security Server to View servers
11. UDP destination port 4172 from Security Server to View servers
12. UDP source port 4172 from view servers to Security Server

13. Additionally, the backend firewalls must be configured to allow IPsec. If a backend firewall is configured between the Security Server and View Connection Servers, firewall rules have to be configured to allow the connections.
14. If enabled, the Windows Firewall will be configured by the Security Server installer and IPsec rules will be added automatically.
15. A logical view of the View Security Server installation and the firewall rules is given below:

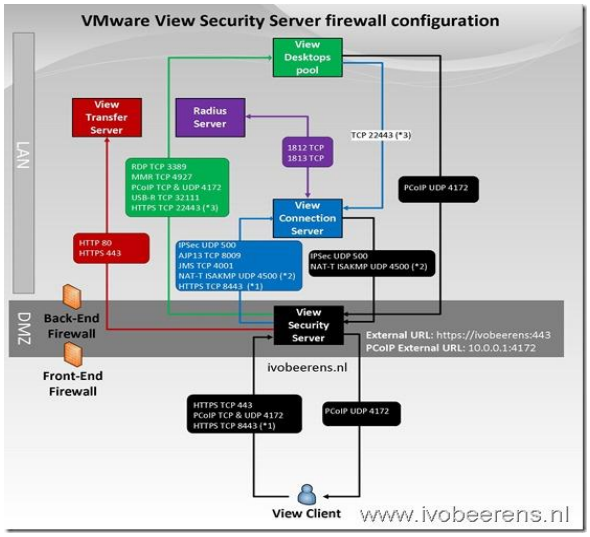
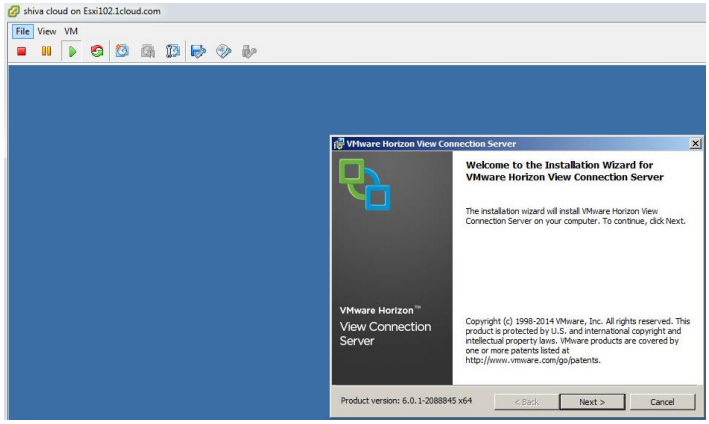
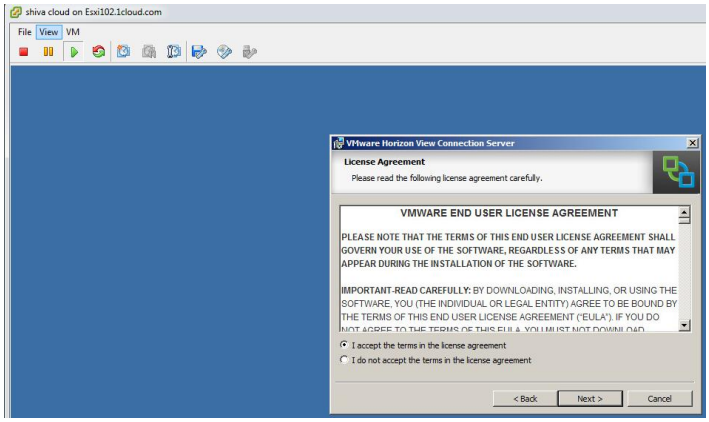


Figure 14. View Security Server Installation Firewall Rules and Ports Configuration (Beerens, 2013)

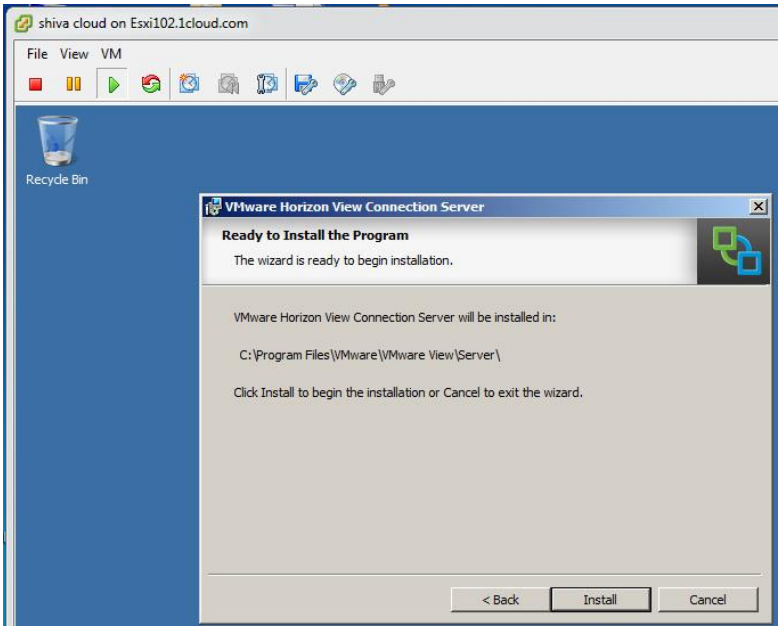
16. The process for installing View Security Server on a Windows Server virtual machine is described below:



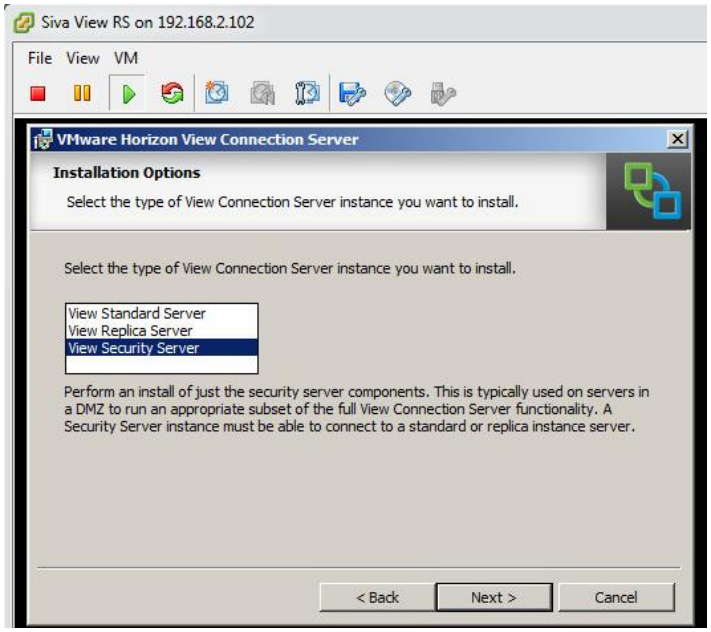
17. Accept the EULA and click Next to continue.



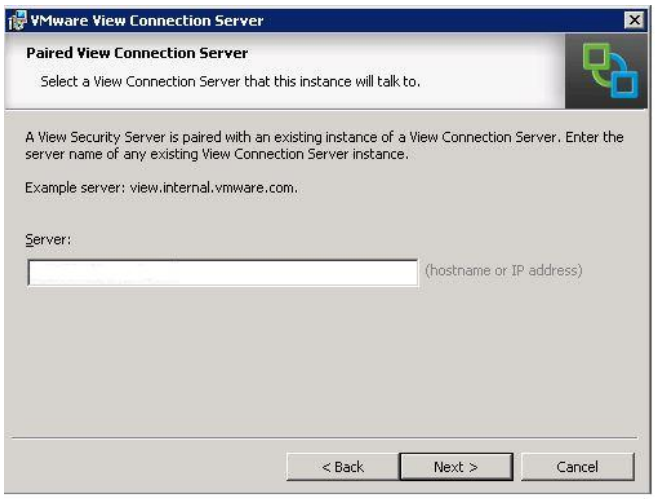
18. Choose an installation location and click Next to continue.



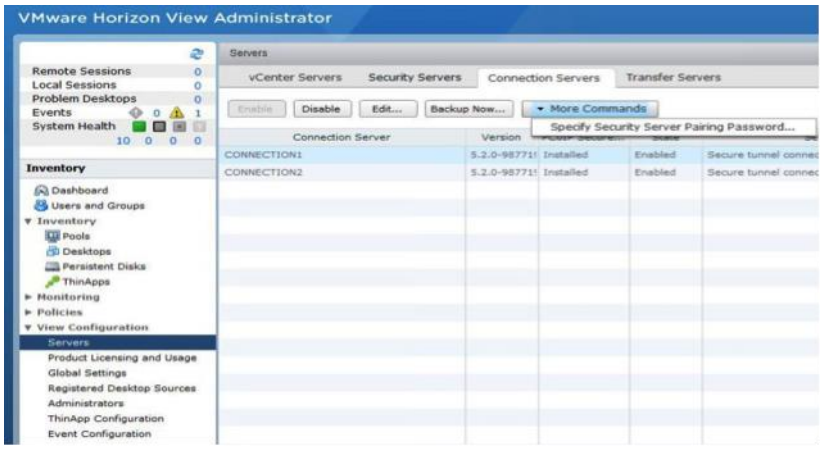
19. Now from the wizard select View Security Server.



20. Enter the fully-qualified name of a View Connection Server with which to pair the new Security Server.



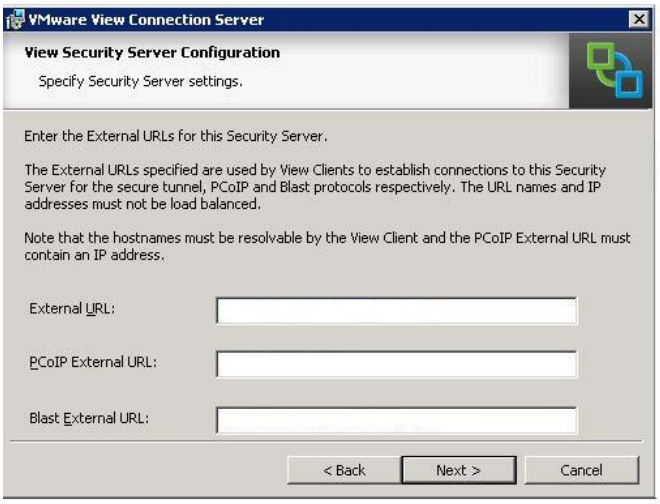
21. At this point, we need to pause for a minute and integrate the View Security Server with the View Connection Server using the web-based management interface. Navigate to Servers under View Configuration, select Connection Servers, select the server, and enter the View Security Server pairing password.



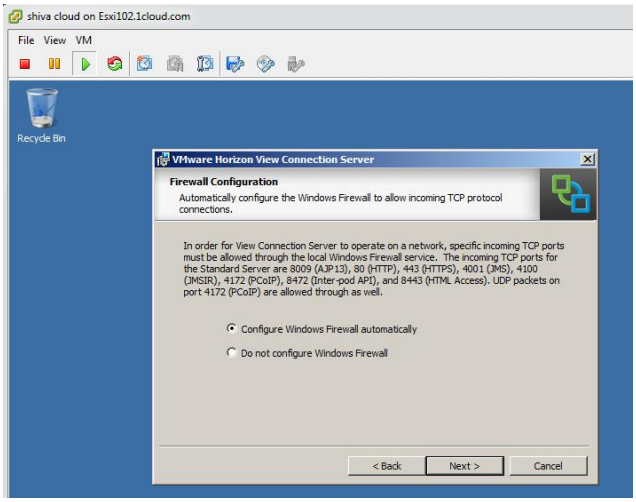
22. Enter the password twice and change the password timeout period, if desired.

23. Return to the installation wizard, and enter the password, and proceed with the installation.

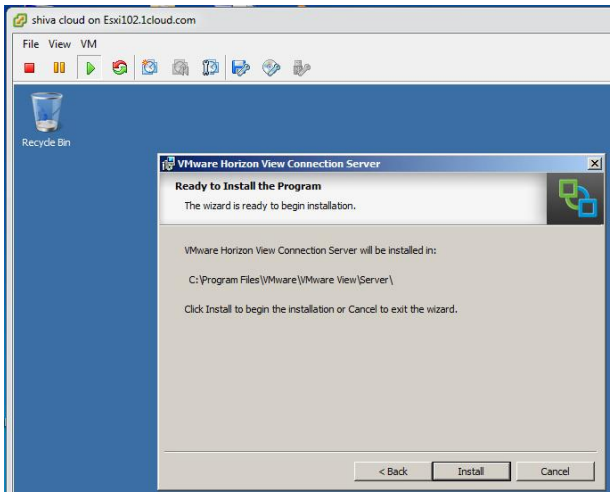
24. Confirm the External URL, PCoIP External URL, and Blast External URL for the Security Server.

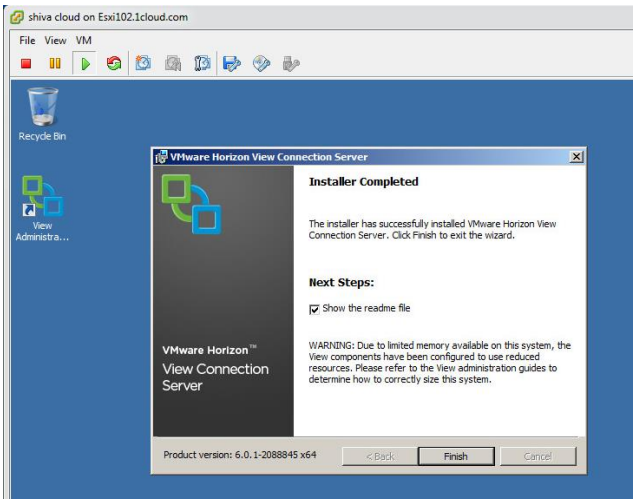


25. Allow the wizard to configure the necessary Windows Firewall rules automatically, and click Next to proceed.



26. Click Install to complete the installation. Click Finish to close the installer.





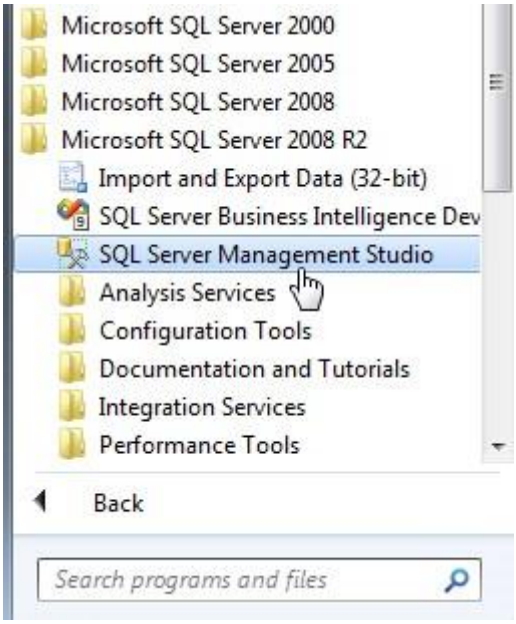
Once the installation is successful, we are able to see the Security Server information from the View Connection Broker administrative interface.

VMware View Composer Server Installation

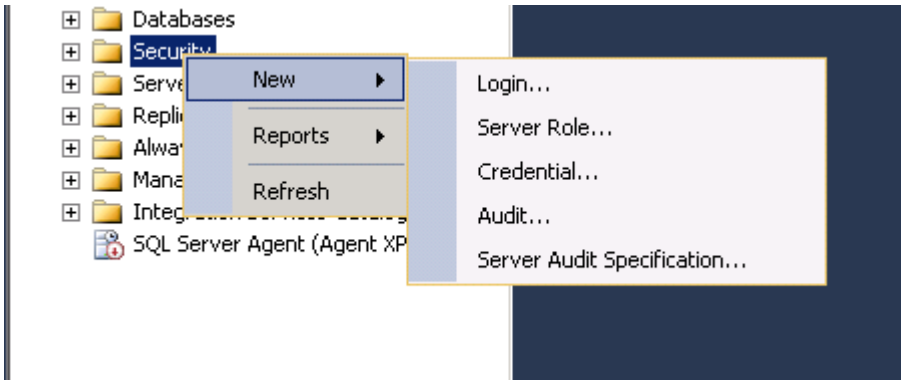
View Composer Server is a Windows service, which can be installed on the vCenter server or a separate Windows Server instance. It interacts with both vCenter Server and also View Connection Server. This component is critical to the creation of linked clone virtual desktops.

View Composer Server requires a database server. We have used Microsoft SQL Server 2008 Express for our proof-of-concept deployment here, but other versions are supported as well. The process of setting up a dedicated database using SQL Server 2008 Express is outlined below:

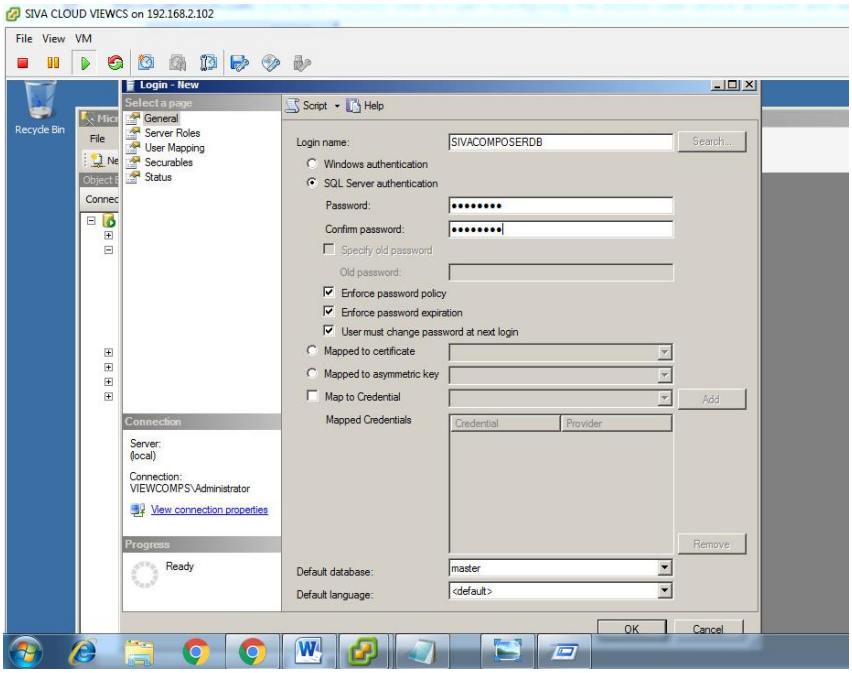
1. Login to the database and launch SQL DB management studio.



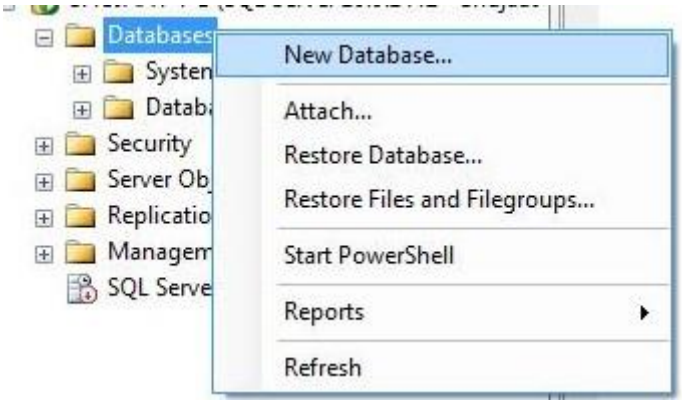
2. Log into the SQL Server Management Studio with an administrative account.



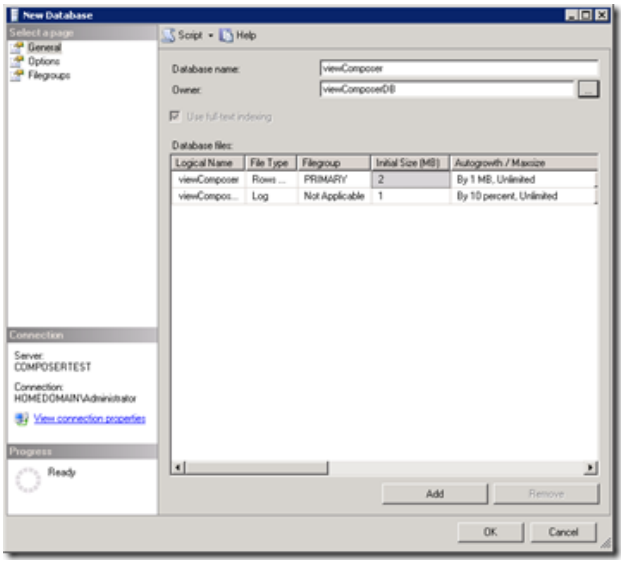
3. Create a new login by navigating to Security logins. Create a new Login.



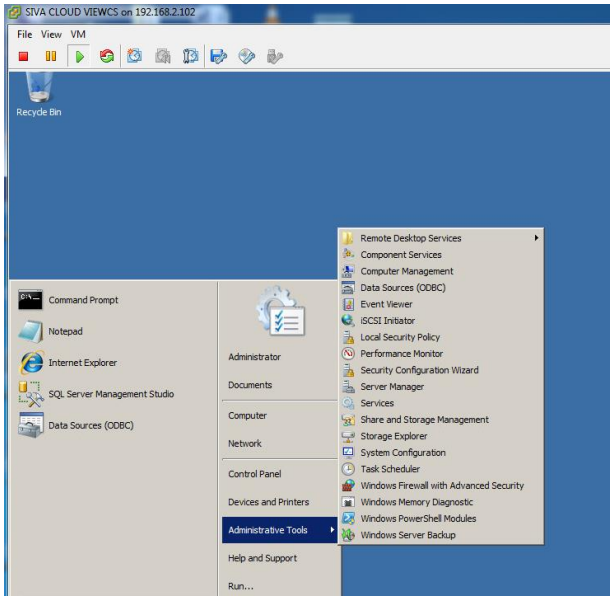
4. Create a new database for Composer. This database will be used by the Composer Server to save the linked clone desktop and replica details.



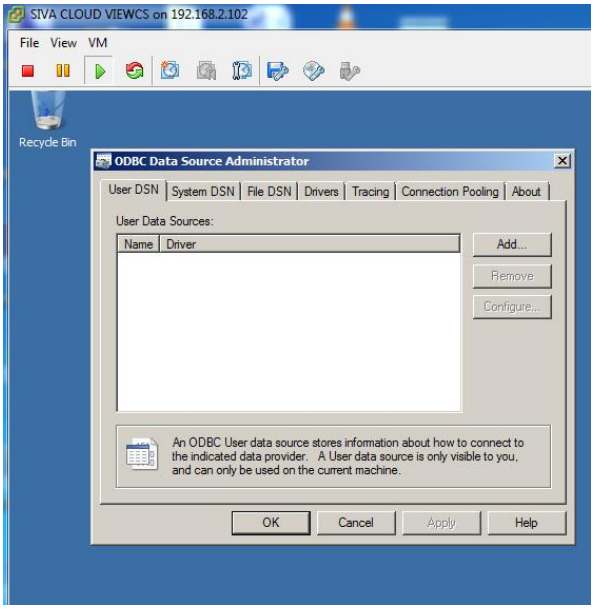
5. Provide a name for the new database. In our deployment, the name is View Composer. Select the newly created account as the database owner.



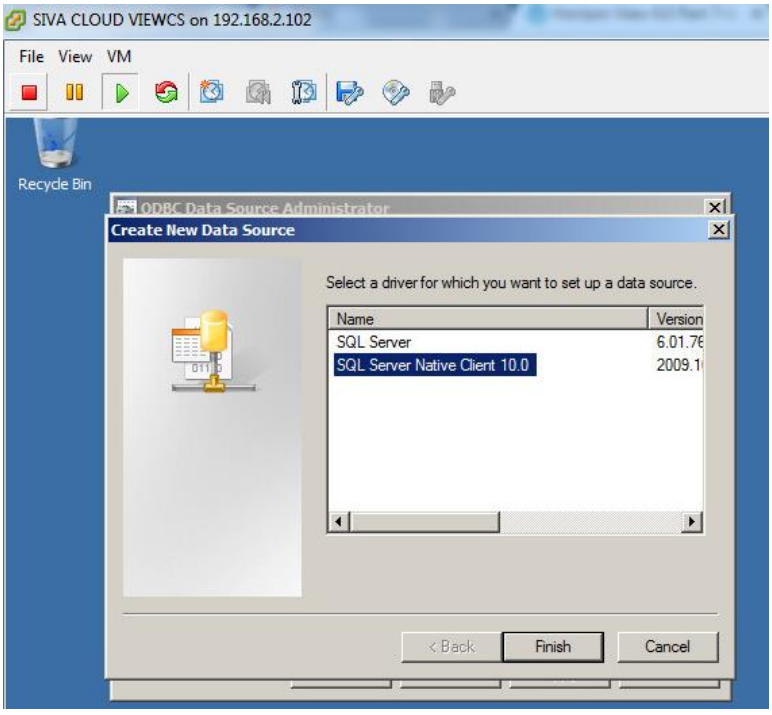
6. Next step is to create an ODBC connection for the Composer database. Click on Start, navigate to Administrative Tools, and click on Data Sources (ODBC). ODBC (Open Database Connectivity) is a standard protocol for programs (such as Microsoft Access) to obtain access to SQL database servers (such as Microsoft SQL Server or Oracle).



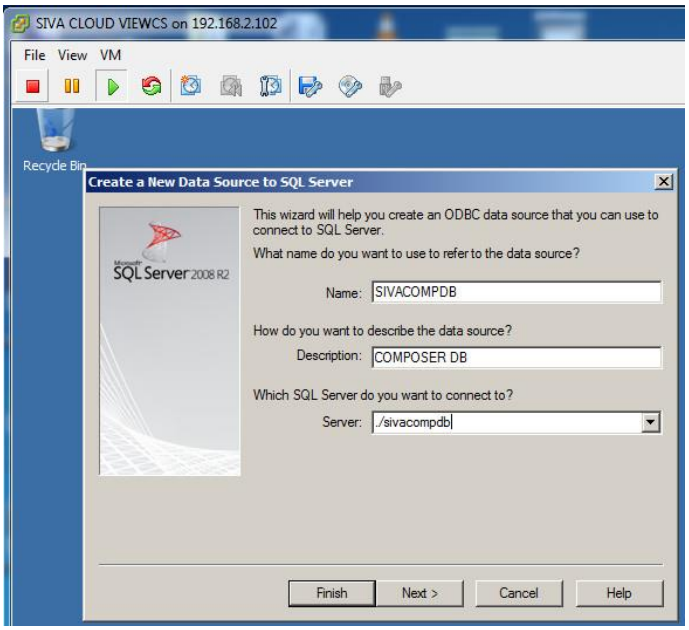
7. Click on System DSN and then click Add. A data source name (DSN) is a data structure that contains the information about a specific database that an Open Database Connectivity (ODBC) driver needs in order to connect to it.



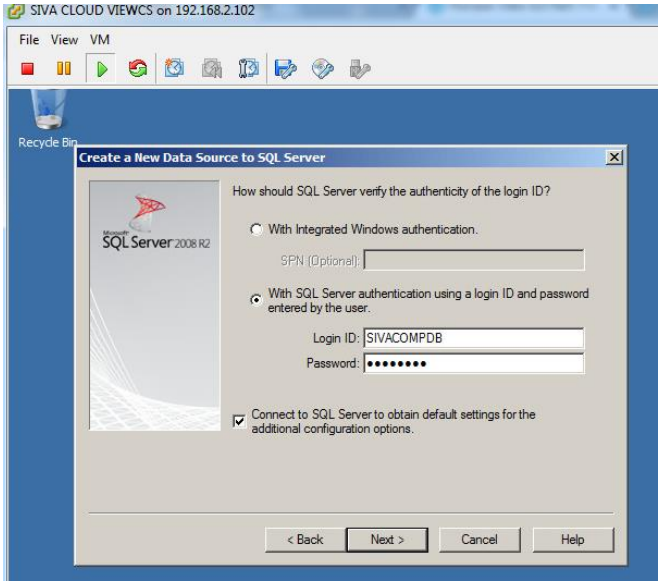
8. Select SQL Server Native Client 10.0 and click Finish.



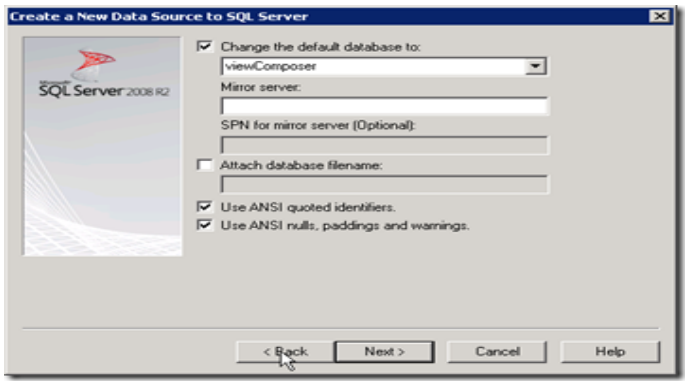
9. On the wizard, enter the DSN, a short description, and the name of the SQL Server on which the database is created.



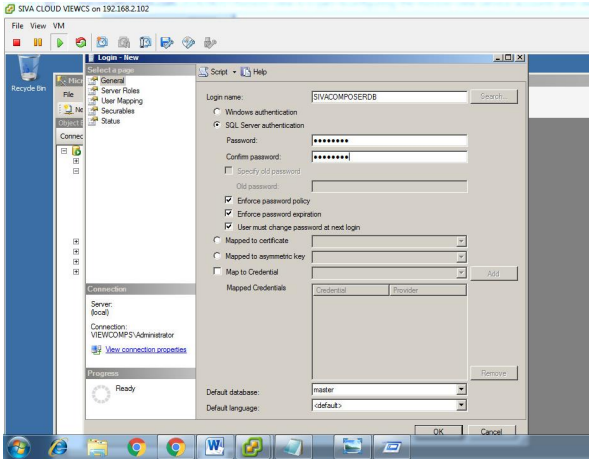
10. Select SQL Server authentication and enter the database username and password created earlier.



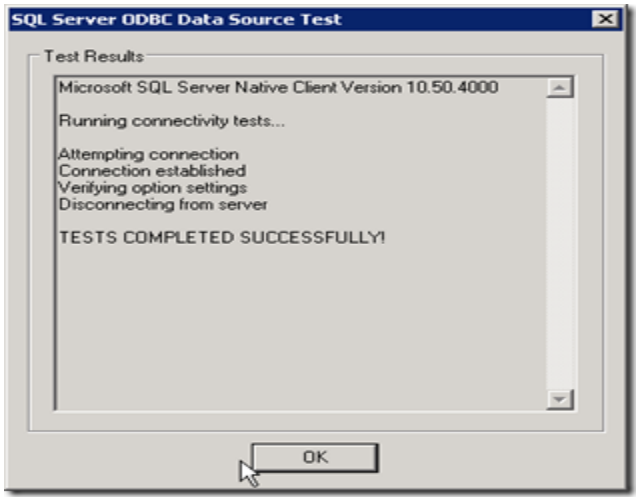
11. Enter the database name that we have created for view composer.



12. Now click the Test Data Source button to test the database connection to verify that the ODBC connection has been configured correctly.



13. If all the tests are successful, a notification will be shown.

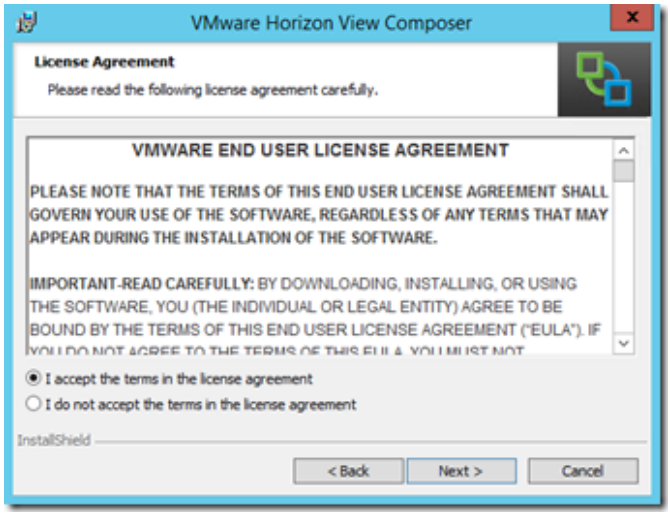


Once the dedicated SQL database has been created successfully, we can continue with the View Composer installation. View Composer requires .NET 3.5 framework to be

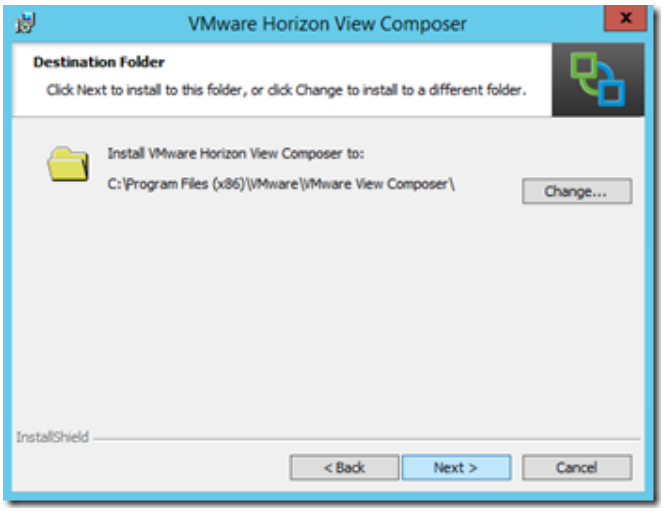
installed prior to starting the installation. The installation process for View Composer is as follows:

14. Start the View Composer installation on the Windows Server instance. Click Next to begin the installation process.

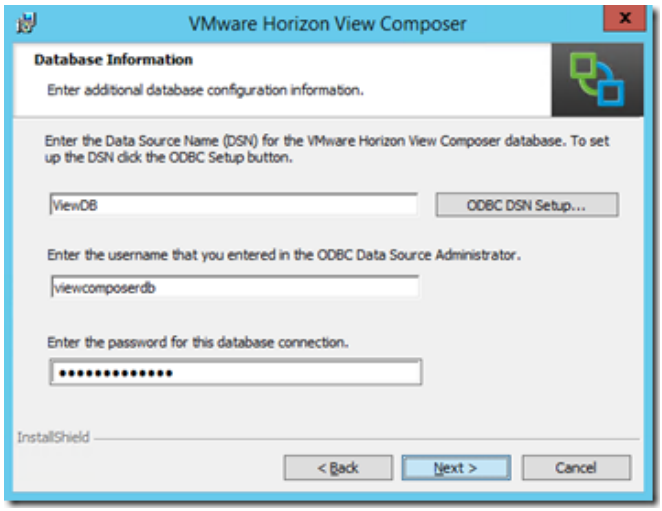
15. Accept the EULA and click Next to continue.



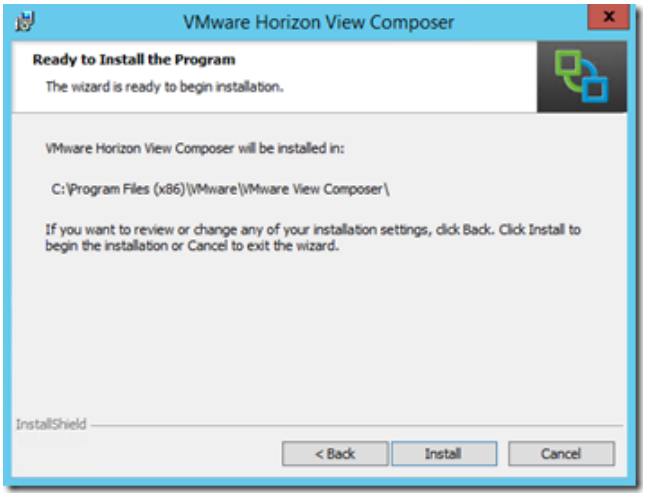
16. Specify the desired install location and click Next.



17. Specify the ODBC connection information and click Next.



18. On the next step of the installer, leave the SOAP port and SSL certificates to the default settings.

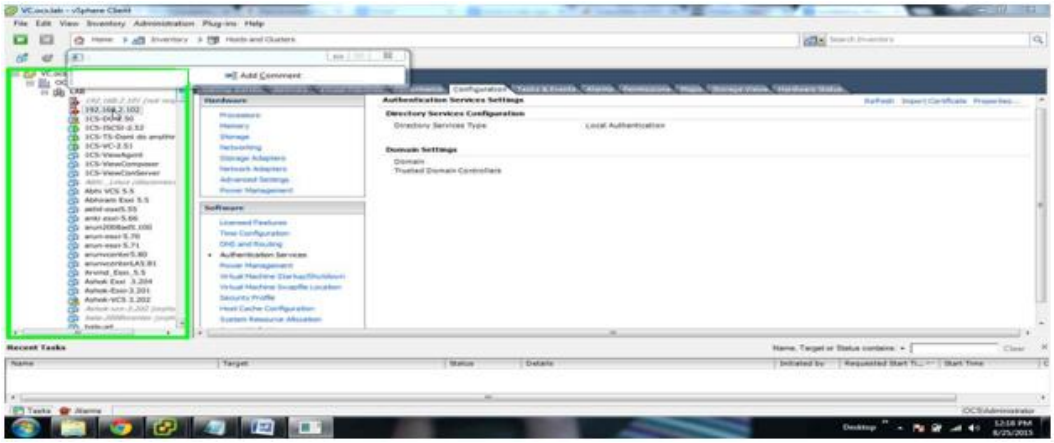


19. Click on Install to complete the installation.

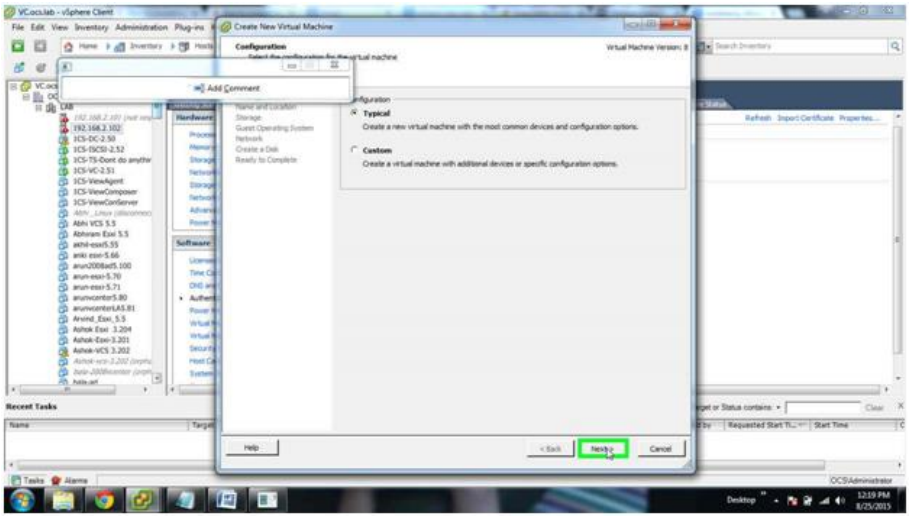
Windows Client OS for Desktop Pool Creation

For creating desktop pools in VMware View, a client operating system is required. For this research paper, Windows 7 Professional is used as the client OS. Once the client installation is complete, the View agent has to be installed in order for View Connection Server to be able to communicate with the client machine. The process for setting up a Windows 7 client VM is as follows:

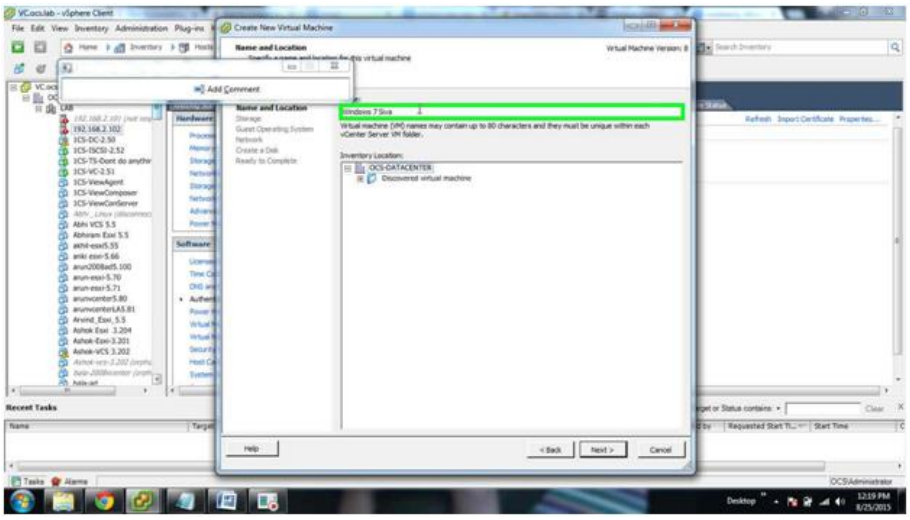
1. Create a new virtual machine on the existing vCenter Server.



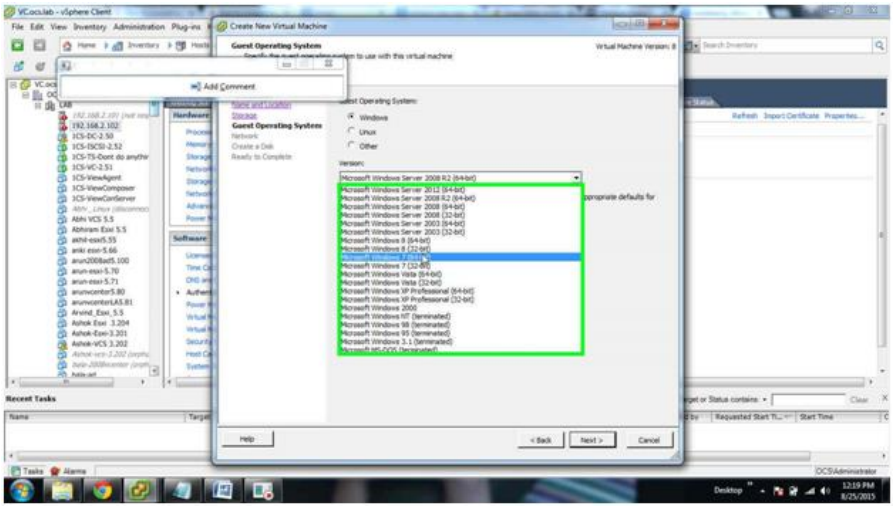
2. Select the Typical configuration and click Next.



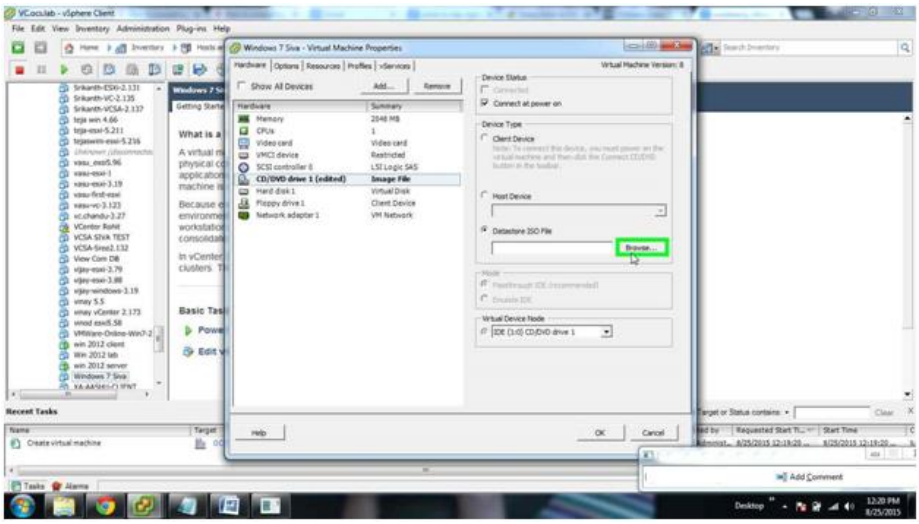
3. Name the virtual machine and click Next.



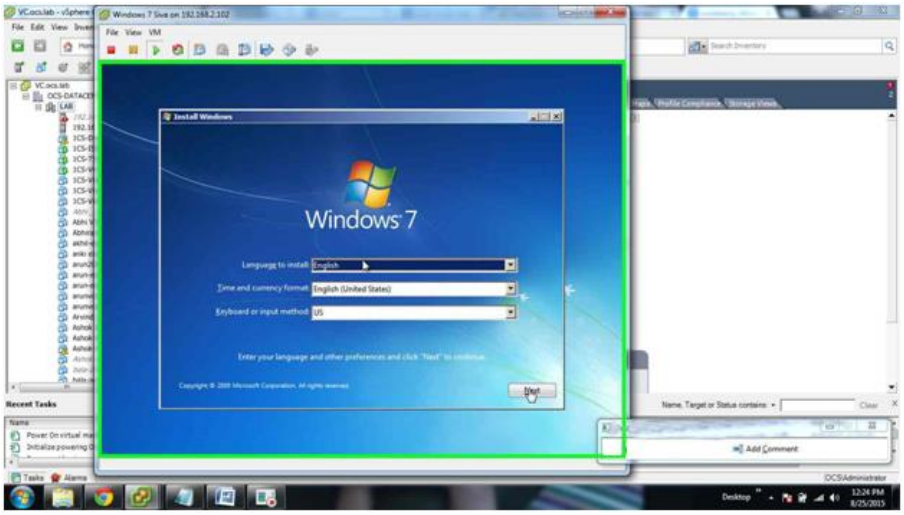
4. Select Windows 7 as the operating system and click Next.



5. Go to Edit Settings of the virtual machine and mount the Windows 7 ISO image from the datastore of the ESXi server.



6. Once the ISO is mounted, click OK to reconfigure the VM and then power it on. The Windows 7 installation will start automatically.



7. Complete the Windows 7 installation in the usual manner. No special settings are needed for View at this point.

View Agent Installation and Configuration

View Agent is a software component which must be installed on all the virtual desktops that are to be managed by vCenter Server and View. View Connection Server will communicate with the View Agent all the virtual desktops.

For this research paper, Windows 7 Professional is being used as the client Operating system, to create virtual full desktops and also linked mode desktops. For connection server to talk to the virtual desktops view agent is a very important component.

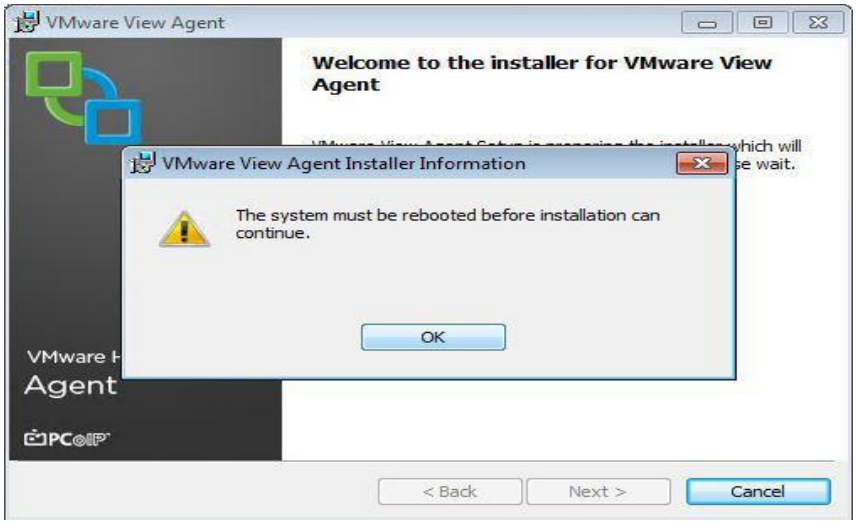
Supported OS

Table 11

View Agent Installation and Configuration Supported OS

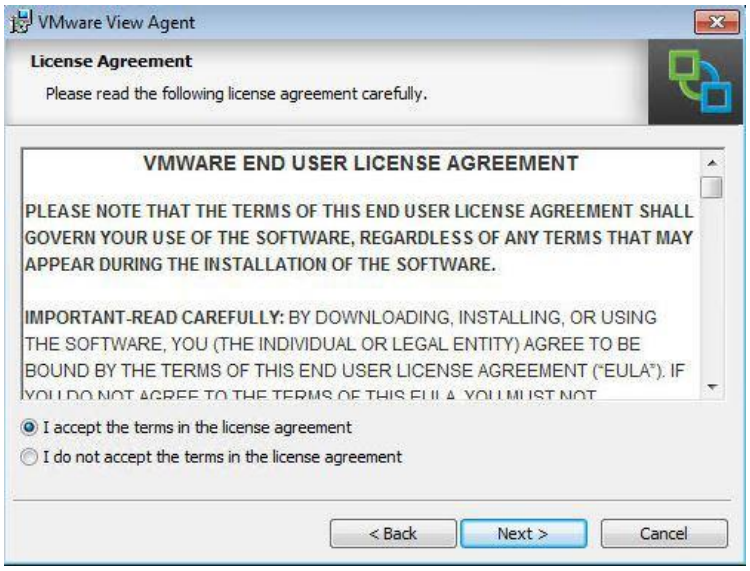
Guest OS	Version	Edition	Service Pack
Windows 8	32 and 64-bit	Professional and enterprise	NA
Windows 7	32 and 64-bit	Professional and enterprise	SP1 and none
Windows Vista	32 bit	Business and Enterprise	SP1 and SP2
Windows XP	32 Bit	Professional	SP3

1. Mount View agent install ISO on the Windows 7 operating and double click to start the installation.

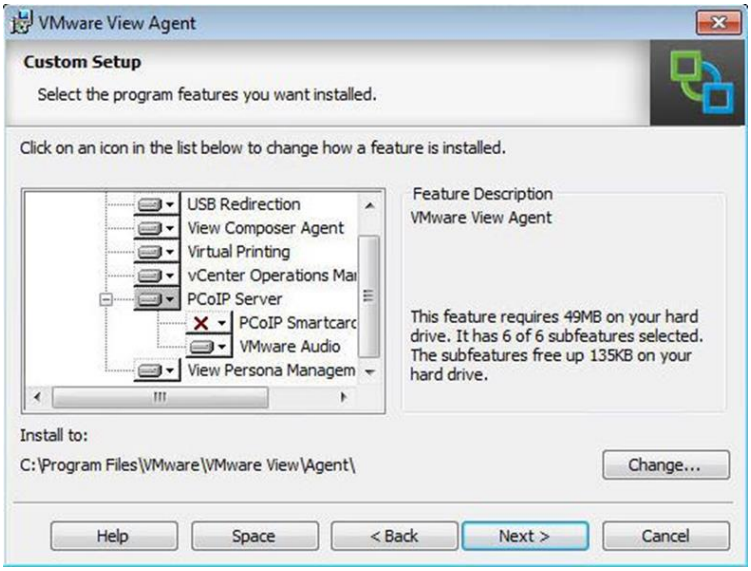


2. The system must be rebooted before the installation starts. Once the machine has started up again, launch the wizard to start the View Agent installation on the Windows 7 desktop.

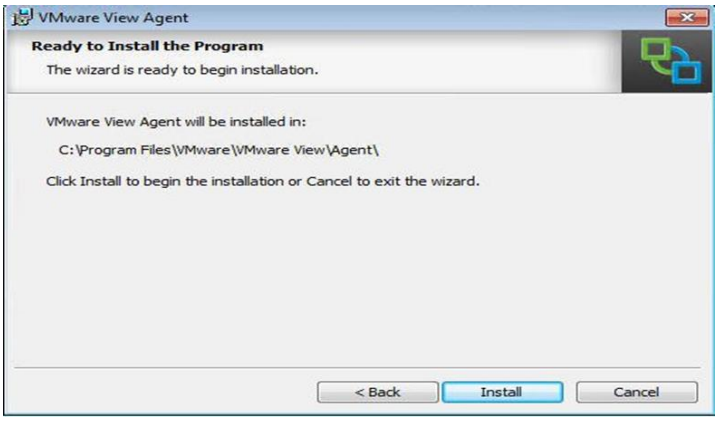
3. Click Next to proceed with the installation.



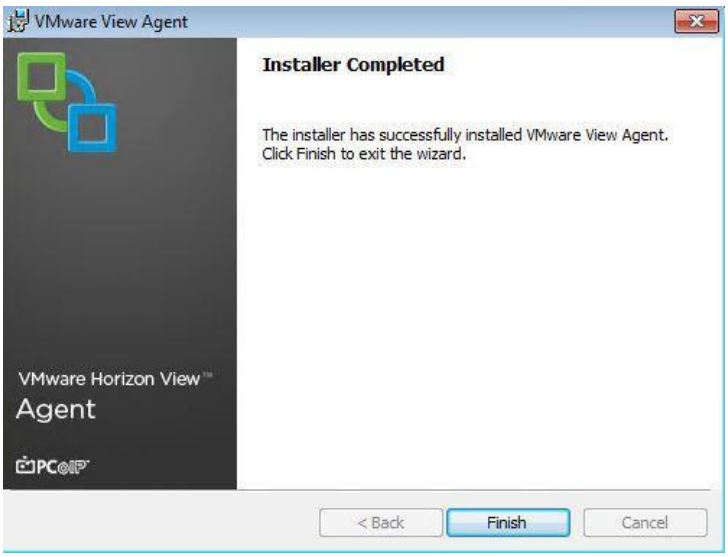
4. Accept the EULA and click Next.



5. Now select all the modules that are required for installation. Every module has a different functionality.



6. Verify the destination and click Next.



7. Click Finish to complete the installation.

Desktop Pools, Types and Creation

The installation procedures outlined above will result in a fully-functional VMware View infrastructure. The next step is to create desktop pools so that virtual desktops can be deployed. There are three types of desktop pools: (a) manual pools, (b) automated pools, and (c) terminal services pools.

Manual Pools

View Connection Server can use existing desktop images to create a desktop pool. These include (a)Virtual machines being managed by vCenter Server, (c) Virtual machines

running on an ESXi server or other virtualization software, (d) Physical desktops, and (e) HP blade physical computers (VMware view can be used to manage Blade PCs as well. All that needs is to install view agent on the blades to start managing them through view connection servers. This falls as part of Manual desktop pools, these are not virtualized machines).

Automated Desktop Pools

We can create two types of Automated Desktop Pools: (a) dedicated pools and (b) floating pools. In Dedicated Pools, the desktop images remain even when a user logs off and back on again. The user will receive the same desktop image each time he/she uses it. In Floating Pools, the user might get the same or a different desktop image each time he/she logs on.

We can also create two kinds of desktop pools: (a) full desktop pools and (b) linked clone desktop pools. Full desktop pools use a virtual machine template to create a desktop pool. Once the VM template is selected, we can create a desktop pool and select the number of spare powered-on desktops that should exist in the pool. It deploys virtual machines from the template provided during the pool creation process. Linked Clone desktop pools use virtual machine snapshots to create desktop pools. Once a snapshot is selected, it starts creating the specified number of desktops specified by the administrator. All the desktops created in this Linked Mode method, which share their base disks with the parent virtual machine.

Terminal Services Pool

There is another method of utilizing View desktop images. This is Terminal Services over VMware Horizon View. VMware View can also securely broker terminal services desktops. To configure this adding the terminal server role on the PC is must and then have to install view agent. This has to be done on a server OS and then view agent has to be installed

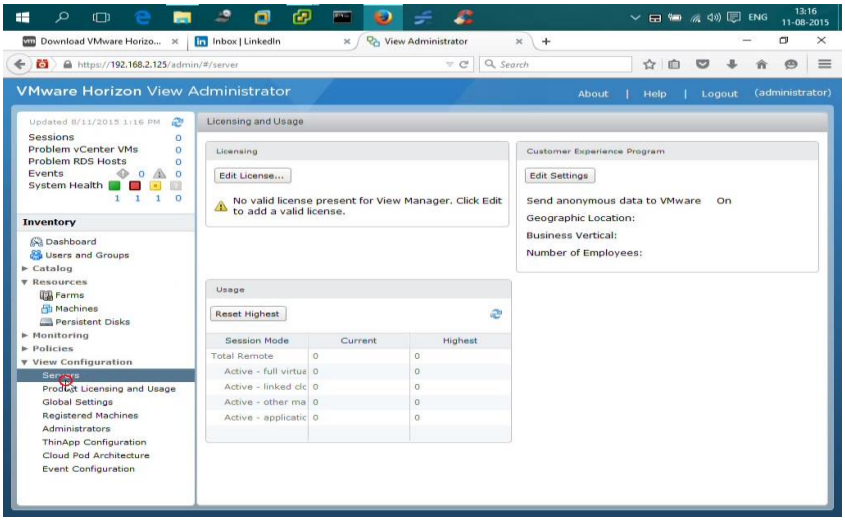
on the same allowing view connection server to communicate. However, this research paper is completely focused on creating automated desktop pools.

Creating a Full Desktop Pool

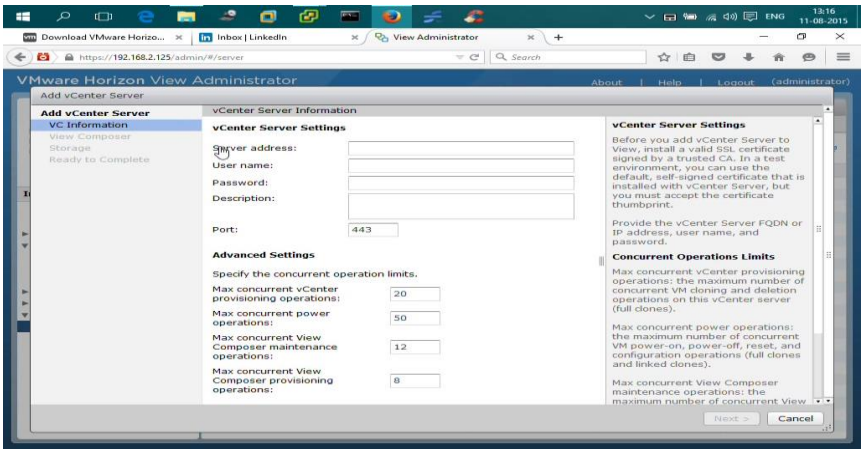
To create a full desktop pool, the following components are required: a client machine with VMware View Agent installed, administrative access to the View portal, a vCenter Server, and one or more ESXi servers. The process to create a new View desktop pool is as follows:

1. Connect to View Connection Server using a web browser.

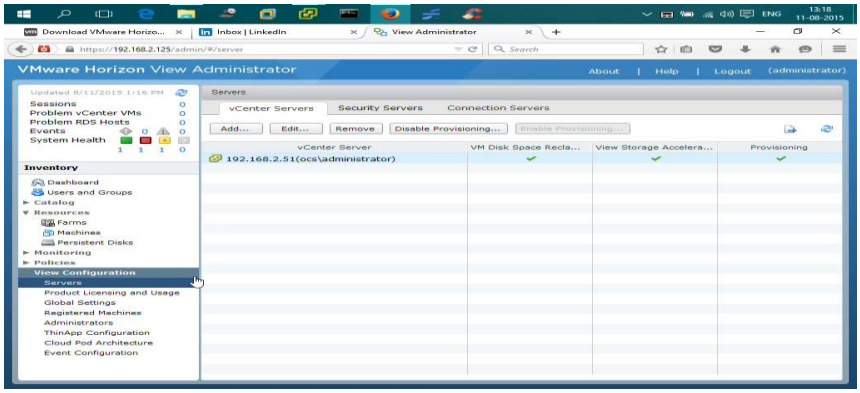
2. Once logged in, click on Servers to add the vCenter Server to View Connection Server. This is because VMware Horizon View uses vCenter server and ESXi servers to create desktop pools.



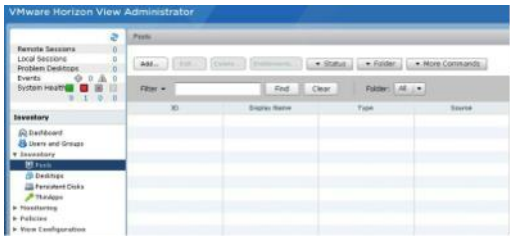
3. From the Servers submenu, click on Add and select the vCenter Server instance to be used for the desktop pool.



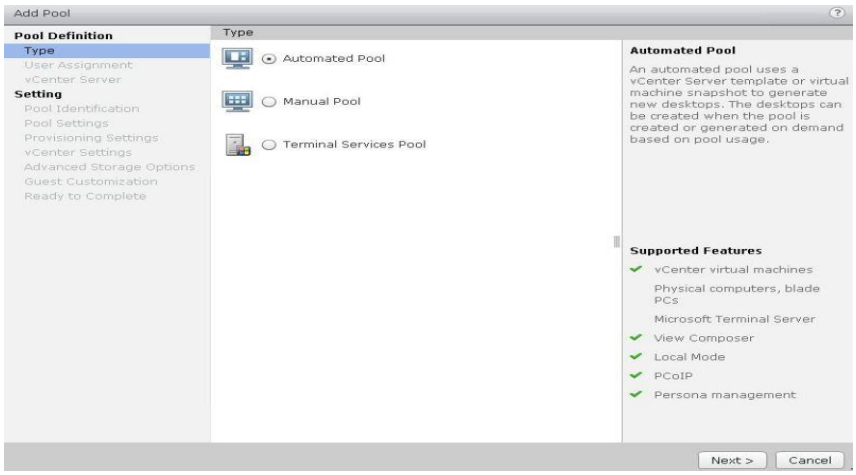
4. Once the vCenter Server is added, a screen similar to the one shown below will be shown. If there are any errors on the screen, fix those before proceeding to the next steps.



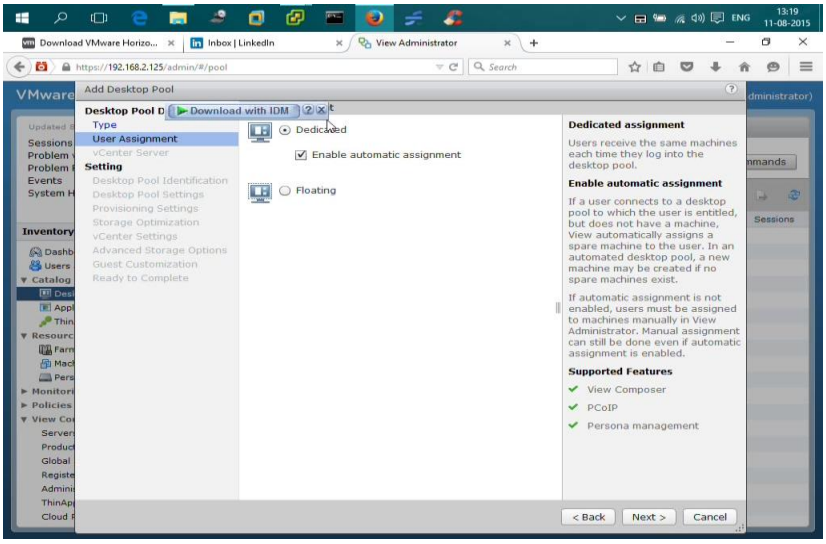
5. On the Inventory screen, click on Pools under Inventory and click on Add.



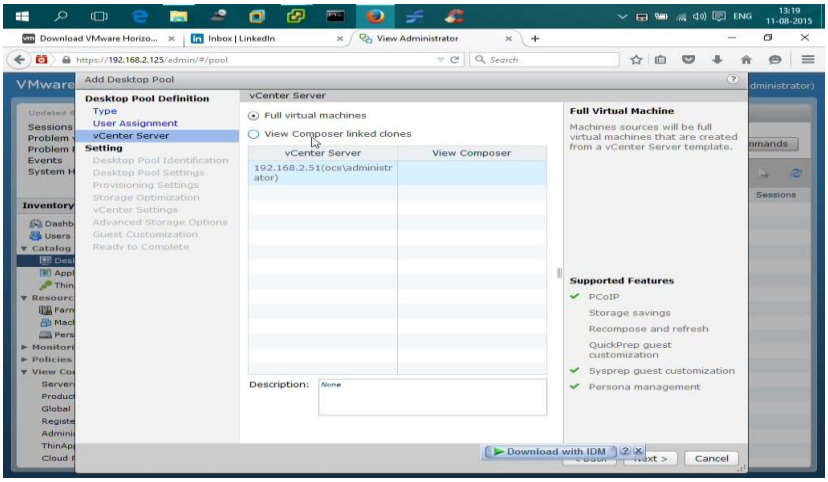
6. On the Add Pool wizard, select Automated Pool and click Next.



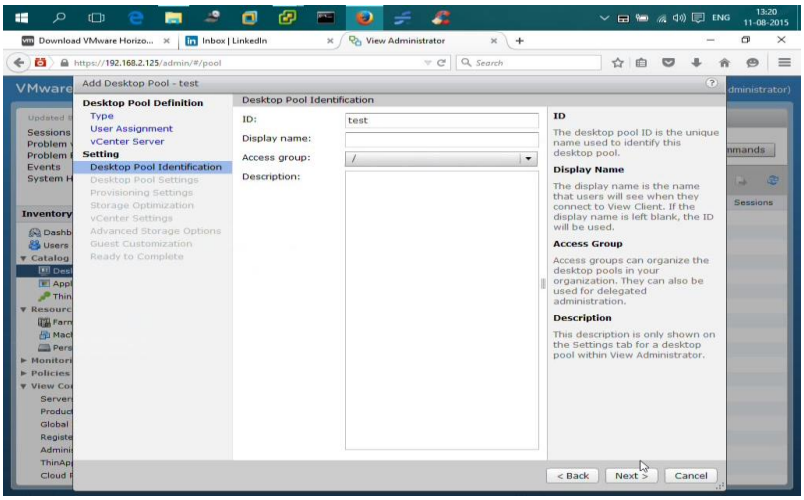
7. The next step involves choosing Dedicated or Floating pool assignment.



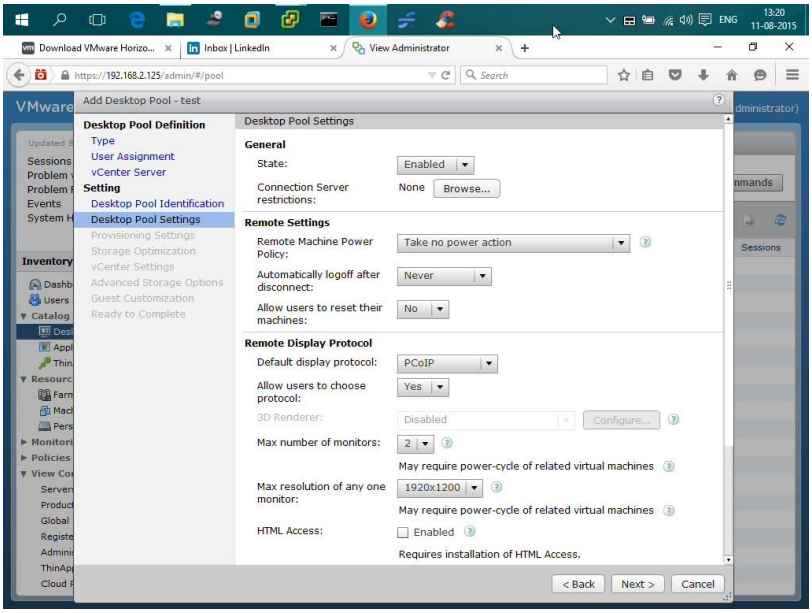
8. On the next page, select Full virtual machines or Linked Clone virtual machines.



9. Specify the Pool ID, Display Name, Access Group and Description for the pool.

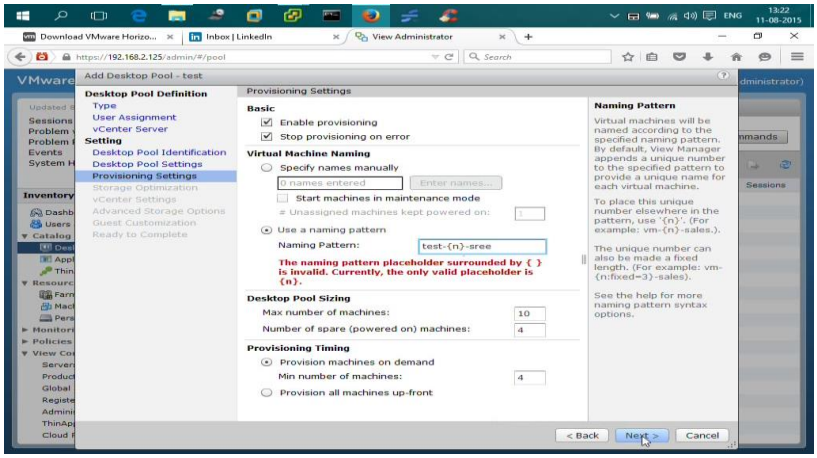


10. Select the desktop pool settings as shown in the image below. These settings include the state of the pool, remote machine power policy, whether to automatically log users off after they disconnect, whether or not to allow users to restart their virtual desktops, the display protocol, and the maximum number of monitors.

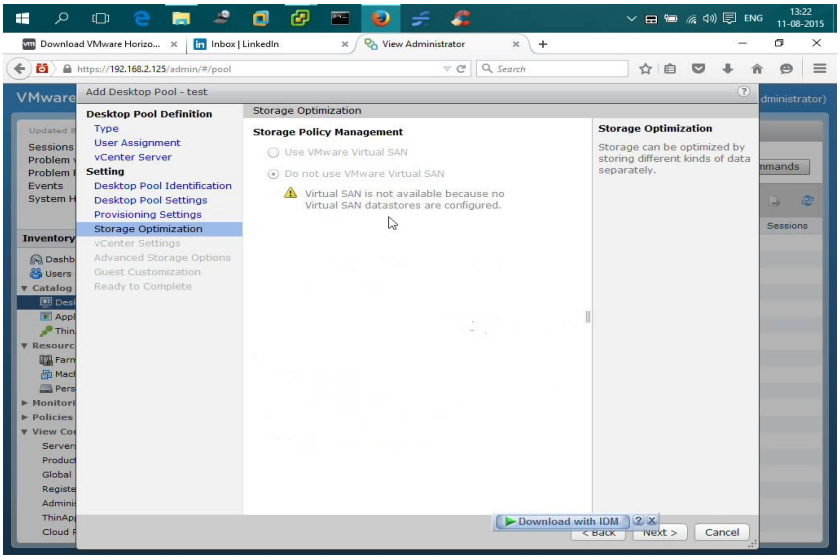


11. The next step in the wizard is to select the provisioning settings. This stage requires the user to select whether or not to enable provisioning, what should happen to the provisioning if an error occurs during the process, a naming scheme

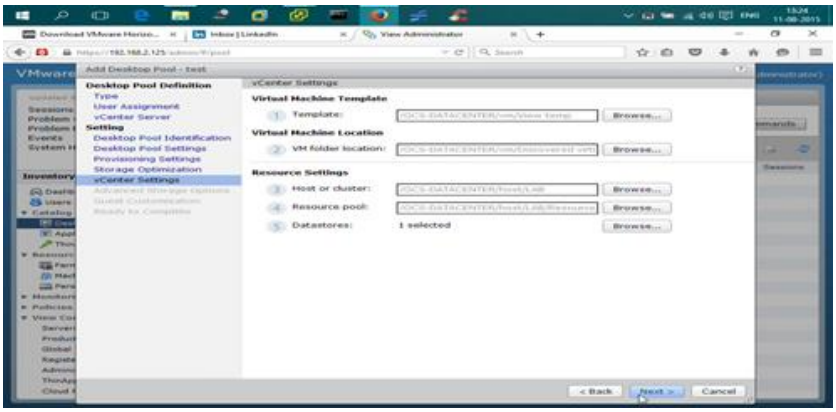
for virtual desktops in the pool, the desktop pool size, and whether to provision the desktops upfront or on-demand.



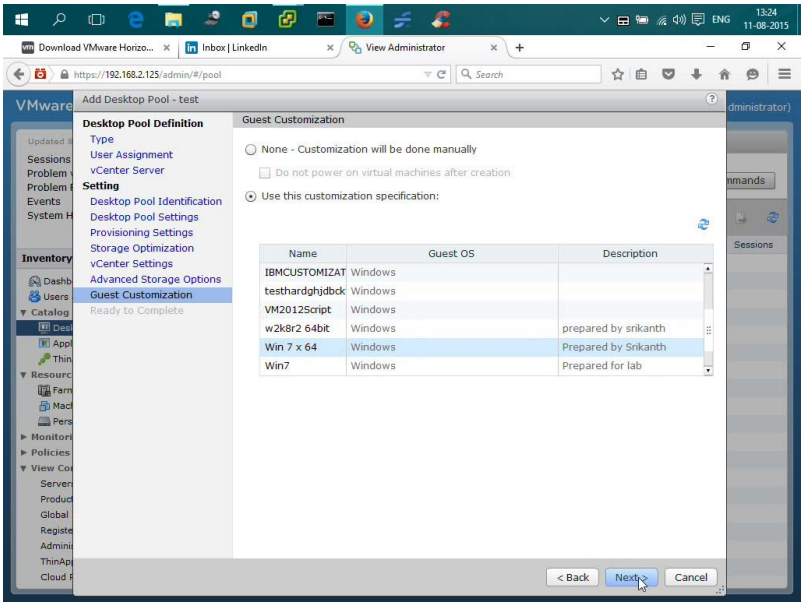
12. The next stage involves selecting whether or not to use Storage Virtual SAN.



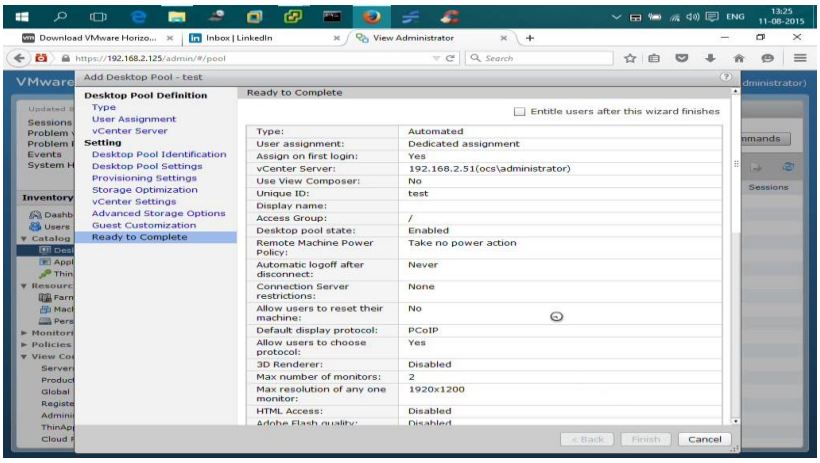
13. Next, we must select the vCenter Server on which to provision the desktop pools. In this step, we must configure the following settings: the template for pool creation, the VM folder location on vCenter, and VM resource/storage options.



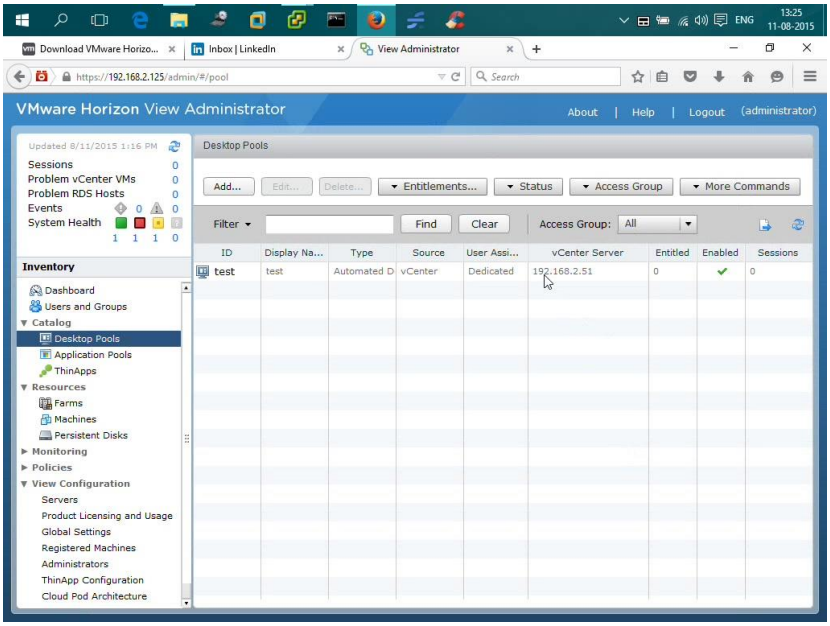
14. Next, we need to configure options for the guest customization wizard, which enables vCenter to provision desktops from the template specified.



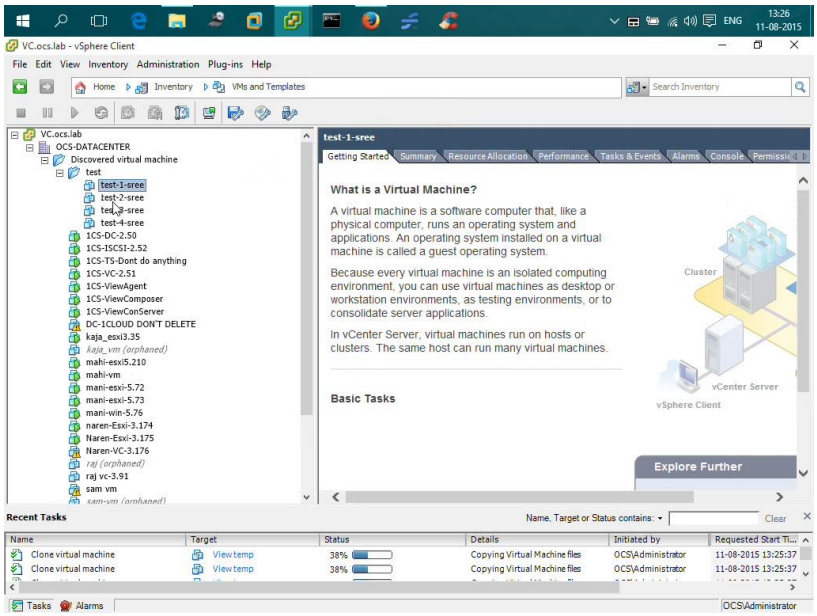
15. Review all of the selections made and click OK to start the provisioning process. The desktop pools will be created on the vCenter Server and under the folder selected.



16. Once the desktop pool is created, the pool information can be viewed and edited from the Desktop Pools option under Catalog as shown below.



17. The provisioned desktops can now be seen in the left-hand pane of the vCenter management console, as shown below.



Linked Clone Desktop Pools

Linked Clone desktop pools can be created only if a View Composer server is present**.** For this research paper, View Composer is used in conjunction with a Linked Mode desktop pool. As mentioned earlier, Linked Clone desktops share a base disk with the parent virtual machine, making deployment easier and vastly reducing the amount of storage space required.

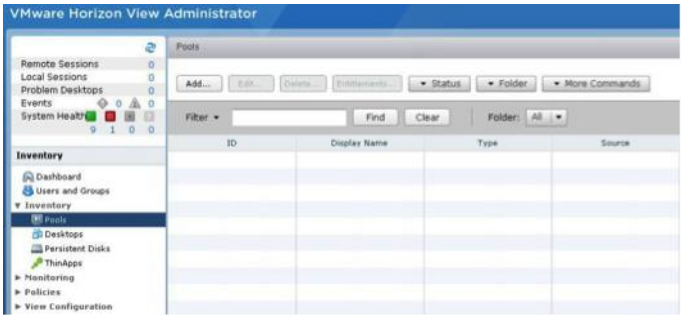
Preparing the parent image is a multi-step process. A virtual machine with a supported operating system must be installed, and the View Agent must be installed so that the Connection Server or View Composer can interact with the parent image. Additionally, all desired applications must be installed onto the parent image and the virtual machine must shut down prior to Linked Clone deployment. For Linked Clone desktop pools, View Composer will utilize the parent virtual machine snapshot. Multiple snapshots can be taken for creating different desktop pools.

Creating Linked Clone Desktop Pools

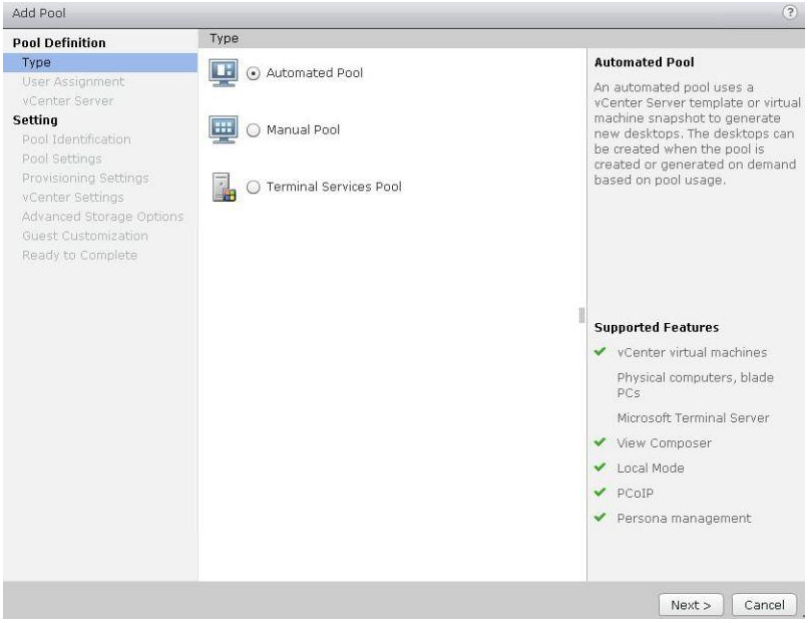
The process of creating Linked Clone desktop pools is described below:

1. Log into the View admin console with a user account that has adequate permissions to manage desktop pools.

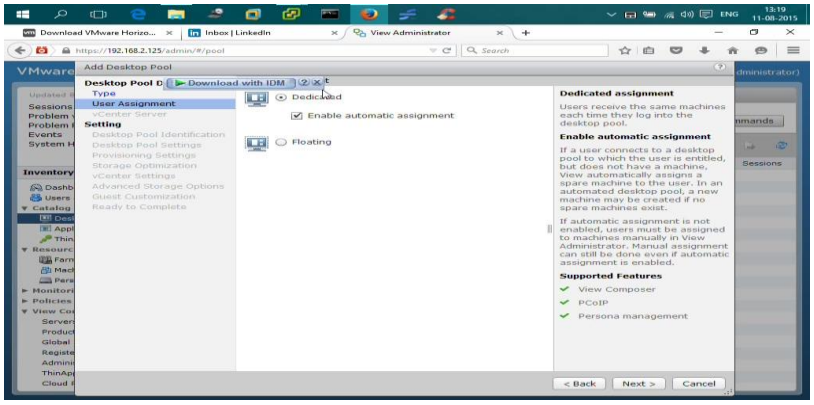
2. Once logged in, expand the Inventory node on the left side of the interface, and click on Pools.



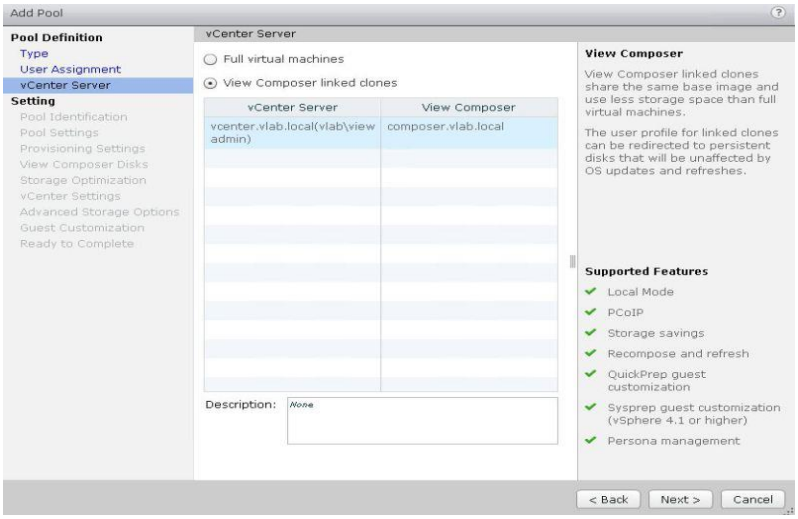
3. Click on Add to launch the Add Pool wizard. Select Automated Pool from the list and click Next.



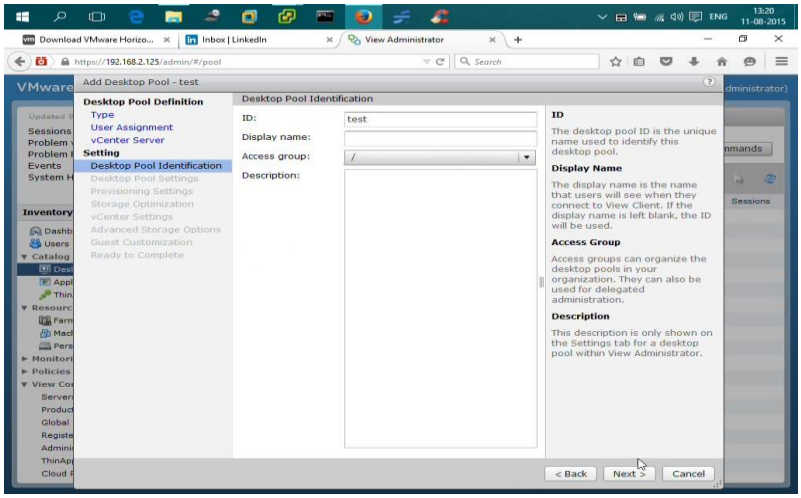
4. Select Dedicated Assignment, which will ensure that users get the same virtual desktop each time they sign on. Continue to the next step.



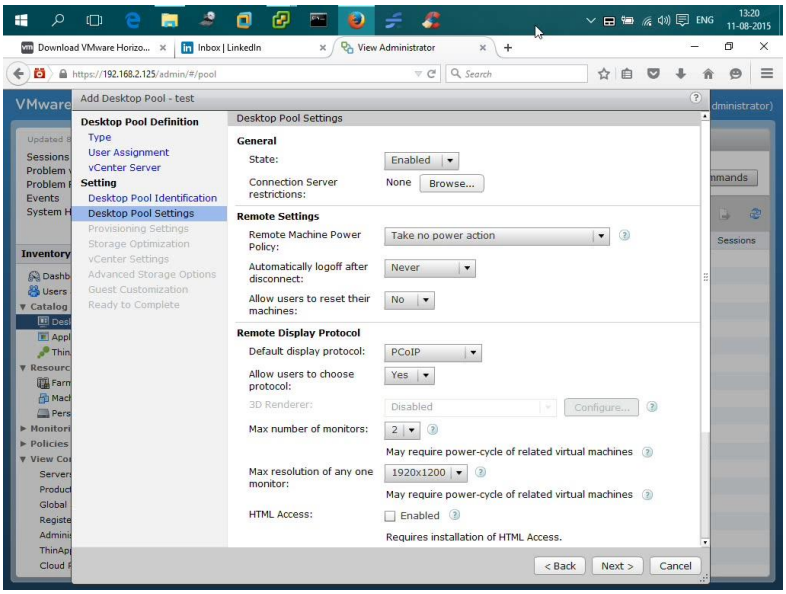
5. Select View Composer linked clones to created linked mode desktops.



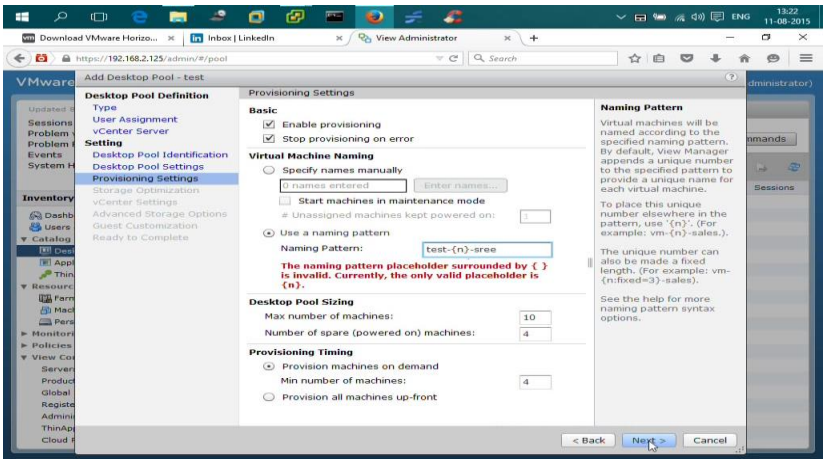
6. Provide the pool ID, display name, access group, and a description of the pool.



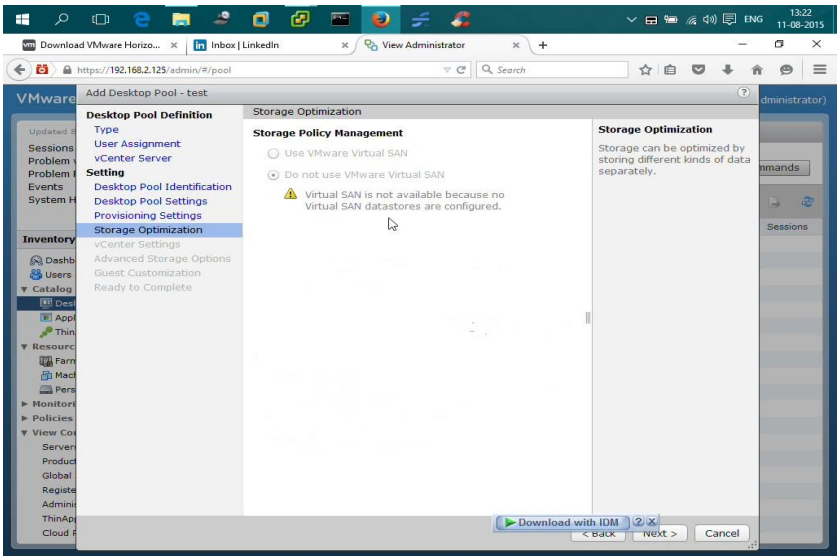
7. Select the desktop pool settings as shown in the image below. These settings include the state of the pool, remote machine power policy, whether to automatically log users off after they disconnect, whether or not to allow users to restart their virtual desktops, the display protocol, and the maximum number of monitors.



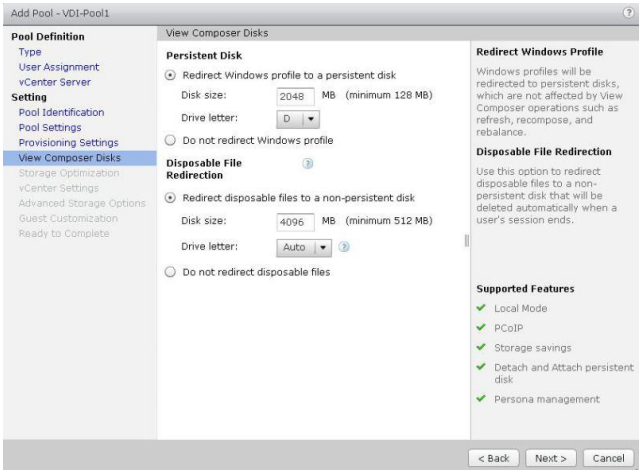
8. The next step in the wizard is to select the provisioning settings. This stage requires the user to select whether or not to enable provisioning, what should happen to the provisioning if an error occurs during the process, a naming scheme for virtual desktops in the pool, the desktop pool size, and whether to provision the desktops upfront or on-demand.



9. The next stage involves selecting whether or not to use Storage Virtual SAN.

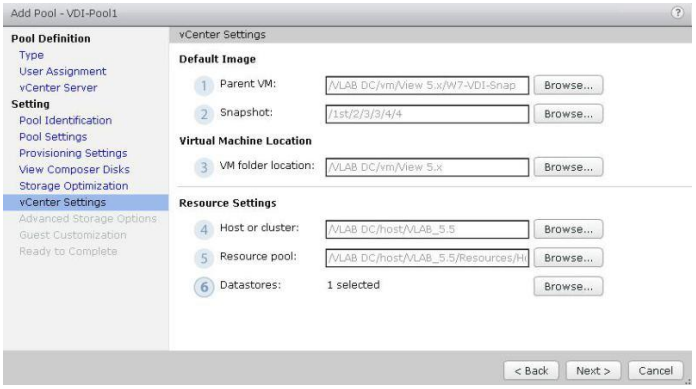


10. Next step involves selecting View Composer disks, which can be either persistent or non-persistent. Persistent disks retain user data and settings between sessions, whereas non-persistent disks revert to the original image state when the user logs off.

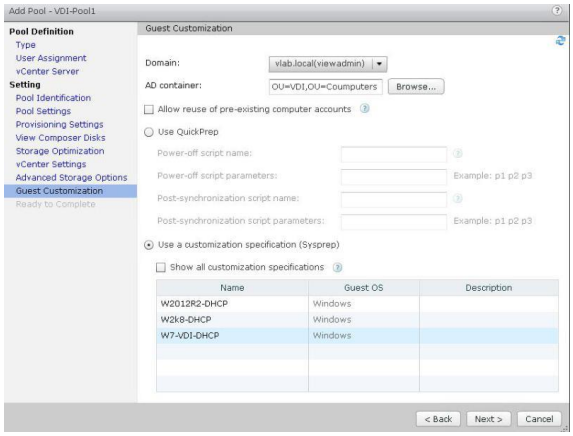


11. Next, we need to configure storage optimization. This step involves selecting the datastore(s) on which persistent and replica disks will be selected.

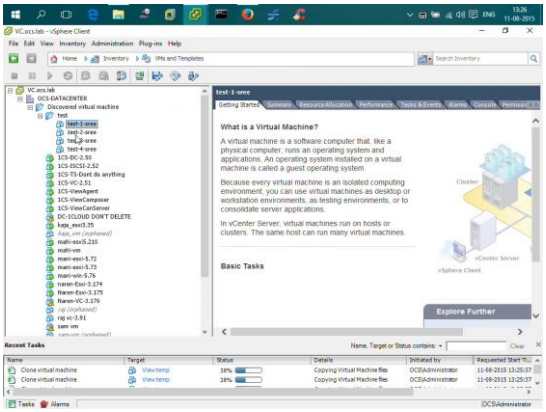
12. The next step involves selecting the parent VM, a snapshot on the parent VM which will be used to create the desktop pools, a folder where the virtual desktops will be placed, the host(s) on which the desktops should be run, the resource pool in which to place the VDI desktops, and the datastores on which the VM files should be placed.



13. Next, we need to configure options for the guest customization wizard, which enables vCenter to provision desktops from the template specified.



14. Click Next to complete the Linked Mode desktop pool creation process. The provisioned desktops can now be seen in vCenter, as shown below.



Chapter VI

CONCLUSION AND FUTURE WORK

In this paper, I have implemented vSphere and VMware Horizon View in order to create a Virtualized Desktop Infrastructure. VMware Horizon View allows administrators to build virtual desktops and deliver them to users on demand. VMware view can solve problems like making all the desktops run centrally in the datacenter and are consolidated on to few ESXi hosts. The desktop disk data is stored and accessed centrally from a storage box, which runs in a datacenter and companies can stay in compliance as the user data disks can be refreshed back to base image states as soon as they log off. Desktop provisioning time and patching time can be reduced drastically. VDI desktops can be brought up even if there is a hardware failure on the ESXi host using HA.

However, the View architecture provided here has some significant limitations. Without further work and additional VMware technologies, it is not easy to deliver high-end applications that require more storage space, or separate applications for different departments within an organization. Future work in these areas would include research on thin apps, app volumes, and user environment manager products from VMware, which provide solutions to these problems cited above.

Research Questions and/or Hypotheses

Research Question 1. How can vSphere High Availability provide an effective and affordable disaster recovery solution?

VMware vSphere HA is a feature, which can protect virtual machines from an unplanned downtime in case of a hardware failure running ESXi or an ESXi OS crash.

HA is a cluster level feature where in 32 ESXi servers can be placed in to a vSphere HA cluster till vSphere 5.5 and 64 ESXi servers can be placed to a HA cluster in vSphere 6.0.

Once HA is enabled on a cluster under vCenter server, FDM aka fault domain manager agents would be invoked on all the servers in the cluster after then they will sit to an election process to elect a master node.

Any ESXi server to become a master should have max number of Data stores and if there are two ESXi servers with the same number of Data stores, then vCenter will decide on which server to be a master on vCenter allocated MOID aka managed object ID which vCenter allocates to every ESXi server when added to vCenter.

Once a master is elected, master will start monitoring all the ESXi hosts in the cluster for a failure. If a slave is not responding to heartbeat process, then the slave is considered either dead or isolated, aster then checks on the Data store heart beating of the slave and then takes appropriate action on the virtual machines.

In the meanwhile, slave also will not be able to ping the master if it is isolated. To conclude, this slave will ping the isolation address configured on the cluster. This isolation address is by default the Default gateway or the router IP. If the slave is able to ping the default gateway, it means that the slave is not isolated; if it cannot ping the default gateway itself concludes as is isolated and writes to a file with the name POWERED ON. The slave now either writes a 0 or a 1 in the first line of the file to let other servers know that it is isolated, where 0 means not isolated and 1 means isolated.

If a server is dead, master will simply restart the virtual machines from the dead server to healthy servers in the cluster.

If a slave is isolated, then master will check on the host isolation response configured on the cluster and then take an appropriate action.

Host isolation response means if a slave is isolated from the network, what should be the master response to the virtual machines on the isolated host.

The host isolation response can be one of the following: (a) Leave Powered On, (b) Power-Off, or (c) Shutdown.

The response can be leave powered on wherein the master will not touch the virtual machines on the isolated slave, master will restart the virtual machines on the isolated slaves to healthy ones in the cluster if the host isolation response if configured to either power off and shutdown.

Research Question 2. How do vCenter Server, View Composer, and View Connection Server work together to provide seamless desktop virtualization?

When a user wants to connect to his desktop, he initiates the connection to the connection server, which is integrated with VMware vCenter Server. Active Directory Server will authenticate user credentials.

VMware vCenter Server will request View Composer Server to build the desktop for the requested user based on their authentication and authorization.

Research Question 3. How does View Composer optimize storage?

View Composer uses a concept of linked clones, which means all the desktops will use the single backup image. This cuts down on the virtual desktop storage requirements.

Research Question 4. How many virtual desktops can be run concurrently on a single ESXi server?

We can build maximum of 512 virtual desktops on a single host using vSphere ESXi version 5.5 and 1024 virtual desktops on vSphere ESXi version 6.0.

Research Question 5. What is the optimal storage design for VMware View?

The storage design for view purely depends on the number of virtual desktops that are to be hosted. As multiple view desktops can run on a single ESXi server, it creates a boot storm when multiple desktops customized and boots up at once.

Research Question 6. How many IOPS (Input/Output Operations per Second) should a storage LUN (Logical Unit Number) be able to provide?

The IOPS dedicated for a desktop would be 20. So depending on the number of desktops running on the LUN, the LUN IOPS should be sized accordingly.

References

3benefitsof. (n.d). *3 benefits of using server racks*. Retrieved from http://www.3benefitsof.com/3-benefits-of-using-server-racks/

Application virtualization. (2015). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Application_virtualization

Beerens, I. (2013). *View security server*. Retrieved from http://www.ivobeerens.nl/2013/03/05/tips-for-implementing-a-vmware-horizon-view-security-server/

Blade server. (2014). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Blade_server

Bright-Streams. (n.d).*View-composer*. Retrieved from http://bright-streams.com/?tag=view-composer

Cisco Systems. (n.d.a). *Cisco Server*. Retrieved from http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html

Cisco Systems. (2015). *Cisco UCS mini, nimble storage, and WMware horizon 6 with mixed workload on Cisco UCS B200 Mc blade servers*. Retrieved from http://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-mini/whitepaper_c11-733474.html

Cisco Systems. (n.d.b). *Cisco blades*. Retrieved from http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-b-series-blade-servers/index.html

Cloud computing. (2015). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Cloud_computing

Courtemanche, M. (2013). *View pros and cons*. Retrieved from http://searchvmware.techtarget.com/feature/Inside-a-successful-VMware-View-setup-VDI-pros-and-cons

Data Center Knowledge. (2012). *Hypervisor*. Retrieved from http://www.datacenterknowledge.com/archives/2012/08/01/hypervisor-101-a-look-hypervisor-market/

Database. (2013). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Database

Dell. (n.d.a).*Poweredge server*. Retrieved from http://www.dell.com/in/business/p/poweredge-tower-servers

Dell. (n.d.b). *Rack servers*. Retrieved from http://www.dell.com/in/business/p/poweredge-rack-servers

Dell. (n.d.c).*Blade server*. Retrieved from http://www.dell.com/in/business/p/poweredge-blade-servers

Desktop virtualization. (2011). *Search virtual desktop*. Retrieved from http://searchvirtualdesktop.techtarget.com/definition/desktop-virtualization

ESXi. (2013*). Linux thoughts*. Retrieved from http://www.linuxthoughts.com/?p=102

Hewlett-Packard. (n.d.a). *Hardware server*. Retrieved from http://shopping1.hp.com/is-bin/INTERSHOP.enfinity/WFS/WW USSMBPublicStore-Site/en_US/-/USD/ViewStandardCatalog-Browse?CatalogCategoryID=aRQQ7EN5k24AAAEuqW0sTi_4

Hewlett-Packard. (n.d.b). *HP server*. Retrieved from http://shopping1.hp.com/is-bin/INTERSHOP.enfinity/WFS/WW-USSMBPublicStore-Site/en_US/-/USD/ViewStandardCatalogBrowse?CatalogCategoryID=4eAQ7EN5gAMAAAEuq08sTi_5

Hewlett-Packard. (n.d.c). *HP blade enclosure server*. Retrieved from http://www8.hp.com/in/en/products/enclosures/product-detail.html?oid=1844065

Hewlett-Packard. (n.d.d). *Products*. Retrieved from http://www8.hp.com/us/en/products/enclosures/

International Business Machines Corporation. (n.d.). *Server hardware*. Retrieved from http://www-03.ibm.com/systems/x/hardware/tower/

Lowe, S. (2013). *Horizon view*. Retrieved from http://www.virtualizationsoftware.com/vmware-horizon-view-5-2/

Malanco, A. (2014). *Horizon view*. Retrieved from http://resources.intenseschool.com/delivering-euc-enabling-byod-with-vmware-horizon-suite/

Massey, S. (2009). *View connection server*. Retrieved from http://seanmassey.net/2014/01/10/horizon-view-5-3-part-8-view-connection-server-requirements-and-installation/

Microsoft. (n.d.). *Active directory*. Retrieved from https://msdn.microsoft.com/en-us/library/windows/desktop/aa746492(v=vs.85).aspx

Packt publishing. (n.d). *Overview-horizon-view-architecture-and-its-components.* Retrieved from https://www.packtpub.com/books/content/overview-horizon-view-architecture-and-its-components

Raido. (n.d.). *Server virtualization*. Retrieved from http://www.raido.be/solutions/server- virtualization/

Rouse, M. (2006). *Tower servers.* Retrieved from http://whatis.techtarget.com/definition/tower-server

Rouse, M. (2011). *Rack server*. Retrieved from http://whatis.techtarget.com/definition/rack-server-rack-mounted-server

Search VMware. (2015). *VMHorizon view composer*. Retrieved from http://searchvmware.techtarget.com/definition/VMware-Horizon-View-Composer

ServerWatch. (2015). *Virtualization*. Retrieved from http://www.serverwatch.com/trends/article.php/3877576/Top-10-Virtualization-Technology-Companies.htm

Suhr, B. (2014). *View implementation*. Retrieved from http://www.virtualizetips.com/2014/06/24/vmware-horizon-6-install-part-1-connection-server/

Techopedia. (n.d.). *Virtualization*. Retrieved from http://www.techopedia.com/definition/719/virtualization

Valli. (n.d). *Dell-tower-server*. Retrieved from http://www.valli.com/images/hardware_large/dell-tower-server.JPG

Virtual machine. (2009). *Wikipedia*. Retrieved from http://en.wikipedia.org/wiki/Virtual_machine

VMware. (2009). *ESX and ESXi*. Retrieved from http://www.vmware.com/files/pdf/VMware-ESX-and-VMware-ESXi-DS-EN.pdf

VMware. (2012). *vmware vsphere 5.1 vmotion architecture, performance, and best practices.* Retrieved from http://www.ntpro.nl/blog/archives/2149-VMware-vSphere-5.1-vMotion-Architecture,-Performance,-and-Best-Practices.html

VMware. (2015). *VMware*. Retrieved from http://en.wikipedia.org/wiki/VMware

VMware. (n.d.a). *vSphere Client*. Retrieved from http://pubs.vmware.com/vsphere-51/topic/com.vmware.vsphere.vcenterhost.doc/GUID-DAB486D6-3E33-4939-B80A-BB17CB3B4E1E.html

VMware. (n.d.b). *View database*. Retrieved from https://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp?topic=/com.vmware.vsphere.installclassic.doc_41/install/prep_db/c_preparing_the_vmware_infrastructure_databases.html

VMware. (n.d.c). *View installation*. Retrieved from http://pubs.vmware.com/view-50/index.jsp?topic=%2Fcom.vmware.view.installation.doc%2FGUID-5B2266B8-EA3C-4F49-BABB-2D0B91DE6C1D.html

VMware. (n.d.d). *Storage vMotion*. Retrieved from https://www.vmware.com/products/vsphere/features/storage-vmotion

VMware. (n.d.e). *High availability*. Retrieved from http://www.vmware.com/products/vsphere/features/availability

VMware. (n.d.f). *vCenter server*. Retrieved from http://www.vmware.com/in/products/vcenter-server

VMware. (n.d.g). *View architecture planning*. Retrieved from http://pubs.vmware.com/view-52/index.jsp?topic=%2Fcom.vmware.view.planning.doc%2FGUID-6CAFE558-A0AB-4894-A0F4-97CF556784A9.html

VMware. (n.d.h). *Hardware compatibility for VMware*. Retrieved from www.vmware.com/resources/compatibility

VMware. (n.d.i). *View*. Retrieved from https://www.vmware.com/support/pubs/view_pubs.html

VMware. (n.d.j). *View composer*. Retrieved from https://www.vmware.com/files/pdf/VMware-View-4-Composer-DS-EN.pdf

VMware. (n.d.k). *View planning*. Retrieved from https://pubs.vmware.com/view52/index.jsp?topic=%2Fcom.vmware.view.planning.doc%2FGUID-6CAFE558-A0AB-4894-A0F4-97CF556784A9.html

VMware. (n.d.l). *View planning*. Retrieved from https://pubs.vmware.com/view51/index.jsp?topic=%2Fcom.vmware.view.planning.doc%2FGUID-57D362EB-AC04-45B8-87AA-05A15A998211.html

VMware. (n.d.m). *esxi-hypervisor*. Retrieved from https://www.vmware.com/products/vsphere/features/esxi-hypervisor

VMware. (n.d.n). *vMotion*. Retrieved from https://www.vmware.com/products/vsphere/features/vmotion

VMware. (n.d.o). *vCenter-server*. Retrieved from https://www.vmware.com/products/vcenter-server/features

VMware. (n.d.p). *Knowledge base*. Retrieved from https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2032741

von Oven, P., & Coombs, B. (2015). *Mastering VMware horizon 6.pdf*. Retrieved from http://blogsdelagente.com/cipocaziqeqa/mastering-vmware-vsphere-5-5-pdf-download/