

**SECURITY FOR VMWARE VIRTUALIZED  
DATACENTER**



**MCS**

by  
Fazeel Ali Awan

A thesis submitted to the faculty of Information Security Department Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

October 2016

Certified that final copy of MS/MPhil thesis written by Mr/MS Fazeel Ali Awan, Registration No. NUST2014-63772-MMCS25214F, of Military College of Signals has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: \_\_\_\_\_  
Name of Supervisor Col Imran Rashid, PhD  
Date: \_\_\_\_\_

Signature (HoD): \_\_\_\_\_  
Date: \_\_\_\_\_

Signature (Dean/Principal): \_\_\_\_\_  
Date: \_\_\_\_\_

## ABSTRACT

A datacenter is a multi-layered and centralized information technology services provisioning facility housing large number of complex servers, storage and network devices. Legacy datacenters are managed by system and network administrators by configuring each device manually. With the advent for virtualization, datacenter environments are moving towards automation based models and devices are configured and services are provided in a very less time.

Organizations face a rising demand of maximum utilization of IT resources and at the same time minimizing the cost of IT expenses. This led to popularity of virtualized datacenters which provide cost effective solutions through consolidation of available IT resources. Nevertheless, advantages of virtualization are not only limited to cost savings but one of the main benefit of virtualization is the system flexibility which helps in faster provisioning of services, increased uptime and efficient disaster recovery.

The benefits of virtualization cannot be overlooked and thus organizations are rapidly moving from traditional datacenters to virtualized environment. However, organizations have hurriedly adopted traditional security architecture in the virtualized datacenters. Organizations need to understand that although the enterprises are conversant with traditional methodology but this can lead to unwanted results if applied on virtualized datacenter environments such as higher complexity and affected performance.

Nonetheless, implementing security in virtual environment is more complex because virtualized datacenters involve security challenges present in both traditional datacenters as well as those prone to virtualization. This research focuses on security challenges pertaining to virtualized datacenter deployment and proposes solutions to address these issues in an enterprise environment.

An implementation of a virtualized datacenter is presented in this thesis. The datacenter is based on VMware virtualization, Huawei server hardware and storage with Juniper and 3ISYS networking equipment. After establishing a virtualized datacenter, security was implemented on new threat vectors introduced by the virtual environment. Resultantly, a secure, fast, scalable and high available virtualized datacenter is proposed and implemented.

## DECLARATION

I hereby declare that no portion of work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

---

Fazeel Ali Awan

Dedicated to:  
My Supervisor,  
My Committee Members,  
My Family members,  
My Teachers and Colleagues  
for their unconditional support, all the way.

## ACKNOWLEDGMENTS

First of all, thanks to all Allah Almighty for giving me strength, knowledge and courage to carry out this research successfully. I am immensely grateful to my supervisor Col Dr. Imran Rashid for his worthy supervision and support that enabled me to complete my thesis work. I would also like to thank my committee members, Asst. Prof. Mian Muhammad Waseem Iqbal and Lecturer Waleed Bin Shahid for their valuable technical support and worthy guidance. Further I am obliged to all my family for their endless support.

## TABLE OF CONTENTS

1.	Introduction .....	1
1.1	Overview .....	1
1.2	Motivation and Problem Statement .....	3
1.3	Objectives .....	3
1.4	Research Questions .....	3
1.5	Significance .....	4
1.6	Scope.....	4
1.7	Limitations.....	4
1.8	Thesis Contributions .....	4
1.8.1	Review of the Existing Security Practices in Datacenters .....	5
1.8.2	Categorization of Security Needs for Virtualization .....	5
1.8.3	Development of Security Model .....	5
1.8.4	Implementation and testing.....	5
1.9	Structure.....	5
1.10	Chapter Summary.....	6
2.	Literature Review.....	7
2.1	Introduction .....	7
2.2	Virtualization Concepts.....	7
2.2.1	History .....	8
2.2.2	Current Situation .....	8
2.3	Benefits of Datacenter Virtualization .....	9
2.4	Hypervisor .....	10
2.4.1	Isolation .....	10
2.4.2	Resource Management.....	10
2.4.3	Type-I Hypervisor.....	10
2.4.4	Type-II Hypervisor .....	11
2.5	Virtualization Workflow .....	12
2.5.1	Full Virtualization .....	13
2.5.2	Para Virtualization .....	13
2.5.3	Hardware Assisted Virtualization.....	14

2.6	Chapter Summary.....	15
3.	VMware vSphere and Virtualized Datacenter .....	16
3.1	Introduction .....	16
3.2	Components of vSphere .....	16
3.3	Virtualized Datacenter Design.....	17
3.4	VMware Virtual Datacenter Features.....	18
3.4.1	vMotion .....	19
3.4.2	Storage vMotion.....	19
3.4.3	High Availability .....	20
3.4.4	Fault Tolerance .....	20
3.4.5	Distributed Resource Scheduler (DRS).....	21
3.4.6	Storage DRS.....	22
3.4.7	Templates .....	22
3.4.8	Clones.....	23
3.4.9	Snapshots.....	23
3.5	Virtual Datacenter Network Design .....	23
3.6	Virtual Datacenter Storage Design .....	24
3.7	vCenter Server .....	25
3.8	Chapter Summary.....	27
4.	Virtualization Security Risk and Vulnerabilities .....	28
4.1	Introduction .....	28
4.2	Malware.....	28
4.3	VM-aware Malware .....	28
4.4	VM-based Malware.....	30
4.5	Network .....	32
4.5.1	VM Sprawl.....	32
4.5.2	Transient VMs in the Network.....	33
4.5.3	Compromise of Centralized Management Software.....	33
4.5.4	Unavailability of Complete vSwitch due to Failure of Physical NIC .....	33
4.5.5	VM Intercommunication .....	34
4.6	Virtualization Software Inherited Threats .....	34
4.6.1	VM Escape and Hyper-jacking .....	34
4.7	Management.....	35



4.7.1	Administration Overhead.....	35
4.7.2	Additional Threats from Virtualization Enhanced Features.....	36
4.7.3	Challenging Security Requirements.....	36
4.7.4	Rollback Threats .....	37
4.8	Auditing and Compliance .....	37
4.9	Chapter Summary.....	37
5.	Research Methodology .....	39
5.1	Introduction .....	39
5.2	Virtualized Datacenter Hardware .....	40
5.3	Network Devices .....	40
5.3.1	Juniper SRX 650 Firewall .....	40
5.3.2	3ISYS CS5500 Switch.....	40
5.4	System Devices .....	40
5.4.1	Huawei RH2288A V2 Server.....	40
5.4.2	Huawei SAN – OceanStor S2600T.....	40
5.5	Virtualized Datacenter Software.....	40
5.5.1	OS .....	40
5.5.2	Virtualization.....	40
5.6	Virtualized Datacenter Setup .....	41
5.6.1	Establishing Infrastructure.....	41
5.6.2	Establishing Physical Network.....	41
5.6.3	Storage Configuration.....	42
5.6.4	Server Configuration.....	42
5.6.5	LOM Configuration - iBMC .....	42
5.6.6	RAID Configuration .....	43
5.6.7	Server Virtualization.....	43
5.6.8	ESXi Installation .....	43
5.6.9	vSphere Client.....	44
5.6.10	Network Configuration .....	44
5.6.11	Storage Configuration.....	44
5.6.12	Management Server VM .....	44
5.6.13	Active Directory.....	45
5.6.14	vCenter Server.....	45

5.6.15	Web Client .....	46
5.6.16	Virtualized Datacenter .....	46
5.6.17	vRealize Operations Manager .....	46
5.7	Chapter Summary.....	46
6.	Proposed Security Model for VMware Virtualized Datacenter .....	48
6.1	Introduction .....	48
6.2	Proposed Security Model .....	48
6.3	Physical Security .....	49
6.3.1	Access Control .....	49
6.3.2	Limited Entry .....	49
6.4	Traditional Security.....	50
6.4.1	Firewall.....	50
6.4.2	Access Control Lists (ACLs).....	50
6.4.3	Redundancy.....	50
6.4.4	MAC Binding.....	50
6.4.5	Port Binding .....	50
6.4.6	Load Balancing and VIPs .....	51
6.4.7	Antivirus Software .....	51
6.4.8	DNS .....	51
6.4.9	Encryption .....	51
6.4.10	Authentication and Authorization .....	51
6.4.11	Unnecessary Services .....	51
6.4.12	Backup.....	51
6.4.13	DR and BCP.....	52
6.5	Monitoring.....	52
6.5.1	Logging .....	52
6.5.2	Auditing.....	52
6.5.3	SIEM (Security Information and Event Management) and IDPS (Intrusion Detection and Prevention System) .....	52
6.5.4	NMS .....	53
6.6	Virtualization Security .....	53
6.7	Virtualization Security Controls .....	54
6.7.1	Isolation - Access Control .....	54

6.7.2	Controls for ESXi Host and Guest VM Communication .....	55
6.7.3	vCenter Controls .....	55
6.7.4	ESXi Hypervisor Controls.....	56
6.7.5	Controlled Management .....	57
6.8	Virtualization Security Policies .....	57
6.8.1	User & Group Security Policies .....	57
6.8.2	Network Security Policies .....	58
6.9	Virtualization Tier Monitoring .....	58
6.9.1	NMS – vRealize Operations Manager .....	59
6.9.2	Auditing & Logging.....	59
6.10	Virtualization DR & BCP Solutions.....	60
6.10.1	High Availability (HA).....	60
6.10.2	Fault Tolerance (FT).....	60
6.10.3	Zero Downtime .....	60
6.10.4	Site Recovery Manager (SRM) .....	61
6.10.5	Backups and vSphere Data protection (vDP) .....	61
6.10.6	vShield.....	61
6.10.7	VMware Virtualized Datacenter Hardening Policies Guidelines.....	61
6.11	Chapter Summary.....	63
7.	Implementation & Analysis.....	65
7.1	Introduction .....	65
7.2	Establishment of VMware Virtualized Datacenter .....	65
7.3	Security Framework Implementation .....	65
7.3.1	Isolated vMotion Traffic.....	66
7.3.2	Reject MAC Spoofing .....	66
7.3.3	ESXi Firewall.....	67
7.3.4	ESXi Host SSH Service.....	69
7.3.5	Enable Lockdown Mode.....	70
7.3.6	Host Image Profile Acceptance Level.....	71
7.3.7	User and Group Policies .....	71
7.3.8	Directory Service & Authentication.....	72
7.3.9	NTP Configuration .....	73
7.3.10	VM File System Permissions and Integrity Check.....	74

7.3.11	Direct Copy/ Pasted Disabled.....	74
7.3.12	Removal of Unnecessary Devices.....	75
7.3.13	Load Balancing.....	76
7.3.14	Monitoring – vRealize Operations Manager.....	76
7.4	Chapter Summary.....	78
8.	Conclusion.....	79
8.1	Introduction.....	79
8.2	Objectives Achieved.....	79
8.3	Limitations.....	79
8.4	Future Direction.....	79
8.5	Concluding Remarks.....	79

## LIST OF FIGURES

<i>Figure Number</i>	<i>Page</i>
Figure 1.1 Virtual Machine Monitoring Approaches .....	2
Figure 2.1 The Basic Virtualization Elements.....	8
Figure 2.2 Type-I Monolithic Hypervisor .....	11
Figure 2.3 Type-II Microkernel Hypervisor .....	11
Figure 2.4 Type-II Hypervisor .....	12
Figure 2.5 Full virtualization.....	13
Figure 2.6: Para virtualization.....	14
Figure 2.7: Hardware assisted virtualization .....	15
Figure 3.1 VMware Virtual Datacenter Design.....	18
Figure 3.2 VMware vMotion. ....	19
Figure 3.3 VMware Storage vMotion.....	20
Figure 3.4 VMware High Availability.....	20
Figure 3.5 VMware Fault Tolerance.....	21
Figure 3.6 VMware Distributed Resource Scheduler .....	21
Figure 3.7 VMware Storage Distributed Resource Scheduler .....	22
Figure 3.8 VMware Templates .....	22
Figure 3.9 VMware Clone.....	23
Figure 3.10 VMware Snapshots.....	23
Figure 3.11 VMware Network Architecture.....	24
Figure 3.12 VMware Storage Architecture .....	25
Figure 3.13 VMware vCenter Server Concept .....	26
Figure 3.14 VMware vCenter Server Architecture .....	27
Figure 4.1 VM-aware Malware Targets .....	29
Figure 4.2 Successful VMware VMs detection by Malware in Two Years.....	30
Figure 4.3 VM-Based Rootkit Operation .....	32
Figure 4.4 VM Escape.....	35
Figure 5.1 High Level Virtualized Datacenter Design.....	39
Figure 5.2 Huawei RH2288A V2 iBMC .....	43
Figure 6.1 Four Major Datacenter Security Domains .....	49
Figure 6.2 Virtualization Security Framework.....	54
Figure 7.1 VMware Virtualized Datacenter .....	65
Figure 7.2 VMware vMotion Isolation .....	66
Figure 7.3 MAC Spoof Rejection Policy.....	67
Figure 7.4 ESXi Firewall Configuration for Incoming Connections.....	67
Figure 7.5 ESXi Firewall Configuration for Outgoing Connections .....	68
Figure 7.6 ESXi Firewall Configuration for Trusted Devices .....	68
Figure 7.7 ESXi Firewall Configuration for Unnecessary Services .....	69
Figure 7.8 ESXi Firewall Configuration for vCenter Update Manager .....	69
Figure 7.9 Restricted SSH Access .....	70

Figure 7.10 ESXi Hosts in Lockdown Mode ..... 70  
Figure 7.11 ESXi Host Image Profile Acceptance Level..... 71  
Figure 7.12 User Permission Assignment ..... 72  
Figure 7.13 User Authentication Services ..... 72  
Figure 7.14 NTP Startup Policy ..... 73  
Figure 7.15 NTP Client and NTP Server Synchronization ..... 73  
Figure 7.16 VMFS Permissions and Integrity Check..... 74  
Figure 7.17 Disabling of Direct Copy/ Paste..... 75  
Figure 7.18 Disabling of Unnecessary Devices..... 75  
Figure 7.19 Preserving Balanced Load..... 76  
Figure 7.20 vROM Dashboards for Efficient Monitoring..... 77  
Figure 7.21 VM Trends and Analysis..... 77  
Figure 7.22 vROM Workload Reports ..... 78

## LIST OF TABLES

<i>Table Number</i>	<i>Page</i>
Table 1 Virtualization Categories .....	9
Table 2 Components of vSphere .....	17
Table 3 Components of Virtual Datacenter .....	18
Table 4 Virtual Machine Associated Files.....	25
Table 5 Virtualized Datacenter Hardening Techniques .....	63

## LIST OF ACRONYMS

ACL	Access Control List
AD	Active Directory
BCP	Business Continuity Planning
DMA	Direct Memory Access
DNS	Domain Name System
DPI	Deep Packet Inspection
DR	Disaster Recovery
DRS	Distributed Resource Scheduler
FC	Fibre Channel
FT	Fault Tolerance
HA	High Availability
HDD	Hard Disk Drive
HIPS	Host Based Intrusion Prevention System
iBMC	Intelligent Baseboard Management
IDPS	Intrusion Detection and Prevention System
iSCSI	Internet Small Computer System Interface
LBR	Load Balancer
LOM	Lights Out Manager
LUN	Logical Unit Number
MAC	Media Access Control
MBR	Master Boot Record
NAS	Network-Attached Storage
NFS	Network File System
NMS	Network Monitoring System
NTP	Network Time Protocol
O&M	Operations & Management
OS	Operating System
PII	Personal Identifiable Information



PoC	Proof-of-Concept
PPC	PowerPC
QoS	Quality-of-Service
RAC	Real Application Cluster
RHEL	Red Hat Enterprise Linux
RMD	Raw Mapping Device
RPC	Remote Procedure Call
SDDC	Software Defined Datacenter
SIEM	Security Information and Event Management
SAN	Storage Area Network
SRM	Site Recovery Manager
vDC	Virtual Datacenter
VIB	vSphere Installation Bundle
VIP	Virtual IP
VLAN	Virtual Local Area Network
VM	Virtual Machine
VMBR	Virtual Machine-Based Rootkits
VMDK	Virtual Machine Disk
VMFS	Virtual Machine File System
VMM	Virtual Machine Monitor
vNIC	Virtual Network Interface Card
VPN	Virtual Private Network
vROM	vRealize Operations Manager
vSwitch	Virtual Standard Switch

## **1. Introduction**

### 1.1 Overview

Virtualization technology is gaining interest in enterprise datacenters primarily because of the cost savings. The concept of virtualization is based on running several separate computer instances as virtual machines (VMs) on a single computer or a physical machine simultaneously. Virtualization achieves this by sharing the hardware resources of a physical machine, also known as host machine, between individual underlying VMs. Ultimately cost on hardware as well as infrastructure is greatly reduced but at the same time performance is not compromised. Besides cost reduction, virtualization significantly enhances flexibility and efficiency of the system.

Because of the clear advantages of virtualization technology, enterprises are migrating their legacy datacenters towards virtualized environments and leading to the formation of cloud setups where deemed necessary. Virtualization has become one of the major topics of discussion in all datacenters, especially due to the compatibility of all latest hardware with virtualization. Virtualization is offering many attractive benefits but since the technology is relatively new in the organizations and their datacenters so generally administrators overlook the added security implications that are introduced in their IT environment. Organizations are swiftly migrating towards the virtualized datacenters due to which they fail to implement security controls to handle the virtualization aware vulnerabilities. This can result in major security incidents leading to loss or theft of confidential data. Organizations need to realize that with the inclusion of virtualization in their environment, many new security risks and threats are introduced. This results in the need of an extra layer of security as traditional security mechanisms are not enough for securing a virtualized datacenter.

One of the proficient methods of security is the continuous monitoring and security controls of VMs which can be achieved in two leading techniques known as host based protection and network based protection.

1. One approach is the implementation and configuration of a network based firewall which provides an efficient protective layer as IDS or IPS as network firewall can detect malicious traffic before entering into the virtual hosts. Figure 1.1[a] describes this technique in which the compute resource requirement for security implementation is

reduced due to centralized protection, however, this cannot effectively monitor the underlying VMs on the physical host due to less visibility at this layer.

- The alternate approach is to implement security on all VMs as shown in Figure 1.1[b]. This approach provides a better level of security as effective monitoring on all virtual machines is achieved. However, this substantially increases the compute and memory requirement for security, thus, compromising the efficiency of a virtual machine.

Thus, both the security tactics have their share of advantages and disadvantages. An administrator has to make a tradeoff between resource utilization and security efficiency while deciding which approach to opt for in the virtualized environment. Another security approach called introspection [1] is also available which combines the two discussed approaches. In this method, a separate VM is created alongside the rest of the virtual machines which is responsible for monitoring of the virtual environment as shown in Figure 1.1[c]. Relatively this method is better than both network based and host based protections as this provides both, a centralized point of security and monitoring with maximum visibility of the virtual machines.

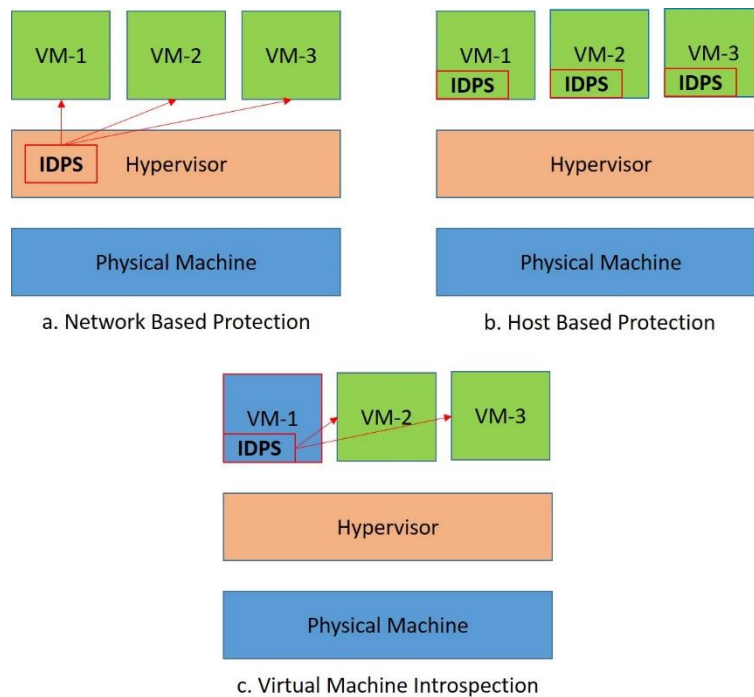


Figure 1.1 Virtual Machine Monitoring Approaches

Continuous monitoring at hypervisor layer and underlying individual VMs is the additional security control which was previously absent in legacy physical environments. In addition to security protocols present in traditional environments, the virtualized datacenters require new and more complex security procedures to cater for the supplementary virtualization threat vectors.

## 1.2 Motivation and Problem Statement

The research is focused on proposing and implementing a complete security framework for virtualized datacenter for safeguarding against virtualization based vulnerabilities. Specifically, the research revolves around presenting the security model for VMware based virtualized datacenters. VMware is by far leading the virtualization technology [2]. Microsoft, Citrix and Oracle are the other emerging vendors in virtualization but flexibility and extended hardware compatibility with different hardware manufacturers makes VMware renowned and ahead in this field. Virtualization security revolves around the implementation of detective and preventive measures for ensuring smooth flow of IT operations. Numerous major security threats will be discussed and their corresponding security control will be designed and implemented in this research.

Motivation behind this research is to find and evaluate the vulnerabilities present in VMware virtualized datacenters, design and implement a complete security model and analyze the developed security standard. Virtualization offers tremendous benefits in enterprise datacenters but these benefits can only be achieved if the virtualized datacenter is security wise reliable and protected. This thesis will present the security guidelines for VMware based virtualized datacenters. Implementation of these guidelines will ensure the protection of virtual machines against virtualization security risks. Security guidelines for virtualized environment are the security protocols that are implemented in addition to traditional security methods.

## 1.3 Objectives

Essential objectives to be carried out in this research are described below:

1. Study and understanding the concept of virtualization and virtualized datacenter.
2. To evaluate security vulnerabilities existing in the virtualization technology.
3. To design and develop security framework that address VMware based datacenter virtualization security concerns.
4. To confirm and authenticate the developed design by implementation and analysis.

## 1.4 Research Questions

1. What are the current virtualization approaches being used in datacenters?
2. What are the inherent weaknesses in these technologies that can lead to a security breach and privacy concerns?
3. Can the developed security model be used to address these security and privacy concerns?

#### 4. How the developed model can be analyzed?

### 1.5 Significance

The research aim is to provide an insight into the security challenges in the datacenter environment with focus on one of the core technologies: Virtualization.

There is a need of a security model that effectively analyses and certifies that the security of a virtualized datacenter is reliable. The need for virtual datacenter security concept can be met by ensuring the hardening of all virtual machines, hypervisor security and host machine security.

The developed security model allows policy makers as well as potential virtualization patrons to evaluate their security and would give organizations a guideline to develop a secure, strong, robust, scalable and a competitive datacenter based on virtualization.

### 1.6 Scope

Data loss or data theft is the vital security concern in datacenter virtualization. Additionally, identity management, access control and detection or prevention of cross VM side channel attacks are the other targeted fields. All these categories are broad areas of study, hence require a dedicated research in each field.

### 1.7 Limitations

This research aims to develop a security model that provides confidentiality, integrity and authenticity in the system. The security model is necessary because organizations need to understand that, although, virtualization in datacenters provides valuable advantages, however, also introduces various security threats in their environment that were not present before which is principally the major limitation of virtualization. However, this limitation is only there if security guidelines are not properly implemented or overlooked on VMs.

Another limitation is that VMware till now is only compatible with intel based X86 (both 32bit and 64bit) architecture and thus a vendor lock-in can occur if datacenters have SUN SPARC or IBM PPC (PowerPC) based servers in the datacenter.

Data is the most valuable asset of any organization and its security and confidentiality compromise is not affordable at any cost. HDDs (Hard Disks/Drives) are provided to virtual machines over the network and thus the corresponding data on these disks exist on networked storage, rather than on HDD of the host machine. This feature in virtualization can be a security threat if proper security at storage is not implemented.

### 1.8 Thesis Contributions

This section provides the direct contributions from this thesis.

### **1.8.1 Review of the Existing Security Practices in Datacenters**

Conducting review of all the computing facilities in a datacenter for effective security configurations and policy planning is vital. This allows understanding of present security implementation and the need of further hardening for catering new security threats.

### **1.8.2 Categorization of Security Needs for Virtualization**

After collecting and analyzing the survey data, the thesis develops and writes the security policies for the virtualized datacenter environments. Two main categories for security implementation can be administrators and domain specific users. The administrators in this case are those who are responsible for provision of virtualization services in datacenter while the users are the underprivileged secondary admins of particular tiers whose servers have been virtualized by the primary administrators. The levels of authority and access rights categorize the security needs.

### **1.8.3 Development of Security Model**

The security model would be developed and tested in the line of using the above defined categories. Nevertheless, the security solution would not be limited to particular area or a category but would cater all variables within a virtual datacenter.

### **1.8.4 Implementation and testing**

The developed solution would be implemented and tested against threat vectors introduced specifically by virtualization of datacenter.

## **1.9 Structure**

Thesis structure briefly portrays the chapter wise content description of this research. The second chapter presents the literature review of virtualization and VMware datacenter virtualization fundamentals. Evolution of virtualization technology to present transformation is discussed in detail. Types of hypervisors and approaches to meet virtualization has been discussed.

The third chapter describes VMware vSphere. All VMware specific virtualization terminologies and features are explained for getting the better picture for focusing and analyzing the security requirements leading to the development of a security model of datacenters.

The fourth chapter presents the security threats and vulnerabilities that exist in datacenter virtualization. These new threat vectors will be studied in detail so that their corresponding control can be worked out. The security threats that exist in legacy environments and the consequences of these issues when introduced in virtualized datacenters are also examined.

Main focus however, will be on vulnerabilities that are only related to datacenter virtualization and their effect on service availability.

The fifth chapter discusses the research methodology. The research is conducted on establishing a mini datacenter with the necessary physical hardware. Traditional security is implemented on the physical level of the datacenter. Then VMware virtualization is installed and configured to obtain a fully functional mini virtualized datacenter. A complete security model is then designed and implemented. Lastly, the formulated security design is tested and analyzed.

The sixth chapter presents a complete security model for the VMware datacenter virtualization. All proposed policies and guidelines are discussed in detail for implementation in virtualized datacenter. Vulnerabilities and threats that are introduced due to virtualization are addressed by proposing a complete security framework. Implementation of the formulated security design will allow the testing and analysis of the datacenter security.

The seventh chapter is responsible for the implementation and testing of the proposed security model. NMS (Network Monitoring System) graphs and different results will certify the datacenter virtualization security model. This will authenticate the reliability of the formulated security design and thus can be used by any organization for securing its virtualized environments.

Finally, the eighth chapter presents the conclusion of the research. Awareness for the need of a secure VMware virtualized datacenter is highlighted as organization need to understand that legacy datacenter security model is unfit for virtualized environments. Although, the proposed security model in the research will suffice for the cloud security model as well, but the research is open for future threats in cloud environment as virtualization and cloud are still a growing technology till date.

## 1.10 Chapter Summary

The concept and benefits of datacenter virtualization is discussed in this chapter, followed by the need of a security model to address the datacenter virtualization security threats. The importance of monitoring of VMs is highlighted which forms the basis of security requirements. Finally, the thesis structure is described.

### **2. Literature Review**

#### **2.1 Introduction**

A detailed appraisal of existing literature regarding virtualization and the concept of VMware datacenter virtualization is described in this chapter. Starting from the history of system virtualization and evolution of virtualization technology to the modern-day virtualization concepts is discussed. After the understanding of virtualization is achieved, the concept of virtualized datacenters is presented. This idea is linked to VMware solutions for datacenter virtualization. Detailed virtualization implementation and VMware specific virtualization terminologies are explained. Understanding of these concepts will lead to formulating a comprehensive security model for virtual environments.

#### **2.2 Virtualization Concepts**

The concept of virtualization was introduced when the need of utilizing maximum system resources, both compute and memory, became a necessity. A lot of budget was spent on IT equipment but at the same time the system resources were not being optimally utilized, especially during the off-peak hours. To achieve efficiency in this regard, the idea of sharing of resources was developed that led to the foundation of virtualization technology.

Virtualization allows sharing of system resources of a single physical machine called physical host or simply host, for running multiple Operating System (OS) instances as virtual machines called guests by multiple users simultaneously; such that, each OS instance is independent of the other. Virtualization does this by installing a layer of management called Virtual Machine Monitor (VMM) or more commonly as Hypervisor. This layer takes control over all hardware resources of physical host for distribution among the virtual machines as per the requirement. Resultantly, the resources are efficiently utilized and a high level of flexibility is achieved. Moreover, this reduces the requirement of additional hardware and thus, cost savings is attained.

Hypervisor provides the system resources of physical machine to the underlying virtual machines that are independent of each other. A virtual machine appears and behaves precisely same as normal computer machine. Users of a VM cannot identify a difference if they are using a physical machine or a virtual one. VM users sense that they are interacting with the hardware directly; however, in reality it is the hypervisor which translates the users' requests towards the real physical hardware. Although VMs are sharing the resources of the



physical host, nevertheless, every VM is virtually provided with dedicated system resources.

Figure 2.1 demonstrates the basic virtualization elements.

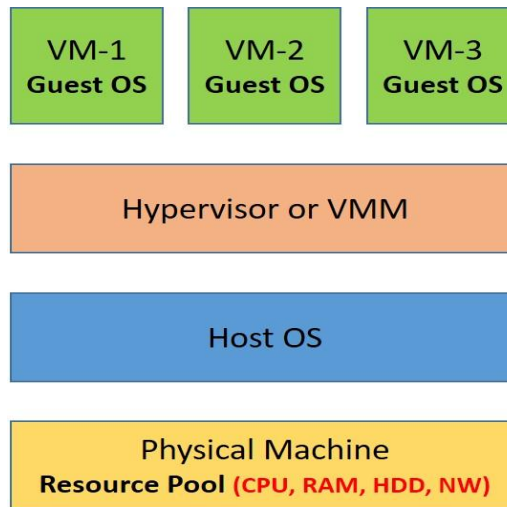


Figure 2.1 The Basic Virtualization Elements

### 2.2.1 History

Computer virtualization has evolved during a span of nearly half a century. As early as in 1960's the technology was initially established. During that time, computer hardware was large mainframes and it was very expensive. Efforts were made to achieve maximum resource utilization of such costly equipment and eventually basis of virtual machine technology was laid by IBM in 1972 by its VM/370 which could provide virtual memory to multiple users simultaneously [3].

Ongoing history of virtualization continued and in October 1998, VMware was granted patent for their techniques. Few months later, first stable virtualization platform for Intel based X86 architecture was developed by VMware.

### 2.2.2 Current Situation

In present day scenarios, IT managers in all organizations are pressurized to provide higher level of services while limit their budget costs. It is for this reason datacenters are moving towards virtualization day by day. The cost saving is remarkable and with efficient sharing of physical resources, QoS (quality-of-service) is also enhanced.

Initially virtualization was introduced to attain efficient resource utilization. But current situation is that virtualization is transforming entire datacenter environments to automated, flexible and agile systems; thus, leading to better service availability and helping organizations to achieve their business goals more efficiently [4].

Since virtualization reduces the hardware footprint so cost saving is not just in procurement of hardware but also in terms of rack space, power consumption and cooling units. The

benefits of virtualization in datacenter are not limited to financial savings but definitive advantage of this technology is the advanced speed, reduced complexity, increased flexibility and higher availability. Furthermore, datacenter virtualization offers better business continuity and disaster recovery solutions as compared to traditional environments [5].

These advantages cannot be achieved by only server virtualization but complete datacenter virtualization implementation will allow the maximum gains of virtualization technology.

Table 1 describes the different categories of virtualization.

Virtualization	Virtualization simply allows simultaneous OS instances as VMs on a single Physical host with its own base level OS.
Server Virtualization	All physical resources of a physical host are controlled by virtualization software or hypervisor. The hypervisor then provides these resources to several independent virtual hosts or VMs.
Datacenter Virtualization	Datacenter virtualization extends the virtualization concepts from server to storage and network.

Table 1 Virtualization Categories

### 2.3 Benefits of Datacenter Virtualization

Virtualization technology has emerged and now sets the platform for cloud implementation. Besides, this technology offers better management and administration of resources and thus better service availability is achieved. Following are some of the major benefits that are provided through datacenter virtualization [6].

1. Automation and flexibility.
2. Optimum resource utilization.
3. Budget savings on hardware, infrastructure and power consumption.
4. Increased performance and higher speed.
5. Increased uptime.
6. Better DR (Disaster Recovery) and BCP (Business Continuity Planning) features.
7. No maintenance downtime.
8. Holistic view of datacenter resources.

These are some of the prime factors why organizations are swiftly migrating towards virtualization in their datacenter environments. Importance of datacenter virtualization cannot be ignored and in due course of time all legacy datacenters will ultimately shift towards virtualized environments.

## 2.4 Hypervisor

The core of virtualization is the hypervisor which is responsible for management of available resources and provision of same to the VMs. Hypervisor is basically an OS itself with limited level of functionality [7]. User interaction at this layer is also very less and is limited to configuration of networking, IP address and OS credentials. The basic level of functionality at virtual machine monitor layer is intentional because complex OS would need more resources for its own proper functionality; whereas, maximum resource availability is desired for VMs. Furthermore, basic level OS are less prone to bugs and vulnerabilities. Primarily, VMM is responsible for resource management and virtual machine isolation.

### 2.4.1 Isolation

All VMs must work in isolation with full control over its available resources [8]. A VM must not be dependent upon the resources of another VM, unless specifically configured in case of over provisioning. Over provisioning involves manual intervention by system administrators and that is why this concept is not recommended on production environment especially on business-critical servers. There must not be any direct mediation between any two VMs and all such interaction must be via the VMM itself to ensure proper isolation.

### 2.4.2 Resource Management

Isolation of VMs is only possible by proper resource management. OS installed on VMs is responsible for the management of resources that are provided to that particular VM, however, the resources of the actual physical host are directly managed by the hypervisor only.

Based on the functionality, hypervisor is classified into two broad categories:

### 2.4.3 Type-I Hypervisor

Type-I or bare metal hypervisors are more suitable in datacenter virtualization as they offer increased flexibility and better performance [9]. ESXi is a VMware based bare metal hypervisor specifically designed for X86 architecture. Such type of VMM is developed with a very basic OS with limited functionality and features. It controls all the resources of the physical host on which it is configured and distributes them as per necessity to the corresponding VMs. This additional layer of hypervisor is very critical and needs proper security consideration by vendors while writing the code and by the administrators as well. Bare metal VMM are further classified into two categories:

### 2.4.3.1 Monolithic

Performance wise, monolithic bare metal hypervisor is better [10]. This involves drivers as essential part of the software code, as shown in figure 2.2. This allows direct communication between software and hardware but naturally this will make OS code very large; thus, making it complex. Obviously, the overhead is very less and thus this is very efficient but hardware compatibility is a drawback because if drivers of any hardware are not supported than such hardware cannot be virtualized. VMware ESXi is based on monolithic hypervisor.

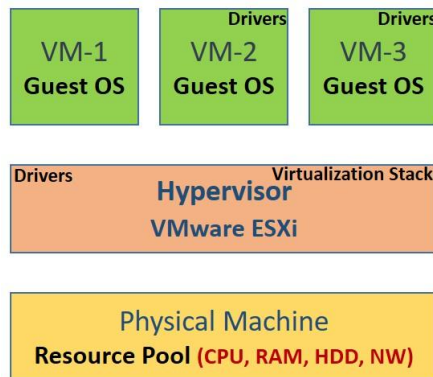


Figure 2.2 Type-I Monolithic Hypervisor

### 2.4.3.2 Microkernel

A separate privileged parent VM has drivers installed on it which provides these drivers to child VMs as shown in figure 2.3. Security wise this is a better approach as attack surface is reduced [11]. Each VM maintains its own device drivers and one driver being compromised will only affect a single VM. But at the same time, in this category if parent VM is affected than rest of the VMs can also become erroneous. Microsoft Hyper V is based on Microkernel hypervisor.

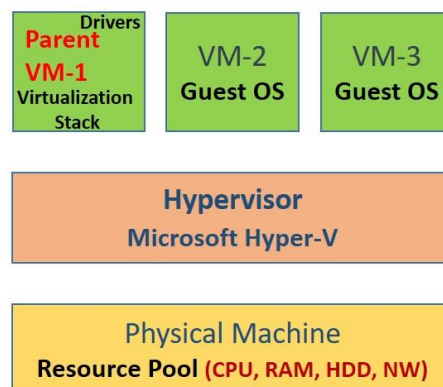


Figure 2.3 Type-II Microkernel Hypervisor

## 2.4.4 Type-II Hypervisor

The second category of virtual machine monitor is the Type II hypervisor or hosted hypervisor. In this type, hypervisor software is installed on the base OS and allows

creation of VMs on it. The VMs communicate with the hardware layer through hypervisor which in turn communicates via the base OS [10]. Figure 2.4 depicts Type-II hypervisor. Generally, these hypervisors are not recommended for production or more specifically, for enterprise environments as the additional layer makes functionality more complex. Moreover, if base OS is compromised then all VMs are affected, thus, system security is completely dependent on the base OS. In addition to being unsecure, hosted hypervisors are performance wise less efficient and limited virtualization functionality is offered by vendors. VMware Workstation and Oracle VirtualBox are two famous type-II hypervisors in the market.

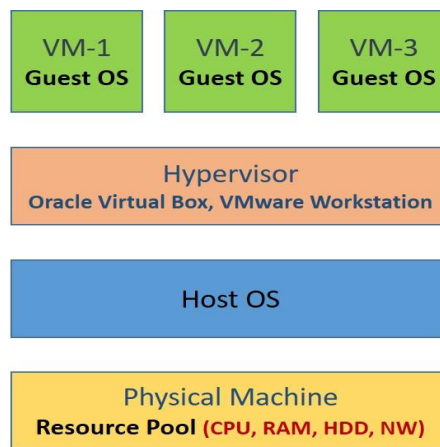


Figure 2.4 Type-II Hypervisor

## 2.5 VirtualizationWorkflow

In X86 CPU architecture, there is a concept of 4 protection run level rings (ring 0-3) in which each ring has a certain level of privileges for executing instructions. Most privileged ring is 0 and executes critical hardware interrupts. Operating system runs on this ring level for directly interacting with hardware. Likewise Ring 3 is least privileged and application software runs on this level.

In case of virtualization, the hypervisor has to interact with hardware directly so it must run at ring 0 and create and manage the VMs according to the resources of the physical [12]. This was achieved by running OS in unprivileged mode so that it should not interfere with hypervisor processes and VMM would be responsible for privileged interrupts translation. This approach allows hypervisor to efficiently manage the hardware but at times software processes may behave erroneously. This is because these processes and procedures are executed at a ring level with less privileges than originally designed to be running at. This critical issue has been addressed on X86 architecture in three distinct methods:

1. Full virtualization.

2. Para virtualization.
3. Hardwareassisted virtualization.

### 2.5.1 Full Virtualization

This technique involves the guest OS to be placed at ring 1 whereas, hypervisor is placed at ring 0, which translates all the necessary interrupts (binary translation) that remained non-virtualized from OS to hardware [13]. With this approach, the guest OS performs routine procedures same as in a physical environment and does not need to know that it is running on virtual environment.

Full virtualization completely separates guest OS and hardware resources. Furthermore, guest OS does not need to be modified in this implementation. But on the downside, this approach adds extra overhead due to constant translation. Application software has access to directly execute unprivileged requests with physical layer while all other requests are executed via guest OS. The concept of full virtualization is explained in below in figure 2.5.

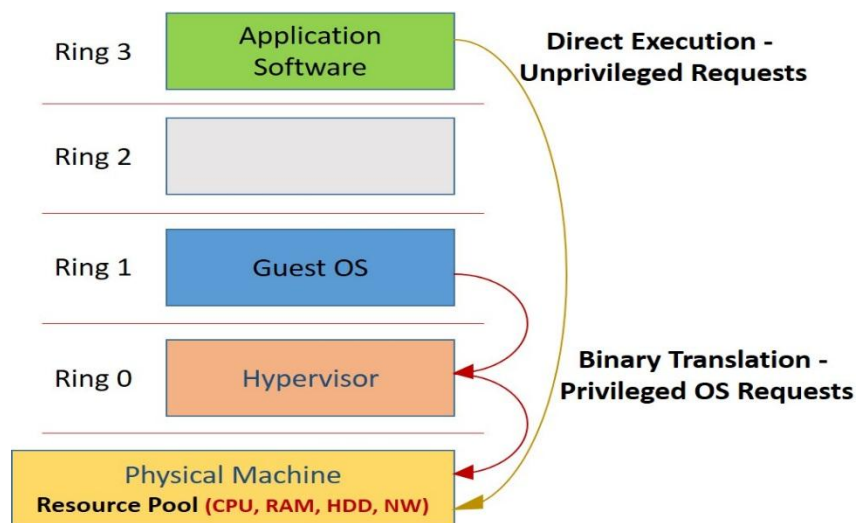


Figure 2.5 Full virtualization

### 2.5.2 Para Virtualization

The second approach is the para virtualization in which guest OS kernel needs to be modified for substituting the non-virtualized privileged interrupts with hypercalls [14]. These hypercalls can interact directly with the VMM which in turn execute these hypercalls, as shown in figure 2.6. This approach allows guest OS to be placed at ring 0.

Para virtualization greatly reduces the complexity and overhead of binary translation due to concept of hypercalls but on the other hand this approach requires OS modification. Open source OS kernel can be modified accordingly but this modification is not possible for closed source OS like Windows and Macintosh.

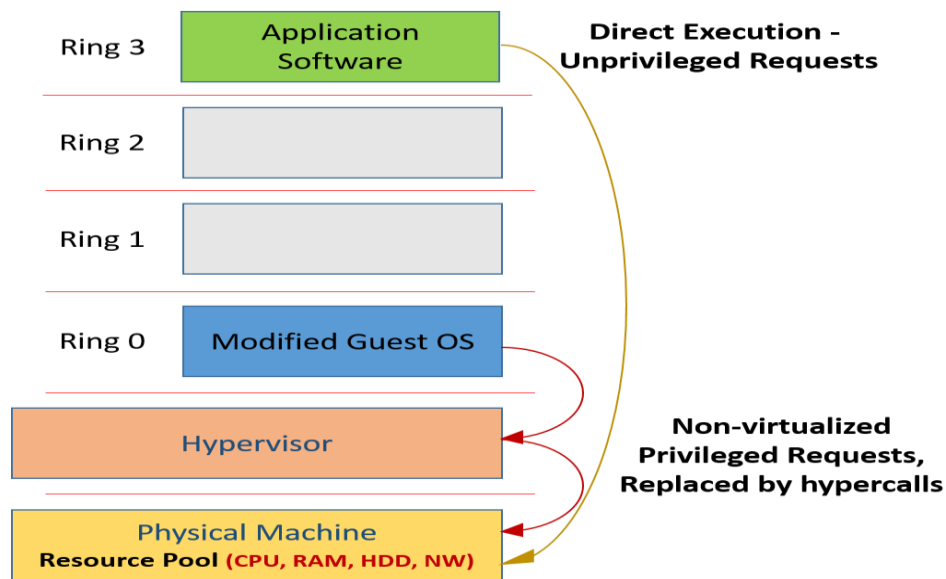


Figure 2.6: Para virtualization

### 2.5.3 Hardware Assisted Virtualization

With the advancement in processor technology many new features like DMA (Direct Memory Access) are available. DMA allows chipsets to directly access the RAM independently of CPU. Similarly, VMs could invoke DMA but sometimes the real physical addresses and virtual physical addresses did not correlate which would result the critical memory locations to be overwritten. Intel and AMD modified the hardware and released new processor technology to assist virtualization and overcome such security issues [15]. In hardware assisted virtualization, the hypervisor is placed at root mode or ring level -1 (higher privileges than ring 0) where guest OS is working at ring 0. Figure 2.7 describes this method of virtualization.

This allowed software to directly interact with hardware as in physical environment. Those interrupts which could not be virtualized are automatically trapped to hypervisor at ring -1 for further execution. This approach removes the need of OS kernel modification leading to reduced complexity and also compatibility issues between OS and hypervisor are addressed. Overhead is decreased so performance is also enhanced.

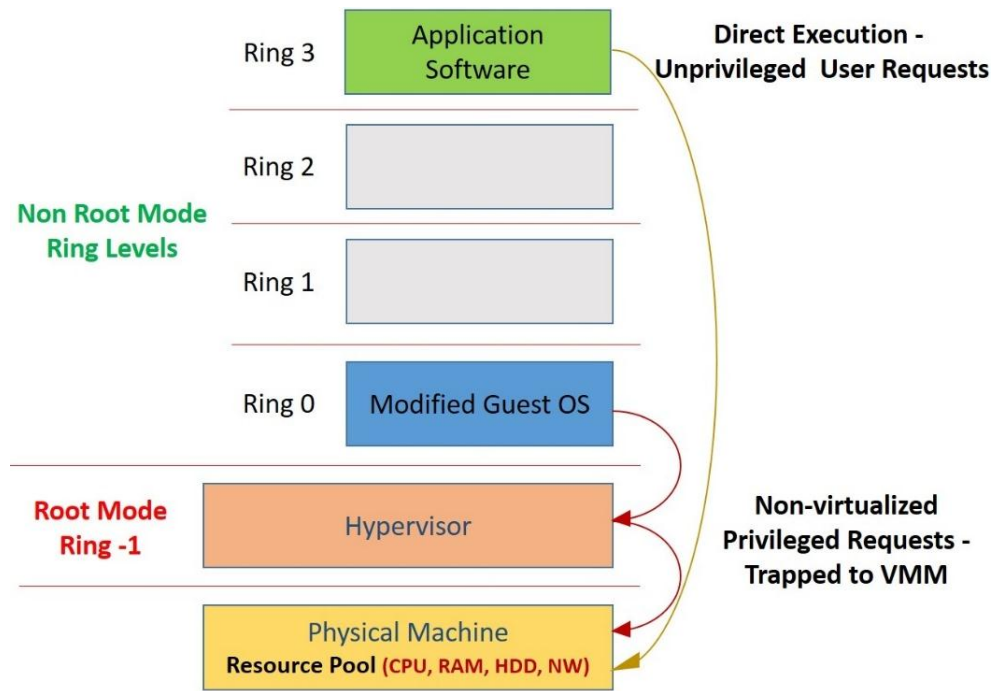


Figure 2.7: Hardware assisted virtualization

## 2.6 Chapter Summary

This chapter introduces basic virtualization concepts and how the virtualization technology evolved through history. Then benefits of virtualization for enterprises and why virtualization is recommended for datacenters is explained. Hypervisor description and the types of VMMs, that are Type-I and Type-II VMMs are clarified in details. This is followed by the three virtualization approaches that is full virtualization, para virtualization and hardware assisted virtualization.



### 3. VMware vSphere and Virtualized Datacenter

#### 3.1 Introduction

VMware vSphere revolutionized the enterprise datacenter environments by providing flexibility, reliability and cost savings in IT services. vSphere administers the physical hardware by creating a resource pool for virtualization. VMs are created by getting the virtual hardware from this resource pool and are utilized for providing revolutionary IT services. vSphere suite manages the hardware by its hypervisor ESXi and the resource pool can be managed directly from the console provided by vSphere client or more recently the web client. For managing a large infrastructure of IT resources in datacenter, vSphere introduces its managing tool called vCenter server and lays the foundation of cloud computing [16].

#### 3.2 Components of vSphere

Highly developed VMware virtualization features are offered through vSphere by comprising a list of different components. Table 2 briefly describes these components [16].

No.	Component	Description
1.	ESXi	VMware Type-I Hypervisor. This is the virtualization layer that installs as OS on Physical host and summaries the compute, storage and other resources for VMs.
2.	vSphere Client and Web Client	Virtualization console that remotely connects the ESXi hypervisor or vCenter for VM management. Web Client allows access through web browser while vSphere client is an exe which is first installed on a Windows system for further remote access.
3.	vCenter Server	VMware's centralized management tool for efficient provisioning of resources. Different intriguing virtualization features are offered through vCenter server.
4.	VMFS and VMDK	VMFS (Virtual Machine File System) is the cluster based file system used to store VMDK (Virtual Machine Disk). The HDD provided to VMs as VMDKs are simply files stored on a VMFS volume.

5.	vSwitch	vSwitch allows network virtualization. The single Ethernet interface or in more advanced machines, the fibre port is converted to a distributed virtual switch. Different VLANs (Virtual Local Area Networks) are configured on this switch for associating the network to VMs. This radically increased the network capacity.
6.	vMotion and storage vMotion	vMotion allows migration of virtual machines among physical hosts within a datacenter. VMs can move between hosts in powered on state with zero downtime, thus increasing availability. Similarly, migration of virtual disks among data stores (storage locations) is storage vMotion. vMotion and storage vMotion cannot be done simultaneously in powered on state.
7.	DRS (Distributed Resource Scheduler) and storage DRS	DRS is a feature that balances the compute resources within a cluster of physical hosts. Similarly, this balance between storage cluster is the storage DRS. VMware allows fully automated to manual balancing of resources.
8.	HA (High Availability)	HA feature allows VM to be restarted on any available host in case of initial host failure.
9.	FT (Fault Tolerance)	FT maintains a secondary copy of the primary VM and keeps the copy updated with the primary. In case of primary failure, the services are restored through secondary VM.

Table 2 Components of vSphere

### 3.3 Virtualized Datacenter Design

VMware virtualized datacenter provides virtualization at all layers of a datacenter which include compute, storage and networking [16]. vCenter server centrally manages the complete datacenter infrastructure for dynamic provisioning of services through VMs. Basic parts of virtual datacenter are briefly described in table 3.

No.	Component	Description
1.	ESXi Host	Physical servers on which VMM ESXi is installed for datacenter virtualization.
2.	Host Cluster	A number of ESXi hosts together forms cluster. The

		number of members in a cluster are based on the requirement of resources in a specific cluster
3.	Data stores and Storage Arrays	Different storage technologies including, SAN, NAS and iSCSI (Internet Small Computer System Interface) array are used for VMFS volumes. A data store is a combination of storage LUNs (Logical Unit Numbers) or NFS (Network File System) volumes for a particular host cluster.
4.	vCenter, vSphere and Web Client	Management tools for distribution and of hardware resources as well as administration of VMs.
5.	Virtual Networks	Different VLANs are configured on distributed vSwitch. This enables high capacity redundant networking.

Table 3 Components of Virtual Datacenter

Presently, VMware products are supported for X86 based processing architecture. ESXi along with storage network present a fully virtualized datacenter. Figure 3.1 presents a typical VMware datacenter architectural design.

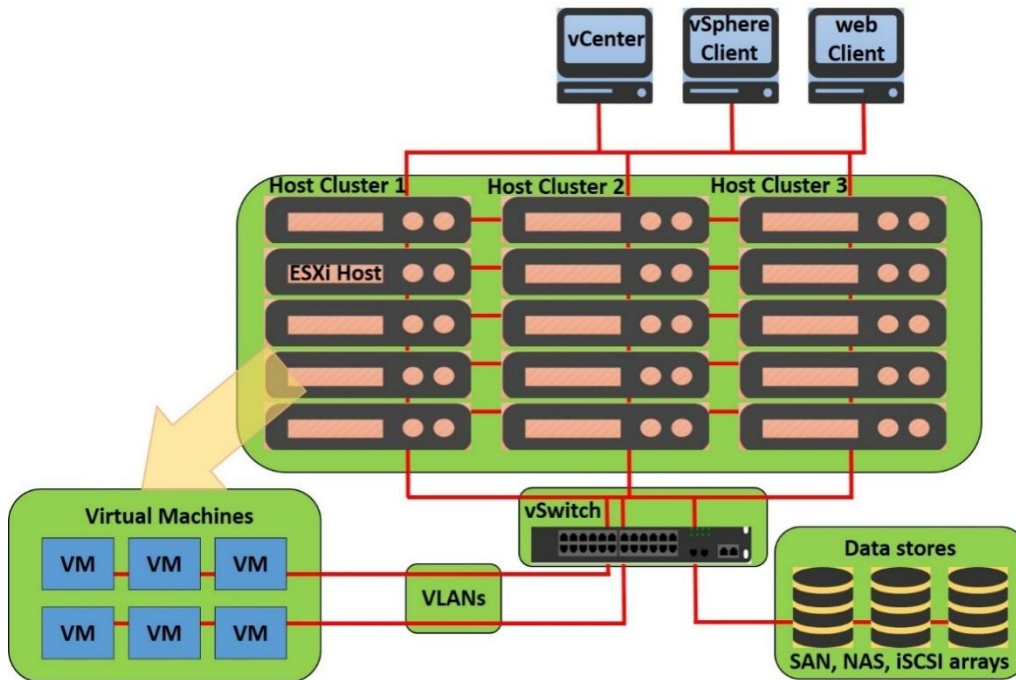


Figure 3.1 VMware Virtual Datacenter Design.

### 3.4 VMware Virtual Datacenter Features

vMotion, DRS, HA and FT are some of the most exciting features offered by VMware. These features enable reduced downtime and automated administration within enterprise datacenters.

### 3.4.1 vMotion

vMotion allows shifting of VMs between ESXi hosts at runtime. Virtual machines do not need to be powered off or make them unavailable from production as vMotion allows the shifting of VMs in powered on state. Functionality and services of virtual machine are not interrupted during migration. Whenever physical host requires maintenance, vMotion allows the transferring of all VMs underlying on that host to any other available hosts inside the cluster. In this way, no down time is required for routine maintenance of servers. vMotion is also utilized by various allied features of virtualization including DRS. Load balancing of VM on ESXi hosts is also carried out by using vMotion functionality. Performance metric is not affected during live migration of virtual machines. Figure 3.2 describes vMotion migration of VMs.

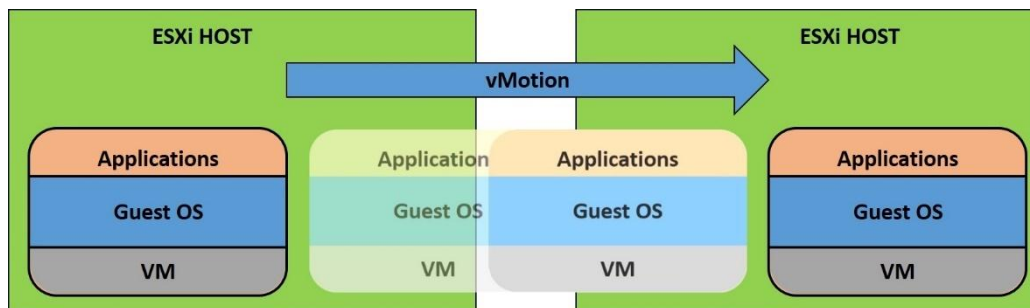


Figure 3.2 VMware vMotion.

### 3.4.2 Storage vMotion

Similar to vMotion, the storage vMotion has same functionality. This feature applies to storage. Simple vMotion shifts the compute resources of a VM within physical host whereas storage vMotion shifts the HDDs provided to a VM. This migration is also done without interruption of services. However, it must be noted that presently both, vMotion and storage vMotion cannot be done simultaneously at powered on state. Either each migration be carried out separately or the VM needs to be powered off for simultaneous migration. Figure 3.3 presents the storage vMotion.

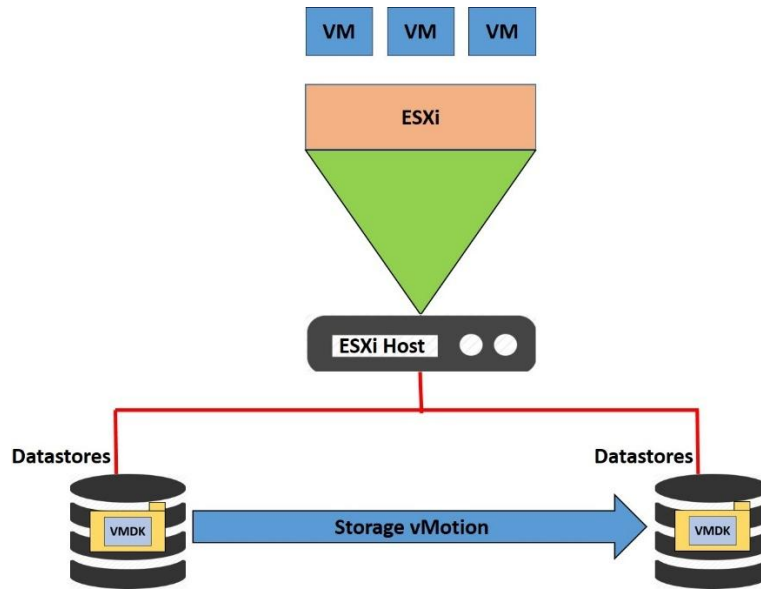


Figure 3.3 VMware Storage vMotion.

### 3.4.3 High Availability

High availability as name suggests is a feature that ensures maximum availability of VMs. This feature drastically reduces the downtime. In an event of a host failure, HA automatically migrates and restarts all the VMs on the failed hosts to any available ESXi hosts. VMs are restarted as the physical host on which they resided has become unavailable. These VMs are then started onto other available hosts which provide them the required compute resources. Figure 3.4 presents the HA feature of virtualization used in datacenters.

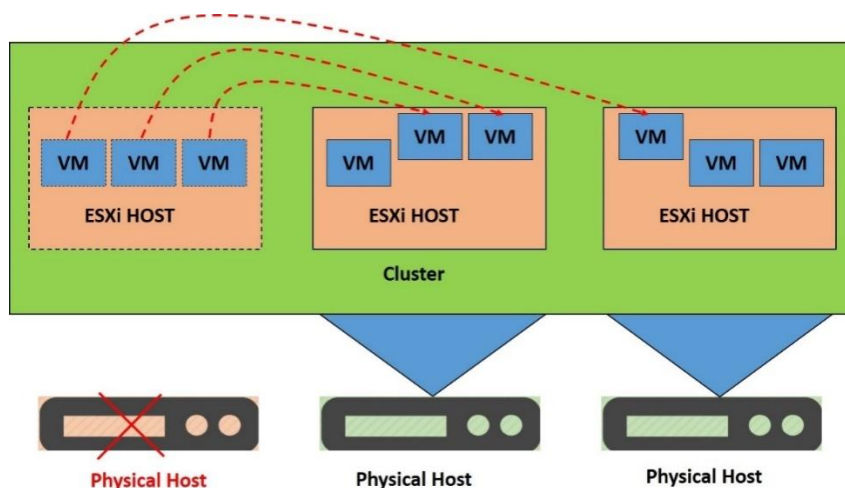


Figure 3.4 VMware High Availability

### 3.4.4 Fault Tolerance

Fault tolerance enables high availability of critical virtual machines within the datacenter, for example, AD (Active Directory). A copy of original VMs is maintained which is synchronized with the changes on the original VM. In a case of original VM failure, the

secondary copy is automatically made available for restoration of services as soon as possible. Figure 3.5 presents fault tolerance. Since both primary and secondary VMs are synchronized so reboot is not required in transfer of services from primary to secondary. FT logging keeps record of any event of primary failure and quickly shifts the services to secondary VM in case of any such event.

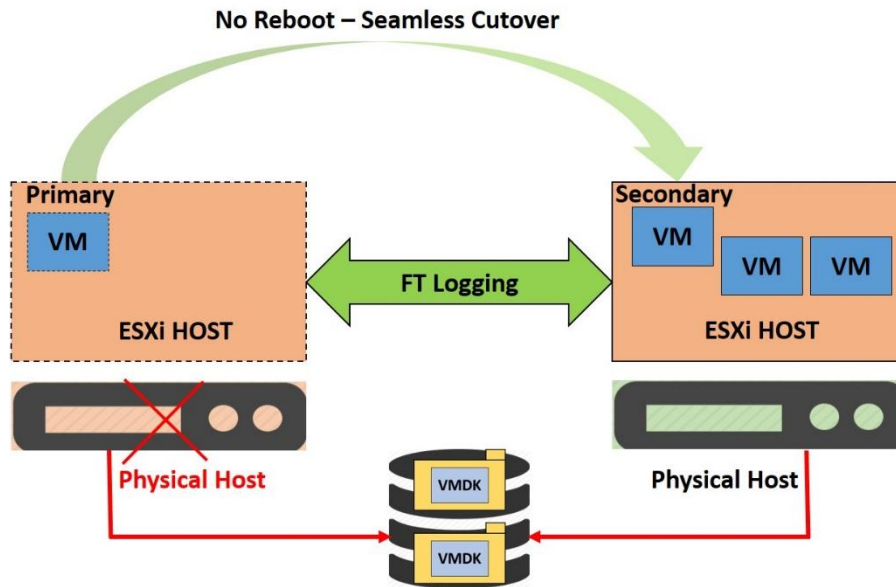


Figure 3.5 VMware Fault Tolerance

### 3.4.5 Distributed Resource Scheduler (DRS)

DRS uses vMotion technology to maintain balance among the cluster hosts. It ensures that hardware resources are equally distributed and no particular host is overworked. This maintenance of balance between hosts can be performed manually as well as fully automated operations. Figure 3.6 describes the DRS procedure.

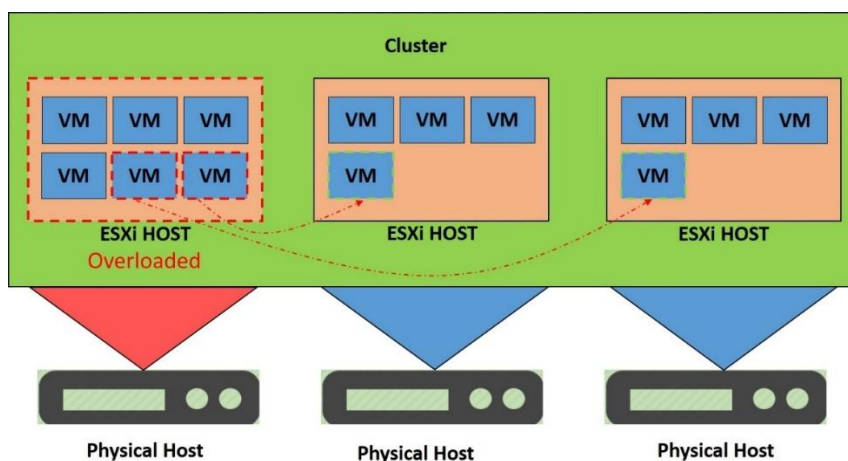


Figure 3.6 VMware Distributed Resource Scheduler

### 3.4.6 Storage DRS

Like DRS, storage DRS maintains balance between the data stores. If any data store is overloaded, then storage DRS migrates few of the VMs from that data store to any other which is available. Storage vMotion technology is used to perform the storage DRS. This feature can also be set manually or fully automated. Figure 3.7 presents the storage DRS process.

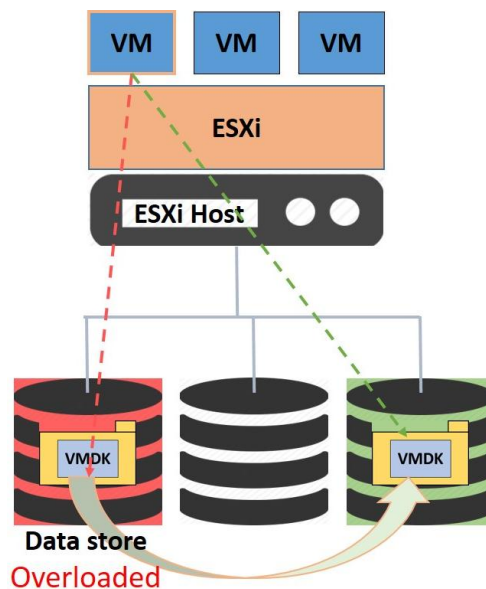


Figure 3.7 VMware Storage Distributed Resource Scheduler

### 3.4.7 Templates

VMware provides the facility to maintain a list of templates for creating VMs. Instead of installing OS from scratch on each VM, a template allows creation of VMs as an exact replica of the template. A VM of any particular OS may be created and all necessary configuration and software installation is done on that VM before saving as a template. VM copies of this template are created on requirement basis for service availability. This feature saves a lot of time for the administrator and a new fully configured running machine is created within minutes. Figure 3.8 presents the templates methodology.

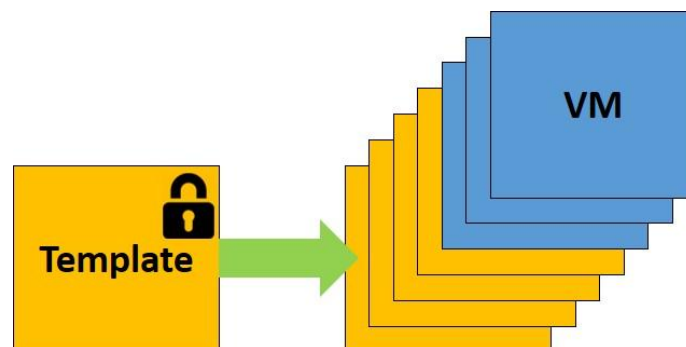


Figure 3.8 VMware Templates

### 3.4.8 Clones

Clones enable the creation of an exact replica a virtual machine. Clones are created especially when redundancy is required. A lot of administration time is saved by the feature of cloning the VMs. Same hardware specifications with replica of software already configured is created through cloning process. In fact, the newly created VM from cloning is the exact mirror image of the parent VM. This is also depicted in figure 3.9.

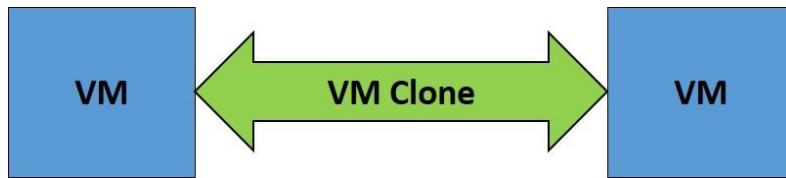


Figure 3.9 VMware Clone

### 3.4.9 Snapshots

Snapshots allow recovery or restoration points in case of software failures or VM crash. Snapshots are created at a fully working and configured point. Snapshots are restored when VM software fails and thus services are restored within seconds. This speedy recovery is very useful in case of troubleshooting. This is presented in figure 3.10.

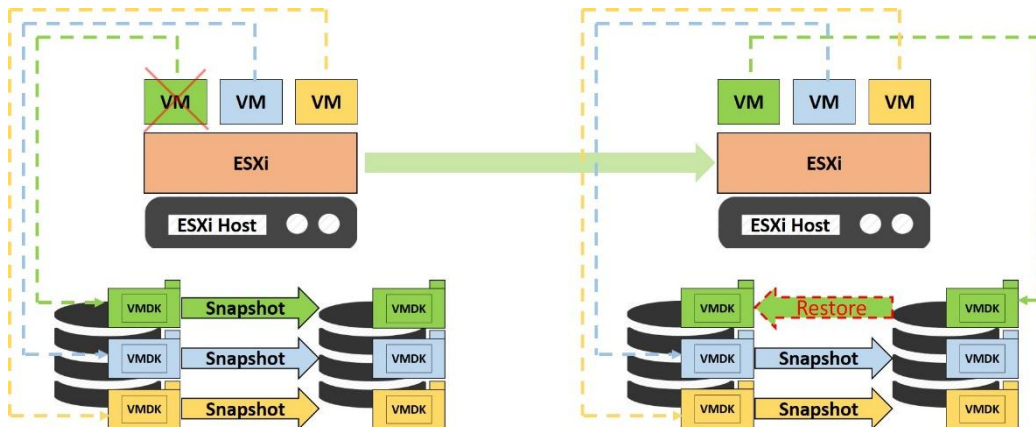


Figure 3.10 VMware Snapshots

## 3.5 Virtual Datacenter Network Design

Networking in virtual datacenter is functionally same as physical networks. The terms vNIC, vSwitch and port groups are widely used in VM networking. Each physical NIC of the physical host is virtualized as a standard vSwitch. Each VM in the physical host is assigned a virtual NIC with a distinct MAC (Media Access Control) address. This vNIC is connected to one of the available VLANs configured in the vSwitch as port group. Traffic from different network subnets is discrete and separated via distinct port groups. Outside world communicates with VM in exactly same manner as in physical environment, so



much so that an outside agent cannot identify if its communicating with a VM. Figure 3.11 present the network architecture in virtualized datacenter environments.

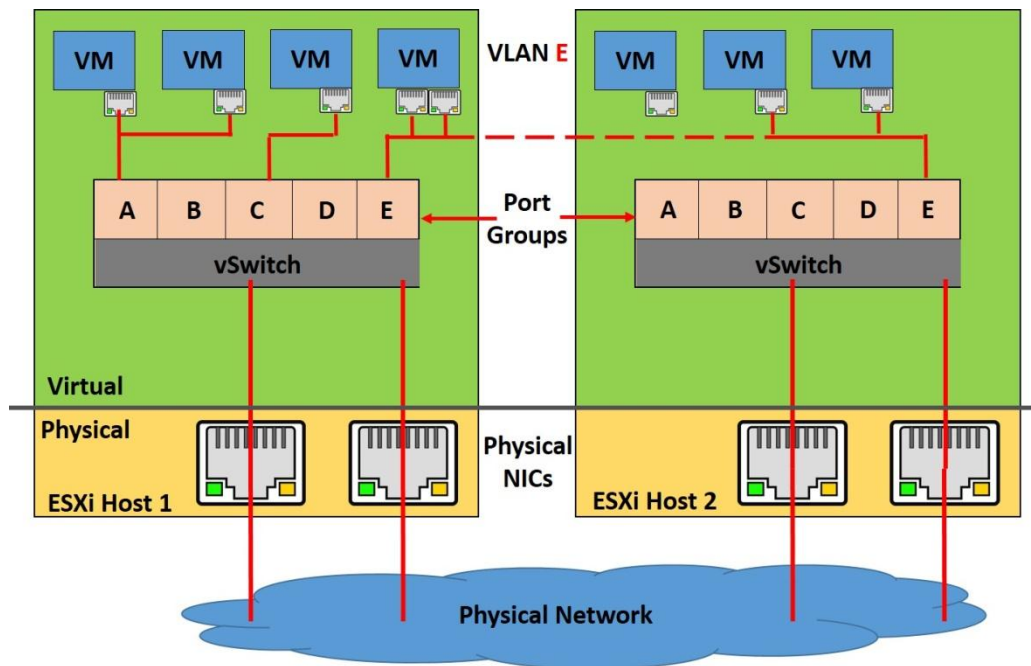


Figure 3.11 VMware Network Architecture

### 3.6 Virtual Datacenter Storage Design

SAN shares as LUNs are mounted on physical host via FC (Fibre Channel) or iSCSI. Where block storage is unavailable than storage can also be provided via Ethernet through NFS shares, however, this practice is not recommended for enterprise datacenters to avoid latency issues. These shares are mounted as VMFS volume in a data store. The data stores are managed and accessed through vCenter server. These data stores are the storage locations for virtual machines hard disks [16]. Each VM is disk-locked by the physical host on which it is powered on so that the same VM may not be powered on by any other host from the shared data stores. In an event of host failure, the disk lock is automatically released and the VMs can now be restarted on different physical hosts in the cluster. For oracle RAC (Real Application Cluster) environment, RDM (Raw Device Mapping) is supported on FC or iSCSI only. Some of the important files of VM HDD are shown in the table 4.

No.	File Extension	Purpose
1.	.log	Log file for troubleshooting
2.	.nvram	BIOS file
3.	.vmdk	VM HDD characteristics
4.	-flat.vmdk	VM HDD data

5.	.vmsd	Snapshots file
6.	.vmsn	Snapshot data
7.	.vmss	Suspend file
8.	.vswp	Swap file
9.	.vmx	Configuration file
10.	.vmxf	Configuration file

Table 4 Virtual Machine Associated Files

Storage virtualization is an incredible feature by VMware. It allows pool of different storage devices over a network to appear as a single aggregated storage resource. Disk management is enhanced due to maximum storage utilization capability and easy expansion. The storage architecture in a VMware virtualized datacenter is depicted in figure 3.12. Data stores are created from different storage devices over a network, whereas, VM users remain unaware of this distribution since storage is appearing in exactly similar fashion as in physical environments.

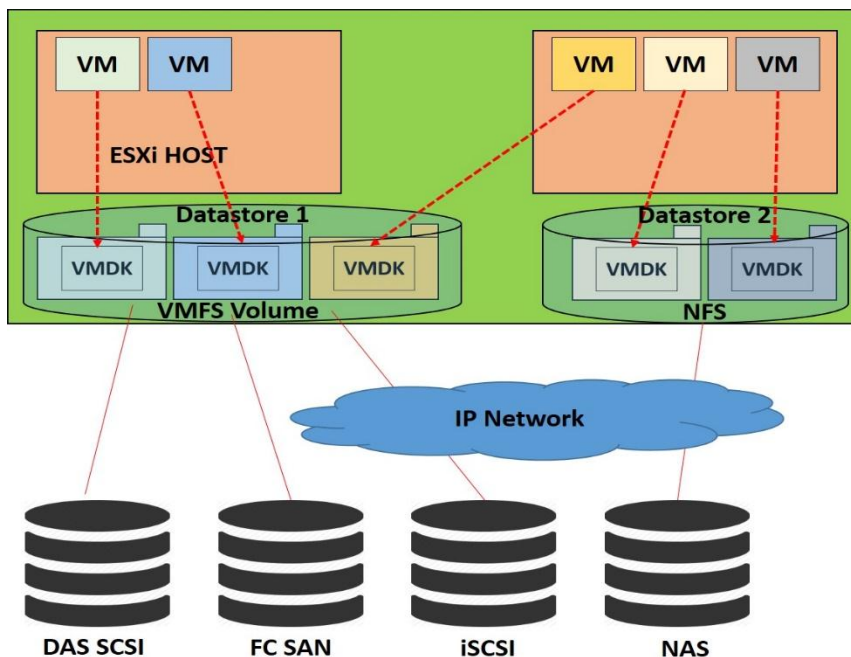


Figure 3.12 VMware Storage Architecture

### 3.7 vCenter Server

vCenter server is a centralized management tool that gives a complete picture of the datacenter including both physical and virtual resources. All physical hosts and data stores are connected to the vCenter server and a central management point is offered to the data center administrators. Administration becomes very efficient due to the flexibility and automation provided by the vCenter server. The flow diagram in figure 3.13 presents the basic vCenter functionality.

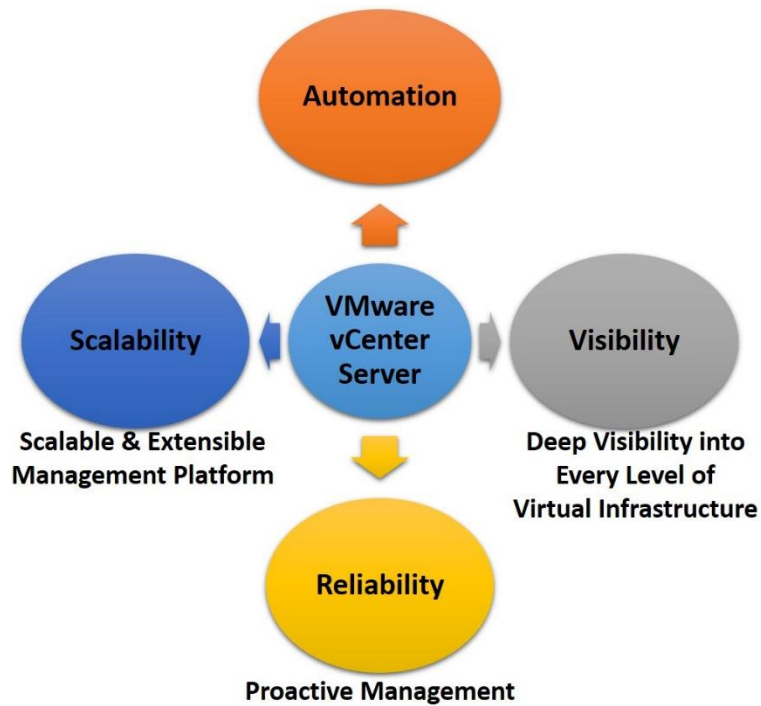


Figure 3.13 VMware vCenter Server Concept

vCenter server provides the statistical view of the resource utilization. All vSphere features including vMotion, DRS, HA, FT, clones, snapshots, templates, etc. are offered through vCenter server. Figure 3.14 presents the architectural design of vCenter server.

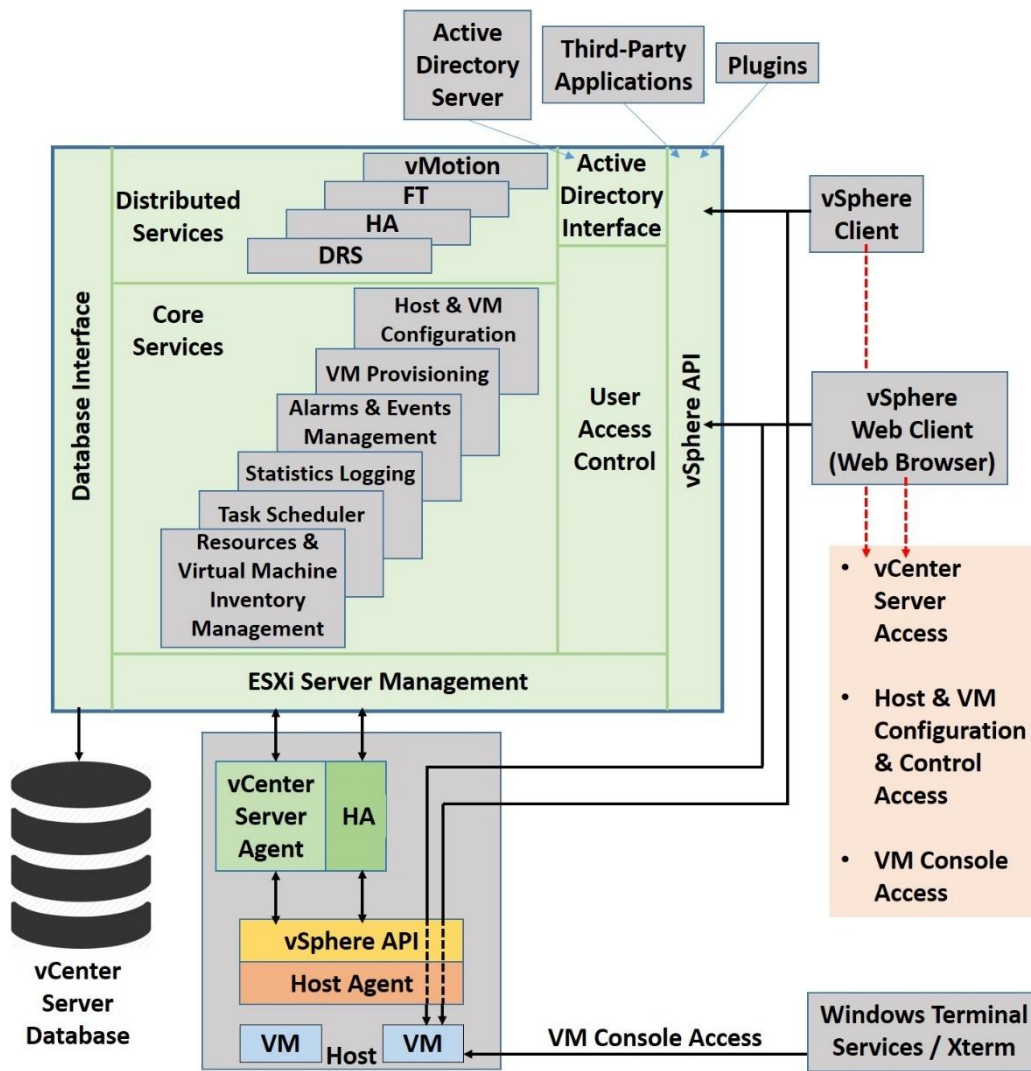


Figure 3.14 VMware vCenter Server Architecture

### 3.8 Chapter Summary

This chapter explains the concept and architecture of VMware virtualized datacenter. All major components of vSphere are discussed to understand the VMware virtualization terminologies. The datacenter virtualization design is described which explains the working of the datacenter. VMware datacenter virtualization offers many exciting features; all these features are described in the chapter. Then the virtual datacenter network and storage design architecture is explained thoroughly. This all gives an understanding of datacenter virtualization. Finally, vCenter server is explained with detailed emphasis on its architecture, since it is the core of virtualization management in datacenters.

### **4. Virtualization Security Risk and Vulnerabilities**

#### **4.1 Introduction**

With the advent of virtualization in datacenters, new attacks methods and exploits have also emerged. Traditional security threats to a physical IT environment are supplemented with new risk vectors specific to virtualization. This led to additional security requirements in the datacenters for addressing the virtualization specific security issues. This chapter describes some major security challenges involved in datacenter virtualization. An understanding of these vulnerabilities is very critical as this will lead to the formation of a complete security framework for virtualized environments. Overall, datacenter virtualization offers many new features for performance enhancement but at the same time new security challenges are also evolved that are needed to be addressed to avoid any major security event.

#### **4.2 Malware**

The term ‘Malware’ refers to any software whose functionality is hostile [17]. The purpose of such software programs is to illegally intrude or break the working of a legitimate program. Malwares can be used to steal confidential data, to degrade the integrity of data or to make data completely or partially unavailable. Malwares could be a script, a piece of executable code or all together a complete software. Malwares is a broader term used to categorize any type of software which has a malicious intent and can include all forms of viruses, worms, trojans, spywares, ad-wares, etc.

Virtualization is always conferred whenever there is a discussion of malwares due to the fact the VMs are always the prime choice of sandboxes for malware analysis. Virtualization technology offers unsurpassed isolation of virtual machines. A VM can work completely independent of its neighboring VMs. Similarly, in case of hosted virtualization, the VMs can work in isolation from the base OS. VMs can be reverted to previous working state whenever deemed necessary making virtualization suitable for malware examination test environments.

#### **4.3 VM-aware Malware**

It is a general perception that legitimate or malicious software cannot detect if they are running on a normal physical machine or VM. Moreover, users consider it insignificant to

find if they are working on virtual machine. However, presence of a virtual machine can be identified by different methods. Similarly, VM-aware malware can find if the host is a VM and as soon as it detects the existence of a VM, the malware can consequently modify its behaviour [18]. By adapting its functionality as per virtual environment, the malware can now either target the guest OS and applications or can directly attack the hypervisor as shown in figure 4.1.

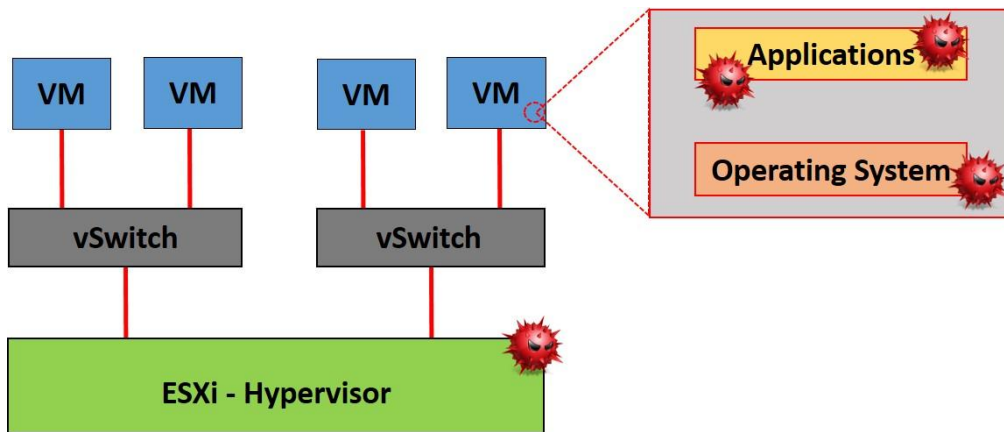


Figure 4.1 VM-aware Malware Targets

Various techniques allow malware to detect a VM presence underneath, some of which are as following:

1. Identifying the vendor software by analyzing MAC addresses of vNIC.
2. Identifying virtualization specific registry entries.
3. Identifying the installation and configuration of VMware tools on guest OS.
4. Identifying virtualization specific services, ports and processes.

**Rebhip** is a dangerous window based worm that can spread usually via removable drives and can steal confidential data and PII (Personally Identifiable Information) [19]. It can detect the presence of a VMware virtual machine by means of backdoor I/O (port name 'VX') which is used by VMware to communicate with the underlying VMs. Various operations on this port can be read to identify the presence of VM, for example 0x0A is used for VMware version [20]. Backdoor functions can be invoked as shown in the following example.

```
MOV EAX, 'VMXh'/*magic number */
MOV EBX, 3C6CF712h/*command-specific perimeter*/
MOV ECX, 10/* backdoor command number */
MOV DX, 'VX'/* VMware I/O port */
IN EAX, DX/*or OUT DX, EAX */
MOV EAX, 1
```

EBX value define the VMware product type:

01h = Express

02h = ESX Server

03h = GSX Server

04h = Workstation

Symantec's statistical data in graphical figure 4.2 illustrates the percentage of malware that successfully detected VMware VMs in last two years [30].

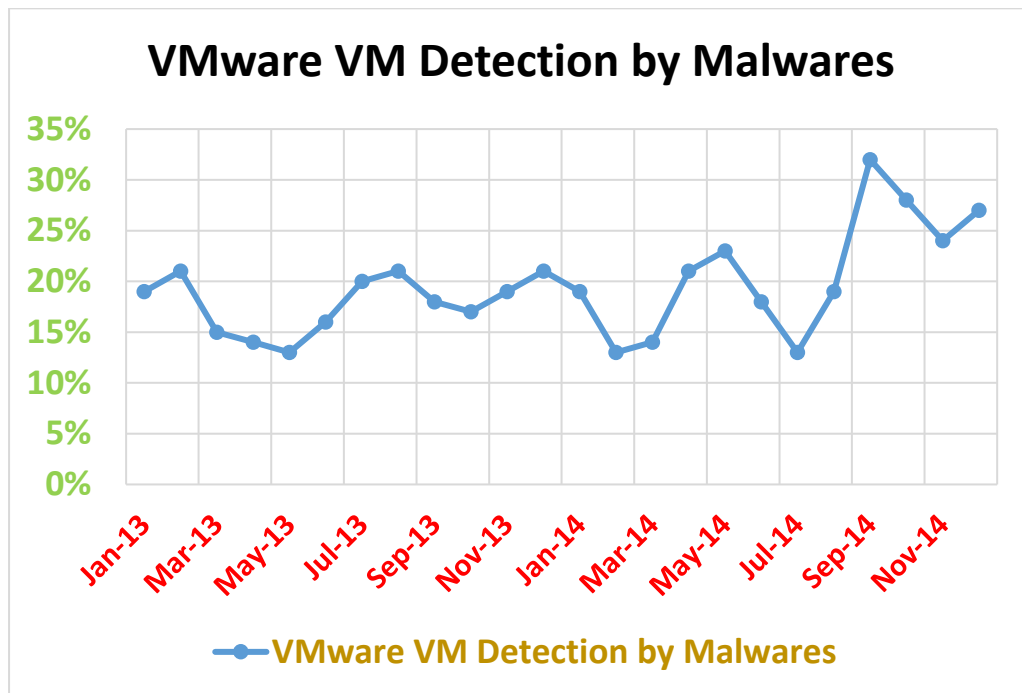


Figure 4.2 Successful VMware VMs detection by Malware in Two Years

This shows that although the success rate of VM detection is not major but a virtual machine needs to be properly safeguarded for protection against malicious programs and security risks.

VM-aware malwares can identify the virtual environment due to differences between the execution and working of a physical and virtual operations. Presently, virtualization technology is not developed with transparent visibility and the significant variances in virtualization implementation as compared to physical environment is due to prime focus on high performance and availability. Although large number of enterprises have been shifting or already shifted to datacenter virtualization and most recent malwares are designed with the presumption that the target machines are running on virtual environment.

#### 4.4 VM-based Malware

VM-based malwares also known as VMBR (Virtual Machine-Based Rootkits) are more complex and the impact level of a successful attacks can be drastic. These malwares are

basically a new generation of rootkits which have the ability to hide themselves by virtualizing the target machine and gaining kernel level access of physical resources, all without the knowledge of system's legitimate users [21]. Although administrator or root privileges are required for rootkit installation, however, various techniques can be utilized by the attacker to attain these rights.

**'SubVirt'** was designed as a PoC (proof-of-concept) to attack virtualization. This malware reboots the target system after infection and installs a hypervisor layer underneath. The rootkit now migrates and launches the original OS inside a VM. SubVirt does this by changing the boot sequence so that MBR (Master Boot Record) boots VMM instead of the original OS. The rootkit is very difficult to detect or terminate, since it is installed below the infected OS level. Now all OS interrupts to physical hardware will be via rootkit VMM. SubVirt uses VirtualPC in Windows systems and VMware in Linux system as its hypervisor [22].

**'BluePill'** is another VMM developed by Joanna Rutkowska. Blue Pill exploits the virtualization techniques of AMD-V and Intel VT-x processor technology. It installs a thin layer of VMM and migrates the OS onto a VM, while the OS still assumes that it is running on physical environment [23]. It is very difficult to detect BluePill due to its customized hypervisor with minor footprint. The same developer also designed **'Red Pill'** which contrary to Blue Pill is a technique to detect the presence of VM [24]. The titles are in fact, a credit to the red pill and blue idea from motion picture, The Matrix.

Similarly, a rootkit named **'Vitriol'** removes the direct access of OS to physical hardware and transfers this access to VMs via hardware virtualization [25].

The working of these rootkits is summarized in four steps:

1. Rootkit infects and gains kernel level privileged access on the target system.
2. After successful infection, rootkit VMM is installed underneath the original OS and some memory required for execution of hypervisor processes is reserved.
3. Originally installed OS is migrated and launched by the rootkit VMM inside a new virtual machine.
4. Rootkit VMM has complete visibility of VM operations and explores and intercepts any privileged system interrupts executed by the OS.

This procedure is also presented in figure 4.3.



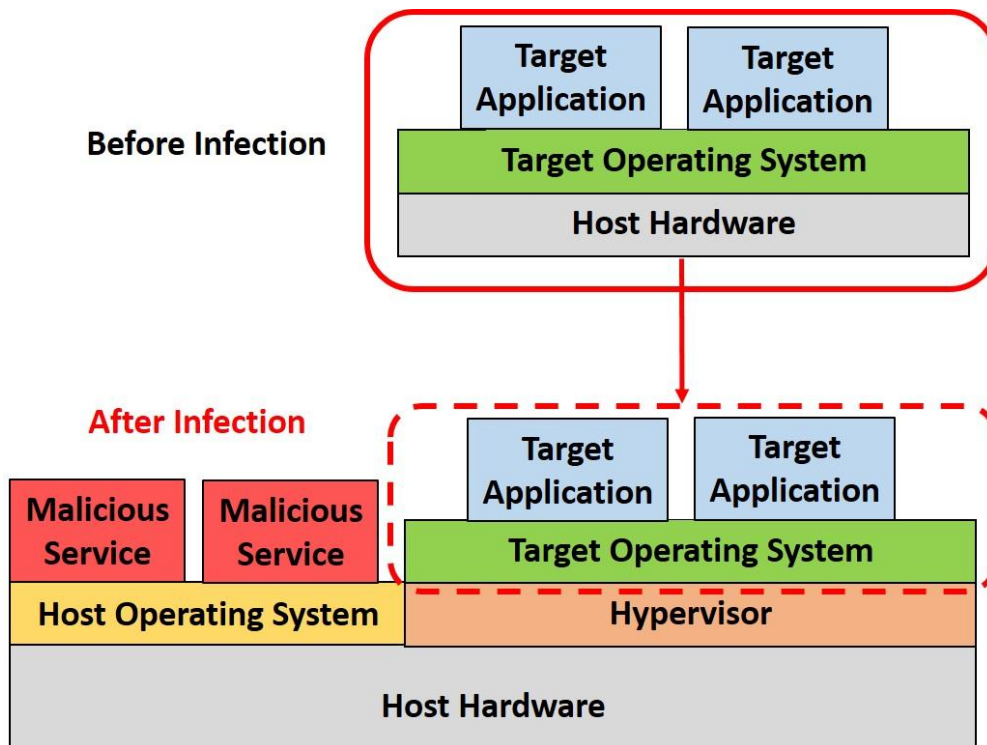


Figure 4.3 VM-Based Rootkit Operation

The main cause of success of these malwares is due to the presence of virtualization footprint in registry and system processes. Till now both VM-aware and VM-based malwares are prototypes or at proof of concept stage, however, this is expected to change in near future. Successful attack of these malware can be highly damaging to production environment and thus proper security of and system safeguarding needs to implemented against such threats.

## 4.5 Network

Where virtualization offers many state-of-the-art benefits it also introduces some potential security concerns. Networking is the backbone of any IT environment and needs to be secured at all costs. Some major network threat in virtualization are discussed below.

### 4.5.1 VM Sprawl

Lack of efficient administration and management can lead to large quantity of VMs in the datacenter. Administrators from different tiers in the datacenter can create additional VMs in the network to meet availability requirements without following appropriate authorization, resulting to VM sprawl [26]. Virtualization sprawl occurs when the number of VMs in the virtualization setups exceeds effective management by system administrator. Large number of VMs in the network without proper control will result in shortage of hardware resources. Resource pool will reach its limit by distributing the resources to

considerably insignificant virtual machines. Moreover, virtual machine application latency can arise due to virtualization sprawl in the network.

#### **4.5.2 Transient VMs in the Network**

One of the major security concern in datacenter virtualization is the presence of transient VMs inside the network. These temporary VMs exist due to the virtualization flexibility which enables them to become available in production without any authorization. In legacy environments, a security event is controlled by initially identifying the origin of malwares followed by managing its impact through security patches in the static systems or any other provisional measure. The datacenter network is effectively brought back to original state after addressing the security event.

On the other hand, virtual environments are dynamic in nature due to scalability and flexibility. In a highly populated datacenter, transient VMs may start for small duration especially during peak hours. If a transient VM is infected, it is possible that during its next launch it may infect other machines in the network and power-off after small period of time. This makes the origin of infection very difficult to locate for the administrators. This deficiency of traceability in virtualization is very appealing for the attackers for covering their tracks. An attacker can launch attacks inside or outside the datacenter network from a VM and afterwards simply powers off the machine while avoiding accountability of actions efficiently. This dynamic nature of datacenters makes it very tough for implementing security updates and patches in complete enterprise IT setups, thus leaving the datacenter networks to be vulnerable [27].

#### **4.5.3 Compromise of Centralized Management Software**

One of the major threat to datacenter virtualization is the compromise of the central management tool. A successful attack to the centralized management gives the attack full visibility and access to the complete virtual datacenter. An illegal access to VMware vCenter server can allow attackers to perform anything inside the network, from stealing confidential data to complete disruption of services. However, in properly design virtual datacenter, the management network is usually kept isolated through VPNs (Virtual Private Networks) and extra layers of security are implemented, making the management server very difficult to infect.

#### **4.5.4 Unavailability of Complete vSwitch due to Failure of Physical NIC**

Virtualization converts the physical network adapters of the host to virtual switch. Several VLANs are configured on the virtual switch for making the requisite network availability to corresponding VMs on the host. Complete network traffic of the physical host to its

underlying VMs passes through this NIC. Hardware failure of the network adapter in this scenario can have drastic implications as all VLANs configured on the vSwitch will become unreachable and corresponding VMs will have network inaccessibility.

#### **4.5.5 VM Intercommunication**

The VMs intercommunicate with each other through embedded virtual switches but the problem in this case is that these software switches add extra overhead if the number of configured VLANs is large and accordingly number of VMs communicating on these VLANs is very high. This can result in network latency if network traffic on a vSwitch exceeds the limits of physical NIC. Moreover, network administrators have very limited visibility and control on the internal VM network for troubleshooting [28]. Although latest virtualization platforms offer network virtualization for this deficiency but it is still emerging and highly expensive.

### **4.6 Virtualization Software Inherited Threats**

Virtualization has revolutionized IT culture with undeniable benefits but there is always a backdrop. Virtualization software are usually closed source and customers are bound to use the vendor software without customization. Developing a software today without potential vulnerabilities is next to impossible and regular security updates are offered as a remedy. However, the impact of vulnerability in a virtualization software is very high as compared to other software. This is due to the fact that any such vulnerability when exploited cannot only compromise the hypervisor layer but also the underlying VMs are affected [29]. The implications are even higher if one of the affected VM is also functioning as a centralized management software.

#### **4.6.1 VM Escape and Hyper-jacking**

VM escape is a serious exploit that depends on virtualization software flaws. In VM escape, the attacker launches some malicious code on VM due to which the guest OS breaks its functionality and can now directly interact with the VMM. Resultantly, the attacker gains access to the hypervisor and all corresponding virtual machines. This phenomenon of compromising VMM by exploiting VM escape is known as hyper-jacking [31].

**CVE-2008-0923** is one such vulnerability developed for VMware that could allow VM escape in Workstation version 5 and 6. **Cloudburst** is another VMware vulnerability which is due to buffer overflow in video memory provided to VM.

VM escape exploits were also identified for Oracle VirtualBox, Xen and QEMU.

‘Venom’ is a dangerous VM escape exploit that compromises Xen and QEMU by utilizing buffer over flow in virtual floppy disk controller. VM Escape process is presented in figure 4.4.

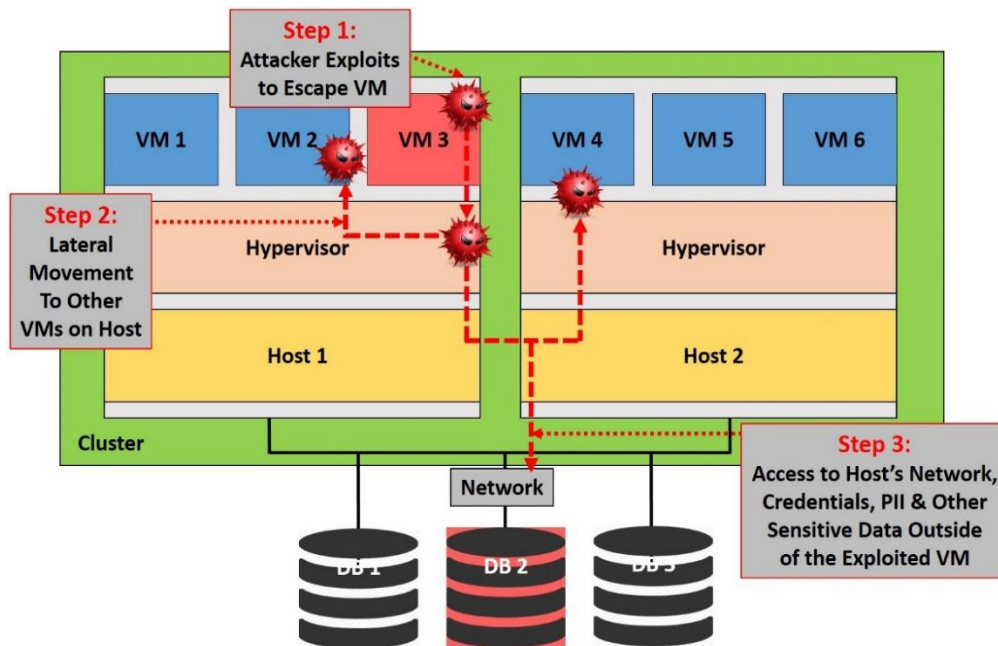


Figure 4.4 VM Escape

Times have gone by in IT revolution and it is now an acceptable circumstance that malware will continue to develop for detecting and exploiting vulnerabilities in software and virtualization is no exception. Complement to traditional software threats, an additional layer of hypervisor bugs is supplemented. Some of the malwares associated with virtualization have already been presented in section 4.2. Efforts are being made by vendors to make their virtualization offers to be highly secured in order to maintain user confidence and meet customer satisfaction. Regular version updates and security patches are released and organization need to implement these updates as soon as they are available. Datacenter virtualization security design is very critical in this regard and needs to be given utmost efforts in employing fool proof security in enterprises.

## 4.7 Management

Virtualization immersion in enterprises has also altered the management operations of datacenters. Additional hardware and human resources are required for smooth functionality of services. This change in management procedures accordingly introduces additional security risks in IT environments.

### 4.7.1 Administration Overhead

Virtualization is an exceptional leap in IT setups. A whole new layer of hypervisor is added between the host and the virtual machine, yet the administration, functionality and

maintenance of VMs is exactly similar to that of physical machines. Administrators of a specific domain (e.g. database) do not, necessarily need to acquire new skills for performing their routine administration and configuration tasks for service availability as their employed operations remain unaffected. However, introduction of a new tier of virtualization requires additional virtualization domain admins. These administrators not only need to have professional virtualization skills but also general expertise in all other datacenter domain as well for efficient and effective availability of services. Subsequently, administration overhead is reasonably increased.

#### **4.7.2 Additional Threats from Virtualization Enhanced Features**

Extraordinary features of virtualization although make datacenter functionality flexible and efficient but at the same time some of these features can introduce serious security concerns. One such feature is the creation of **templates**. Template is an image of a fully configured OS instance with requisite applications installed. Sensitive and confidential data may also be kept in these templates. An intruder now does not need to attack a working VM with security implemented on it. Rather, same intruder can copy the template file and generate VMs from it in a separate environment altogether, thus successfully stealing confidential data while effectively remaining untraceable. Same threat is true for **snapshots** and **offline redundant VMs** in the environment.

#### **4.7.3 Challenging Security Requirements**

Security in traditional datacenters has been addressed with detailed policies, procedures and guidelines in every tier. Although it can never be claimed that a particular IT setup is 100% secure and free from any security risks, however, a lot of efforts have already been made in making datacenter security to be considered as acceptable. Presently, securing a legacy physical environment has been recognized as a common and an established task. In case of a physical server, hardware peripherals are controlled by a single operating system which run only a required number of applications and thus can be effectively secured. However, virtual environments are fairly complex in this regard. Hardware resources are now distributed dynamically via VMM to a variety of OS instances with number of applications. NICs are converted to vSwitches and serve a number of different networks. Also, visibility of internal working of virtualization is also very limited. This diverse and multipart functioning of virtualization technology makes security a severely challenging and heavily demanding job.

#### 4.7.4 Rollback Threats

Recovery to previous state from snapshot can be risky in a sense that system is restored to state where latest security patches have not been applied [8] [32]. Although immediate problem is resolved by restoration process but the VM is now more vulnerable to malware attacks.

#### 4.8 Auditing and Compliance

Enterprises are bound to provide services in accordance with regulatory compliance and can be directed to internal or external audits. However, virtualization features can provide a loophole. In case of any event not in accordance with compliance regulations, the administrators can roll back later to original condition and can effectively escape from audit [33].

Additionally, several crypto procedures are based on generating seeds from device configuration, in order to get hashes and nonce. These cryptographic algorithms are based on generating unique seeds for ensuring integrity, however, if a VM is reverted to a previous state then a previously used seed could be regenerated making the authenticity of implemented cryptographic solution questionable.

#### 4.9 Chapter Summary

This chapter presented detailed security risks in virtualization environments. Virtualization setups are prone to both traditional security risk present in legacy datacenters and virtualization specific threats. Different types of malware especially designed for virtualization have been presented including VM-aware and VM-based. Then risk to virtualization networking are described. Network is prone to security threats from VM sprawls and transient VMs. Also, Centralized management software compromise can make the entire network vulnerable. Moreover, unavailability of NIC can bring a number of networks to be inaccessible through vSwitch. In addition to network threat, there are many new threats introduced due to inherited flaws in hypervisor or virtualization software.

Finally, several new security risks are introduced in the management operations of datacenters. Administration overhead is increased. Many virtualization features supplement to providing better functionality also introduce security risk. Resultantly, new and complex security requirements are needed.

Another issue in virtualization is the loophole which allow to avoid auditing and regulatory compliance. Inherited rollback feature is one such technology that can be carefully used in this scenario. Overall, virtualization offers unique and remarkable benefits in running IT

services but at the same time is not safe from security risk. A deliberate effort is required for planning an effective and acceptable virtualized datacenter security design.

## 5. Research Methodology

### 5.1 Introduction

This chapter pertains to research methodology and explains how a traditional mini datacenter is setup, virtualized and ready for security implementation. Initially, two Juniper Firewalls (SRX-650) and three 3iSys Switches are configured. Separate VLANs have been configured for distinct services and the Ethernet port mode was set to trunk. Two Huawei RH2288A servers are used for system services. These servers were virtualized with VMware ESXi and vCenter server version 6. The version used was latest available at the time of research. Huawei SAN is configured as storage for VMs through NFS. HA was ensured at all tiers and traditional datacenter security was applied at network firewall and system services. Ethernet services are used in this research, however in production environments, network and storage is provided via FC. Besides a VM for vCenter, additional VMs were created for AD, Database, and Application services which form the fundamental tiers in any datacenter. High level design of this datacenter is shown in figure 5.1

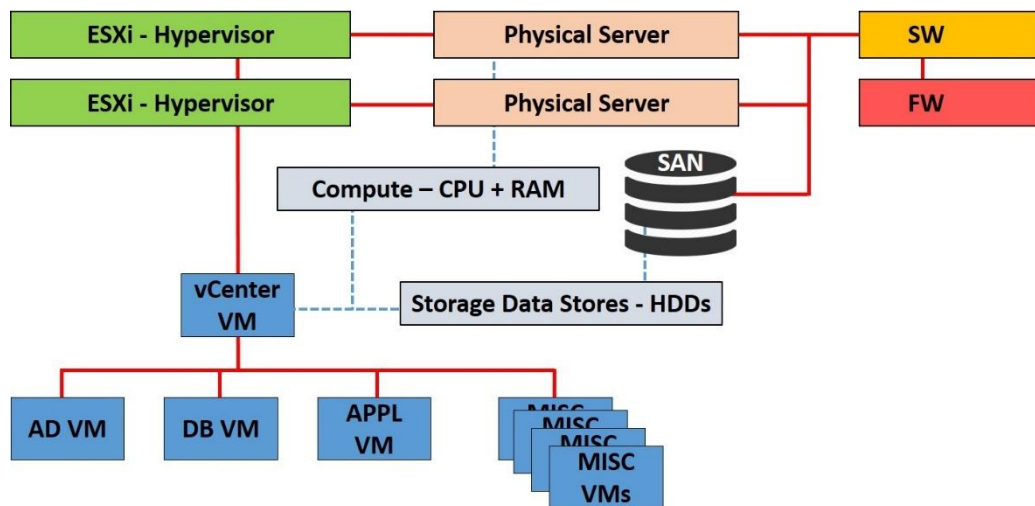


Figure 5.1 High Level Virtualized Datacenter Design

All devices are connected with AD for authentication services. In addition, the DNS (Domain Name System) and NTP (Network Time Protocol) services are also configured on AD. Oracle DB is used for database services and applications are deployed on Application servers. Several supplementary VMs are also created for miscellaneous services in datacenter.



## 5.2 Virtualized Datacenter Hardware

Hardware used for establishing a virtualized datacenter is described here. All devices used in this research are modern IT equipment, providing redundancy in their services. These devices are extensively used in various production datacenters.

## 5.3 Network Devices

Hardware used in this research for networking is from Juniper and 3ISYS.

### 5.3.1 Juniper SRX 650 Firewall

This firewall is suitable for middle range enterprise networks and is highly efficient and cost-effective in providing network and gateway services, scalability, routing integration and security protocols.

### 5.3.2 3ISYS CS5500 Switch

This network switch is an enterprise level datacenter device which is very effective for gigabit networks. It provides efficient VLAN functionality and improved QoS. Link aggregation and some security controls are available in this switch.

## 5.4 System Devices

Details of system devices are described here.

### 5.4.1 Huawei RH2288A V2 Server

This a rack mounted server which provides high performance, smart power control, efficient management, flexible maintenance and intelligent storage expansion. This server is common choice for customers having mid-range enterprise environments.

### 5.4.2 Huawei SAN – OceanStor S2600T

This SAN is widely used in enterprise environments due to its broad variety of features including virtualization support, SAN and NAS integration and efficient management of data and backups.

## 5.5 Virtualized Datacenter Software

### 5.5.1 OS

Windows Server 2008 R2 and RHEL (Red Hat Enterprise Linux) 6.2 have been used in different VMs. Active Directory has been configured on Windows OS. Linux OS has been used for DB and Application Servers.

### 5.5.2 Virtualization

VMware ESXi 6 has been used as hypervisor for virtualization and vCenter Server 6 has been used as managing tool for virtualized data center. In addition, vRealize Operations Manager 6 has been used as monitoring tool for virtualization.

## 5.6 Virtualized Datacenter Setup

A virtualized datacenter has been established using VMware. A firewall and switch was configured with traditional security settings in place. ACL (Access Control List) is defined on the firewall and distinct VLANs are configured on the switch for unique services or tiers. Huawei storage has been configured for provisioning of storage services. All hard disks for VMs are provided through this storage. Storage data stores are configured and mounted on through NFS protocol over Ethernet. Finally, 2 Huawei servers have been configured for creating a virtualized datacenter. Step by step deployments of developing a virtualized datacenter are described below.

### 5.6.1 Establishing Infrastructure

Infrastructure is the fundamental area of any technical setup. Details of infrastructure are beyond the scope of this research; however, essentials are described here.

For power arrangements, 10 KVA APC UPS with 4 battery modules has been setup for stable power supply where as a backup generator of 50 KVA is in place. Two APC racks are installed for mounting of hardware devices. Cooling requirements of the datacenter are met by installing two standard split air conditioners.

Redundant power and cooling requirements are deployed in the datacenter to avoid infrastructure events.

### 5.6.2 Establishing Physical Network

After establishing datacenter infrastructure, the next phase involves setting up of physical network. Juniper SRX 650 Firewall has been configured as datacenter core device for controlling network traffic and implementing traditional network security protocols and ACLs.

Then a 3ISYS CS5500 switch is installed as core switch. All VLANs are defined on this switch for segregating distinct network traffic. Since virtualization is being implemented so the Ethernet port on which VLANs are defined is set to trunk mode. This will enable all traffic to pass through this port simultaneously with unique VLAN ID in packet header for segregation.

Trunk mode is always beneficial in case of virtualization because each physical NIC is converted to a virtual switch by ESXi. Also, limited amount of NICs and large number of VLANs make the trunk mode choice to be suitable. Additionally, less cabling is involved in this approach. However, network bandwidth must be kept in mind while establishing this network.

### **5.6.3 Storage Configuration**

Huawei OceanStor S2600T is deployed as storage for provisioning of data stores for VMs. The data stores can be mounted as LUNs over FC. Same LUNs can also be mounted over Ethernet via iSCSI. Another method for providing storage for data stores is through NFS. This method is used via Ethernet in this research as PoC, however, production environments generally do not use this technique. Storage is mounted as NFS share on each physical server in the vCenter. This NFS share is available as data stores for providing HDDs to the VMs.

It is pertinent to mention here that local storage of physical servers is not utilized here. This is due to the fact that vMotion requires shared storage. Thus, in case of any event or disaster to the physical server, the data is still secured. VMs are then simply migrated to any other available physical server for compute resources. HDDs of VMs being stored on SAN are accordingly available to the new physical server and services are easily restored. The size of data store directly depends on the available storage. Storage can be made available in two techniques. Either configure a large data stores of fewer number or configure small data stores in large quantity. Efficient disk is utilized in case of larger data stores but performance wise the latter option is considered to be more appropriate. In this research, two data stores of 2TB have been mounted on physical servers.

### **5.6.4 Server Configuration**

Two Huawei RH2288A V2 servers are used in the datacenter virtualization in this research. The servers used in this research have 2 Intel Xeon 2.5GHz Quad Core processors along with 128GB of RAM. 2 500GB HDDs are installed. Both memory and storage can be enhanced as per requirements.

### **5.6.5 LOMConfiguration - iBMC**

Initially, LOM (Lights Out Manager) called iBMC (Intelligent Baseboard Management Controller) of both servers is configured. This involves assigning IP address to the management console and setting up of login credentials. Furthermore, iBMC is used to check the overall physical hardware of the server. All alarms and warnings can be monitored through this console. Figure 5.2 shows the iBMC console homepage.

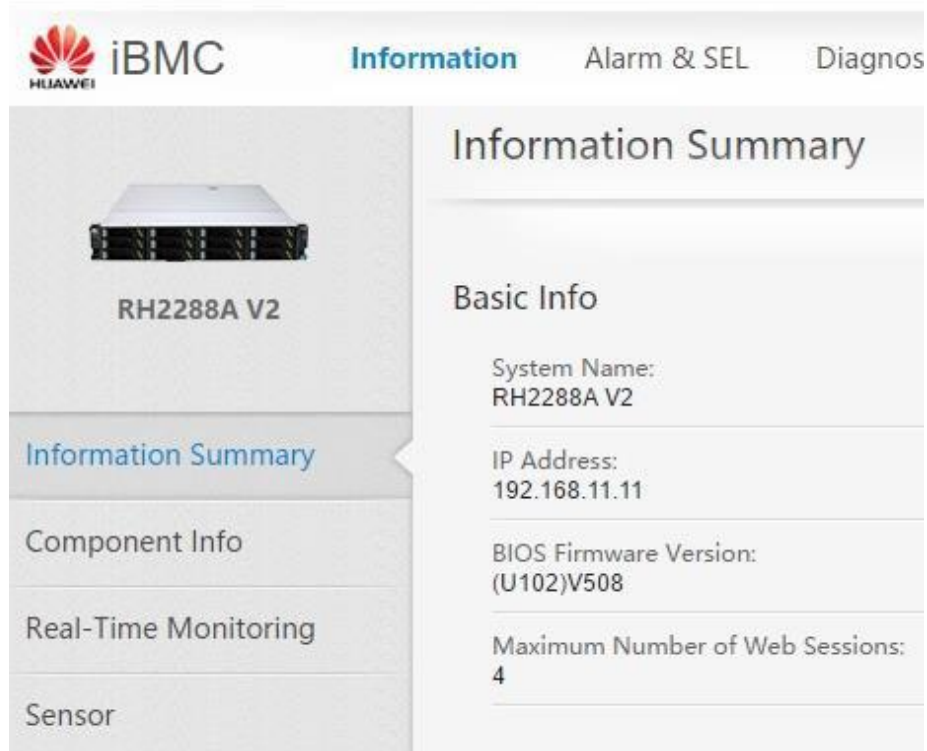


Figure 5.2 Huawei RH2288A V2 iBMC

iBMC is now accessible over the network via the management NIC. This NIC is independent of the physical NICs that are available with servers. These physical NICs are used for network traffic.

### 5.6.6 RAID Configuration

The servers are now powered on from the management console or iBMC. At first startup, RAID of the local HDDs of these servers is configured as a one-time measure. These servers are available with two 500GB SATA. RAID 1 is configured on the HDDs for data replication and redundancy.

After initial setup of LOM and RAID, the servers are now ready for deployment. Traditionally OS is installed at this step, however in case of virtualization, this step is replaced by installation of hypervisor.

### 5.6.7 Server Virtualization

All virtualization pre-requisites are met at this stage and both physical servers are now available for server virtualization and thus leading to the establishing of a virtualized datacenter.

### 5.6.8 ESXi Installation

VMware hypervisor software called ESXi version 6 is now configured on both Huawei servers. The version used was the latest available version at the time of this research. ESXi installation involves assigning of IP address for availability over the network via vSphere

Client. In addition to networking assignment, the ESXi login credentials are also set at the end of installation. Since the Huawei server consists of two quad core processors so we have eight logical CPU units as processing resource while almost complete 128GB of memory for VMs.

### **5.6.9 vSphere Client**

After ESXi is installed, the servers can now be accessed over the network via the IP address and login credentials that are setup during ESXi installation. vSphere client is a Windows OS based software which provides a holistic view of the physical servers. All compute, storage and network resources of the machine are visible and VMs can now be created based on the available resources.

### **5.6.10 Network Configuration**

After accessing the server through vSphere client, the next step involves network configuration. ESXi installation has converted the physical Ethernet card into a virtual switch. By default; this switch is a 128-port virtual switch, however the number of ports can be increased as per requirements. All VLANs created in the 3ISYS switch are now defined on this virtual switch as well for completing the network flow. These newly created VLANs can now be assigned to the corresponding VMs and, thus, VMs would be available over the network.

### **5.6.11 Storage Configuration**

The next step is the configuration of storage and availability of data stores to the physical servers. These data stores would be hosting the HDDs of all the VMs in the virtual data center. The data stores must be available to all the physical servers so that vMotion is supported. The data stores are created by providing storage shares from Huawei SAN via Ethernet as NFS shares. Two data stores of 2TB each are mounted on both servers for meeting storage requirements of VMs.

Access control can be implemented on data stores. The visibility of a particular data store can be restricted between ESXi host clusters. Each of the created data store is available to both of the physical hosts.

### **5.6.12 Management Server VM**

The virtualization environment is now ready after the completion of network and storage configuration. It is at this stage when VMs can be created and services can be provided through virtualization.

The first VM created is a management server for routine management and administration of the datacenter. The VM constitutes of 8GB RAM and 2 CPU units. Windows Server

2008 R2 has been installed and all management software including vSphere client is installed on the management servers. From this point, onwards, all management and administration is done from this management server only. Management VLAN is defined in the networking and has been assigned accordingly to the vNIC of the management server.

### **5.6.13 Active Directory**

AD is the most important machine in any data center and is regarded as the core of system. Accordingly, the second VM is created for providing authentication and directory services. Supplement to these, the feature of DNS and NTP is also configured on the AD. Windows Server 2008 R2 OS is installed on a VM created for AD whose specifications are 8GB memory, 40 GB HDD and 2 CPUs.

After setting up of AD, all VMs, physical servers and datacenter devices are connected with it for authentication, time synchronization and DNS services.

### **5.6.14 vCenter Server**

The next major step is deployment of vCenter server. VMware offers vCenter server to be deployed from a setup or from a pre-configured template. In this research, vCenter Server version 6 is deployed from the setup on a VM with virtual hardware specifications of 8GB RAM, 2 CPU units and 60GB HDD. The version used was latest available at the time of research.

vCenter server requires a proper database for keeping the record of the physical hosts, available resources, network and storage configurations, clusters and the VMs in the environments. A separate DB instance can be created for this purpose, however, vCenter server also offers an inbuilt embedded DB. This embedded option is more suitable for small or mid-range environments. vCenter creates this DB itself during the installation, thus curtailing complexity.

vCenter is the overall management and administration tool for complete virtual datacenter as it has the complete visibility and control of all the physical and virtual devices. Due to its criticality, vCenter is generally deployed in HA in enterprise level datacenter, however, a separate DB instance is required in HA.

vCenter server can also be deployed on a separate physical server, however, best practice is the installation of vCenter on a virtual machine inside the virtualized datacenter.

During installation, vCenter also creates a local level AD for single sign on and authentication of virtualization specific services, however, it can also join the datacenter AD for user authentication. A single vCenter server is setup with an embedded DB and local level AD on a virtual machine with Windows Server 2008 R2 as OS in this research.

This VM was later joined with the datacenter AD created before for granting accessibility to authorized users only.

#### **5.6.15 Web Client**

Like vSphere client, Web client is a similar administration tool for accessing vCenter and ESXi hosts. vSphere is a Windows only software and needs to be installed on management server for accessing the virtual datacenter. This limitation is removed with the availability of Web Client. This software is installed as a supplement to vCenter deployment. This allows vCenter to be accessed from internet browsers of any machine or OS.

#### **5.6.16 Virtualized Datacenter**

After configuration of above mentioned pre-requisite tools and hardware, a proper VMware virtualized datacenter is established and ready for offering IT services. vCenter server is accessed through vSphere or Web client and vDC is created. All ESXi hosts are added in the vDC and cluster of hosts are created as per requirement. All network and storage configuration are checked for their availability in the vCenter and finally VMs are created for provision of services.

All VMware functions including vMotion, DRS, HA and other smart features are configured for efficient and enhanced datacenter administration.

#### **5.6.17 vRealize Operations Manager**

The last step is the installation of vRealize Operations Manager. This is a very smart monitoring tool for virtualized datacenter. It keeps monitoring virtual and physical resources of the virtual datacenter and recommends suitable actions for smooth running of operations. vRealize operations manager can be considered as NMS because it provides the administrators a complete picture of datacenter functionality and eases the routine O&M (Operations and Management) procedures.

### **5.7 Chapter Summary**

In this chapter a fully functional VMware virtualized datacenter was established for proposing and implementing a complete security design and policies. The research methodology adopted has been discussed in detail about all the steps involved in setting up the vDC and later this vDC would be used to design a security framework.

The hardware and software used in the research are described in detail and every step for hardware and software configuration is explained. High level virtual datacenter design is formulated and then a virtual datacenter is accordingly deployed. Infrastructure was setup and hardware was configured for providing network, storage and compute for

virtualization. Then all physical servers are virtualized and vCenter server is setup for efficient management. All services are checked and vDC is buildup.



### **6. Proposed Security Model for VMware Virtualized Datacenter**

#### **6.1 Introduction**

With the popularity of virtualization in enterprises, administrators are rapidly virtualizing their IT setups. Simultaneously security teams are tasked to check and test the security of virtual datacenters. Security experts have realized that traditional datacenter security policies and controls are not sufficient for virtualization and new security design is required to avoid any serious event. Although, a lot of work has been done in securing data center operations but proper security model for virtual and cloud environments is not readily available.

This research is carried to design a proper security model for virtual datacenter. Since, VMware is the most widely used virtualization software [2] so it has also been selected in this research. The security model is proposed in a way that traditional security is first applied on a datacenter including physical security. Then proper security policies and guidelines that are used in physical environments are applied. Finally, virtualization part is analyzed and security design is proposed meeting all tiers involved in virtualization.

The defense in depth approach is opted and special stress is laid upon monitoring through NMS, as proactive monitoring will prevent major incidents from happening. In addition to security model, numerous guidelines are also proposed in the research, implementation of which will ensure the confidentiality, integrity and availability of virtualization environments.

The major aspects of proposed security model include access control and network security. In addition, different control for management and user security are presented. Another prime area of security is the interaction between the host and guest OS. Finally, it must be noted that the security framework is designed in such a way that although, security is to be ensured but simultaneously the QoS is not impacted.

#### **6.2 Proposed Security Model**

Broadly, the proposed security model consists of the four distinct parts; physical security, traditional security, virtualization security and monitoring. The combined implementation of these four domains can ensure security in enterprise virtual environments. Figure 6.1 presents these major security domains that must be collectively executed.

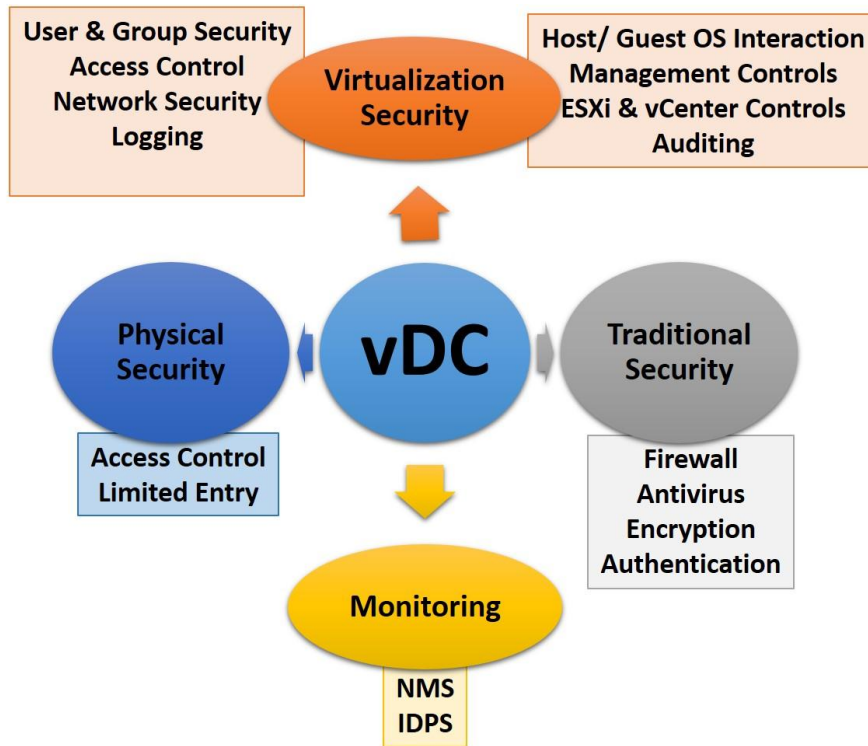


Figure 6.1 Four Major Datacenter Security Domains

Although, all four domains are very critical for datacenter security, however, the main focus of this research is virtualization security and same will be discussed in detail while rest of the aspects are briefly presented.

### 6.3 Physical Security

Datacenter must be established in a secure and controlled environment for its physical protection and safeguarding. Security cameras must be deployed which cover all regions of the datacenter. Backup of camera feed must be maintained for auditing. The physical security is the first security layer in datacenter and is divided into two sub-categories.

#### 6.3.1 Access Control

Access Control system must be installed at physical entry points of data center. Smart card access with biometric verification supplemented with password entry ensures that only authorized people can enter inside the equipment area premises. User rights can also be segregated via access control so that security wise clear personnel can only get access up to the level they are cleared for.

#### 6.3.2 Limited Entry

Datacenter and equipment area are a high tech critical areas and must be operated tactfully at all times. Organizations' businesses are running from these datacenters and live transactions are taking place around the clock. Thus, it must be ensured that only limited entry is allowed in datacenter, especially inside equipment area. Unnecessary entry and

equipment handling can lead to major disaster. A record of entry and exit must be maintained. Entry should be granted after proper approval in emergency situations. Even authorized staff should be advised to restrict equipment area entry.

## **6.4 Traditional Security**

A lot of work is done and large amount of literature is also available in traditional enterprise datacenter security. Although, this does not directly link with virtualized part of datacenter but at the same time this is a highly critical area as it ensures security of the real or physical part of the datacenter. This includes implementation of firewall, antivirus installation, encryption techniques and authentication mechanism. Security policies involved in traditional security must be properly defined and updated regularly.

### **6.4.1 Firewall**

Firewall at the gateway must be installed and configured as a core firewall. All traffic entering or exiting the datacenter must pass through core firewall so that every packet is monitored and illegitimate traffic is restricted its access. If edge locations are involved in datacenter operations than firewalls must be installed at all such locations. Security configuration must be explicitly defined in firewalls for all traffic.

### **6.4.2 Access Control Lists (ACLs)**

Access control list must be clearly defined in network devices. It is recommended that all traffic must be initially denied thorough security policy and then one by one legitimate traffic is allowed in ACL for enhanced security measures.

### **6.4.3 Redundancy**

All critical devices must be redundant and deployed in HA architecture. This ensures zero downtime in case a critical device gets malfunctioned. Another good practice is that in addition to redundant devices, a pre-configured offline device must also be in place as a replacement in case of an event.

### **6.4.4 MAC Binding**

Media Access Controlbinding must be enabled in all network devices. This is an acceptable security feature to restrict illegitimate access.

### **6.4.5 Port Binding**

In addition to MAC binding, port binding should also be implemented in datacenter network. All required port must be clearly identified and remaining unnecessary ports must be closed to restrict unauthorized access. Security wise it is also considered to be a good practice that all default port numbers should be replaced with unique numbers.

#### **6.4.6 Load Balancing and VIPs**

Load balancing of core devices must be implemented. Depending upon budget a hardware or software LBR (Load Balancer) should be installed after the core firewall. VIPs (Virtual IPs) are configured on LBR, particularly of a different subnet than the real IP scheme. Real IP addresses of all devices are private and their confidentiality is maintained via LBR implementation.

#### **6.4.7 Antivirus Software**

Antivirus software must be installed and regularly updated in all machines inside datacenter. Updates must be checked on sandboxes before implementing on production servers. In addition, all machines must be scanned regularly for any malware. A proper security policy should be maintained that enforces periodic scan and updates.

#### **6.4.8 DNS**

IP addresses are confidential and must be secured. DNS should be configured in the environments for address translation. Lookup services must be updated regularly to avoid any legitimate address translation.

#### **6.4.9 Encryption**

One of the most important security technique is the encryption of data. Sensitive data must not be stored in plain text. Although a lot of processing is involved in encryption and decryption of real time traffic so trade-off is there. Proper security procedures and guidelines ensure that critical data is always secured via encryption.

#### **6.4.10 Authentication and Authorization**

User authentication must be ensured at all tiers of the datacenter and access must be allowed only to authorized people. Proper password policy should be implemented which ensures that users regularly change their password and only strong password is accepted. In addition, AD must be configured and all user authentication should be done through it. This guarantees user authentication and authorization.

#### **6.4.11 Unnecessary Services**

OSs are running various services after startup that are unnecessary. This is not only performance degradation factor but also a security threat. An unnecessary OS service can be used to comprise or gain access illegitimately. Therefore, required OS services must be clearly identified and rest all services should be stopped.

#### **6.4.12 Backup**

Data backup is very crucial in IT environments. Datacenters house highly sensitive and critical data and its regular backup, preferably offsite must be maintained. Storage

unavailability or malfunctioning is a common threat in datacenter but this is curtailed via taking periodic backups at multiple locations.

#### **6.4.13 DR and BCP**

Another major area in traditional security is DR and BCP on datacenter operations. Generally, large enterprises have multiple datacenters at different locations. The system design should be such that one datacenter performs as a DR site for another datacenter and thus, business continuity in a disaster situation is maintained within minimum downtime.

### **6.5 Monitoring**

After physical and traditional security, the next major security layer is the proactive monitoring. This allows administrators to identify any potential threats and vulnerabilities in the environment. Health status of IT devices should be regularly and proactively observed. Any warnings, alarms or event logs are keenly examined to avoid any security, hack or spam event. Proactive monitoring allows improved reliability, enhanced productivity and ultimately cost efficiency. Monitoring is divided in to following sub-categories.

#### **6.5.1 Logging**

Logs are the best source of technical information provided that if they are regularly reviewed. Problem identification and analysis is readily done by reviewing log activity. Different log analyzers are available which filter out unnecessary details and present meaningful or critical data. Logging is thus the basic parameter for focused security, awareness and policy implementation. Logging and auditing collectively certify that only sanctioned activity is performed and all security and operational polices are in place.

#### **6.5.2 Auditing**

Regular security audits allow to identify the strength and weaknesses of implemented security in an organization's IT setup. Both internal and external/ outsourced audits should be conducted to certify that security practices are in place and vulnerabilities are determined beforehand.

#### **6.5.3 SIEM(Security Information and Event Management) and IDPS(Intrusion Detection and Prevention System)**

SIEM are importing security tools for datacenter proactive monitoring because of their capability to analyze real time data and identify security threats and weakness in the environments. SIEM must be deployed and properly configured in the datacenter to determine and address any malicious activity or potential security risk.

IDPS (Intrusion Detection and Prevention System) must also be deployed in enterprise datacenters. IDPS identifies and prevents malicious activity in the network or system devices. DPI (Deep Packet Inspection) and HIPS (Host Based Intrusion Prevention System) thoroughly examine every activity within the datacenter and potential threats and vulnerabilities are timely addressed.

SIEM and IDPS agents must be configured in all devices of the datacenter to ensure proactive monitoring and security. IBM's QRadar is famous log and forensic analyzer. It gives a holistic view of all tiers of datacenters and presents any security event in detail to the administrators for timely action.

#### **6.5.4 NMS**

NMS are efficient monitoring software that ease administration of daily operations. Graphical dashboards are created which provides health levels and alarms of all datacenter devices. NMS agents should be configured on every device in the system for effective problem identification. IBM's Tivoli is a series of famous NMS tools that are suitable for enterprise datacenters.

### **6.6 Virtualization Security**

The topmost consideration in this thesis is the security involved in virtualization tier. Securing virtualization domain of datacenter is a bit complex. Already discussed security measures in this chapter are not enough for defense in depth. A complete security framework is presented in this section for datacenter virtualization which comprises of four distinct tiers. These tiers are security controls, security policies, monitoring and business continuity. These four tiers are further divided to various sub-categories and are described here in detail. Figure 6.2 presents the graphical view of high level proposed virtualization security model.

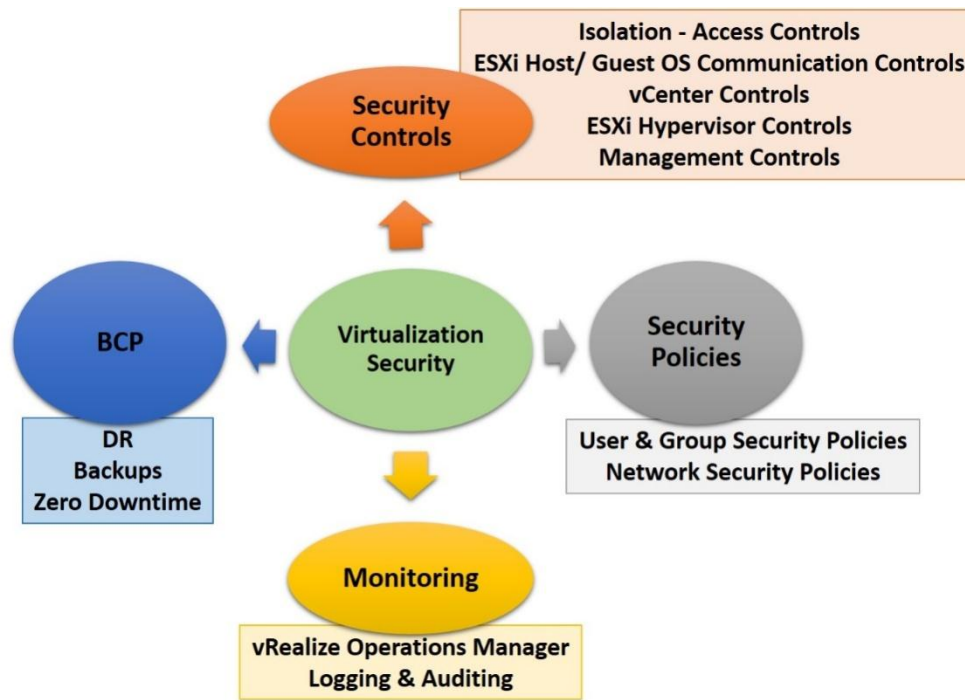


Figure 6.2 Virtualization Security Framework

## 6.7 Virtualization Security Controls

Security controls are protective measures that are implemented to identify, restrict, respond, or curtail potential security threats and vulnerabilities in the datacenter. Different security controls are proposed for addressing virtualization security risks.

### 6.7.1 Isolation - Access Control

Access control is the most important security protocol in virtual environments [34]. These controls restrict unauthorized user access and only legitimate traffic flows through the network. Following access control in VMware are proposed.

#### 6.7.1.1 Segregate vMotion Traffic

vMotion is the live migration of VMs between ESXi hosts. To ensure availability during migration of VMs, this traffic is transmitted in plain text. Therefore, vMotion data needs to be secured via isolation from other networks. This is achieved by configuring a separate VLAN and port group for vMotion. Additionally, a separate Physical NIC is proposed in highly sensitive organizations [35]. This control safeguards confidentiality.

#### 6.7.1.2 Isolate Management Network

Datacenter management network is strictly used by administrators and user traffic must always be segregated from management network. Generally, management network has access to all the VLANs in the network and its security policies are less strict as compared to the access networks [36]. It is proposed that user VMs must never be created on management network and isolation of this network must be ensured.

## **6.7.2 Controls for ESXi Host and Guest VM Communication**

Several RPCs (Remote Procedure Calls) are initiated by VMs with the ESXi hosts all the time. This direct communication between the guest and the host can be a potential threat which is why it is proposed that it should be restricted [37]. Following controls are proposed that limit direct communication between VM and ESXi host.

### **6.7.2.1 Restrict Direct Copy Paste**

It is proposed that direct copy paste between local and virtual machines from vSphere console must be deactivated on all VMs. This control safeguards both confidentiality and integrity.

### **6.7.2.2 Disable Unauthorized Control on Virtual Hardware**

It is proposed that VM users should have limited privileges on the virtual hardware assigned to their VM. These users should not have access to modify the compute, storage and other virtual resources directly. Alternatively, this would be done legitimately via virtualization administrators of datacenter after formal approval. This control limits the threat of data leakage.

### **6.7.2.3 Remove Unnecessary Virtual Hardware**

By default, many unnecessary virtual hardware is assigned to the newly created VM including floppy drives. It is proposed to remove all such devices from all VMs, especially in sensitive organizations. Implementation of this control lessens various security risks.

## **6.7.3 vCenter Controls**

One of the most critical resource in a VMware datacenter is the vCenter server and thus its protection is very important. Unauthorized access to vCenter server can result in loss of overall virtualization setup as the malicious user gains access to both physical and virtual resources along with their configurations. Following controls are proposed in this research to remove vCenter threats and hacking incidents.

### **6.7.3.1 Controlled vCenter Network Access**

vCenter Network is one of the most critical VLAN because it is communicating with all ESXi hosts, VMs, and network storage. It is therefore, proposed that vCenter Network must be properly secured. Explicit firewall policies should be defined for controlling vCenter network access. Supplement to security policies, all unnecessary ports should be blocked and traffic must be monitored for any malicious activity. Only authorized users and from dedicated terminals should be granted access to vCenter. This control restricts untrusted network exposure.



### **6.7.3.2 *Controlled vCenter Management***

vCenter access should be controlled and logged due to its criticality. It is proposed that built-in windows administrator account should not be used to access the vCenter. The vCenter Windows VM should join active directory and only AD accounts of authorized users should get the access for logon and management. This control avoids misuse of privileged rights of built-in administrator account.

### **6.7.3.3 *Hardening of vCenter VM***

It is proposed that security of vCenter server VM must be hardened. All local accounts should be disabled and only domain login of authorized users should have access. All unnecessary ports, peripherals and Windows services should be blocked. OS and antivirus should be regularly updated and periodic scan should be conducted. Implementation of this control restricts unauthorized access.

### **6.7.3.4 *Avoid Using vCenter as a Management Server***

It is proposed that vCenter server should not be taken as local management server by the administrators. Even vSphere client should not be installed on this machine. No software or data should be stored in vCenter HDD. This control prevents unauthorized access and data leakage threats.

### **6.7.3.5 *Restrict Self Signed Certificates***

It is proposed that vCenter by default uses its own self signed certificates which is a security risk. A trusted certification authority should be used, particularly in highly sensitive organizations for assigning and authorizing certificates. This control secures from the threat of man in the middle attacks.

### **6.7.3.6 *Patches and Updates***

vCenter security updates are released by VMware time to time. Same must be applied as soon as they are available to avoid any serious security event in the future.

## **6.7.4 *ESXi Hypervisor Controls***

Hypervisor security is of chief importance in virtualization. Unauthorized access or malicious activity on hypervisor layer can have severe consequences and may lead to complete disruption of services. This research proposed following controls at hypervisor layer, implementation of which prevent several hacking attacks.

### **6.7.4.1 *Controlled ESXi Administration***

It is proposed that ESXi host should be accessed via vCenter only and direct access should be granted only when vCenter server is unavailable. This control prevents VM lockout and resource congestion.

#### **6.7.4.2 ESXi Management**

ESXi is based on customized version of Unix OS with specific services pertaining to virtualization. In spite of many resemblances, it is proposed that ESXi host should not be managed like Unix administration. This control prevents unauthorized and malicious activity on the hypervisor.

#### **6.7.4.3 Patched and Updates**

Hypervisor must be regularly updated but it is proposed that Unix patches should not be applied on ESXi hosts. VMware releases specific customized patches of ESXi time to time. These are tested updates and only these should be implemented. This control prevents loss of host integrity.

#### **6.7.5 Controlled Management**

Supervised administration and controlled management reduces risks of unauthorized or malicious activity. Management of virtual machines must be limited to authorized users only. Rights must be explicitly assigned to legitimate login accounts. In highly sensitive environments, minimum number of users should be granted administrator rights for implementation of controlled VM and ESXi management.

### **6.8 Virtualization SecurityPolicies**

Different security controls are suggested for virtualization hardening. In addition to controls, several security policies are also proposed for designing a complete datacenter virtualization security model.

#### **6.8.1 User & Group Security Policies**

Virtualization is a complex platform and its administration and management needs to be monitored. Only authorized users should have administration rights with clearly defined privileges. In this regard, following security policies for users and groups are proposed, whose implementation ensure security enforcement.

##### **6.8.1.1 Domain Authentication**

It is proposed that an active directory must be setup in virtualization implementation. All user accounts should be created and authenticated via AD and local OS accounts should be deactivated. This security policy ensures that all activity is being monitored and properly logged. Furthermore, user and group policy management becomes efficient and unauthorized access is prevented.

### **6.8.1.2 SSH Disabled**

It is proposed that SSH service to access ESXi directly via shell prompt must be disabled from vSphere console of every host. Implementation of this security policy prevents brute force attacks and unauthorized remote access.

### **6.8.1.3 Controlled Root and SUDO Access**

Root access to ESXi must be controlled and individual administration accounts for authorized users should be created. It is proposed that “**sudo**” should be employed in all ESXi hosts and use of “**su**” should be limited. Implementation of this security policy in virtualized datacenters avoids misuse of privileged rights of root account.

## **6.8.2 Network Security Policies**

Security controls enforce datacenter hardening and safeguarding from malicious threats. Combined with these control, several security policies are supplemented for achieving defense in depth. These security procedures mostly aim at obtaining network segregation and isolation. Some important techniques regarding virtualization are presented in this research.

### **6.8.2.1 ESXi Firewall**

ESXi security profile allows configuration of local firewall which blocks unauthorized ports. It is proposed that local profile of ESXi firewall should be selected as high security for all hosts. Furthermore, when some legitimate traffic is blocked. then instead of changing the security level of firewall to medium or low, it is strongly suggested that only required port should be unblocked for data transit. Implementation of this security policy prevents unauthorized traffic and man in the middle attacks.

### **6.8.2.2 MAC Spoofing**

VMware ESXi assigns MAC addresses automatically to its underlying VMs but these addresses can be changed easily. However, ESXi also allow a setting in which MAC address changing is unauthorized. This security policy allows prevention of masquerading and man in the middle attacks. Denial of service attacks are also curtailed with this setting.

## **6.9 Virtualization Tier Monitoring**

The third major security tier of virtualization is the continuous and proactive monitor of environment. The prime contribution of monitoring is the provision of accountability and system transparency. Several controls and policies are often overlooked by IT administrators due to meeting up of timelines. These security loopholes are major system vulnerabilities which if exploited can result in a serious security event. Monitoring reveals

these faults well in time and several problems are resolved beforehand. Monitoring is also linked with security audits and log analysis. This research proposes that monitoring should be given chief importance in IT environments for smooth functioning of system.

### **6.9.1 NMS – vRealize Operations Manager**

Monitoring needs to be efficient and effective. A proper NMS must be deployed for comprehensive and intelligent management. This research proposes installation of vRealize Operations Manager or vROM in the virtualized environment. This software integrates with vCenter servers as it is specifically designed for monitoring and analysis of virtualized datacenter. vROM offers smart and transparent visibility of both physical and virtual resources. It analyzes the system completely and suggests best practices for the datacenter virtualization operations. It provides intelligent dashboards of all resources for better monitoring and rectification of various issues in the environments. vROM configurations also offer automated management of various events.

### **6.9.2 Auditing & Logging**

In virtualized setups, both auditing and logging are of prime importance. Both parameters ensure policy implementations and regulatory compliance enforcement. Logs are particularly the central source of problem troubleshooting, issue handling and overall monitoring of the virtualization. ESXi, vCenter and VM logs are very helpful in rectification of critical faults. Both auditing and logging also contribute in forensic analysis of any malicious activities. This research suggests to pay extra vigilance towards logging & auditing and proposes following security control in this area.

#### **6.9.2.1 *Maintaining File System Integrity***

Storage data stores contain sensitive data files of VMs and virtualization configuration. Due to their criticality, it is strongly recommended that these files and data stores must be regularly inspected to maintain their integrity. Proper file permissions and policy must be explicitly applied to avoid unauthorized change and illegal access. Implementation of this control ensures file system integrity and prevents illegitimate modification.

#### **6.9.2.2 *Implementing NTP Configuration***

All ESXi hosts, VMs, external storage and any other virtual resource must synchronize their time periodically. This is particularly important for enhanced performance and effective employment of security. It is proposed that NTP server should be deployed and NTP setting of all devices must be configured for continuous update of local time with NTP server. This control also helps in forensic analysis and incident response.

### **6.9.2.3 Saving Logs Externally**

Log files are very critical for problem determination, fault rectification, forensics and auditing. It is proposed that all critical log files relating to virtualized datacenter must be archived by exporting to an external location, periodically. Furthermore, proper security checkups should be conducted for confirming that log file integrity is maintained in order to prevent any unauthorized change or removal of log file data. This control is particularly important for meeting compliance requirements. **Vmware, vmkernel, vmwarning, vpxa** and **messages** are the important log files that must be exported off at remote storage.

## **6.10 Virtualization DR &BCP Solutions**

DR and BCP are the most vital aspects of any organization's incident response management. They describe a company's strategy to respond in the event of a security incident, complemented with the recovery of operations in the minimum duration of time. Virtualized datacenters offer excellent DR &BCP techniques which have been tested and proven to be very successful. Besides cost effectiveness, incident response planning is essential feature of virtualization which resulted in its huge popularity, especially in enterprise level IT environments. This research proposes following solutions in this area which should be implemented in order to achieve actual in depth security.

### **6.10.1 High Availability (HA)**

HA is a very essential feature offered by vCenter server. It is proposed that HA configuration should be enabled in virtual datacenter. HA requires the threshold of storage and compute resources to be 50% available at all time. This can be implemented in very sensitive organizations where zero downtime is an essential requirement. However, in most cases this option is not cost effective. This research proposes that only core devices should be kept in HA whose unavailability can seriously impact the datacenter operations.

### **6.10.2 Fault Tolerance (FT)**

Fault tolerance enables high availability of critical virtual machines within the datacenter, for example, AD. A copy of original VMs is maintained which is synchronized with the changes on the original VM. In a case of original VM failure, the secondary copy is automatically made available for restoration of services as soon as possible. It is proposed that all critical devices must be configured in HA and FT.

### **6.10.3 Zero Downtime**

Virtualization in datacenter allows zero or minimal downtime. The research proposes that DRS and storage DRS must be enabled, preferably to fully automatic. In case of host or

data store maintenance requirement, the activity can be performed with zero downtime by live migration of VMs. However, in a situation of host failure, the VMs are automatically migrated and balanced to remaining available hosts but this scenario involves a VM restart.

#### **6.10.4 Site Recovery Manager (SRM)**

SRM offers fully automated recovery of datacenter operations from a redundant site. Critical VMs are deployed as backup in secondary location which are periodically synchronized with primary location. SRM offers reliable, speedy and efficient recovery of operations in case of complete site failure. This research proposes that SRM should be configured in highly sensitive organizations.

#### **6.10.5 Backups and vSphereData protection (vDP)**

Regular backups are essential in every IT environment. In this regards, vDP should be deployed in virtualized environments. This is an efficient recovery tool which integrates with vCenter server and offers automatic remote exporting of backups. The research recommends vDP should be included in the organization’s incident response plan.

#### **6.10.6 vShield**

vShield offers essential network security features for VMware virtualized datacenters. In addition to vROM, it is proposed that vShield should be deployed and integrated with vCenter to have better monitoring and visibility of network traffic.

#### **6.10.7 VMware Virtualized Datacenter Hardening Policies Guidelines**

A complete in defense in depth security framework has been proposed above involving four major tiers of virtualization security that include security controls, security policies, monitoring and DR & BCP. Moreover, several additional virtualization security hardening techniques are presented in Table 5 whose implementation further enhance the overall security model.

No.	Policy/ Guideline	Description
1.	ESXi.apply-patches	Keep ESXi system properly patched
2.	ESXi.audit-exception-users	Audit the list of users who are on the Exception Users List and whether they have administrator privileges
3.	ESXi.config-ntp	Configure NTP time synchronization
4.	ESXi.config-persistent-logs	Configure persistent logging for all ESXi host
5.	ESXi.config-snmp	Ensure proper SNMP configuration
6.	ESXi.disable-mob	Disable Managed Object Browser (MOB)

7.	ESXi.enable-chap-auth	Enable bidirectional CHAP, also known as Mutual CHAP, authentication for iSCSI traffic
8.	ESXi.enable-remote-syslog	Configure remote logging for ESXi hosts
9.	ESXi.set-account-auto-unlock-time	Set the time after which a locked account is automatically unlocked
10.	ESXi.set-account-lockout	Set the count of maximum failed login attempts before the account is locked out
11.	ESXi.set-dcui-timeout	Audit DCUI timeout value
12.	ESXi.set-shell-timeout	Set a timeout to limit how long the ESXi Shell and SSH services are allowed to run
13.	ESXi.TransparentPageSharing-intra-enabled	Ensure default setting for intra-VM TPS is correct
14.	ESXi.verify-acceptance-level-accepted	Verify Image Profile and VIB Acceptance Levels
15.	ESXi.verify-acceptance-level-certified	Verify Image Profile and VIB Acceptance Levels
16.	ESXi.verify-acceptance-level-supported	Verify Image Profile and VIB Acceptance Levels
17.	vCenter.verify-nfc-ssl	Enable SSL for Network File copy (NFC)
18.	VM.disable-console-copy	Explicitly disable copy/paste operations
19.	VM.disable-console-drag-n-drop	Explicitly disable copy/paste operations
20.	VM.disable-console-paste	Explicitly disable copy/paste operations
21.	VM.disable-disk-shrinking-wiper	Disable virtual disk shrinking
22.	VM.disable-hgfs	Disable HGFS file transfers
23.	VM.disable-independent-nonpersistent	Avoid using independent nonpersistent disks
24.	VM.disable-unexposed-features-autologon	Disable certain unexposed features
25.	VM.disable-unexposed-features-biosbbs	Disable certain unexposed features
26.	VM.disable-unexposed-features-getcreds	Disable certain unexposed features
27.	VM.disable-unexposed-features-launchmenu	Disable certain unexposed features
28.	VM.disable-unexposed-features-	Disable certain unexposed features

	protocolhandler	
29.	VM.disable-unexposed-features-shellaction	Disable certain unexposed features
30.	VM.disable-unexposed-features-toporequest	Disable certain unexposed features
31.	VM.disable-unexposed-features-trashfolderstate	Disable certain unexposed features
32.	VM.disable-unexposed-features-trayicon	Disable certain unexposed features
33.	VM.disable-unexposed-features-unity	Disable certain unexposed features
34.	VM.disable-unexposed-features-versionget	Disable certain unexposed features
35.	VM.disable-unexposed-features-versionset	Disable certain unexposed features
36.	VM.disable-VMtools-autoinstall	Disable tools auto install
37.	VM.disconnect-devices-serial	Disconnect unauthorized devices
38.	VM.TransparentPageSharing-inter-VM-Enabled	Check for enablement of salted VM's that are sharing memory pages
39.	VM.verify-PCI-Passthrough	Audit all uses of PCI or PCIe passthrough functionality
40.	vNetwork.enable-bpdu-filter	Enable BPDU filter on the ESXi host to prevent being locked out of physical switch ports with Portfast and BPDU Guard enabled
41.	vNetwork.limit-network-healthcheck	Enable VDS network healthcheck only if you need it
42.	vNetwork.restrict-port-level-overrides	Restrict port-level configuration overrides on VDS

Table 5 Virtualized Datacenter Hardening Techniques

## 6.11 Chapter Summary

A complete security model for VMware virtualized datacenter has been proposed in this chapter. Defense in depth approach has been followed and all aspects of security have been covered. Security is proposed in four distinct tiers of physical security, traditional security, virtualization security and monitoring. All tiers have been discussed in detail with special emphasis on virtualization security. Virtualization security is further sub-categorized into



security controls, security policies, monitoring and DR & BCP. In addition, a summary of miscellaneous security hardening techniques has also been presented for enhanced security.

## 7. Implementation & Analysis

### 7.1 Introduction

In this chapter the proposed security framework has been implemented for testing and analysis. A virtual datacenter on VMware has been established, proposed security policies have been implemented and vROM has been deployed for monitoring purposes.

### 7.2 Establishment of VMware Virtualized Datacenter

VMware virtualized datacenter has been set up on two physical servers. ESXi is installed on both servers, and then vCenter server along with management server and active directory has been setup. Local domain of **vdc.poc** has been created for vCenter in which a virtual datacenter namely vDC has been configured. A single cluster called Virtualized Datacenter-Cluster containing two ESXi hosts has been configured in vDC. Finally, VMs have been created and a fully functional datacenter is up and running. This implementation is shown in figure 7.1.

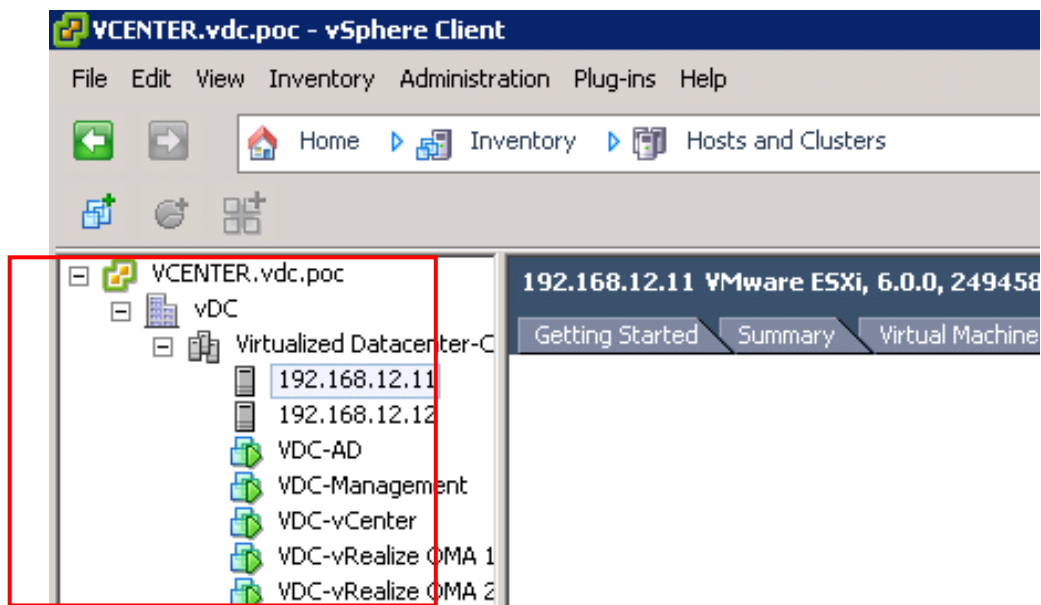


Figure 7.1 VMware Virtualized Datacenter

All versions of VMware software that are utilized in the research were latest available at the time of conduct.

### 7.3 Security Framework Implementation

Implementation and analysis of proposed security design is presented here.

### 7.3.1 Isolated vMotion Traffic

vMotion VLAN and port group have been segregated for achieving isolating of vMotion traffic. No virtual machine is assigned the vMotion VLAN and separate VLANs for all necessary traffic has been configured. Implementation is shown in figure 7.2

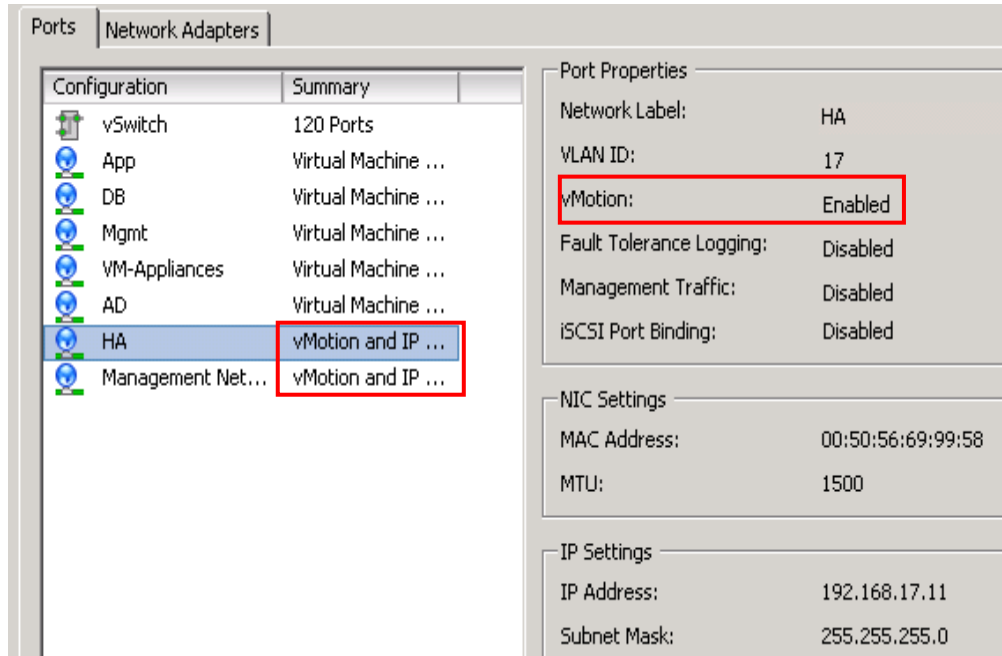


Figure 7.2 VMware vMotion Isolation

#### 7.3.1.1 Analysis

This control implements network segregation and isolation. This is highly useful in maintaining network and data confidentiality.

### 7.3.2 Reject MAC Spoofing

MAC address changing for all VMs has been disabled. vCenter server, initially assigns MAC address to the VMs which can be modified in future. This control recommends that MAC address change request must be rejected and initially assigned address remains unchanged. Implementation of this control is shown below in figure 7.3. Forged transmits and MAC address changes options should be set to reject for employment of this security recommendation. Additional security settings can also be configured in Traffic Shaping and NIC Teaming.

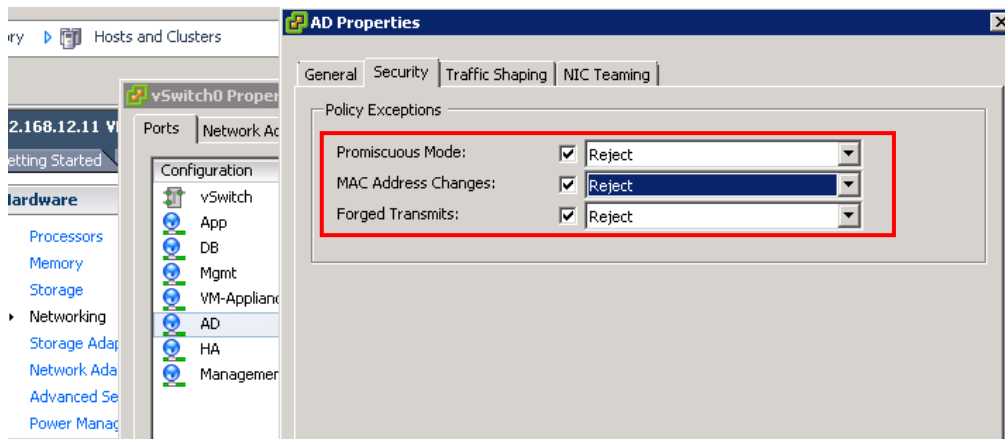


Figure 7.3 MAC Spoof Rejection Policy

### 7.3.2.1 Analysis

This security control prevents man in the middle and other eavesdropping attacks. Moreover, integrity of network at data link layer is maintained.

### 7.3.3 ESXi Firewall

ESXi local firewall settings should be set to high and all unnecessary ports should be blocked to ensure reliable flow of traffic. This has been implemented as shown in following figures. Figure 7.4 shows that only required services and ports for incoming connections have been allowed access.

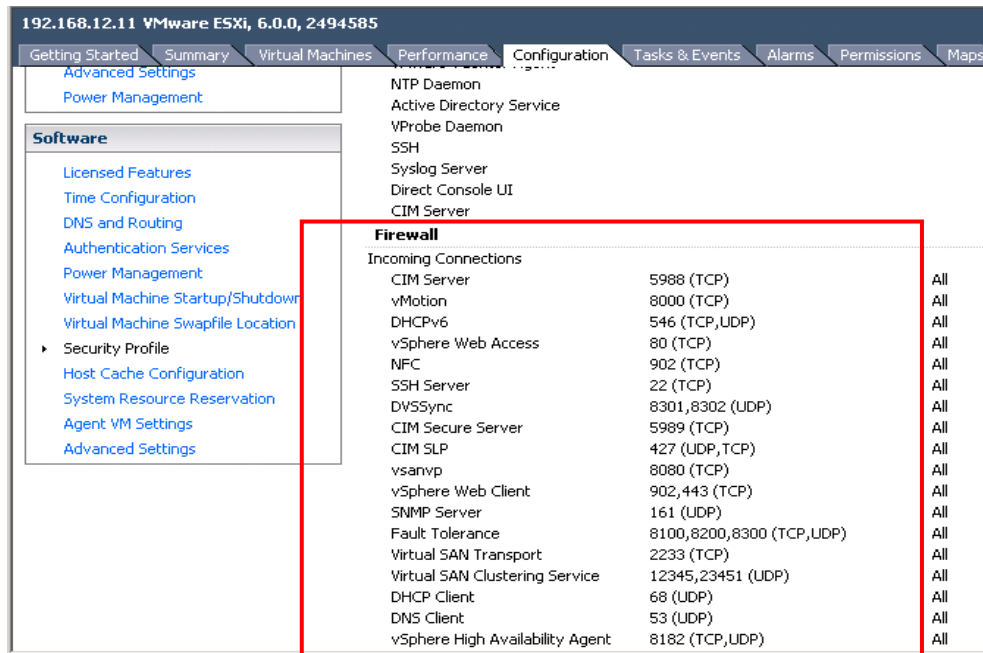


Figure 7.4 ESXi Firewall Configuration for Incoming Connections

Similarly, same criteria have been applied for outgoing connections as shown in figure 7.5.

Label	Incoming Ports	Outgoing Ports	Protocols	Daemon
vsanvp	8080	8080	TCP	All
vSphere Web Client	902,443	902,443	(TCP)	All
SNMP Server	161	161	(UDP)	All
Fault Tolerance	8100,8200,8300	8100,8200,8300	(TCP,UDP)	All
Virtual SAN Transport	2233	2233	(TCP)	All
Virtual SAN Clustering Service	12345,23451	12345,23451	(UDP)	All
DHCP Client	68	68	(UDP)	All
DNS Client	53	53	(UDP)	All
vSphere High Availability Agent	8182	8182	(TCP,UDP)	All
<b>Outgoing Connections</b>				
DHCPv6		547	(TCP,UDP)	All
rabbitmqproxy		5671	(TCP)	All
NFC		902	(TCP)	All
CIM SLP		427	(UDP,TCP)	All
HBR		31031,44046	(TCP)	All
vCenter Update Manager		80,9000-9100	(TCP)	All
vsanvp		8080	(TCP)	All
DHCP Client		68	(UDP)	All
vMotion		8000	(TCP)	All
Fault Tolerance		80,8100,8200,8300	(TCP,UDP)	All
WOL		9	(UDP)	All
Virtual SAN Transport		2233	(TCP)	All
Virtual SAN Clustering Service		12345,23451	(UDP)	All
VMware vCenter Agent		902	(UDP)	All
NFS Client		0-65535	(TCP)	20.60 42.101
DNS Client		53	(UDP,TCP)	All
vSphere High Availability Agent		8182	(TCP,UDP)	All
DVSSync		8302,8301	(UDP)	All

Figure 7.5ESXi Firewall Configuration for Outgoing Connections

Rules for any trusted VM and device has been explicitly defined and configured in the firewall for allowing of only legitimate traffic flow. Figure 7.6 shows that a trusted device has been added and access will be granted to its connections.

Label	Incoming Ports	Outgoing Ports	Protocols	Daemon
<input type="checkbox"/> VM serial port connected over net...	23,1024-65535	0-65535	TCP	N/A
<input type="checkbox"/> httpClient		80,443	TCP	N/A
<input type="checkbox"/> NSX Distributed Logical Router Ser...	6999	6999	UDP	N/A
<input checked="" type="checkbox"/> DNS Client	53	53	UDP, TCP	N/A
<input checked="" type="checkbox"/> vsanvp	8080	8080		
<input checked="" type="checkbox"/> vSphere Web Access	80			
<input checked="" type="checkbox"/> SNMP Server	161			
<input type="checkbox"/> gdbserver	1000-9999,50000-5...			
<input type="checkbox"/> FTP Client	20	21		
<input checked="" type="checkbox"/> vMotion	8000	8000		
<input type="checkbox"/> Active Directory All		88,123,137,139		
<input checked="" type="checkbox"/> rabbitmqproxy		5671		
<input checked="" type="checkbox"/> DVSSync	8301,8302	8302,8301		

**Firewall Settings**

Allowed IP Addresses

Allow connections from any IP address

Only allow connections from the following networks:

192.168.100.16/29

Separate each network with a comma.  
Example:  
192.168.0.0/24, 192.168.1.2, 2001::1/64, fd3e:29a6:0a81:e478::/64

OK

**Firewall Settings**

Allowed IP Addresses: 192.168.100.16/29

Figure 7.6ESXi Firewall Configuration for Trusted Devices

Several unnecessary services are also blocked by firewall. Figure 7.7 shows that DHCP client service has been disabled. This has been implemented to avoid automatic IP assignment.

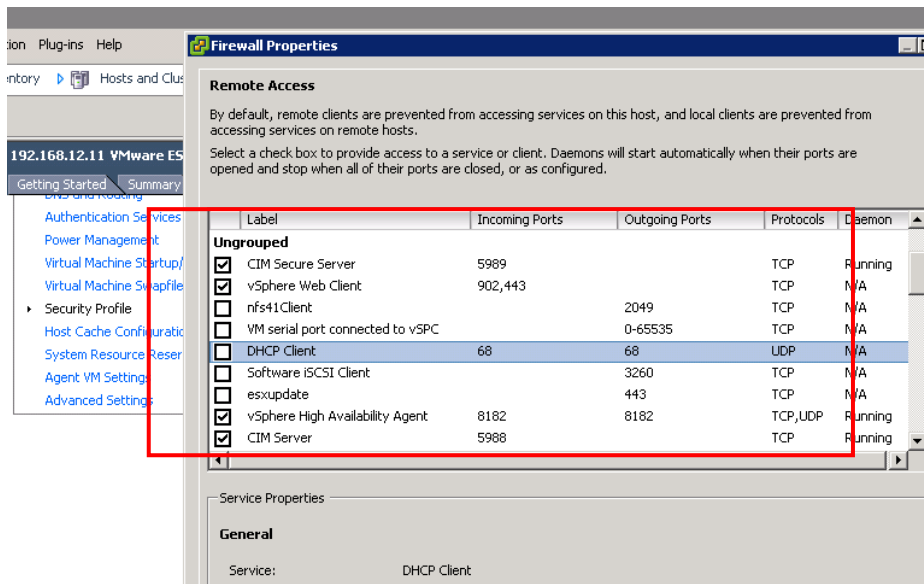


Figure 7.7ESXi Firewall Configuration for Unnecessary Services

Similarly, vCenter Update service has also been disabled for ensuring scheduled update on approved downtime and after proper quality control testing of the update as shown in figure 7.8.

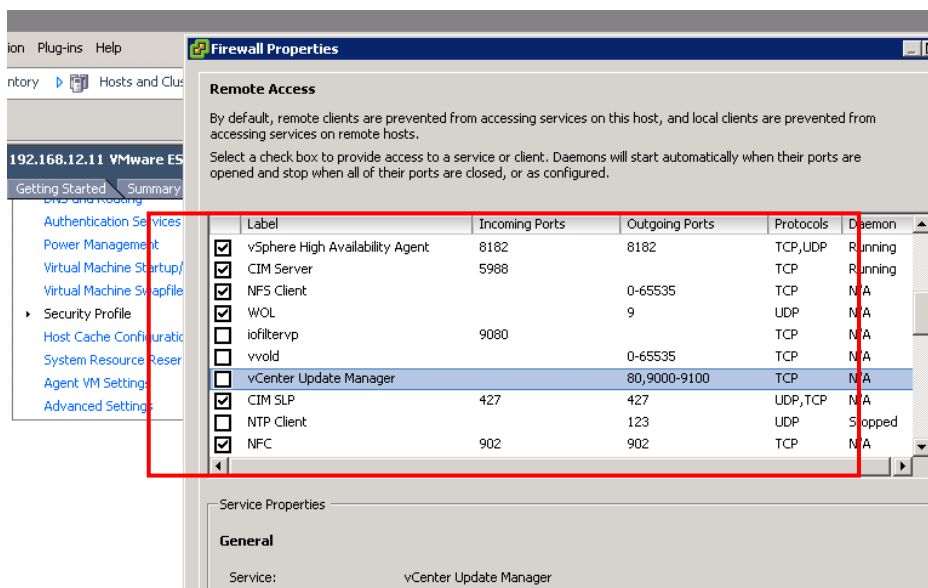


Figure 7.8ESXi Firewall Configuration for vCenter Update Manager

### 7.3.3.1 Analysis

Configuration of ESXi firewall enhances network security. This control prevents unauthorized access from unnecessary opened ports and exploitation of system services for malicious activity.

### 7.3.4 ESXi Host SSH Service

SSH service remotely provides direct access to ESXi hosts from shell prompt. This service is disabled and will only be allowed in emergency situation or standalone maintenance. All

management of ESXi must be done via vCenter servers. Figure 7.9 shows implementation of this security setting.

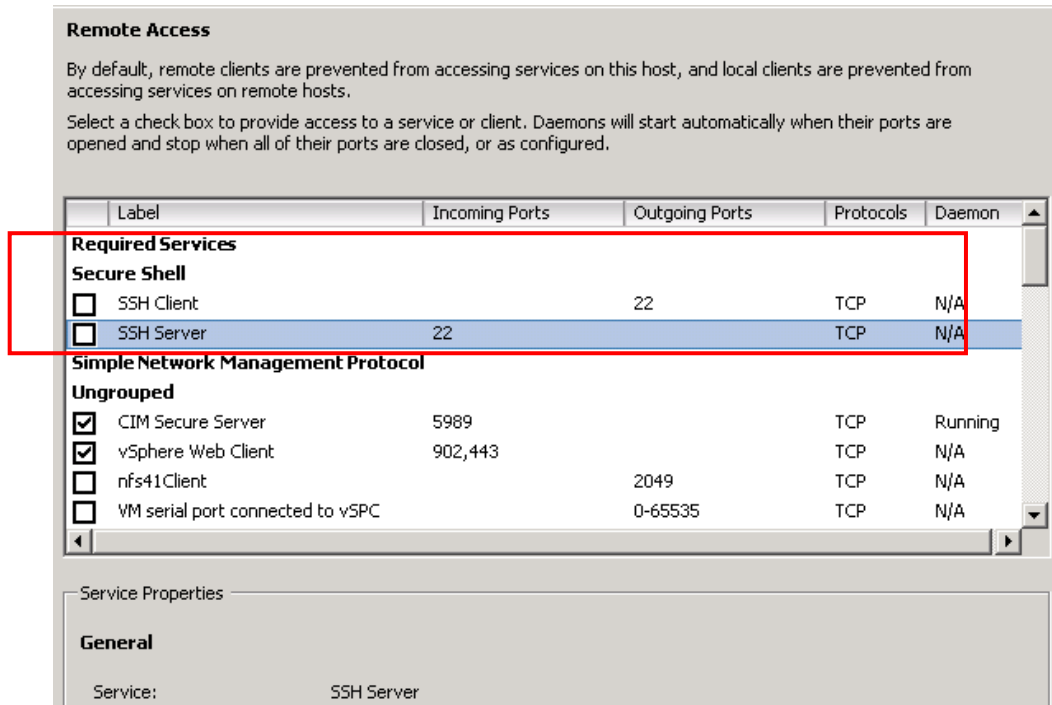


Figure 7.9 Restricted SSH Access

### 7.3.4.1 Analysis

Implementation of this control is necessary to thwart any attempt of unauthorized remote access. Root access via SSH to an attacker can cause complete disruption of services and loss of confidential data. In a scenario where authorized SSH access is required for administrative support or maintenance, temporary access may be granted after formal approval. Same setting must be immediately disabled after the sanctioned activity is completed. Furthermore, the activity may be properly monitored and logged.

### 7.3.5 Enable Lockdown Mode

All ESXi hosts are set in lockdown mode. This control allows host to be managed only via vCenter Server. This implementation is shown in figure 7.10 where lockdown mode is enabled.

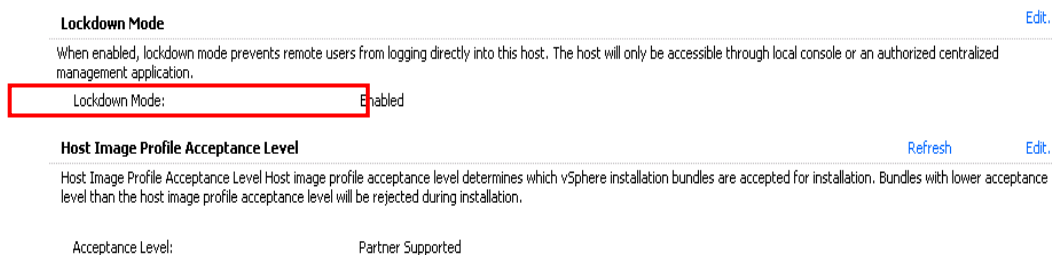


Figure 7.10 ESXi Hosts in Lockdown Mode

### 7.3.5.1 Analysis

Lockdown mode enhances security and no user is granted direct access to host. All operations can now be only managed via vCenter server. However, SSH servers is independent from this setting and needs to be separately disabled as previously discussed.

### 7.3.6 Host Image Profile Acceptance Level

vSphere Installation Bundles (VIBs) are offered by various sources. Host image profile acceptance level allows to configure this setting which should be set to accept only VMware Certified VIBs as shown in figure 7.11. The trust level of other available VIBs including VMware accepted, partner supported and community supported can be uncertain.

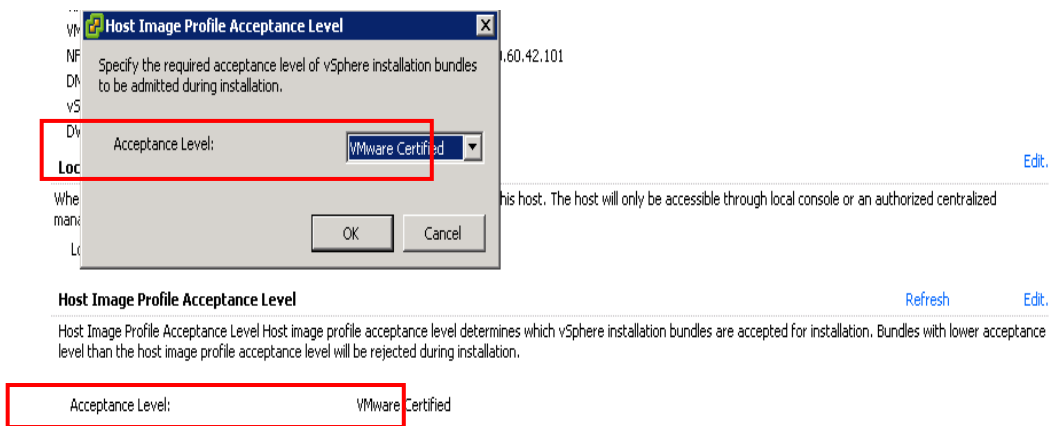


Figure 7.11ESXi Host Image Profile Acceptance Level

#### 7.3.6.1 Analysis

Setting this control to accepts only VMware certified VIBs ensure that all installation bundles are authentic and reliable. Additionally, this increases the confidence level of administrators regarding the integrity of patches and updates.

### 7.3.7 User and Group Policies

User and group policies define the access rights of VM users. These policies must be thoroughly scrutinized for every user in granting access from read only till administrator privileges. Implementation is presented Figure 7.12 in which a user test1 is granted read-only access while user test2 has administrator privileges on vDC.



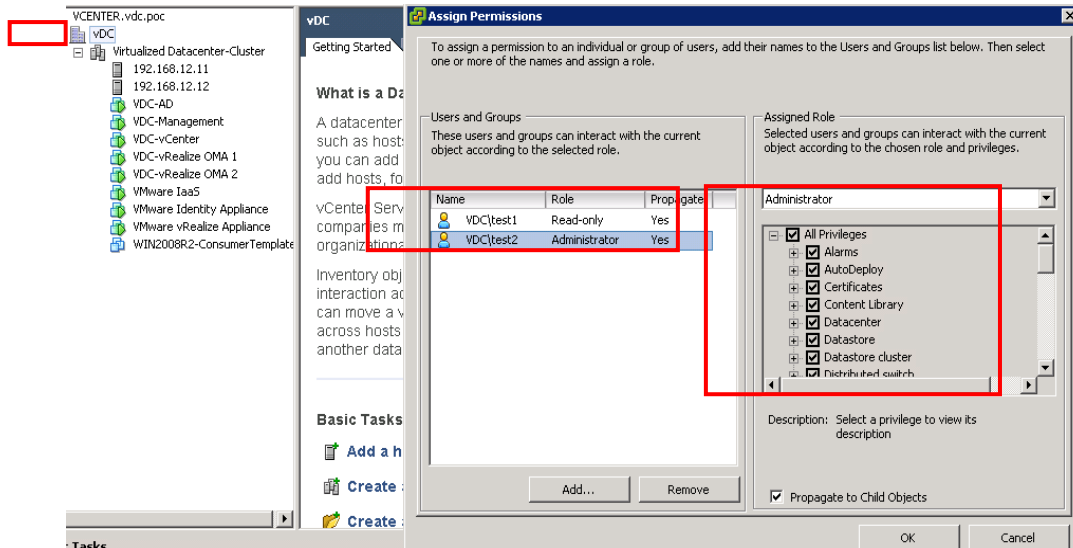


Figure 7.12 User Permission Assignment

### 7.3.7.1 Analysis

Proper user permission assignment and access rights ensure confidentiality and integrity of datacenter operations. Unauthorized access for malicious activity is prevented by this control.

### 7.3.8 Directory Service & Authentication

All users must be properly authenticated while logging on to VMs or vCenter server. This control is implemented by creating a local active directory for provision of authentication services as shown in figure 7.13. Domain name vdc.poc has been setup and user account test1 of this domain is granted access to vCenter server. All users are created on this AD and later granted access rights as per approval.

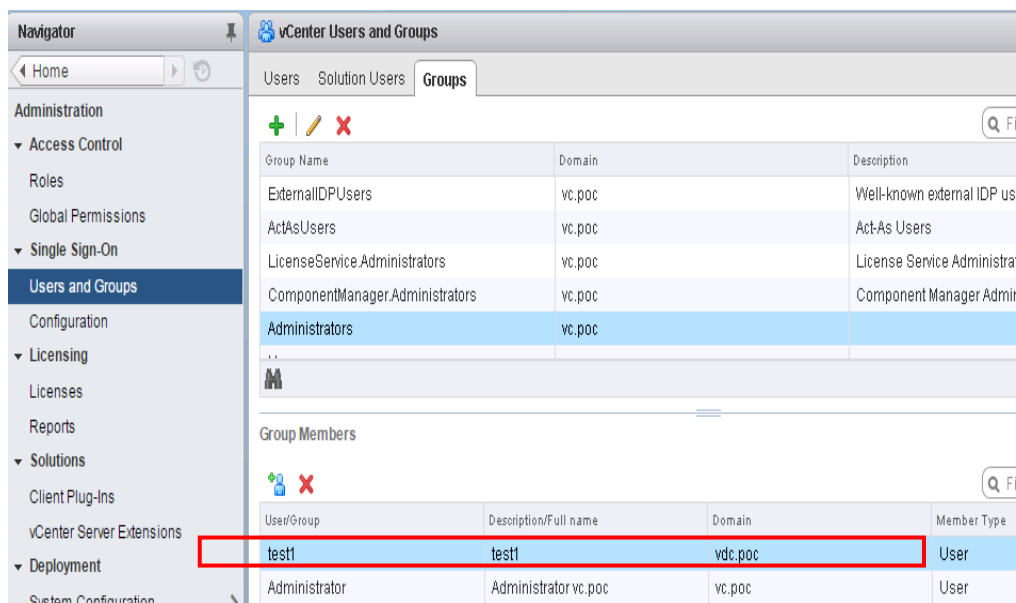


Figure 7.13 User Authentication Services

### 7.3.8.1 Analysis

Implementation of authentication services via AD ensure authorized user access, thus, help in maintaining confidentiality and integrity.

### 7.3.9 NTP Configuration

Clocks of all devices need to be synchronized all the time. Online transactions are occurring 24/7 which make NTP configuration very crucial. NTP setting of ESXi hosts is set to start automatically for time synchronization with active directory as shown in figure 7.14. AD is configured as NTP server.

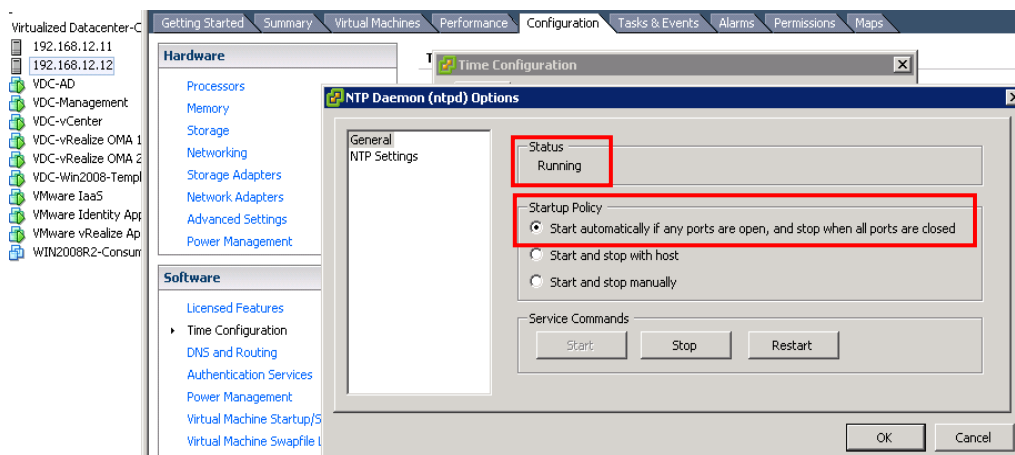


Figure 7.14 NTP Startup Policy

NTP service of ESXi hosts(NTP clients) is running and configured to synchronize with AD. This is depicted below in figure 7.15. AD is also configured as NTP server for provision of this service across network.

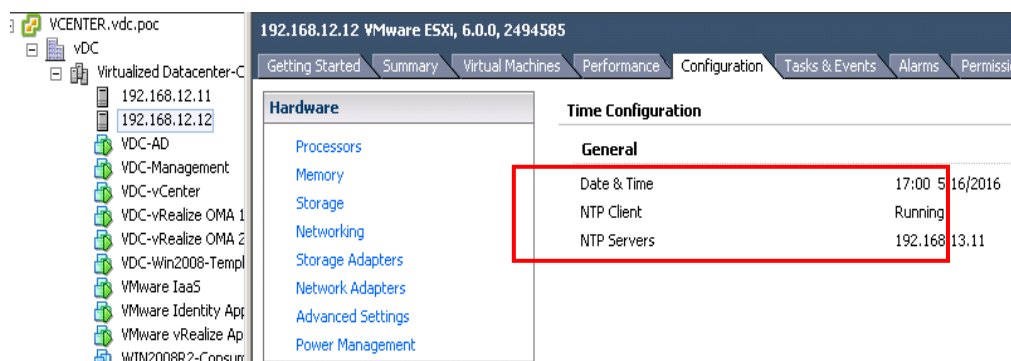


Figure 7.15 NTP Client and NTP Server Synchronization

### 7.3.9.1 Analysis

Time synchronization ensure all transactions and procedures are successfully handled. Security wise NTP configuration is essential for regulatory compliant requirements, auditing and forensic analysis.

### 7.3.10 VM File System Permissions and Integrity Check

VMFS integrity is very crucial for smooth flow of operations. Permissions of all files must be defined and all mount points and data files, especially log files must be continuously monitored for unauthorized modification as shown in figure 7.16.

```
192.168.12.11 - PuTTY
[root@localhost:~] df -h
Filesystem      Size  Used Available Use% Mounted on
NFS              1.5T 190.7G    1.3T   13% /vmfs/volumes/DS1
NFS              2.9T  77.3G    2.9T    3% /vmfs/volumes/DS2
VMFS-5          1.1T  978.0M    1.1T    0% /vmfs/volumes/datastore1
vfat            249.7M 172.7M    77.0M   69% /vmfs/volumes/042bb977-1fc838b9-5889-3eea0ef14785
vfat            4.0G   59.9M     3.9G    1% /vmfs/volumes/56ab7854-ea2764bb-b798-845b123a32b0
vfat            249.7M 160.2M    89.5M   64% /vmfs/volumes/e34da379-dfeed8cb-c780-29048f91c29c
vfat            285.8M 206.2M    79.6M   72% /vmfs/volumes/56ab7848-d4b42a86-240d-845b123a32b0
[root@localhost:~] cd /vmfs/volumes/DS1/
[root@localhost:/vmfs/volumes/1885b670-d6c9aed5] cd vCenter/
[root@localhost:/vmfs/volumes/1885b670-d6c9aed5/vCenter] ls -lrth
total 17346432
-rw-r--r--  1 root    root      43 Feb  3  09:02 vCenter.vmsd
-rw-----  1 root    root    12.0G Feb 16  08:01 vCenter-35544976.vswp
-rw-----  1 root    root    193.0M Feb 17  03:31 vmx-vCenter-894716278-2.vswp
-rw-----  1 root    root         0 May  2  03:04 vCenter.vmx.lck
-rw-r--r--  1 root    root      87 May  2  03:04 vCenter-13f4e28c.hlog
-rw-----  1 root    root    193.0M May  3  02:51 vmx-vCenter-894716278-1.vswp
-rw-----  1 root    root    236.0K May  6  11:54 vmware-84.log
-rw-----  1 root    root    234.0K May  9  12:30 vmware-85.log
-rw-----  1 root    root    236.4K May 10  11:50 vmware-86.log
-rw-----  1 root    root    233.9K May 11  10:55 vmware-87.log
-rw-----  1 root    root    235.6K May 12  11:44 vmware-88.log
-rw-----  1 root    root    238.2K May 13  12:42 vmware-89.log
-rw-----  1 root    root      520 May 16  02:34 vCenter.vmdk
-rw-----  1 root    root     8.5K May 16  02:34 vCenter.nvram
-rw-----  1 root    root     3.8K May 16  11:41 vCenter.vmx
-rw-----  1 root    root    234.9K May 16  11:41 vmware.log
-rw-----  1 root    root    80.0G May 16  11:58 vCenter-flat.vmdk
[root@localhost:/vmfs/volumes/1885b670-d6c9aed5/vCenter]
```

Figure 7.16 VMFS Permissions and Integrity Check

#### 7.3.10.1 Analysis

Unauthorized modification to file system is prevented by this control. Furthermore, integrity checkups ensure compliance to regulatory requirements and benefits in auditing.

### 7.3.11 Direct Copy/ Pasted Disabled

Management to VM direct copy/ paste from console can be vulnerable because copied data is placed in OS clipboard and can be transferred to unauthorized storage locations. This direct copy/ paste feature has been disabled via command line as a best practice, as shown in figure 7.17. This is done by configuring ESXi host config file. The file location is /etc/vmware/config.

```

192.168.12.11 - PuTTY
libdir = "/usr/lib/vmware"
authd.proxy.nfc = "vmware-hostd:ha-nfc"
authd.proxy.nfcssl = "vmware-hostd:ha-nfcssl"
authd.proxy.vpxa-nfcssl = "vmware-vpxa:vpxa-nfcssl"
authd.proxy.vpxa-nfc = "vmware-vpxa:vpxa-nfc"
authd.fullpath = "/sbin/authd"
isolation.tools.copy.disable = "FALSE"
isolation.tools.paste.disable = "FALSE"
~

```

Figure 7.17 Disabling of Direct Copy/ Paste

### 7.3.11.1 Analysis

Implementation of this control prevents unauthorized data transfer. This control is essential for ensuring confidentiality.

### 7.3.12 Removal of Unnecessary Devices

All associated devices at the time of VM creation must be manually disabled. Security risks are lessened by removing these unnecessary devices as shown in figure 7.18. USB controller is a common threat point in computer systems. Unnecessary USB ports are blocked in physical environments whereas same are manually removed in case of VMs. Although, floppy drive can also be removed but modern computer systems are designed without this peripheral, being obsolete.

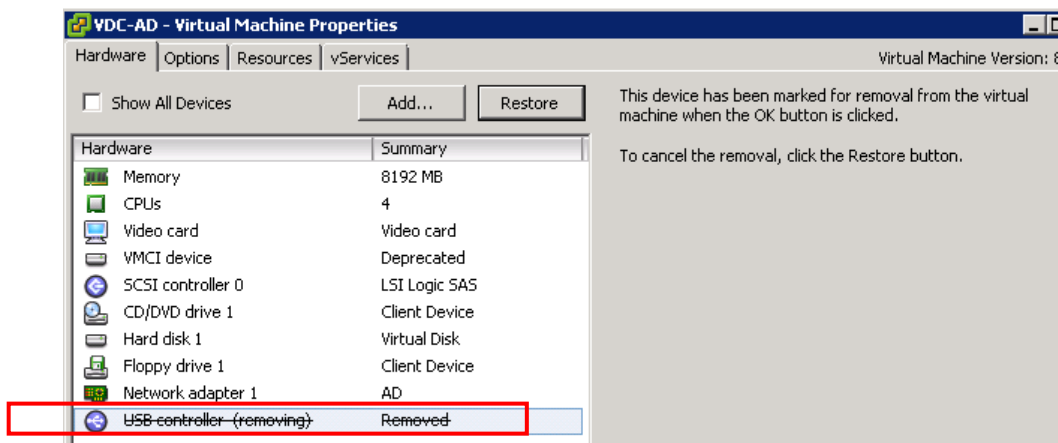


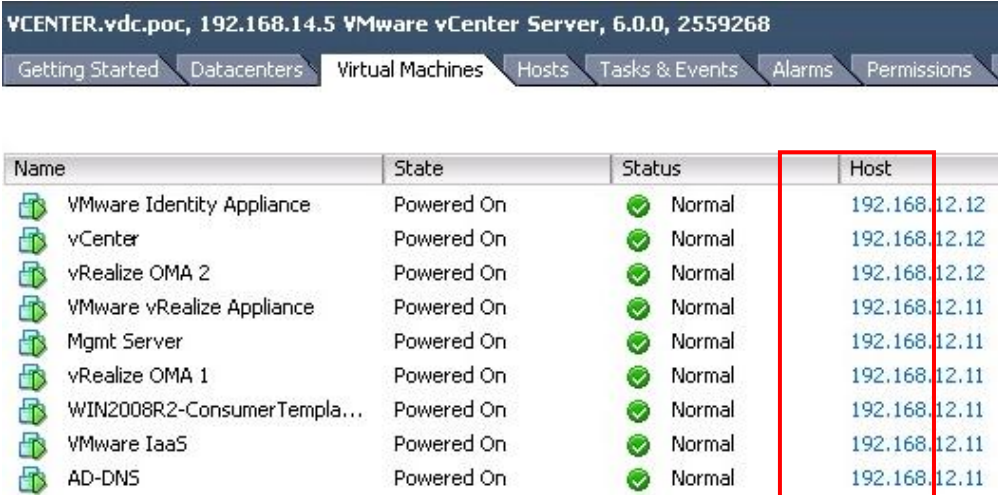
Figure 7.18 Disabling of Unnecessary Devices

### 7.3.12.1 Analysis

Removal of unnecessary devices help in maintaining confidentiality and reducing the overall security threat environment of the datacenter. This control is essential for preventing data leakage via needless devices.

### 7.3.13 Load Balancing

Load balancing is very important for smooth running of datacenter operations. A cluster of two ESXi hosts is setup in which VMs are balanced and also threshold is maintained for meeting HA requirements, as shown in figure 7.19. It must be noted that load balancing does not necessarily means equal amount of VM distribution per host, as some of the VMs consume more computational resources.



The screenshot shows the VMware vCenter Server interface. The title bar reads "VCENTER.vdc.poc, 192.168.14.5 VMware vCenter Server, 6.0.0, 2559268". The navigation tabs include "Getting Started", "Datacenters", "Virtual Machines", "Hosts", "Tasks & Events", "Alarms", and "Permissions". The "Virtual Machines" tab is active, displaying a table of VMs. The table has columns for Name, State, Status, and Host. The Host column is highlighted with a red box. The VMs listed are: VMware Identity Appliance, vCenter, vRealize OMA 2, VMware vRealize Appliance, Mgmt Server, vRealize OMA 1, WIN2008R2-ConsumerTempla..., VMware IaaS, and AD-DNS. All VMs are in a "Powered On" state with a "Normal" status.

Name	State	Status	Host
VMware Identity Appliance	Powered On	Normal	192.168.12.12
vCenter	Powered On	Normal	192.168.12.12
vRealize OMA 2	Powered On	Normal	192.168.12.12
VMware vRealize Appliance	Powered On	Normal	192.168.12.11
Mgmt Server	Powered On	Normal	192.168.12.11
vRealize OMA 1	Powered On	Normal	192.168.12.11
WIN2008R2-ConsumerTempla...	Powered On	Normal	192.168.12.11
VMware IaaS	Powered On	Normal	192.168.12.11
AD-DNS	Powered On	Normal	192.168.12.11

Figure 7.19 Preserving Balanced Load

#### 7.3.13.1 Analysis

Maintaining balanced load is necessary for efficient performance. This control is the best practice for preventing VM sprawl.

### 7.3.14 Monitoring – vRealize Operations Manager

Monitoring is the one of the vital aspect in datacenter security which is more effective and advantageous through NMS. vROM is a specially designed monitoring tool for VMware environments. Same has been deployed in this research for efficient monitoring. Due to its criticality and effectiveness, vROM is configured in cluster for maintaining failover. vROM provides several customizable graphs and dashboards views for getting a clear visibility of alarms and events, as shown in figure 7.20.

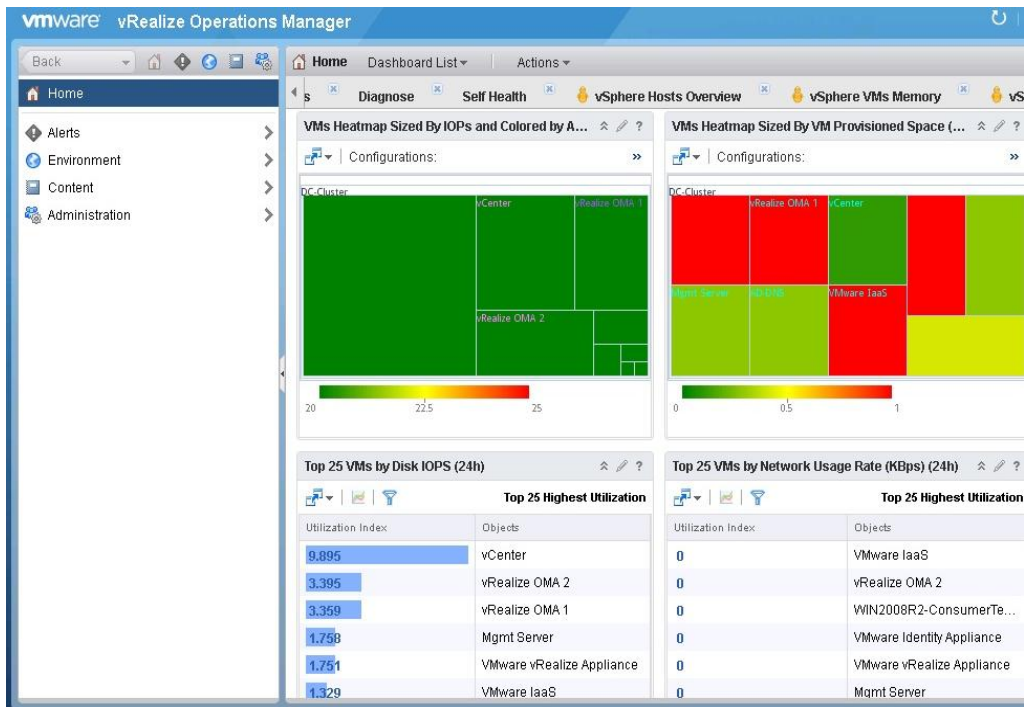


Figure 7.20vROM Dashboards for Efficient Monitoring

vROM continuously evaluates the overall virtual environment and suggest best practice recommendations based on its analytical data over a period of time. In addition to health status and alarms, vROM also suggests if computational and storage resources are enough for near future depending upon the VM growth rate, or additional resources are required for meeting forthcoming VM requirements. Figure 7.21 and figure 7.22 present the essential features of vROM in virtual datacenters.

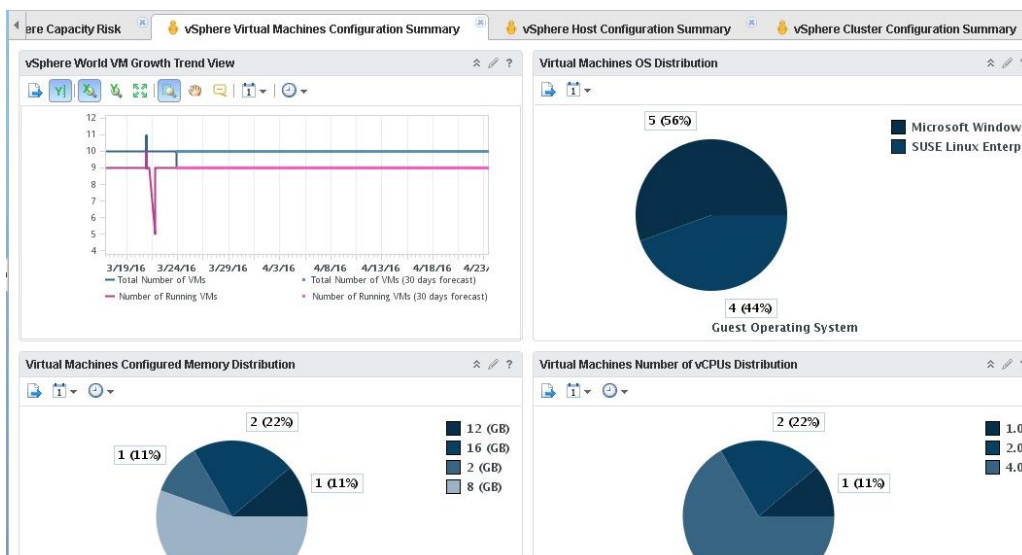


Figure 7.21VM Trends and Analysis

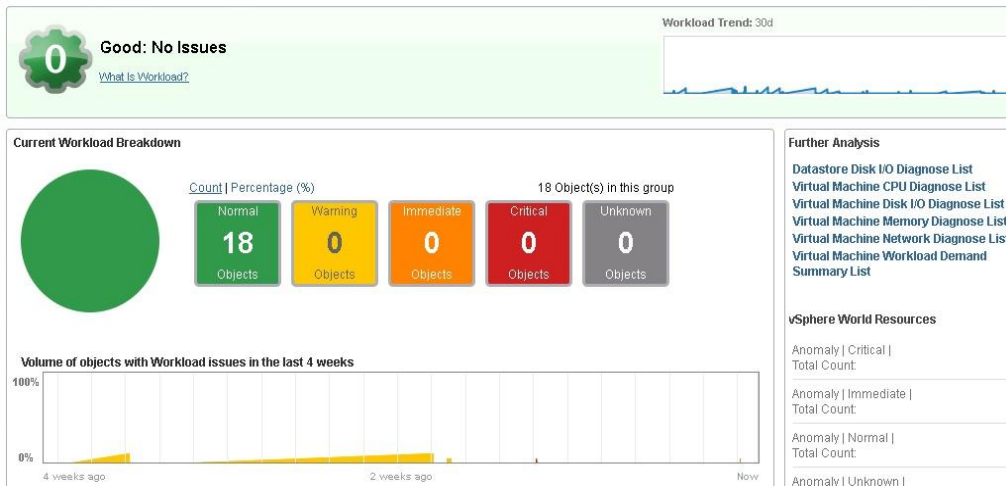


Figure 7.22vROM Workload Reports

### 7.3.14.1 Analysis

vROM deployment is very useful in VMware virtualized datacenters due to its runtime monitoring. Its deployment is independent of VMs so no installation of agents is required. vROM simply integrates with the vCenter server and provides essential recommendations for efficient running of operations after continuous examination of the environment. Overall, proactive monitoring becomes very relaxed and a lot of time as saved by the administrators.

## 7.4 Chapter Summary

This chapter is the actual implementation and analysis of the security model designed in previous chapter. Proposed security model has been implemented and results are analyzed. Different security controls have been employed in the virtualized datacenter to achieve overall in depth defense. This is followed by deployment of NMS for proactive monitoring. The results and benefits of vROM have been analyzed and finally a secured datacenter on virtual environment is established.

### **8. Conclusion**

#### **8.1 Introduction**

The benefits of virtualization in datacenters cannot be ignored and organizations will continue to virtualize their IT environments with VMware being the first option for virtualization platform [2]. Due to increased popularity, this document presents a virtualization security framework based on defense in depth approach as traditional security models will not suffice for VMware virtualized datacenters.

#### **8.2 Objectives Achieved**

Following objective are achieved:

1. Study and understand datacenter virtualization.
2. To identify the security threats and vulnerability of employing datacenter virtualization.
3. To propose a complete security framework for VMware based datacenter virtualization.
4. To implement and analyze the proposed security design for testing and evaluation.

#### **8.3 Limitations**

The limitations are as follows:

1. The security model is developed for VMware environments only, although VMware is the leading virtualization platform.
2. The security model was implemented on Ethernet NICs; however, FC is the choice of network in modern datacenters. Nonetheless, the security design will suffice regardless of network interface.

#### **8.4 Future Direction**

The future directions could be as follows:

1. Development of security design and architecture for cloud environments.
2. SDDCs (Software Defined Datacenters) are one of the latest technology in virtualized setups. The research can be extended to incorporate security of SDDCs.

#### **8.5 Concluding Remarks**

This document presents a secured deployment model of VMware datacenter virtualization. Carelessly planned configurations of the virtualized system are serious system weaknesses



and can result in severe security incidents. VMware implementation is very beneficial in terms of cost and performance but its security needs thorough consideration and efforts which was targeted in this research.

## BIBLIOGRAPHY

- [1] Yacine Hebbal, Sylvie Laniepce and Jean-Marc Menaud, “*Virtual Machine Introspection: Techniques and Applications*”, IEEE 10th International Conference on Availability, Reliability and Security (ARES), Aug 2015.
- [2] Michael Adams - VMware, “*Once Again, VMware Named a Leader in Gartner Magic Quadrant*”, <http://www.vmware.com/radius/vmware-named-leader-gartner-magic-quadrant-x86-server-virtualization-infrastructure/>, 2016
- [3] Jim Smith and Ravi Nair, “*Virtual Machines: Versatile Platforms for Systems and Processes (The Morgan Kaufmann Series in Computer Architecture and Design)*”, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.
- [4] J.Praveen Immanuel Paulraj and R.KannigaDevi, “*Efficient Resource Provisioning Using Virtualization Technology in Cloud Environment*”, International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014.
- [5] IBM Global Technology Services, “*Virtualizing Disaster Recovery Using Cloud Computing*”, Thought Leadership White Paper, January 2012.
- [6] David A. Smith, “*Datacenter Migration and Implementation using VMware*”, 2010.
- [7] Nancy Arya, Mukesh Gidwani and Shailendra Kumar Gupta, “*Hypervisor Security - A Major Concern*”, International Journal of Information and Computation Technology. ISSN 0974-2239 Volume 3, Number 6 (2013), pp. 533-53.
- [8] Doug Hyde, “*A Survey on the Security of Virtual Machines*”,<http://www.cse.wustl.edu/~jain/cse571-09/ftp/vmsec/index.html>, April 2009.
- [9] Radhwan Y Ameen and Asmaa Y. Hamo, “*Survey of Server Virtualization*”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 11, No. 3, 2013.
- [10] Hasan Fayyad-Kazan and Luc Perneel, “*Benchmarking the Performance of Microsoft Hyper-V server, VMware ESXi and Xen Hypervisors*”, Journal of Emerging Trends in Computing and Information Sciences, Vol. 4, No. 12, December 2013.

- [11] Nirmal Sharma, “*Hyper-V and VMware vSphere Architectures: Pros and Cons*”, <http://www.serverwatch.com/server-tutorials/microsoft-hyper-v-and-vmware-vsphere-architectures-advantages-and-disadvantages.html>, 2013.
- [12] Mohamed Fawzi, “*Virtualization and Protection Rings (Welcome to Ring -1)*”, <https://fawzi.wordpress.com/2009/05/24/virtualization-and-protection-rings-welcome-to-ring-1-part-i/>, May 2009.
- [13] S. Suresh, Dr. M. Kannan, “*A Study on System Virtualization Techniques*”, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2014), Vol. 2, Issue Special 1, Jan-March 2014.
- [14] P. Barham, B. Dragovic et al, “*Xen and the Art of Virtualization*”, In Proceedings of the 19th ACM Symposium on Operating Systems Principles, Oct 2003.
- [15] Kamanashis Biswas and Md. Ashraful Islam, “*Hardware Virtualization Support in Intel, AMD and IBM Power Processors*”, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.
- [16] VMware White Paper “*VMware Infrastructure Architecture Overview*”, 2006.
- [17] Robert Moir – Microsoft Security MVP, “*Defining Malware: FAQ*”, <https://technet.microsoft.com/en-us/library/dd632948.aspx>, October 2003.
- [18] D. Balzarotti, M. Cova, C. Karlberger, C. Kruegel, E. Kirda, and G. Vigna, “*Efficient Detection of Split Personalities in Malware*”, in Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, CA, February 2010.
- [19] <https://sites.google.com/site/chitchatvmback/backdoor>
- [20] Dhilung Kirat, Giovanni Vigna and Christopher Kruegel, “*BareBox: Efficient Malware Analysis on Bare-Metal*”, Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC), December 2011.
- [21] Nada Alruhaily, Behzad Bordbar and Tom Chothia, “*Analysis of Mobility Algorithms for Forensic Virtual Machine Based Malware Detection*”, The 13th IEEE International Symposium on Parallel and Distributed Processing with Applications, August 2015.

- [22] Samuel T. King, Peter M. Chen and Yi-Min Wang, “*SubVirt: Implementing Malware with Virtual Machines*”, Proceedings of the IEEE Symposium on Security and Privacy, Pages 314 - 327, 2006.
- [23] A Zhi Wang and Xuxian Jiang, “*HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity*”, 31st IEEE Symposium on Security & Privacy, Oakland CA, May 2010.
- [24] Fannon, Robert C, “*An Analysis of Hardware-Assisted Virtual Machine Based Rootkits*”, <http://hdl.handle.net/10945/42621>, June 2014.
- [25] Iain Kyte, Pavol Zavorsky and Dale Lindskog, “*Enhanced Side-Channel Analysis Method to Detect Hardware Virtualization Based Rootkits*”, IEEE (WorldCIS) World Congress on Internet Security, June 2012.
- [26] Mayank Mishra, Anwasha Das and Purushottam Kulkarni, “*Dynamic Resource Management Using Virtual Machine Migrations*”, IEEE Communications Magazine, Volume: 50, Issue: 9, September 2012.
- [27] Rahul Singh, Prateek Sharma, David Irwin, Prashant Shenoy, and K.K. Ramakrishnan, “*Here Today, Gone Tomorrow: Exploiting Transient Servers in Data Centers*”, IEEE Internet Computing, Volume: 18, Issue: 4, Aug 2014.
- [28] Hanqian Wu, Yi Ding and Chuck Winer, “*Network Security for Virtual Machine in Cloud Computing*”, 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Dec 2010.
- [29] Candid Wueest, “*Threats to Virtual Environments*”, Symantec Internet Security Threat Report, Version 1.0, 12 August 2014.
- [30] Symantec Corporation, “*Internet Security Threat Report*”, Volume 20, April 2015.
- [31] Bart Coppens, Ingrid Verbauwhede, Koen De Bosschere and Bjorn De Sutter, “*Practical Mitigations for Timing-Based Side-Channel Attacks on Modern X86 Processors*”, 30th IEEE Symposium on Security and Privacy, pp 45–60, May 2009.
- [32] Yubin Xia, Yutao Liu, Haibo Chen, Binyu Zang, “*Defending Against VM Rollback Attack*”, IEEE/IFIP 42nd International Conference, 2012.

- [33] Ramalingam Dharmalingam, Arun Nagarle Shivashankarappa and Leonid Smalov, “*Information Security Audit in Virtual Environment*”, The Research Bulletin of Jordan ACM, Volume II(III), 132-136, 2012.
- [34] R. Jithin and Priya Chandran, “*Virtual Machine Isolation - A Survey on the Security of Virtual Machines*”, Second International Conference, SNDS 2014, Trivandrum, India, March 2014.
- [35] Karim Elatov - VMware, “*Best Practices for Virtual Networking*”, <http://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/support/landing-pages/virtual-support-day-best-practices-virtual-networking-june-2012.pdf>, 2009
- [36] Balasubramanian Chandrasekaran, Kyon Holman, Cuong T. Nguyen, and Scott Stanford, “*Enabling VMware ESX Server VLAN Network Configurations*”, Dell Power Solutions, February 2006.
- [37] Azhagarasu A, “*VCP6-DCV Study Guide Part 2: Secure ESXi, vCenter Server, and vSphere Virtual Machines*”, <http://sanenthusiast.com/vcp6-dcv-study-guide-part-2-secure-esxi-vcenter-server-and-vsphere-virtual-machines/>, December 2015.

