



UNIVERSIDADE DA BEIRA INTERIOR
Engenharia

Performance Implications For the Use of Virtual Machines Versus Shielded Virtual Machines in High-Availability Virtualized Infrastructures

Evaldo dos Prazeres Saraiva Chindele

(Versão Definitiva Após Defesa Pública)

Dissertation for obtaining the degree of Master of Science in
Computer Science and Engineering
(2nd Cycle Studies)

Advisor: Prof. Dr. Mário Marques Freire

Covilhã, Julho 2018

Dissertation prepared at Instituto de Telecomunicações, within IT Branch - Covilhã, by Evaldo dos Prazeres Saraiva Chindele, Bachelor of Science in Computer Science by Universidade Lusíada de Angola (Angola), advised by Dr. Mário Marques Freire, Senior Researcher of the Instituto de Telecomunicações and Full Professor of the Department of Computer Science at Universidade da Beira Interior, and submitted to Universidade da Beira Interior for obtaining the degree of Master of Science in Computer Science and Engineering.



Dedicatory

I dedicate this work to my family.

Acknowledgements

This work is the culmination of a very important stage in my academic life, which could not be achieved without the support and dedication of very important people whom I express my humble gratitude. Heartfelt thanks goes:

To almighty God creator of heaven and earth.

To my parents, André Bumba Chindele and Isabel Chindele for being my base and my foundation. For all the emotional support, they gave me during this work.

To my brothers and sisters, Leandro, Hino, Hugo, Sádía, Bruno, Anderson and Ariana, for all love and support during this phase.

To My fiancée, Elsa Évora Lopes, my greatest supporter. Thank you for all love. Thank you for the patience of seeing my dream come true, thank you for always taking care of me, even at distance, and giving me a shoulder and a lap in those difficult moments and for always being by my side every day. This victory is also your love. Love you boo.

To my advisor, Professor Mário Freire, for all the wisdom and patience demonstrated in the accomplishment of this work. In addition, to all the teachers that I had during the Master's degree for sharing the knowledge that I will take forever.

To all my friends and colleagues who always gave me a support during the accomplishment of this work.

To Dr. Raimundo Wapota, dean of the ISPH, and all the people who made possible the coming to Portugal for the accomplishment of the master's degree.

To INABE for making the scholarship available for the master's degree.

To David de Carvalho, UBI Informatics Specialist, for the willingness to help whenever possible in the practical part of the work.

Resumo

O uso da virtualização em centro de dados ou provedores de serviços ou mesmo em ambientes de computação em nuvem traz muitos benefícios. A virtualização, seja para serviços, aplicações ou servidores, não é mais uma tendência a ser uma realidade em muitos setores e áreas, seja dentro ou fora da área de tecnologia. Portanto, com esse uso emergente de virtualização, as empresas têm vindo a questionar muito sobre o desempenho e a segurança do uso de máquinas virtuais em infraestruturas de alta disponibilidade. Controlar o acesso às máquinas virtuais é um problema de segurança que todos os *hypervisors* possuem, como *VmWare vSphere*, *Hyper-V* ou *KVM*. Para tornar as máquinas virtuais mais seguras, a Microsoft introduziu as máquinas virtuais blindadas.

Neste sentido, esta dissertação apresenta um estudo sobre conceitos-chave por trás de máquinas virtuais, *Guarded Fabric*, *Host Guardian Service*, *Guarded Hosts* e máquinas virtuais Blindadas. Uma Máquina Virtual Blindada é um recurso da Geração 2 (com suporte no *Windows Server 2012* e posterior) que vem com um *Trusted Platform Module (TPM)* virtual, e que apenas pode ser executada em hospedeiros protegidos e aprovados na *fabric* e é criptografada usando o *BitLocker*.

Para dar suporte ao nosso estudo foi configurado um ambiente de teste experimental, envolvendo um *failover cluster* com virtualização nativa ao nível de *hardware* com o *Windows Server 2016 Hyper-V*. No ambiente de teste, foi implementado e configurado um *failover cluster*, *FreeNAS Storage*, *iSCSI Target*, Máquinas Virtuais, *Guarded Fabric* e Máquinas Virtuais Blindadas. Após a implementação do ambiente de teste, um conjunto de testes e experiências foram realizados para estudar as implicações dos desempenhos das máquinas virtuais versus máquinas virtuais Blindadas em Infraestruturas Virtualizadas de Alta Disponibilidade. Por fim, fizemos a análise nos resultados trabalhados através dos testes, de acordo com os conceitos definidos no segundo capítulo da dissertação e com o ambiente de teste implementado.

Um conjunto de experiências foram realizadas em máquinas virtuais regulares e máquinas virtuais blindadas para avaliar o desempenho em termos de CPU, RAM e velocidade de escrita no disco. Os resultados mostram que o uso de máquinas virtuais blindadas conduz a uma pequena degradação do desempenho em comparação com o uso de máquinas virtuais regulares, mas, por outro lado, também se verificou que as máquinas virtuais blindadas permitem restringir o acesso às máquinas virtuais apenas para correrem em hosts confiáveis, além de impedirem que administradores não autorizados e malwares comprometam a máquina virtual.

Palavras Chave

Segurança de virtualização, Máquina Virtual Blindada, *Hyper-V*, *Datacenter*, *Host Guardian Service*, *Guarded Fabric*, *failover cluster*, Desempenho

Abstract

Use of virtualization in datacenter or service providers or even in cloud computing environments brings many benefits. Virtualization, whether it is for services, applications or servers, is no longer a trend to be a reality in many industries and areas, whether in or outside the technology area. Therefore, with this emergent use of virtualization companies have been asking a lot about the performance and security of using virtual machines in a highly availability infrastructures. Controlling the access to Virtual Machines is a security issues that all the hypervisors have, such as, VMware vSphere, Hyper-V or KVM. To make virtual machines more secure Microsoft has introduced the concept of Shielded virtual machines.

Taking this into account, this dissertation presents a study on key concepts behind virtual machines, Guarded Fabric, Host Guardian Service, Guarded Hosts and shielded virtual machines. A Shielded VM is a Generation 2 feature (supported on Windows Server 2012 and later) that comes with a virtual Trusted Platform Module (TPM), which can only run on healthy and approved hosts in the fabric and is encrypted using BitLocker.

In order to support our study an experimental bed test has been setup, involving a failover cluster with native virtualization at the hardware level with Windows Server 2016 Hyper-V. In the test environment, a failover clustering, FreeNAS Storage, iSCSI Target, VMs, Guarded Fabric and Shielded virtual machines have been implemented and configured. After the implementation of the bed test, a set of tests and experiments have been made in order to study the performance implications for the use of virtual machines versus shielded virtual machine in High Availability Virtualized Infrastructures. Finally, an analysis at the results worked through the tests has been made, according to the Background made in the first part and the bed test deployed.

A set of experiments has been made in virtual machines and shielded virtual machines in order to evaluate its performance in terms of CPU, RAM and writing speed. The results show that the use of shielded virtual machines leads to a small degradation of performance compared to the use of regular virtual machines, but, on the other hand, it has also been shown that the shielded virtual machines allows to restrict access to the virtual machines only for run on trusted hosts, and prevent unauthorized administrators and malwares from compromising the virtual machine.

Keywords

Virtualization security, Shielded virtual machine, Hyper-V, Datacenter, Host Guardian Service, Guarded Fabric, Failover cluster, Performance

Resumo alargado

O uso da virtualização em centro de dados ou provedores de serviços ou mesmo em ambientes de computação em nuvem traz muitos benefícios. A virtualização, seja para serviços, aplicações ou servidores, não é mais uma tendência a ser uma realidade em muitos setores e áreas, seja dentro ou fora da área de tecnologia. Portanto, com esse uso emergente de virtualização, as empresas têm vindo a questionar muito sobre o desempenho e a segurança do uso de máquinas virtuais em infraestruturas de alta disponibilidade. Controlar o acesso às máquinas virtuais é um problema de segurança que todos os hypervisors possuem, como VmWare vSphere, Hyper-V ou KVM. Pode acontecer, por exemplo, que alguém mal-intencionado possa obter e deixar uma empresa com várias máquinas virtuais, isto porque elas estão todas centralizadas em um diretório. Uma Máquina Virtual é praticamente um arquivo armazenado no disco. Se uma máquina virtual sair de uma organização, seja maliciosa ou acidentalmente, essa máquina virtual pode ser executada em qualquer outro sistema. Este é um problema muito perigoso para cada plataforma de virtualização hoje, seja *VMware*, *Hyper-V*, *Qemu*, *KVM* ou qualquer outro *hypervisor*. A principal prioridade é proteger ativos de alto valor na organização, como servidores de arquivos confidenciais, controladores de domínio e sistemas de recursos humanos. Um exemplo perfeito é o controlador de domínio. Imagine se o controlador de domínio de alguma forma sair da empresa. O controlador de domínio é literalmente a chave de uma rede empresarial.

As máquinas virtuais também têm problemas de desempenho: atualmente, não há métodos consolidados para medir o desempenho de ambientes virtualizados. No entanto, a introdução de uma camada extra de *software* entre o sistema operacional e o hardware, o *Virtual Machine Monitor* ou o *hypervisor*, gera um custo de processamento mais elevado comparando com plataformas não virtualizadas. Outro ponto importante a ser observado é que não se sabe exatamente quantas máquinas virtuais podem ser executadas por processador, sem perda de qualidade de serviço. Para tornar as máquinas virtuais mais seguras, a Microsoft introduziu as máquinas virtuais blindadas.

Neste sentido, esta dissertação apresenta um estudo sobre conceitos-chave por trás de máquinas virtuais, *Guarded Fabric*, *Host Guardian Service*, *Guarded Hosts* e máquinas virtuais Blindadas. Uma Máquina Virtual Blindada é um recurso da Geração 2 (com suporte no Windows Server 2012 e posterior) que vem com um *Trusted Platform Module (TPM)* virtual, que apenas pode ser executada em hospedeiros protegidos e aprovados na *fabric* e é criptografada usando o *BitLocker*. Isso significa que a máquina virtual blindada protegerá as máquinas virtuais de administradores comprometidos ou mal-intencionados no ambiente seguro, como administradores de armazenamento, administradores de arquivos ou todos os administradores do sistema em geral, criptografando o disco usando *BitLocker* e o estado das máquinas virtuais de forma que somente os donos das máquinas virtuais ou administradores autorizados possam ter acesso as máquinas virtuais. Para dar suporte ao nosso estudo, foi configurado um ambiente

de teste experimental, envolvendo um *failover cluster* com virtualização nativa ao nível de hardware com o *Windows Server 2016 Hyper-V*. No ambiente de teste, foi implementado e configurado um *failover cluster*, *FreeNAS Storage*, *iSCSI Target*, Máquinas Virtuais, *Guarded Fabric* e Máquinas Virtuais Blindadas. Após a implementação do ambiente de teste, um conjunto de testes e experiências foram realizadas para estudar as implicações dos desempenhos das máquinas virtuais versus máquinas virtuais Blindadas em Infraestruturas Virtualizadas de Alta Disponibilidade. Por fim, fizemos a análise nos resultados trabalhados através dos testes, de acordo com os conceitos definidos no segundo capítulo da dissertação e com o ambiente de teste implementado.

Um conjunto de experiências foram realizadas em máquinas virtuais regulares e máquinas virtuais blindadas para avaliar o desempenho em termos de CPU, RAM e velocidade de escrita no disco. Os resultados mostram que o uso de máquinas virtuais blindadas conduz a uma pequena degradação do desempenho em comparação com o uso de máquinas virtuais regulares, mas, por outro lado, também se verificou que as máquinas virtuais blindadas permitem restringir o acesso às máquinas virtuais apenas para correrem em hosts confiáveis, além de impedirem que administradores não autorizados e malwares comprometam a máquina virtual

Contents

Dedicatory.....	v
Acknowledgements	VII
Resumo	IX
Abstract.....	XI
Resumo alargado	XIII
Contents	XV
List of figures.....	XVII
List of tables.....	XIX
Acronyms	XXI
1 Introduction	1
1.1 Focus and Scope	1
1.2 Problem Definition and Objectives	2
1.3 Adopted Approach to Solve the Problem	2
1.4 Main Contributions.....	3
1.5 Limitations of This Work.....	3
1.6 Organization of the Dissertation	3
2 Background on Shielded virtual machines.....	5
2.1 Introduction.....	5
2.2 Basics of Virtualization Concepts	5
2.2.1 Virtual Machines.....	7
2.2.2 Implementation Level of Virtualization	9
2.2.3 Advantages and Disadvantages of Virtual Machines.....	11
2.2.4 Failover Clustering and VM Migration.....	13
2.3 Shielded virtual machines and Guarded Fabric in Windows Server 2016	15
2.3.1 Guarded Fabric	16
2.3.2 Attestation Modes in the Guarded Fabric.....	18
2.3.3 Assurances Provided by the Host Guardian Service	20
2.3.4 Cryptographic Keys Used for Shielded VMs	21
2.3.5 Shielded Data	22
2.4 Types of Virtual Machines that a Guarded Fabric Can Run.....	24
2.5 Encryption of Virtual Machines in VMware vSphere 6.5.....	25
2.6 Conclusions	26
3 Specification and Implementation of the Experimental Test Bed	27
3.1 Introduction.....	27
3.2 Architecture of The Experimental Test Bed	27

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures	
3.2.1	Used Tools for the Implementation of the Test Bed 27
3.2.2	Overview of the High Availability Architecture with VMs 28
3.2.3	Overview of the Guarded Fabric and Shielded VM Architecture 29
3.3	Implementation of the Failover Cluster in Windows Server 2016 Hyper-V 31
3.4	Deploying the Guarded Fabric and Shielded virtual machines..... 38
3.5	Conclusions 48
4	Experiments and Results 49
4.1	Introduction..... 49
4.2	Performance Metrics 49
4.2.1	Benchmarking..... 49
4.2.2	Virtual Machines..... 50
4.2.3	Shielded virtual machines 50
4.3	Virtual Machine Workloads 50
4.4	Performance Evaluation Using the First Workload 51
4.5	Performance Evaluation Using the Second Workload..... 56
4.6	Conclusions 58
5	Conclusions and Future Works..... 59
5.1	Main Conclusions 59
5.2	Directions for Future Work..... 60
References 61

List of Figures

Figure 2.1 Computer Without Virtualization -----6

Figure 2.2 Computer With Virtualization -----7

Figure 2.3 Native Virtualization -----8

Figure 2.4 Hosted Virtualization-----9

Figure 2.5 Virtualization level from hardware to application (adapted from [7]).----- 10

Figure 2.6 Schematic representation of a 2-node failover----- 14

Figure 2.7 Host Guardian Service Attestation and Key Protection (adapted from [4]) ----- 17

Figure 2.8 Verification process of Shielded virtual machine (adapted from [4]). ----- 20

Figure 2.9 Shielding data file and elements (adapted from [4]).----- 23

Figure 3.1 Experimental Setup of Failover Cluster of the Virtual Machine 29

Figure 3.2 Experimental deploy of Shielded virtual machine 30

Figure 3.3 Available Disks on FreeNas Seen on the Web Interface 33

Figure 3.4 Configuration of the Block Level and Portal Group ID on FreeNas..... 33

Figure 3.5 Individual Disks Assigned in FreeNas 34

Figure 3.6 Configuration of FreeNas Target and Extent..... 34

Figure 3.7 Installation of the Hyper-V Role..... 35

Figure 3.8 Adding iSCSI Target Portal Address for Connect the Host with FreeNAS..... 36

Figure 3.9 Command to create the Hyper-V Cluster 37

Figure 3.10 Overview of the Cluster Resources 38

Figure 3.11 Command to Install the HGS Role 39

Figure 3.12 Setting the Admin Password for the HGS Server 40

Figure 3.13 Command for Installation the HGS Service 40

Figure 3.14 Commands to Create a Self-signed Certificate and Export 41

Figure 3.15 Commands to Create an Encryption Certificate and Export..... 41

Figure 3.16 Commands to initialize the HGS server Using Admin-Trusted Attestation 42

Figure 3.17 DNS forwarder from The HGS Domain to the Fabric Domain 42

Figure 3.18 DNS Forwarder from The HGS Domain to the Fabric Domain (netdom) 42

Figure 3.19 DNS Forwarder From the Fabric Domain to the HGS Domain..... 43

Figure 3.20 Adding a Security Group in the HGS Server to be Used to Identify the Hosts that
Are Trusted to run the Shielded VMs. 43

Figure 3.21 Configuration of the Host’s Key Protection and Attestation URLs of the Guarded
Host..... 43

Figure 3.22 Rung Diagnostics of the HGS Server Configuration 44

Figure 3.23 Preparing an Operating System VHDX for Windows Template Disk 44

Figure 3.24 Installation of Shielded VM Tools and Creation of a Self-Signed Certificate 45

Figure 3.25 Shielded Template Disk Creation Wizard 45

Figure 3.26 Obtain a Certificate for a Remote Desktop and Installation of a Guarded Fabric
Tools 46

Figure 3.27 Command to Create a Shielding Answer File 46

Figure 3.28 Selected Trusted Fabric..... 47

Figure 3.29 Command to Create a New Shielded virtual machine 47

Figure 4.1 Regular Virtual Machine Performance Evaluation..... 51

Figure 4.2 Shielded virtual machine Performance Rating..... 52

Figure 4.3 Shielded virtual machine versus Virtual Machine Performance Rating..... 53

Figure 4.4 Memory Performance Between Virtual Machines and Shielded VM 54

Figure 4.5 Time to Install an Operating System 54

Figure 4.6 Boot time of Shielded VM and Virtual Machine 55

Figure 4.7 Comparison of Memory Consumption between VM and Shielded VM 57

List of Tables

Table 2.1	Attacks that Shielded VMs can defend against (adapted from [19]).	18
Table 2.2	Attestation modes (adapted from [4]).	19
Table 2.3	Types of virtual machine that a guarded fabric can run	24
Table 2.4	Differences between encryption-supported and shielded VMs (adapted from [4]).	25
Table 3.1	Network Planning for the Failover Cluster	32
Table 3.2	Networking planning to implement the Guarded Fabric	38
Table 4.1	Summary of the Performance Results	56
Table 4.2	Script Runtime	56
Table 4.3	CPU performance for the Scrip execution	57

Acronyms

AD - Active Directory

ADDS - Active Directory Domain Service

API - Application Program Interface

AES-NI - Advanced Encryption Standard - New instruction

CA - Certificate Authority

CPU - Central Processing Unit

CSV - Cluster Shared Volume

DNS - Domain Name System

DISM - Desktop Image Service Manager

DR - Disaster Recovery

DC - Domain Controller

FQDN - Fully Qualified Domain Name

GPT - Guid partition

GPU - Graphic Processing Unit

HGS - Host Guardian Service

HAL - Hardware Abstraction Layer

HR - Human Resources

ID - Identifier

IP - Internet Protocol

I/O - Input/output

IT - Information Technology

ISA - Instruction Set Architecture

ISCSI - Internet Small Computer Systems Interface

JVM - Java Virtual Machine

KMIP - Key Management Interoperability Protocol

KMP - Key Management Server

KP - Key Protector

KVM - Kernel-based Virtual Machine

LAN - Local Area Network

LM - Live Migration

NAS - Network-Attached Storage

NLB - Network Load Balancing

NTFS - New Technology File System

OS - Operating System

PKI - Public Key Infrastructure

PFX - Personal Information Exchange

RAID - Redundant Array of Independent Disks

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures

RAM - Random Access Memory
RDP - Remote Desktop Connection
SVM - Shielded virtual machine
SSL - Secure Sockets Layer
SID - Security Identifier
SSH - Secure Shell
TPM - Trusted Platform Module
URL - Uniform Resource Locator
VHDX - Hyper-V Virtual Hard Disks
VHD - Virtual Hard Disk
Vtpm - Virtual Trusted Platform Module
VM - Virtual Machine
VMM - Virtual Machine Monitor
WS - Windows Server

Chapter 1

Introduction

1.1 Focus and Scope

Virtual machines (VMs) are nowadays essential for large-scale computing infrastructures, being virtualization presently used in many industries, not only in the computer technology sector. With the widespread use of virtual machines, the need to protect VMs is emerging, leading to the creation of several security mechanisms against unauthorized use, e.g. by administrators. Since it is easier to live migrate, backup and replicate virtual machines [1] and, in practical terms, each virtual machine may be seen as a file stored on disk, this means that it may be easier to modify or even copy all network settings to an external storage device which may be carried out to the company or one can get and leave the company with multiple VMs and run the VMs anywhere else. These are very serious security flaws allowed by current hypervisors [1], such as VMware ESXi [2], KVM (Kernel-based Virtual Machine) [3], Xen [4], Microsoft Hyper-V, among others [1], [5].

Shielded virtual machines have been proposed to protect against security flaws, including the ones reported above and were introduced in Windows server 2016 and in other recent hypervisors [1]. A shielded virtual machine is a Generation 2 feature supported on Windows Server 2012 and later that includes a virtual Trusted Platform Module (TPM), which is encrypted using BitLocker, and can only run on healthy and approved hosts in the fabric [6]. This means that shielded virtual machines will protect virtual machines from compromised or malicious administrators in the fabric, such as storage administrators, file administrators, or all the system administrators in general by encrypting disk using BitLocker and the state of virtual machines in a way that only virtual machines or tenant administrators can access the VMs [1].

In this dissertation, we intend to study the performance implications for the use of virtual machines versus shielded virtual machines in virtualized infrastructures of high availability.

1.2 Problem Definition and Objectives

Virtualization is the core of cloud computing and brings many benefits to companies. However, the use of virtual machines introduces new security flaws. Recently, shielded virtual machines have been proposed to provide a protection against those security flaws, but the use of shielded virtual machines lead to a performance degradation. Therefore, it is necessary to quantify the performance degradation due to the use of shielded virtual machines in order to allow further tradeoff studies between security and performance.

The research problem addressed in this dissertation consists of evaluating the performance of shielded virtual machines and comparing it with the performance of virtual machines in high-availability virtualized infrastructures.

The main objective of this dissertation is to specify and implement a failover cluster with native virtualization at the hardware level that includes virtual machines and shielded virtual machines and to study the performance issues due to the use of virtual machines versus shielded virtual machines over the implemented failover cluster.

As specific objectives, we have the following ones:

1. To study the key concepts associated with native hardware virtualization and highly available virtualized infrastructures;
2. To study and compare native hypervisors that support shielded virtual machines;
3. To specify and implement an experimental test bed, involving a failover cluster with native virtualization at the hardware level, with support for shielded virtual machines;
4. To test and validate the implemented test bed;
5. To evaluate experimentally the performance implications for the use of virtual machines versus shielded virtual machines over the implemented failover cluster.

1.3 Adopted Approach to Solve the Problem

The use of virtualization in datacenter or in cloud computing environments brings many benefits and one of them is cost reduction. Thus, it is natural companies nowadays opt for virtualizing their computing infrastructures. Therefore, with this emergent use, companies have been asking about performance and security of using virtual machines in highly-availability infrastructures. To increase the security of the virtual machines Microsoft introduced shielded virtual machines or protected virtual machines. To solve the problem one has to implement a test bed, involving a failover cluster with native virtualization at the hardware level with

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures
Windows Server 2016 Hyper-V, supporting a guarded fabric to study the performance implications for the use of virtual machines versus shielded virtual machines.

1.4 Main Contributions

The main contribution of this work is the study of performance impact for the use of Virtual Machines versus Shielded virtual machines in a failover cluster based on Windows Server 2016 and the deployment of a Guarded Fabric and shielded VM through Admin-trusted attestation.

1.5 Limitations of This Work

In the opinion of the author, the present work has the two following limitations:

- Lack of additional equipment that was not expected to be necessary at the beginning of the research work, to implement shielded virtual machines with high-availability;
- The tests need to be validated in real production environments.

1.6 Organization of the Dissertation

This dissertation consists of five chapters and references. After this chapter dedicated to the introduction of the dissertation, the remaining chapters are chapter 2 - Background on shielded virtual machine, chapter 3 - Specification and Implementation of the experimental test bed, chapter 4 - Experiences and Results and finally, chapter 5 - Conclusions and Future Works. Chapter 2 describes the main concepts and technologies for the accomplishment of this work. First, it presents the basics of virtualization and then defines the concept of Guarded Fabric and shielded virtual machines. Chapter 3 describes the architecture of the test bed and provides a description of the implementations and configurations of failover clustering, FreeNAS Storage, Internet Small Computer Systems Interface (iSCSI)-Target, VMs, Guarded Fabric and shielded virtual machines. Chapter 4 presents and discusses experiments performed over the test environment and the results. Finally, chapter 5 presents the main conclusions and directions for future work.

Chapter 2

Background on Shielded virtual machines

2.1 Introduction

This chapter presents a study of the main concepts and technologies that formed the basis for the accomplishment of this work. At the outset, it will address the emergence of **virtual machines**, as well as the corresponding definition and the main types of virtualization that exist. We will show the main advantages and disadvantages of using virtualization in high performance environments and the need for the emergence of mechanisms and techniques capable of guaranteeing better security and protection of the machines, such as, the Shielded virtual machines. In addition, at the end we will discuss shielded virtual machines and how they work in order to be able to encrypt and make the virtual machines more secure.

2.2 Basics of Virtualization Concepts

Information Technology (IT) has been experiencing a dynamic and highly specialized task oriented, in all its area of activity [7]. For this reason, several new tendencies were appearing, and a huge challenge arose in order to be able to control, guarantee and manage computer infrastructures on a large scale [7]. The challenge was to create mechanisms that allow the expansion of IT infrastructures to be able to meet the requirements of the current ones, as far as IT environments [7] are concerned, creating the possibility of, for example, having multiple machines running in a small place without having many hardware equipment concentrated in the place.

Small businesses with little background at their inception are unable to set up a large Data Center Infrastructure because hardware and maintenance costs are too high as they could simply rent infrastructure, platform, or software services to companies that already have a large amount of equipment available and they can cede some to these small businesses. Therefore, to solve these and more problems in the IT environment, the trend of cloud computing has been created. “Cloud computing is a technology of inter-connected servers and resources that use virtualization to utilize the resources, flexibility and scalability”[8]. Virtualization can simplify management and improve resource efficiency, playing thus, a big role in Cloud Computing. It should be pointed out that many people may consider cloud

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures computing and virtualization similar, although they are quite different in nature and applicability [7].

The emergence and use of virtualization technologies have somehow provided a great opportunity for the development and growth of cloud computing, as well as, cluster, parallel, distributed and grid computing. Virtualization technology benefits the computer and IT industries by enabling users to share expensive hardware resources multiplexing VMs on the same set hardware hosts [9].

“Virtualization is a computer architecture technology by which multiple virtual machines (VMs) are multiplexed in the same hardware machine” [9]. A conventional computer has a single OS image. This offers a rigid architecture that tightly couples application software to a specific hardware platform. Some software running well on one machine may not be executable on another platform with a different instruction set under a fixed OS. Virtual machines (VMs) offer novel solutions to underutilized resources, application inflexibility, software manageability, and security concerns in existing physical machines [8].



Figure 2.1: Computer without virtualization.

In figure 2.1 we have a traditional architecture of a normal computer without virtualization, we have first the hardware: CPU, Memory, Network interfaces, Disk; and then we have the host operating system that will be sending the instructions for the hardware by the applications.

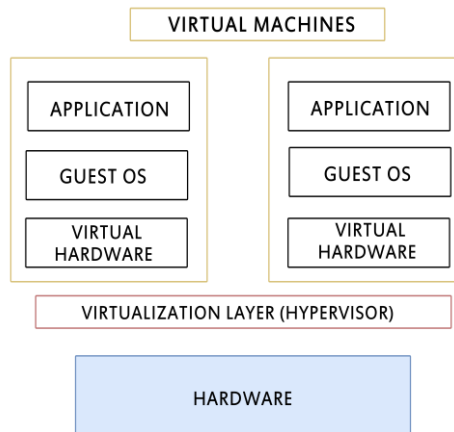


Figure 2.2: Computer with virtualization.

Figure 2.2 shows the concept of a traditional computer changed, when the virtualization came out. On the bottom of the figure, we have the Hardware running the Host OS, then there is another layer that we call **Virtualization layer, Hypervisor or Virtual Machine Monitor (VMM)**, that is the middleware between the underline hardware and Virtual Machines. Virtualization creates a virtual hardware to hold the Guest OS of the Virtual Machine installed. In my opinion, based on the figure 2, we can say that, the virtual machine is made up on top of the “*virtual hardware*”, working as if it were real hardware in which we can install the operative System and later the applications.

2.2.1 Virtual Machines

Virtual machines (VMs) offer innovative solutions for:

- Underutilized resources;
- Inflexibility at the application level;
- Software management;
- Security concerns in an existing physical machines.

According to [10], a **Virtual machine (VM)** is an operating system (OS) or application environment that is installed on software, which imitates dedicated hardware. This mean that, the end user will work as the same c on a virtual machine as they would have on dedicated hardware.

Guest OS: Operating system running in a virtual machine environment that would otherwise run directly on a separate physical system.

Virtualization layer: middleware between the underlying hardware and virtual machines also referred to as **hypervisor** or **virtual machine monitor (VMM)**.

Whatever operating system we want to use we can install in a VM, and this machine will be built with the resources managed by a guest operating system (guest OS). In order for the virtual machine to be able to perform specific tasks as if it were a real computer, it is necessary to install a middleware layer called a **hypervisor** or **Virtual Machine Monitor**. The VM approach provides operating system and application independence from hardware [9].

Type of Hypervisors:

- **Native VM (native / bare metal):** Installed through a VMM designated by hypervisor in privileged mode.

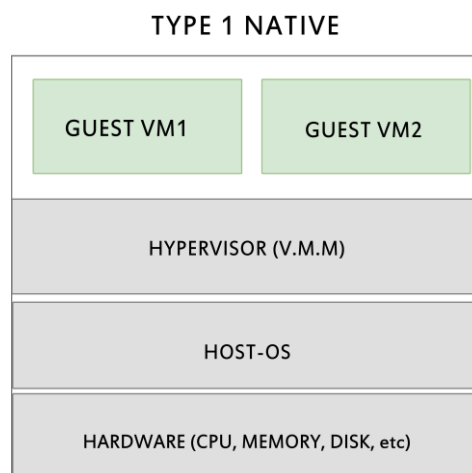


Figure 2.3: Native virtualization.

Type 1 hypervisors , named Native Virtual Machine, will run straightly on the host’s equipment to control all the fitting and guest operating systems and have direct communication with the hardware, eliminating this way the need for an OS [7][8].

At this dissertation, a failover cluster with **native** virtualization at the **hardware level** that includes virtual machines versus shielded virtual machines was implemented.

- **VM hosted:** Here, the VMM runs in non-privileged mode. The host operating system (host OS) does not need to be modified.

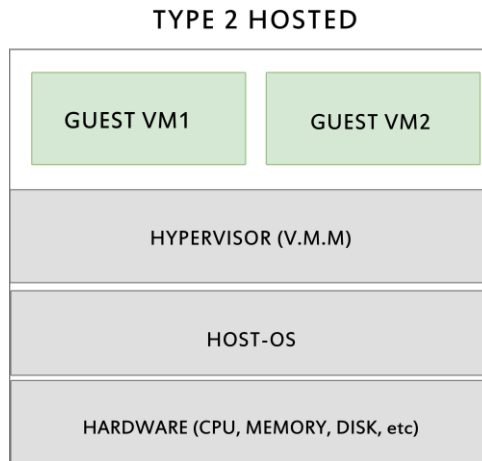


Figure 2.4: Hosted virtualization.

Type 2 hypervisors, named Hosted, will run directly on host OS framework including the layer of hypervisor, they will require a base operating system to be installed since they are practically adding the virtualization feature to the base operating system. Although it seems to gain points because of flexibility with configuration policies, any security issues in the underlying operating system can affect the whole system, that is, it affects all virtual machines installed on top of the OS host [8], [7].

2.2.2 Implementation Level of Virtualization

The main function of the software layer for virtualization, or the hypervisors is to virtualize the physical hardware of a host machine into virtual resources (virtual hardware) to be used exclusively by VMs. Virtualization software creates abstraction of VMs by interposing a multi-level virtualization layer of a computer system [9], [11].

Common virtualization layers include [9]:

- The instruction set architecture level (ISA);
- The hardware level;
- The operating system level;
- The library level of support,
- The application level.

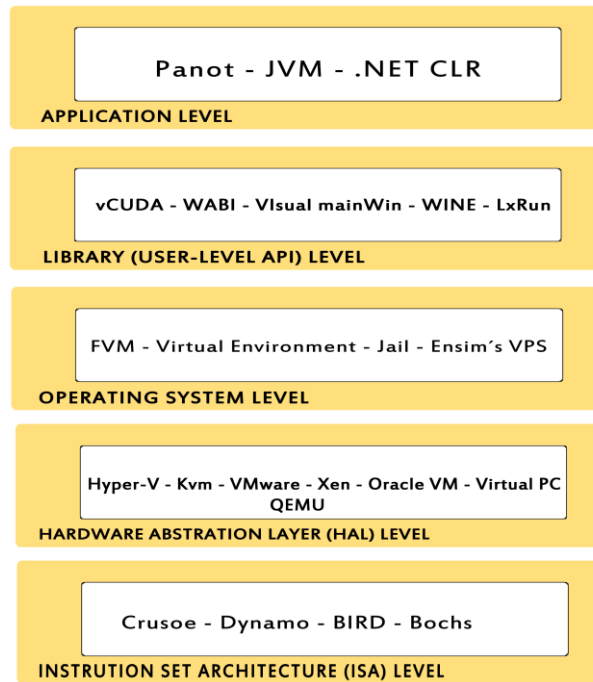


Figure 2.5: Virtualization level from hardware to application (adapted from [7]).

As how we show in figure 5, we have five levels of virtualization, starting from ISA level to the application level. In this dissertation, we focus more on the Hardware level, setting up a failover cluster with native virtualization at the hardware level that includes virtual machines versus shielded virtual machines.

At the **ISA level**, as it is shown on the figure, the main Hypervisors are Crusoe, Dynamo, BIRD and Bochs. On this virtualization level, the virtualization is performed by emulating a given ISA by the ISA of the host machine; this means that for example, MIPS binary code can run on an x86-based host machine with the help of ISA emulation and the basic emulation method is through code interpretation. During the emulation an interpreter program interprets the source instruction to target instructions one by one [9].

At the **HA level**, the level above the ISA level, as the main hypervisors we have: Windows Server 2016 Hyper-V, which is the hypervisor that we are using in this dissertation to create our bed test, KVM, VMware (Vsphere, Workstation), Xen, Oracle VM, Virtual PC and some many others. At this level, the approach is to generate a virtual environment for a VM and the process manages the underlying hardware through virtualization. The idea here, is to virtualize the computer's hardware resources, such as memory, disks, processors and I/O devices by upgrading the hardware utilization rate by multiple users concurrently [9].

Above the HA level, we will find the **Operating System level**. In figure 2.5, we show the examples of the hypervisors that can operate at this level of virtualization such as FVM, Virtual Environment, WINE and LxRun.

At this level, the hypervisors virtualize the system call interface, they can control what user-space processes can do and capture calls from user-space to kernel-space. This level, creates isolated *containers* on a single physical server and the OS instances to utilize the hardware in data centers, and which means that the container will behave like real servers [9].

At the **Library level** as it shown in the figure 2.5, we find vCuda, WABI, Visual mainWin, WINE and LxRun. The library level intercept API calls to redirect to different implementations. Most applications use APIs exported by user-level libraries rather than using system calls by the OS [9]. By controlling the communication link between applications and the rest of a system through API, makes possible the virtualization with library interfaces [9].

Finally, we have the **Application level**; some examples are Java Virtual Machine (JVM), Panot, NET, and CLR. Here, the run-time will go to implement a virtualization layer as an application that serves as a virtual machine. A good example for this type of virtualization is the Java Virtual Machine.

2.2.3 Advantages and Disadvantages of Virtual Machines

Like almost all-new emerging technology, there will always be some advantages and disadvantages and the VMs are not exempt. Thus, there are below some advantages and disadvantages that virtual machines present.

Virtual Machine Advantages

There are many advantages for using virtualization. Some of them are as shown below [12]:

- **High Availability:** By distributing load across virtualized machines, virtual hosts are able to ensure high availability of applications, data and services. This mean that even if one server fails, another virtual machine can replace it with little waste of time and data;
- **Familiar interfaces:** In virtual environment, we will have similar interfaces that are already known or familiar, because the objective of virtualization is to build similar environment as the physical ones;
- **Easy Cloning:** it is easier to clone a virtual machine than a physical one;

- **Scalability:** adding additional resource of “hardware” to a virtual machine is easier and can be done in a few minutes, while for physical machines it would take much longer;
- **Backup and disaster recovery:** In a server or in a Desktop environment files can be corrupted, while with virtualization it will be easier to recovery data. The virtualization platform and now cloud computing offer strong solutions for data recovery and backup.

Virtualization has many advantages yet, some are listed below:

- Centralized management;
- Less Power consumption;
- Hardware independence
- Reliability ;
- Cost reduction.

Another of the many benefits of the VM is the **Workload mobility**. Hypervisors provide an abstraction that presents hardware resources as virtualized representation that are running independent of the underlying hardware which happens unlike in normal platforms in which the Operating System and the applications are installed directly in the physical hardware thus keeping sometimes stuck with specific attributes of the own hardware. VM can be migrated across the LAN, if the hypervisors are compatible and adequate with computing resources on the destination server that will support the VM, from one physical system to another with little interruption to the VM [13]. In this dissertation, we are implementing a failover cluster and then the evaluation of performance implications considering either standard migration either live migrations using VM versus Shielded VM. The live migration subject will be more detailed in the next subchapter.

Virtual Machine disadvantages

Challenges or the disadvantages of the use of virtualization were the main research problem of this dissertation. As we have already talked about earlier virtualization has brought many advantages to the IT world, but like all emerging technologies, virtualization also has its challenges.

One of the main disadvantages that VMs have is the **security**. Since they are all centralized, all system administrators have access to VMs. With this access, malicious administrators can appear for example and make copies of the virtual machines that should not have access and do what they want with the information that it has. This problem has been solved with the appearance of Shielded Virtual Machines in Windows Server 2016 Hyper-V.

Other disadvantages in the use of VM are related to **performance** and **resource** use. Introducing an extra layer of software between the operating system and the hardware, generates a higher processing cost than you would have without virtualization and the hypervisors allows the physical computer's resources to be shared[13]. The Hypervisors will practically build *virtual hardware's*, obviously requiring the physical machine to have more resources to be shared with virtual machines and often **excessive oversubscription** can occur causing thus major problems with the performance of some virtual machines even causing **workload instability**. Therefore the physical machine hardware resources must be well allocated by system administrators to avoid **oversubscription** [13].

2.2.4 Failover Clustering and VM Migration

In order to perform the study of performance implications for the use of virtual machines versus shielded virtual machines, we set up a test environment where we implemented a failover cluster with native virtualization at the hardware level, considering both standard migrations and live migrations of virtual machines (more on chapter 3).

The use of multiple computers and redundant connections to form a single system that is highly available is considered **Clustering**. Some very important applications or services in a Network Infrastructure that need to be always available by distributing the workload will be protected with a cluster, that is, the cluster will work in such a way that in the event of a failure in one system, the service will be available in another one without loss of system data [14]. Remembering that these computers can be hosts or Virtual Machines.

Principal types of clustering existing at windows platform are:

- **Network Load Balancing clusters (NLB);**
- **Failover cluster.**

If a computer fails, for example, or if it is even intentionally turned off, the cluster will ensure that the services and processes that are running alternate to another machine that is available in the cluster. This entire process of switching from one machine to another will happen without interruption or the immediate intervention of a system administrator, thus offering a high availability solution, making critical data on a network available at all time [14][15][16].

According to Gerend J [15], a failover cluster is a grouping of independent computers (called Nodes) that work together to increase scalability and availability of clusters roles, providing highly available resources for a network. Clustered servers (nodes) can be connected by software and by physical network cables. The failover cluster will have a common disk subsystem; each node's member of the cluster has its own individual disk storage as well, which

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures means that if one cluster node falls, another node in the cluster that is available will take responsibility for the services that the dropped node was running [15][14].

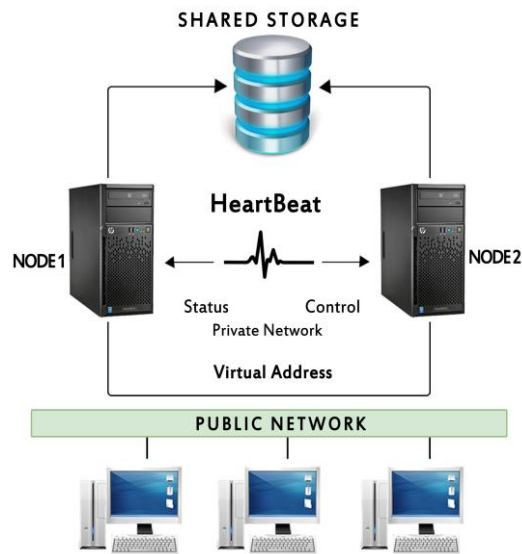


Figure 2.6: Schematic representation of a 2-node failover.

A Failover cluster provides [14]:

- High scalability by allowing administrators to assign up to 16 nodes to one cluster increase performance and availability significance, which makes the system more scalable because it allows for incremental growth;
- High availability by increasing the reliability of applications and services, and reducing unplanned downtime.

Failover Clustering has many practical applications, including [15]:

- Highly or continuously available file share storage for applications such as, Microsoft SQL Server and Hyper-V virtual machines;
- Highly available clustered roles that run on physical servers or on virtual machines that are installed on servers running Hyper-V.

Virtual Machine Live Migration

Live migration of VMs is a major feature in virtual datacenter environments during these days. Servers dynamic resource management techniques, load balance and power saving are all under

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures live migration feature in virtual datacenters [17]. We can consider live migration as the process of moving a running virtual machine from one host to another without perceived downtime.

Live migration has many benefits for the network. The primary benefit of live migration is flexibility; for running Virtual Machines that aren't tied to a single host machine, in a network, we will have more than one host configured. When live migration match with Windows Failover Clustering, live migration allows the creation of highly available and fault tolerant systems [17] - [18].

2.3 Shielded virtual machines and Guarded Fabric in Windows Server 2016

The main problem definition of this dissertation has to do with the security and the performance on the use of virtual machines in a High Availability Virtualized Infrastructures. Windows server 2016 Hyper-V has done a lot of investment on the area of the virtualization security.

In the virtualization environment in addition to protecting hosts or other virtual machines that are run by malicious software that can attack the services that are running on the specific VM affected, the VM also needs to be protected from a compromised host [6][19]. Shielded VMs can protect it from attacks via the network system, storage, or while backed up [20].

It can happen for example, that someone mischievous can get and leave a company with multiple virtual machines, because they are all centralized in a directory. VM is practically just a file stored on disk [1][20]. If a Virtual machine get out of an organization, either maliciously or accidentally, that virtual machine can be run on any other system. This is a very dangerous problem for every virtualization platform today, whether it is VMware, Hyper-V, Qemu, KVM or any other hypervisor. The top priority here consists of protecting high value assets in the organization, such as sensitive file servers, domain controllers and HR systems [20].

Many organizations including hosting providers or cloud environments need a way to secure and protect VMs from rogue administrators. The protection from administrators is needed for many reasons [20][19]. John Saville [19] mentioned some, as they will be shown below:

- Insider attacks
- Phishing attacks
- Stolen administrator credentials

Shielded virtual machines introduced in Windows server 2016 Hyper-V to make VM more secure, helping protect against compromised fabric. According to [20], “ **A Shielded virtual machine** is a generation 2 feature (supported on windows server 2012 and later) that comes with a virtual Trusted Platform Module (TPM), is encrypted using BitLocker, and can only run on healthy and approved hosts in the fabric”. This mean that the Shielded VM will protect virtual machines from compromised or malicious administrators in the fabric, such as storage admins, file admins, or all the system administrators in general by encrypting disk using BitLocker and state of virtual machines in a way that only VM or tenant admins can access the VMs.

Microsoft Hyper-V hosts must be running Windows server 2016, but the guest OS in the Virtual machine can be running Windows server 2012 and later [19].

2.3.1 Guarded Fabric

According to [20], “ *a **guarded fabric** is a windows server 2016 Hyper-V fabric capable of protecting tenant workloads against inspection, theft, and tampering from malware running on the host, as well as from system administrators*”. These virtualized tenant workloads protect both when they are off and when they are on, are called **Shielded virtual machines** [20].

Guarded fabric is made up of [20]:

- **Host Guardian Service (HGS), that are typically running on a cluster of 3 nodes;**
- **One or more guarded hosts;**
- **A set of shielded virtual machines.**

Host Guardian Service (HGS) has a role of windows server that will be installed on a secured cluster of a bare-metal servers that is capable to release keys to healthy Hyper-V hosts when powering-on or live migrating shielded VMs and measure the health of a Hyper-V host [20]. As we shall see later on, these two abilities are fundamental to a shielded VM solution and are referred to as the **Key protection services** and the **attestation services** respectively [20][21].

Other element of the Guarded Fabric is the guarded host. **Guarded host** is nothing more or nothing less than a Hyper-V host on which shielded VMs can run, only if the host can attest that they are running in the Host Guardian Service.

When a tenant (Virtual machine owner) creates shielded virtual machine that is running on a guarded fabric, the shielded VM and the Hyper-V hosts themselves are protected by the HGS. The Host Guardian Service offers two distinct services: **key protection and attestation**. The Key Protection Service provides the necessary keys to power the Virtual Machines on and to live

migrate the VM to other guarded hosts while the Attestation service has the mission of ensuring only trusted Hyper-V hosts can run shielded VMs [20].

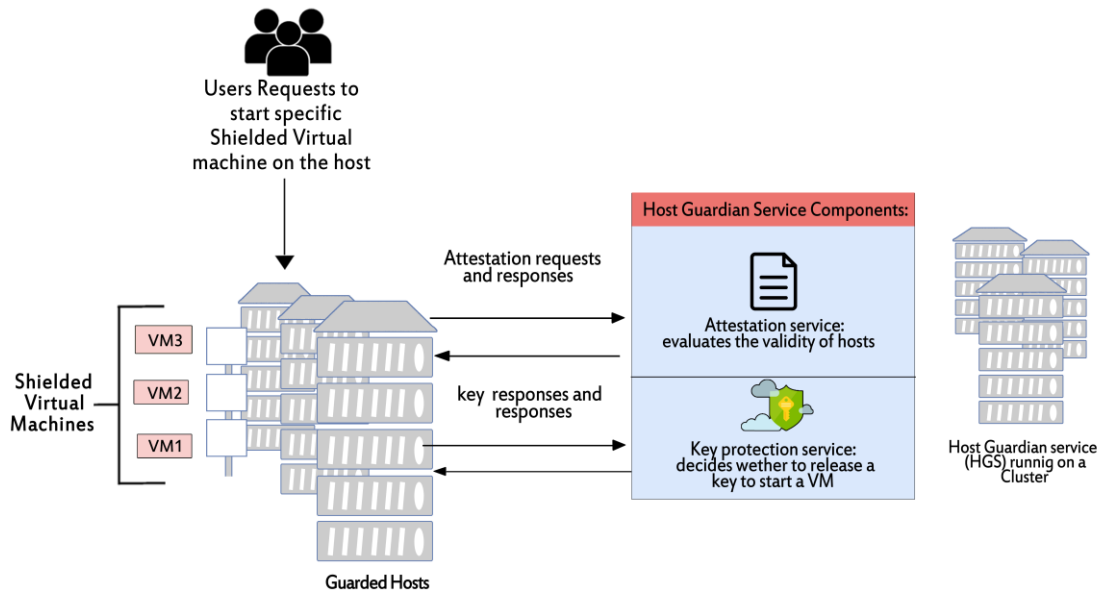


Figure 2.7: Host Guardian Service attestation and key protection (adapted from [4]).

Figure 2.7 represents the functioning of the Host Guardian Service; it shows how Host Guardian Service will ensure only valid hosts can start the shielded virtual machines through attestation service. The figure shows as well, how the keys for shielded virtual machines are going to be securely released from HGS by the Key protection Service.

The process works as follows: users will request to start specific shielded VMs on the guarded host. Then, Guarded host will send an attestation and a key request do the Host Guardian Service running on a cluster. After the Host Guardian Service has, received the attestation requests and the key request, respectively, attestation service will evaluates the validity of hosts and the Key Protection Service decides whether to release a key to start a VM and then comes the HGS responses to the Guarded Host.

Since the objective of Shielded virtual machines is to guarantee more security for the VMs, there are many possible attack vectors that shielded VMs can protect against [21]. Table 2.1 shows a few examples, along with how shielded VMs protect against the attack, according to Apolinario [21].

Table 2.1 - Attacks that shielded VMs can defend against (adapted from [21]).

Attack vector	Shielded VM defense
Injecting malware on a Hyper-V host	All software (user mode, kernel mode and drivers) running on a host is measured.
A malicious admin steals VHDs	Shielded VMs' VHD are encrypted
A malicious admin attempts to move a Shielded VM to an untrusted host	Trusted hosts are added to HGS using an identifier unique to their TPM; the new host will not be recognized because it wasn't added
Attach a debugger to the Hyper-V host	HGS won't release keys to hosts with debuggers attached. This is something we measure in HGS.
Inject malware into a VM template disk	Shielded VMs are only deployed from template disks that match known healthy ones

A malicious admin steals VHDs : in our bed test, all Shielded VM VHDs were not accessible by users without permission, and even if they had access it was not possible to copy the disk because they are encrypted, thus proving the protection effectiveness of Shielded virtual machines against malicious admin trying to steal the VHD. On the other hand, with the regular virtual machines it is possible for any administrator who has access to the VHD of the VM to steal and take it wherever they want, being a security problem already solved with the implementation of Shielded VM.

A malicious admin attempts to move a Shielded VM to an untrusted host: in the Guarded fabric of the project, only one Guarded Host has been configured. Due to the experiences made, it is not possible to move a Shielded VM from a Guarded Host to an untrusted host because the host has been designated as guarded by setting in a security group that was created in AD DS, therefore it must have a confidence relationship established between fabric AD and HGS's forest.

Inject malware into a VM template disk: Shielded VMs are only deployed from template disks that match as healthy.

2.3.2 Attestation Modes in the Guarded Fabric

It is very important to decide which type of attestation to use when a guarded fabric is deployed for the first time. The Hyper-V hosts that planned to run a Shielded virtual machine necessary attest with their Host Guardian Service before they can load a Shielded virtual machine [6].

There are two different attestation modes for a guarded fabric that the HGS supports according to [20]:

- **Admin-trusted attestation mode** (Active Directory based): it is easier to deploy, however, provides lesser assurances;
- **TPM-trusted attestation mode** (Hardware based): host hardware and firmware must include TPM 2.0 and UEFI 2.3.1 with secure boot enable, however, needs more configuration steps, but offers the strongest possible protections.

TPM-trusted attestation (Hardware level) is important because it offers stronger confidence, but it requires that the Hyper-V of the host has TPM 2.0 [20][6]. If the Hyper-V does not have TPM 2.0, then you can use **Admin trusted attestation**. If for example there is a need to move to TPM-trusted attestation when new hardware is purchased, just switch the attestation mode on the Host Guardian Service with brief or no interruption to your fabric [20].

Table 2.2 - Attestation modes (adapted from [20]).

Attestation mode admin choose for hosts	Hosts Assurances
<p>Admin-trusted attestation mode</p> <ul style="list-style-type: none"> • Support existing hardware where TPM 2.0 is not available • Requires less configuration steps • Compatible with commonplace server hardware 	<p>Only hosts that the admin projected as guarded hosts can decrypt and start Shielded VMs. The admin designates hosts as guarded by setting them in a security group that the admin create in Active Directory Domain Services (AD DS). A confidence relationship must be established between fabric AD and the HGS's forest.</p>
<p>TPM- Trusted attestation</p> <ul style="list-style-type: none"> • Host hardware and firmware must include TPM 2.0 and UEFI 2.3.1 with secure boot enabled • Offers the strongest possible protections • Requires more configuration steps 	<p>Host Guardian Service will approve the guarded hosts that can run Shielded VMs, based on a membership in a designate Active Directory Domain Services (AD DS) security group. This means that, only hosts that the admin designated as guarded hosts and that are running code the admin has identified as trusted, can start Shielded VMs.</p>

Table 2.2 is related to the level of assurance offered by the two modes of attestation used in a guarded fabric.

The following figure 2.8, explain better step by step, how the Host Guardian Service uses attestation mode, to guarantee that only know and valid hosts can start the Shielded virtual machine, and key protection service to securely release the keys for shielded VMs.

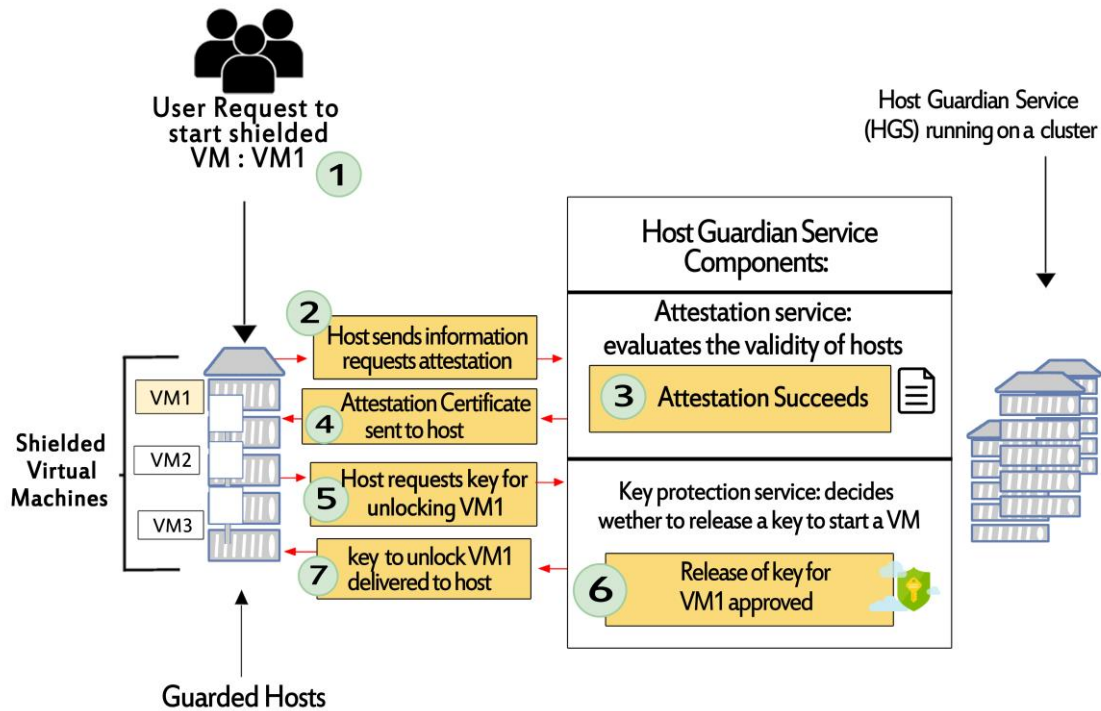


Figure 2.8: Verification process of shielded virtual machine (adapted from [4]).

The process occurs as follows:

- 1- User requests to start the VM1;
- 2- Host requests attestation to the Host Guardian Service;
- 3- Attestation succeeds or can fail;
- 4- HGS sends an attestation certificate to host;
- 5- Host requests key for unlocking VM1;
- 6- HGS analyses the request and approved the key release;
- 7- HGS sends a key to unlock VM1 to the host;
- 8- Host unlocks VM1 and start the VM.

2.3.3 Assurances Provided by the Host Guardian Service

Host Guardian Service, along with the methods for creating shielded VMs, helps to provide the following assurances, according to [20]:

- 1- **BitLocker encrypted disks** (data disks and OS disks): in order to ensure greater security BitLocker will encrypt the disks of the Shielded VMs. Shielded virtual machine's virtual

TPM use a secure measure boot to protect the BitLocker keys that are needed to boot the VM and decrypt the disks. Shielded VM's Data drives can be encrypted as well along with the operating system disk that are encrypted and protected automatically by the Shielded virtual machine;

- 2- **Deployment of new shielded VMs from “trusted” template disks/images:** tenants are able to stipulate which template disks they trust when deploying new shielded VMs. At a point in time when disks content, is considered trustworthy, shielded template disks have signatures that are computed. After this point, the disk signatures are then stored in a signature catalog that is securely provided by the tenants to the fabric when the shielded virtual machine is created. Shielded VMs are only implemented if the disk signatures (computed again), match the trusted signatures in the catalog, otherwise, the shielded template disk is considered untrustworthy and the deployment fails;
- 3- **Protection of passwords and other secrets when a shielded VM is created:** it's important to guarantee that the VM secrets, such as the password of the VM's local Administrator account, RDP certificates and the trusted disk signatures are not disclosed to the fabric when VMs are created. The secrets of the VM's are stored in an encrypted file called a shielding data file (a .PDK file), from which they are uploaded to the fabric by the tenant, and protected by tenant keys. This assurance is provided when a shielded VM is created, and the tenant will then select the shielded data to use which securely provides these secrets just to the trusted components within the guarded fabric;
- 4- **Tenant control of where the VM can be started:** a list of the guarded fabrics on which a particular shielded VM is permitted to run is also stored in Shielding data. In cases where a shielded VM typically resides in an on-premises private cloud but may need to be migrated to another (public or private) cloud for disaster recovery purposes this is helpful, for example. The target fabric or cloud must support shielded VMs and the shielded VM must allow the fabric to run it.

2.3.4 Cryptographic Keys Used for Shielded VMs

As already shown in table 1, that Shielded VMs will protect the VMs from many attacks. The most of this protection capacity comes from encryption. BitLocker will encrypt the disks of the Shielded VMs. Shielded VMs will use various other encrypted elements to be protected from virtualization fabric attack vectors, which can only be decrypted by:

- **One or more Guardians(Host Guardian Keys):** each guardian of the fabric will represent a virtualization fabric on which an owner authorizes shielded VMs to run[20].

Companies sometimes have both a primary and a disaster recovery (DR) virtualization fabric, and authorize their shielded VMs to run on both fabrics. There have been cases, sometimes, that a public cloud provider might host the disaster recovery fabric. The private keys for any guarded fabric are kept only on the virtualization fabric, while its public keys can be downloaded and are kept within its guardian [20][5].

- **An owner key:** this is a cryptographic key kept by the virtual machine owner. VM owner is responsible for keeping owner keys in a secure location and the key is typically used for last resort troubleshooting or recovery [20].

Two certificates can represent an owner key. The certificates are for signing and for encryption. The certificates can be created by using your own PKI infrastructure or get SSL certificates from a public certificate authority(CA) [20]. For a group of VMs that share the same security, risk level, and for administrative control it's recommended the use of a single owner key. The single owner key can be shared for all the domain joined shielded VMs and ensure that domain administrators will manage the owner key [20].

2.3.5 Shielded Data

According to [20], a shielded data file (also called a provisioning data file or PDK) is an encrypted file that a VM owner or tenant creates to protect important VM configuration information, such as domain-join credentials, RDP and other identity-related certificates, the administrator password, and so on. Although the fabric administrator can use the shielded data to create the shielded VM, he is unable to use or view the information contained in the file [22][20].

The following figure, explain how the shielding data file and elements behave: First there is a Shielded VM template which can be managed with a VMM, then the VHDX files are signed, creating in this way a volume signature catalog (VHDX files are identified). The shielding data file is created to protect the important VM configuration information, such as customization data (RDP certificates), allowed template disks and Key protector.

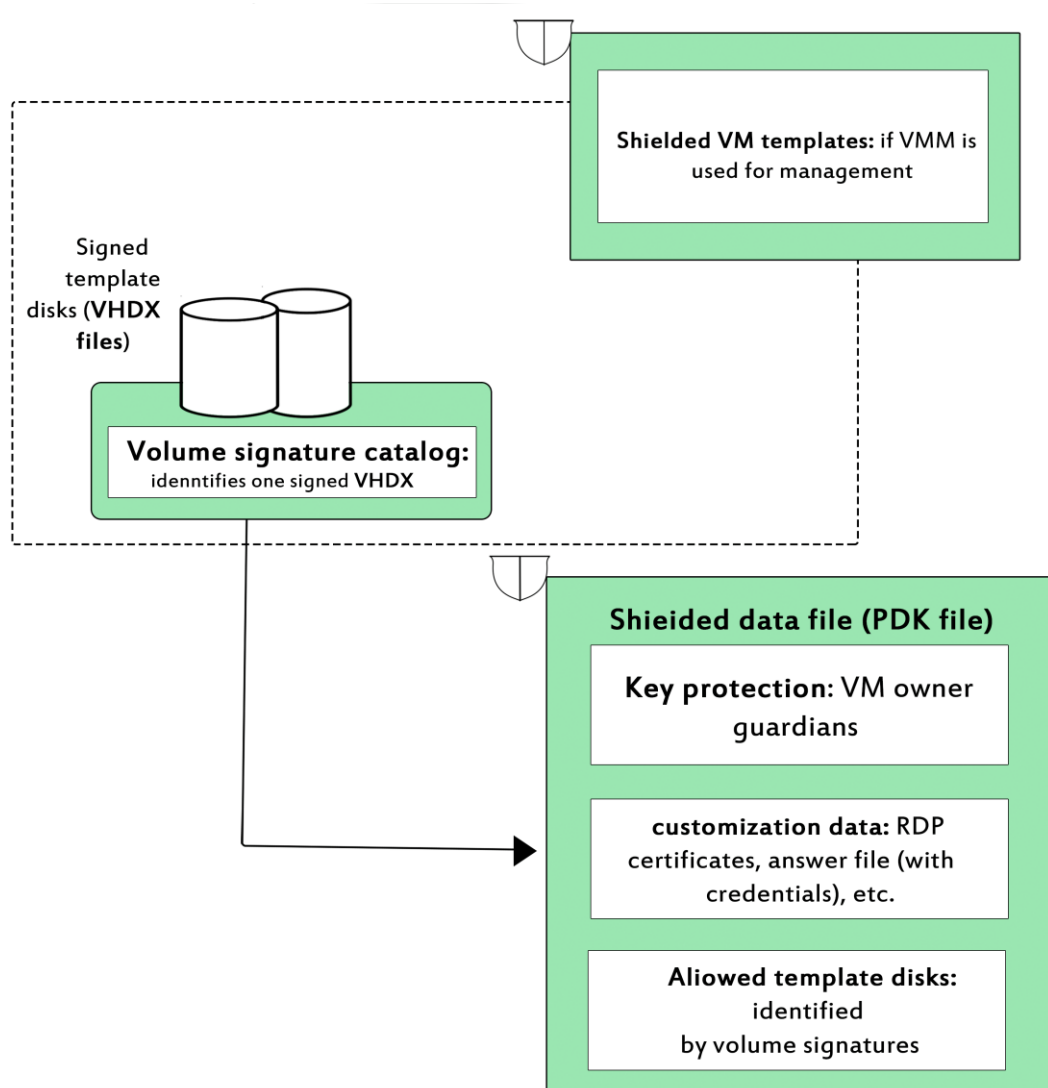


Figure 2.9: Shielding data file and elements (adapted from [4]).

The secrets that a shielding data file contains, among others, according to [20] are:

- A key protector (KP) that defines which guarded fabrics a shielded VM is authorized to run on;
- An RDP certificate to secure remote desktop communication with the VM;
- Administrator credentials;
- A security policy that determines if the VMs created using the specific shielding data are configured as encryption supported or shielded;
- An answer file (unattend.xml);
- A volume signature catalog that contains a list of trusted, signed template-disk signatures that a new VM is enable to be deploy.

2.4 Types of Virtual Machines that a Guarded Fabric Can Run

There are three possible ways that guarded fabrics are capable of running a VMs [20]:

Table 2.3 - Types of virtual machine that a guarded fabric can run

Types of VM	Type of security
A normal VM	Offering any protections above and beyond previous versions of Hyper-V
A shielded VM	The protection is all switched on and cannot be disabled by a fabric admin.
An encryption-supported VM	The protections can be configured by a fabric admin.

As it is shown above on table 2.3 a Guarded Fabric can run three types of virtual machines, such as a normal VM, an encryption-supported VM and a shielded VM.

Shielded VM are planned to run in fabrics where the state and data of the VM need to be protected for both untrusted software and fabric administrator that might be running on the Hyper-V hosts [20]. An example can be if a malicious admin wanted to steal VHDs of a VM, a shielded VM will never permit that, because the shielded VMs' VHD are encrypted.

On the other hand, the encryption-supported VMs are planned for use where the fabric admins are entirely trusted [20]. An example, imagine if a company might deploy a guarded fabric with the view to guarantee VM disks are encrypted at-rest for compliance purposes. Despite this level of security, fabric administrators can still use the convenient management features, such as PowerShell Direct, console connections and other day-to-day troubleshooting tools and management [20].

Differences between Shielded VMs and Encryption-supported VM are many. The main ones are shown on the following table:

Table 2.4 - Differences between encryption-supported and shielded VMs (adapted from [20]).

Capability	Generation 2 Encryption supported VM	Generation 2 Shielded VM
Vtpm	It's required but configurable	It's required and enforced
Secure boot	It's required but configurable	It's required and enforced
Encrypt VM state and live migration traffic	It's required but configurable	It's required and enforced
Virtual machine Connection (Console), HID devices (e.g. Mouse, keyboard)	On and cannot be disabled	Disabled (cannot be enabled)
Integration components	Configurable by fabric admin	Certain integration components blocked (e.g. PowerShell Direct, data exchange)
Attach a debugger (to the VM process)	Supported	Disabled (cannot be enabled)
COM/Serial ports	Supported	Disabled (cannot be enabled)

Despite the great differences between encryption-supported and shielded VMs, they are both to continue supporting commonplace fabric management capabilities, such as VM checkpoints, Hyper-V replica, Live Migration, and much more [20].

2.5 Encryption of Virtual Machines in VMware vSphere 6.5

Besides Microsoft Windows Server 2016, VMware vSphere 6.5 is addressed by encryption feature. It is possible to create encrypted virtual machines and encrypt existing ones with vSphere 6.5. Its operation is very similar to the Shielded virtual machines in Windows.

Key management is carried out based on KMIP 1.1. Standard and the VMs encryption works based on AES-NI algorithm. They providing a complete security against all data security attack by encrypted immediately the disk of Virtual Machine when the I/O operations comes [23].

According to VMware [23], the Encryption feature supports encrypting virtual disks files, core dump files and virtual machine files. The components of vSphere Virtual Machine Encryption are [23]:

- Key Management Server;
- The vCenter Server System;
- ESXi hosts.

Encryption process of the Virtual Machines in VMware vSphere 6.5 occurred as follow: after vCenter Server connected to the KMS, only the users with the required privileges are able to create encrypted disks and virtual machines. They can also perform other encryption tasks such as decrypting encrypted virtual machines or encrypting existing virtual machines in environment [23].

After users assigns VM encryption policy, for the VM, a random key is generated and encrypted with a key from the Key Management Server. VCenter server receives the key from the Key Management Server when VM is powered on and sends it to VM encryption module on ESXi server, which unlocks the key in the hypervisor. Finally all I/O operations are carried out through encryption module, which will encrypt all input and output SCSI-commands transparently for guest OS [23].

2.6 Conclusions

This chapter served as the basis for the Background over Shielded virtual machines. Before talking properly about the Shielded virtual machines, a review was made of the main concepts about virtual machines, as well as their advantages and disadvantages. In addition, we still addressed the migration of virtual machines and failover clustering.

In addition to the basic concepts about VM, it was also shown how Shielded VM are implemented within a Guarded Fabric. The guarded fabric it is constituted by Host Guardian Service (HGS) that Microsoft recommends running on a cluster of three nodes for high availability; one or more guarded hosts and a set of shielded virtual machines.

Chapter 3

Specification and Implementation of the Experimental Test Bed

3.1 Introduction

Previous chapter was devoted to the background on Shielded virtual machines and in accordance with the objectives of this dissertation, an experimental bed test needs to be designed and configured, involving a failover cluster with native virtualization at the hardware level, supporting shielded virtual machines in windows server 2016 Hyper-V. This chapter describes the architecture of the testing environment and reports the implementations and configurations of the failover clustering, FreeNAS Storage, iSCSI Target, virtual machines, shielded virtual machines and Guarded Fabric.

3.2 Architecture of The Experimental Test Bed

Due to the limitation of this work, the test environment was divided into two parts. In the first part, we setup the environment for the high availability of the VMs. In the Second part, we deployed the Guarded Fabric along with the shielded virtual machines and Guarded Hosts.

Nowadays, when one think about designing and engineering virtual infrastructures for the enterprise datacenter, one of the critical requirements is the high availability solution It is important that when one think about making Hyper-V highly available to not rely on a single point of failure regarding the considered Hyper-V host architecture [24]. This means it is important to provide multiple hosts that can assume the control in the case of a host failure, that is, Hyper-V makes use of windows Server clustering technology to make this available to Hyper-V.

3.2.1 Used Tools for the Implementation of the Test Bed

Main technologies used to implement the architecture of the testing environment include the following ones:

- **Windows Server 2016:** Microsoft windows Server 2016 is a server operating system. The hosts of the environment are all running Windows Server 2016 Datacenter edition;
- **Hyper-V:** For our bed test, we used Hyper-V 2016 as Hypervisor for the virtual machines. Hyper-V is a Microsoft hardware virtualization product available as a role in Windows Server 2016;
- **FreeNas:** According to [25], FreeNAS is an embedded open source network-attached storage (NAS) operating system which is based on FreeBSD and released under a 2-clause BSD license. A NAS has an operating system optimized for sharing and file storage. It provides a browser-based, graphical configuration interface. The built-in networking protocols give storage access to multiple operating systems. A plugin system is provided for extending the built-in features by installing additional software. FreeNAS supports iSCSI and File Transfer Protocol for block storage or Common Internet File System/Server Message Block (CIFS/SMB), AFP or Network File System for storing files. It supports most major virtualization platforms, including Microsoft, VMware and Citrix. The version of the FreeNAS used in this project is 11.0-44;
- **iSCSI:** Microsoft iSCSI Initiator is a tool that connects external iSCSI-based storage to host computers with an Ethernet network adapter. The iSCSI is a protocol that allows the block level storage data to be transported over the TCP/IP network;
- **RAID 1: (Mirroring):** it is a mode that allows the use of two hard drives (HDs). The second HD will store an identical image to the first one. In practice, it will be as if it only has one hard drive installed, but if the disk holder fails for any reason, there is a backup stored on the second disk. In this project, a RAID 1 system has been implemented to increase system reliability.

3.2.2 Overview of the High Availability Architecture with VMs

Figure 3.1 shows the architecture of the high-availability virtualized infrastructures that were setup in our test environment for the virtual machines. The shielded virtual machine architecture will be represented in figure 3.2.

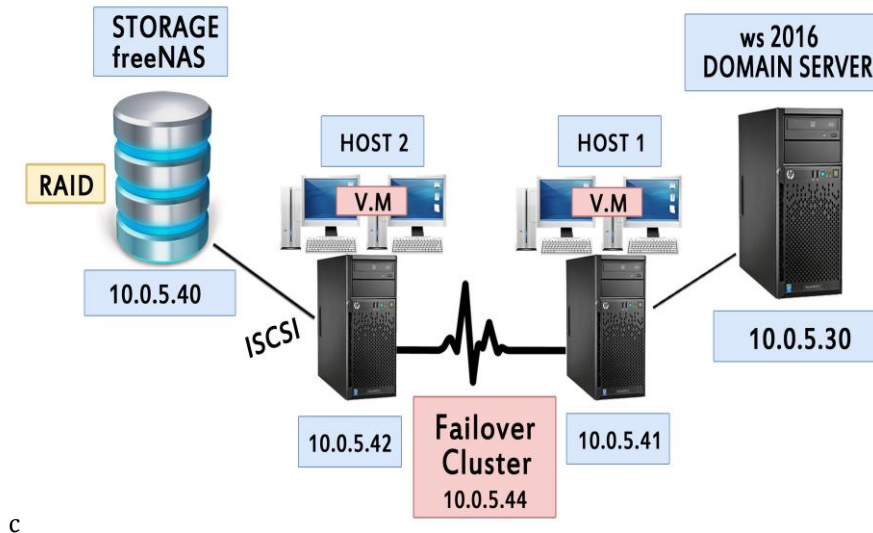


Figure 3.1: Experimental setup of the failover cluster with virtual machines.

As shown in the figure 3.1, we have four physical servers, namely: a Server for Storage, two servers for the failover cluster and a domain server.

Storage Server consists of three disks, the first disk with a size of 500 Megabyte is where FreeNAS is installed and the other two disks, with a size of one terabyte each, have been configured in RAID 1 in order to increase the system reliability. For the Hosts to have access to the disks as shown in the figure, the iSCSI protocol has been initialized on both hosts and connected to the Storage via TCP/IP, taking into account that FreeNAS has a graphical environment for configuration that can be accessed via Web.

The two servers used for the failover cluster, both run Windows server 2016, because the virtual machines will be created in Hyper-V. The virtual machines were installed on the failover cluster created between Host 1 and Host 2. We have another server in our architecture that works as the Network Domain Server as show in the figure 3.1.

In terms of network and according to the tests that were carried out in the NMCG laboratory at University of Beira Interior, a VLAN has been used, assigned by the Department System Administrator. The IP network diagram is shown in the implementation part.

3.2.3 Overview of the Guarded Fabric and Shielded VM Architecture

In the second part of the bed test, the Guarded Fabric has been deployed. It has three physical servers, all of them running Windows server 2016, Datacenter Edition, namely: DNS server, the HGS server and the Guarded Host. The system capable of protecting the boot and unauthorized use of virtual machines in a network is called guarded fabric as it is shown in figure 3.2. On the

DNS server, in addition to the DNS role, Active Directory Domain Services and DHCP have been configured.

Host Guardian Service has been configured on a single server for the testing environment, but Microsoft recommends configuring it on a cluster of at least three nodes for high availability. The HGS will release the keys to trusted Hyper-V host (guarded host) to live migrate or to power on the Shielded VM. HGS is made up of the Key Protection Services and the Attestation Service.

In Chapter 2, it is mentioned the existence of two types of attestation modes, but, for the scenario herein considered, Admin-trusted attestation was selected due to the lack of resources. Admin-trusted attestation allow hosts that should be designated as guarded hosts in Active Directory to decrypt and start shielded VMs. The hosts are designated as guarded by placing them in a global security group that is created in AD. To work properly, this mode a trust relationship must be set up between the HGS forest. Many companies are more likely to use this mode [26].

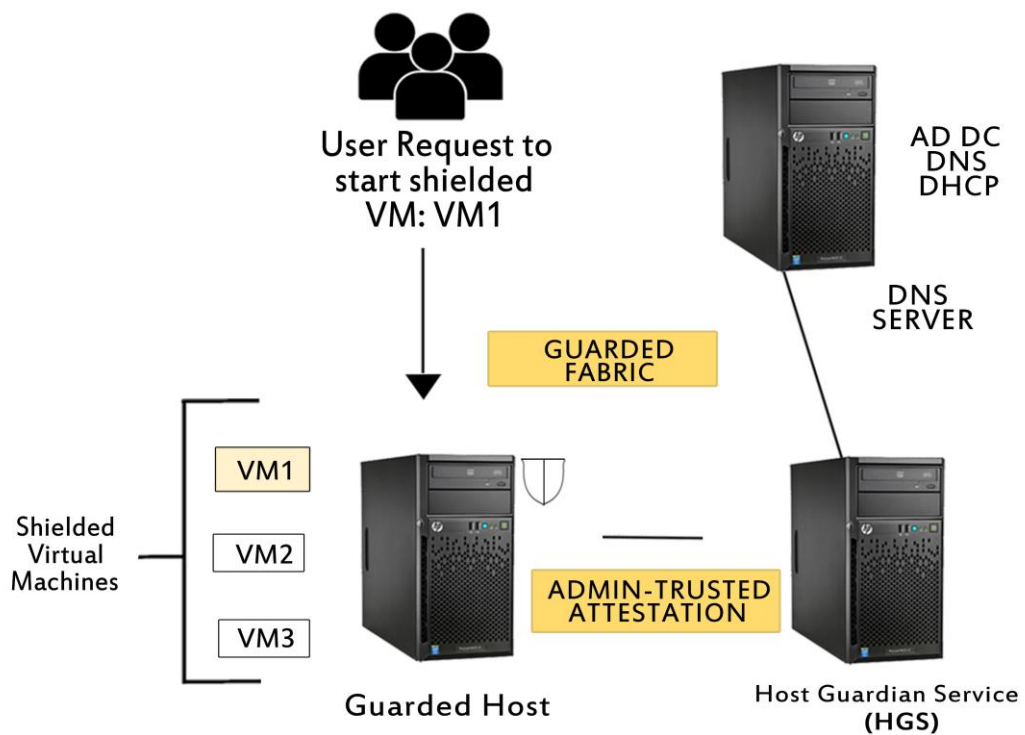


Figure 3.2: Experimental deployment of shielded virtual machines.

Requirements and limitations for using Shielded VM and HGS

According to [26], the requirements for using shielded VMs and the HGS are:

- **Windows Server Datacenter Edition:** the feature and the ability to create and run the HGS and Shielded VM is only supported by Windows Server 2016 Datacenter Edition;
- **One Bare metal host:** it is possible to deploy the Shielded VMs and the HGS with just one host as shown in figure 3.2. Nevertheless, Microsoft recommends clustering HGS for high availability;
- **For Admin-Trusted attestation mode:** we choose this mode for this project because it only needs to have a Server hardware capable of running Hyper-V in Windows Server 2016 TP5 or higher;
- **For TPM-trusted attestation:** The servers must have UEFI 2.3.1 and TPM 2.0 and they must boot in UEFI mode. The hosts should also have secure boot;
- **Hyper-V role:** the role must be installed on the guarded host;
- **Host Guardian Service Role :** must be added to one physical host;
- **A fabric AD domain;**
- **An HGS AD;**
- **Generation 2 VMs.**

3.3 Implementation of the Failover Cluster in Windows Server 2016 Hyper-V

All the steps, needed for the implementation of the architecture explained above, are detailed and explained in this section, namely:

- **Implementation of the High-Availability of the VMs**
- **Implementation of the Guarded Fabric and Shielded VM**

It is important to think on Servers individually before thinking about the Hyper-V hosts as a cluster to perform the initial configuration of the hosts themselves before clustering both servers. The initial configuration of our high availability environment for the hosts involves much of the same steps of the preparation of any Windows Server, such as patching and network configuration. For the cluster communications and the communication with the shared storage, it is also important that the network is well configured [24]. Both servers are needed to be joined at the same domain: *clusterae.pt*

The table below shows the Network Planning for the failover cluster:

Table 3.1: Network Planning for the Failover Cluster.

Purpose	IP	FQDN	Initial Configuration
First Cluster Node	10.0.5.41 /25	Host1.clusterae.pt	WS 2016 Data Center Edition / Hyper-V
Second Cluster Node	10.0.5.42 /25	Host2.clusterae.pt	WS 2016 Data Center Edition / Hyper-V
Cluster Storage	10.0.5.40 /25	Freenas.clusterae.pt	FreeNas 11.0-U4
Domain Server	10.0.5.30 /25	DC.clusterae.pt	WS/AD DC / DNS
Cluster	10.0.5.44 /25	ElsaEvora.clusterae.pt	Virtual Machines
Gateway	10.0.5.1 /25		

Steps to implement the failover cluster in Hyper-V are:

- 1- iSCSI Storage Target Setup (FreeNas);
- 2- Installation of the Hyper-V Role and setting up the storage;
- 3- Hyper-V cluster creation; Configuration of the disks for a failover cluster (Cluster Shared Volume); High availability VM.

1- iSCSI Storage Target Setup (FreeNas)

Before the installation of the OS for the shared storage of the bed test herein considered (FreeNAS 11.0-U4), firstly, a RAID (Mirror) has been configured on the two disks of one terabyte each other that was put on the server. The configuration of the RAID is very simple and was setup in the bios of the Server.

After the Mirror configuration, the FreeNas 11.0-U4 has been installed and configured on the server. Figure 3.3 shows the overview of the FreeNAS accessed via Web The figure provides an overview of the FreeNAS environment, the name of the disks available on the Storage (ada0 and ada1) and their respective size (1.0 TB).

iSCSI service in FreeNas and the setup of the network configuration on the storage network must match for the objective of the Hyper-V hosts [24]. After that, a Portal has been configured in order to listen the iSCSI traffic on FreeNas. Figure 3.4 shows the Portal Group ID created and its respective IP address (10.0.5.40). FreeNas only has the Block level Storage available for the 32

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures

ISCSI configuration. Block level is commonly deployed in Storage area environments, like our environment.

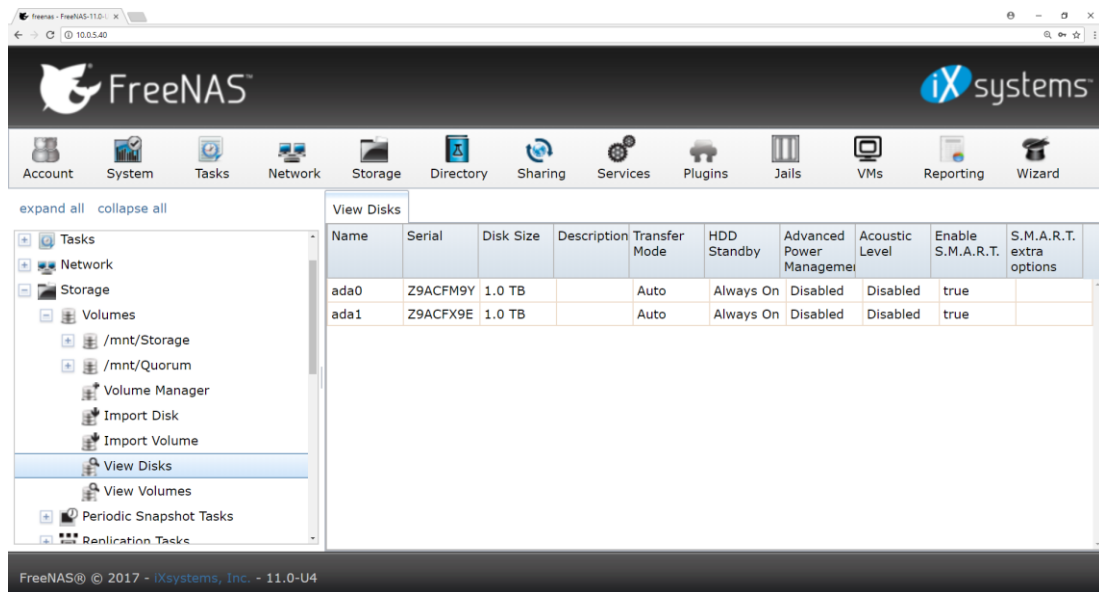


Figure 3.3: Available disks on FreeNas seen on the Web interface.

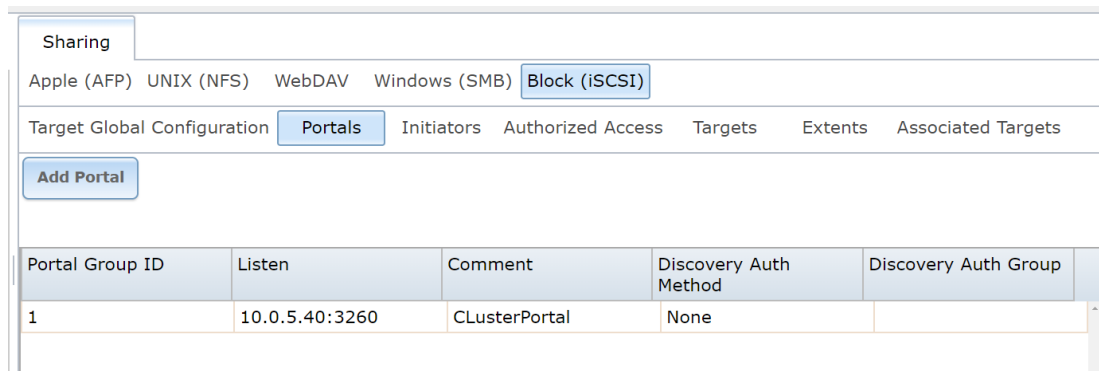


Figure 3.4: Configuration of the block level and portal group ID on FreeNas.

After that, the iSCSI target names were setup. The targets name are for the Hyper-V cluster. Two targets names: “quorum” and “storage” have been created. The two volumes have been created, and the “quorum” is to be used as disk witness and the “storage” will be used for the cluster-shared volume (CSV), where all virtual machines will be hosted. The configurations continue, and after that, the extents needs to be added. Figure 3.5 shows the two Extent created, the Extent Type and the path to the extent.

Extent Name	Serial	Extent Type	Path to the extent	Logical Block Size	Disable Physical Block Size Reporting	Available Space Threshold (%)	Comment	Enable TPC	Xen initiator compat mode	LUN RPM	Read-only
QuorumExt	18d6c702	File	/mnt/Quorum	512	false			true	false	SSD	false
StorageExt	18d6c702	File	/mnt/Storage	512	false			true	false	SSD	false

Figure 3.5: Individual disks assigned in FreeNas.

Targets must be associated with their respective Extents so that the targets are mapped to the storage in FreeNas. As may be seen in figure 3.6), the Target quorum associates with the Extent QuorumExt and the storage associates with the StorageExt, respectively.

Target	LUN ID	Extent
quorum	0	QuorumExt
storage	0	StorageExt

Figure 3.6: Configuration of FreeNas Target and Extent.

There are several items that should be verify when one is planning to deploy a Hyper-V cluster, “pre-cluster planning”, such as networking planning, storage target configuration and host configuration [24]. Since the Storage target configuration is set up, the next step is the configuration of the failover cluster.

2- Installation of the Hyper-V Role and setting up the storage

After we have made the initial settings that are required for a failover cluster on both physical servers, it is possible now the installation of the Hyper-V role and setting up the storage. After that configuration it is possible to create the Windows failover cluster with the two hosts that are enabled for the Hyper-V role [24].

The command for installing Hyper-V role service In Windows PowerShell command prompt is shown below:

- **Install -WindowsFeature Hyper-V -IncludeAllSubFeature -IncludeManagementTools -Restart**

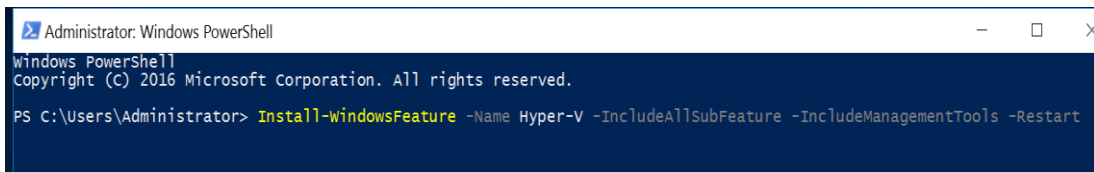


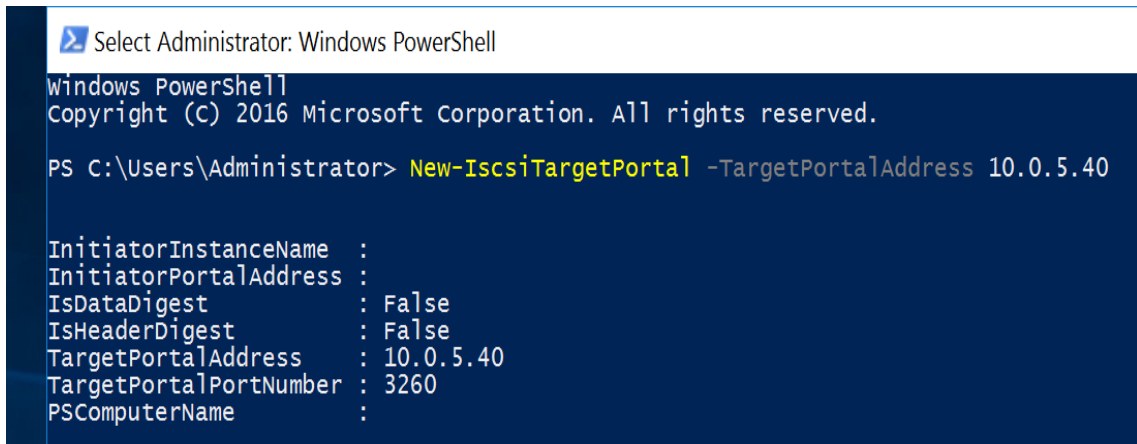
Figure 3.7: Installation of the Hyper-V Role.

After the installation of the Hyper-V features and sub features, in both servers, the Microsoft iSCSI service has been set and started. In this project, the service to automatic and then start the service has been set as it can be demonstrated by the commands below:

- **Set-Service -Name msiscsi -StartupType Automatic**
- **Start-Service msiscsi**

iSCSI service in Hyper-V hosts must have a target portal address, in order to be able to connect to the target portal address that was set in the FreeNas. Figure 3.8 shows the command to add the iSCSI target portal address in the Hyper-V hosts. The target portal address is the IP of the Storage: 10.0.5.40 and the target portal number is 3260 as it is shown in figure 3.8.

- **New-iscsitargetportal -targetportaladdress 10.0.5.40**



```

Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-IscsiTargetPortal -TargetPortalAddress 10.0.5.40

InitiatorInstanceName :
InitiatorPortalAddress :
IsDataDigest           : False
IsHeaderDigest         : False
TargetPortalAddress    : 10.0.5.40
TargetPortalPortNumber : 3260
PSComputerName         :

```

Figure 3.8: Adding iSCSI target portal address to connect the host with FreeNAS.

Specific iSCSI targets that were created in FreeNas appliance must be connected. Commands to add the FreeNAS targets to the Hyper-V hosts provisioned for the cluster are:

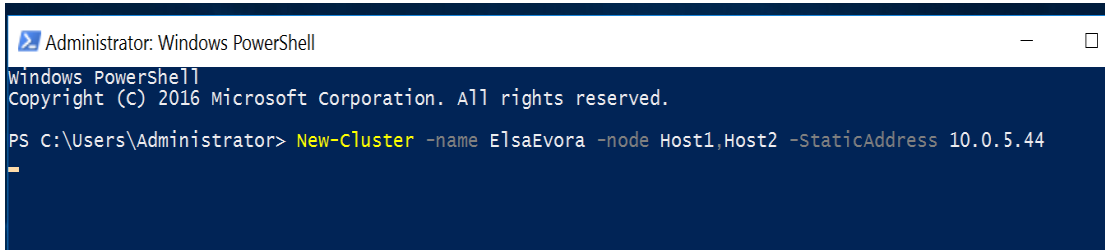
- **Connect-IscsiTarget -NodeAddress iqn.2005-10.org.freenas.ctl:quorumvol1 -IsPersistent \$True -IsMultipathEnabled \$True -InitiatorPortalAddress 10.0.5.41 -TargetPortalAddress 10.0.5.40**
- **Connect-IscsiTarget -NodeAddress iqn.2005-10.org.freenas.ctl:clustervol1 -IsPersistent \$True -IsMultipathEnabled \$True -InitiatorPortalAddress 10.0.5.41 -TargetPortalAddress 10.0.5.40**

Virtual network adapters provided by the Hyper-V to its virtual machines are going to communicate with the virtual switch. An External virtual Switch has been configured on both Host servers to enable live migration. It should be remembered that virtual switch names must be configured identically.

After the installation of the Hyper-V role on both hosts, setting up the shared Storage on both hosts as well as the creation of the virtual switches, the infrastructure is now ready for the cluster creation.

3- Hyper-V cluster creation; Configuration of the disks for a failover cluster (Cluster Shared Volume); High availability VM.

Creation of the Hyper-V failover cluster can be made using Windows PowerShell. Before running the command for the creation of the cluster, a validation of the hosts configuration to see if they are in a position to host the cluster was made. Figure below shows the command to create the failover cluster.



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> New-Cluster -name ElsaEvora -node Host1,Host2 -StaticAddress 10.0.5.44

```

Figure 3.9: Command to create the Hyper-V cluster.

Above command creates a new cluster named "*ElsaEvora*", with the two cluster nodes, Host1 and Host2 respectively and the static IP address for the cluster.

Storage of the VMs must be setup on a cluster shared volume. Cluster shared volume was designed by Microsoft to be used with the Hyper-V role, to permit a virtual machine to have a Virtual Hard Disk (VHD) files that can be accessed by any node in the cluster [27]. This means that all the virtual machines that will be created in the Cluster will be stored in this specific Cluster Shared Volume, which is a Disk that is physically stored on the Storage Server. The command used to add a volume to a cluster shared volume is :

- **Get-ClusterResource -Name "Cluster Disk 2" | Add-ClusterSharedVolume**

Settings were all made and the "*ElsaEvora*" failover cluster has been successfully created. The process of creating virtual machines is done through the failover Cluster Manager Console, and it is possible to add many virtual machines. The VHD of the respective machines will be stored in the Cluster Shared Volume. After the implementation of the high-availability environment of the virtual machines, some tests will be performed, as reported in Chapter 4.

Figure 3.10 shows the state of the failover cluster, in which the state of the two hosts (Host 1 and Host 2) can be seen set with **UP** and its respective **IDS**. The state of other elements of the failover cluster can still be seen in the figure, such as the virtual machines installed in the cluster and Cluster IP Address. In addition, at the bottom of the figure, we can see the available disks on the Storage Server, the "**HealthStatus**" is "**Healthy**" and The "**OperationalStatus**" is "**online**".

```

Select Administrator: Windows PowerShell
PS C:\Users\administrator.CLUSTERA> Get-ClusterNode

Name      ID      State
----      -
Host1     2       Up
Host2     1       Up

PS C:\Users\administrator.CLUSTERA> Get-ClusterResource

Name                                     State OwnerGroup ResourceType
----
Cluster Disk 1                          Online Cluster Group Physical Disk
Cluster IP Address                       Online Cluster Group IP Address
Cluster Name                             Online Cluster Group Network Name
Storage QoS Resource                     Online Cluster Group Storage QoS Policy Manager
Virtual Machine Cluster WMI              Online Cluster Group Virtual Machine Cluster WMI
Virtual Machine Configuration VM01        Online VM01 Virtual Machine Configuration
Virtual Machine Configuration VM02_Fedora Online VM02_Fedora Virtual Machine Configuration
Virtual Machine Configuration VM03_Ubuntu Online VM03_Ubuntu Virtual Machine Configuration
Virtual Machine Configuration VM04_WS2016 Online VM04_WS2016 Virtual Machine Configuration
Virtual Machine VM01                     Online VM01 Virtual Machine
Virtual Machine VM02_Fedora               Online VM02_Fedora Virtual Machine
Virtual Machine VM03_Ubuntu               Online VM03_Ubuntu Virtual Machine
Virtual Machine VM04_WS2016               Online VM04_WS2016 Virtual Machine

PS C:\Users\administrator.CLUSTERA> Get-ClusterAvailableDisk
PS C:\Users\administrator.CLUSTERA> Get-disk

Number Friendly Name Serial Number HealthStatus OperationalStatus Total Size Partition Style
-----
0       ST1000DM01... Z9ACG3SE Healthy Online 931.51 GB GPT
3       TOSHIBA Tr... DC Healthy Online 14.45 GB MBR
2       FreeNAS iS... 18d6c7023e5701 Healthy Online 1 TB GPT
1       FreeNAS iS... 18d6c7023e5700 Healthy Online 1 TB GPT
    
```

Figure 3.10: Overview of the cluster resources.

3.4 Deploying the Guarded Fabric and Shielded virtual machines

Table 3.2 below shows the planning for the network to set up the Guarded Fabric:

Table 3.2 - Networking planning to implement the Guarded Fabric.

FQDN	Purpose	Initial Configuration	IP Address
Host1.shielded.com	HGS Server	WS 2016 Data Center Edition	10.0.5.41
dc.clusterae.pt	DNS Server	WS 2016 Data Center Edition / DNS / AD DC / DHCP	10.0.5.30

Host2.clusterae.pt	Guarded Host	WS 2016 Data Center Edition	10.0.5.42
--------------------	--------------	--------------------------------	-----------

Necessary steps to deploy a Shielded VM are as follows:

- a) Deployment of Host Guardian Service
- b) Creation of Self-Signed Certificates for HGS
- c) Initialization of the HGS server Using Admin-Trusted Attestation
- d) Configuration of the Fabric DNS resolution and Creation of a Security Group
- e) Deployment of Guarded Host
- f) Deployment of Shielded VMs

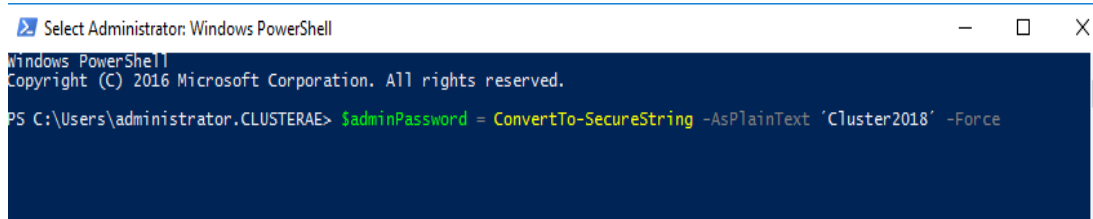
a) Deployment of Host Guardian Service

Before using the Shielded VMs, it is necessary to deploy the Host Guardian Service. The role has been installed in the HGS Server. Figure 3.11 shows the command used to add the Host Guardian Service Role.

```
PS C:\Users\Administrator> Install-WindowsFeature -Name HostGuardianServiceRole -IncludeManagementTools -Restart
Success Restart Needed Exit Code      Feature Result
-----
True     No           NoChangeNeeded {}
```

Figure 3.11: Command to install the HGS role.

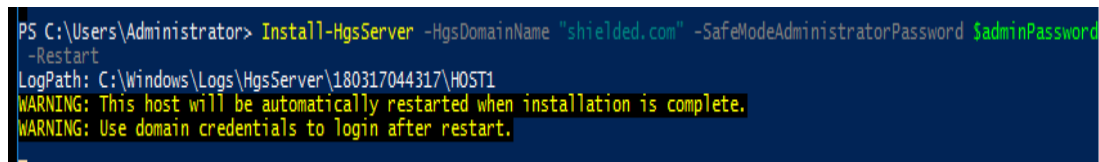
As may be seen in figure 3.11, after the execution of the command, the server restarts and it is now ready for the installation of the HGS. The command used to install the HGS is shown in figure 3.12 and 3.13. The command sets the HGS service and its dependencies and set up the Active Directory forest for HGS. HGS should not be joined to a domain before performing these steps, because when this command run on our Unique HGS server will promote the Server to the primary domain controller [20], [26].



```
Select Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.CLUSTERA> $adminPassword = ConvertTo-SecureString -AsPlainText 'Cluster2018' -Force
```

Figure 3.12: Setting the Admin Password for the HGS Server.



```
PS C:\Users\Administrator> Install-HgsServer -HgsDomainName "shielded.com" -SafeModeAdministratorPassword $adminPassword
-Restart
LogPath: C:\Windows\Logs\HgsServer\180317044317\HOST1
WARNING: This host will be automatically restarted when installation is complete.
WARNING: Use domain credentials to login after restart.
```

Figure 3.13: Command for installation the HGS service.

HGS AD domain name is “shielded.com” and the server produces a Log path of the installation.

For production environments, Microsoft recommends that the HGS configuration be done in a high availability cluster of at least three nodes to allow the Shielded VMs to be connected even if an HGS node is turned off. It is possible to add additional HGS nodes in the infrastructure [26], [20].

b) Creation of Self-Signed Certificates for HGS

Certificates must be created for the HGS service to use for signing purposes and encryption. There are three modes to use certificates with the HGS according to Michael Otey [26]:

- 1- With self-signed certificates;
- 2- With your own PKI certificate and a PFX file;
- 3- Via a certificate backed by a Hardware Security Module.

For the project, the **self-signed certificates** have been used because they have been recommended for evaluation and testing. Figure 3.14 shows the sequence of commands to create a Self-signed certificate as well as the command to export the self-signed certificate and its output.

```

PS C:\Users\Administrator> $certificatePassword = ConvertTo-SecureString -AsPlainText "Cluster2018" -Force
PS C:\Users\Administrator> $signingCert = New-SelfSignedCertificate -DnsName "signing.shielded.com"
PS C:\Users\Administrator> Export-PfxCertificate -Cert $signingCert -Password $certificatePassword -FilePath "C:\signing
Cert.pfx"

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
-a----            3/17/2018  5:07 AM             2630 signingCert.pfx

PS C:\Users\Administrator>

```

Figure 3.14: Commands to create a Self-signed certificate and export.

After the creation of the self-signed certificate, the encryption certificate has been created and exported. Commands and their output are shown below:

```

PS C:\Users\Administrator> $encryptionCert = New-SelfSignedCertificate -DnsName "encryption.shielded.com"
PS C:\Users\Administrator> Export-PfxCertificate -Cert $encryptionCert -Password $certificatePassword -FilePath "C:\encr
yptionCert.pfx"

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
-a----            3/17/2018  5:11 AM             2639 encryptionCert.pfx

PS C:\Users\Administrator>

```

Figure 3.15: Commands to create an encryption certificate and export.

c) Initialization of the HGS server Using Admin-Trusted Attestation

The sequence of commands used in the project to initialize the HGS server Using Admin-Trusted Attestation is the following:

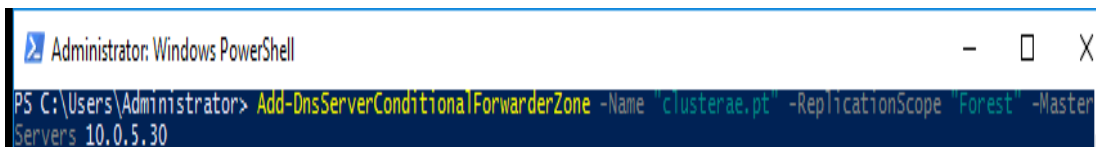
```
PS C:\Users\Administrator.HOST1> Initialize-HgsServer -HgsServiceName "chindeleHGS" -SigningCertificatePath "C:\signingCert.pfx" -SigningCertificatePassword $certificatePassword -EncryptionCertificatePath "C:\encryptionCert.pfx" -EncryptionCertificatePassword $certificatePassword -TrustActiveDirectory
LogPath: C:\Windows\Logs\HgsServer\180506025210\HOST1
PS C:\Users\Administrator.HOST1>
```

Figure 3.16: Commands to initialize the HGS server Using Admin-Trusted Attestation.

The cmdlet “initialize-HGSserver” use the encryption and the exported signing certificates to set the HGS to use Admin-Trusted attestation mode.

d) Configuration of the Fabric DNS resolution and Creation of a Security Group

Fabric DNS has been configured on the DNS server. For admin-trusted attestation, the DNS forwarder from the HGS domain to the fabric domain must be set up to enable Guarded Hosts to resolve the HGS server names. In this mode of attestation, the legitimate hosts are identified through a global Active Directory security group in the fabric DNS domain.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Add-DnsServerConditionalForwarderZone -Name "clusterae.pt" -ReplicationScope "Forest" -MasterServers 10.0.5.30
```

Figure 3.17: DNS forwarder from The HGS Domain to the Fabric Domain.



```
PS C:\Users\Administrator> netdom trust shielded.com /domain: "clusterae.pt" /userD:clusterae.pt\Administrator /password:"Cluster2018" /add
To improve the security of this external trust, security identifier (SID) filtering is enabled. However, if users have been migrated to the trusted domain and their SID histories have been preserved, you may choose to turn off this feature.

For more information about SID filtering and how to turn it off, see the help for netdom trust /FilterSids or see Help and Support.

The command completed successfully.
PS C:\Users\Administrator>
```

Figure 3.18: DNS Forwarder from The HGS Domain to the Fabric Domain (netdom).

In order to set up a DNS forwarder from the fabric domain to the HGS domain, the following command has been used:


```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-DnsServerConditionalForwarderZone -Name "shielded.com" -ReplicationScope "Forest" -Master
Servers 10.0.5.41
PS C:\Users\Administrator>
```

Figure 3.19: DNS Forwarder from the fabric domain to the HGS domain.

e) Deployment of Guarded Host

To deploy the Guarded Host in the guarded fabric of the project, a security group has been created in the fabric domain and added the Hyper-V host that will run the Shielded VM in our test bed. The command to create the Global security group is **“Get-ADGroup GuardedHostGroup”**. After the creation of the group, the register of the SID of the security group with the HGS server was necessary found. The command is shown on the figure 3.20:

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-HgsAttestationHostGroup -Name "GuardedHostGroup" -Identifier "5-1-5-21-295674899-19649766
2-1372754953-1119"
5-1-5-21-295674899-196497662-1372754953-1119:GuardedHostGroup
PS C:\Users\Administrator>
```

Figure 3.20: Adding a security group in the HGS server to be used to identify the hosts that are trusted to run the shielded VMs.

Figure 3.21 shows the configuration of the Attestation URLs and the host key protection on the guarded host.

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Set-HgsClientConfiguration -AttestationServerUrl "http://testehgs.shielded.com/Attestation" -
KeyProtectionServerUrl "http://testehgs.shielded.com/KeyProtection"
```

Figure 3.21: Configuration of the host key protection and attestation URLs of the guarded host.

After having made all this settings, it was necessary to validate them to see if they were ready to start the Shielded VM. Figure 3.22 shows the command to run the configurations Diagnostics and its overall Results.

```

PS C:\Users\Administrator> Get-HgsTrace -RunDiagnostics
Overall Result: Pass

Traces have been stored at "C:\Users\Administrator\AppData\Local\Temp\HgsDiagnostics-20180508-004252".

PS C:\Users\Administrator>

```

Figure 3.22: Run diagnostics of the HGS Server configuration.

As it can be seen in the figure above, the Overall result is *Pass*, meaning that HGS has been configured correctly.

f) Deployment of Shielded VMs

After the configuration of the guarded fabric, the infrastructure is now ready to deploy the Shielded VM. The main topic of this project it is to guarantee and create more security in the Virtualized infrastructures in Datacenter environments, and shielded VM in order to be able secure the environment. The steps necessary to deploy the shielded VM are explained below:

Creation of the Windows template disk

Before the creation of the Windows template disk, an OS disk has been created that will later be used to run through the Shielded Template Disk Creation Wizard. In order to create the disk a Microsoft Desktop Image Service Manager (DISM) has been used. Disk configuration must meet the requirements to support generation 2 VM or Shielded VM, such as Guid partition (GPT) disk, NTFS as file system, the operating system installed on the VHDX should be Windows Server 2012, Windows Server 2012 R2 or Windows Server 2016 (we have installed Windows Server 2016 on the project) and the operating system must be generated.

```

Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Users\Administrator\Desktop\WS2016\sources
C:\Users\Administrator\Desktop\WS2016\sources>Dism /apply-image /imagefile:install.wim /index:1 /applyDir:D:\
Deployment Image Servicing and Management tool
Version: 10.0.14393.0

Applying image
[=====                21.0%                ] _

```

Figure 3.23: Preparing an Operating System VHDX for windows template disk.

```

Select Administrator: Windows PowerShell
PS C:\Users\Administrator> Install-WindowsFeature RSAT-Shielded-VM-Tools -Restart

Success Restart Needed Exit Code      Feature Result
-----
True      No           Success      {Shielded VM Tools}

PS C:\Users\Administrator> New-SelfSignedCertificate -DNSName publisher.clusterae.pt

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\MY

Thumbprint                               Subject
-----
6AD9333E8E9A77AC81A7E8E27E04ACC694B6DE4F  CN=publisher.clusterae.pt

PS C:\Users\Administrator>
    
```

Figure 3.24: Installation of shielded VM tools and creation of a Self-Signed certificate.

To finish the process of the creation of the windows template disk, in Shielded template Disk Creation Wizard, the template disk has been generate. The Wizard will create the Volume Signature Catalog (stored in the VHDX metadata), compute the hash of the disk and enable BitLocker on the template disk [20].

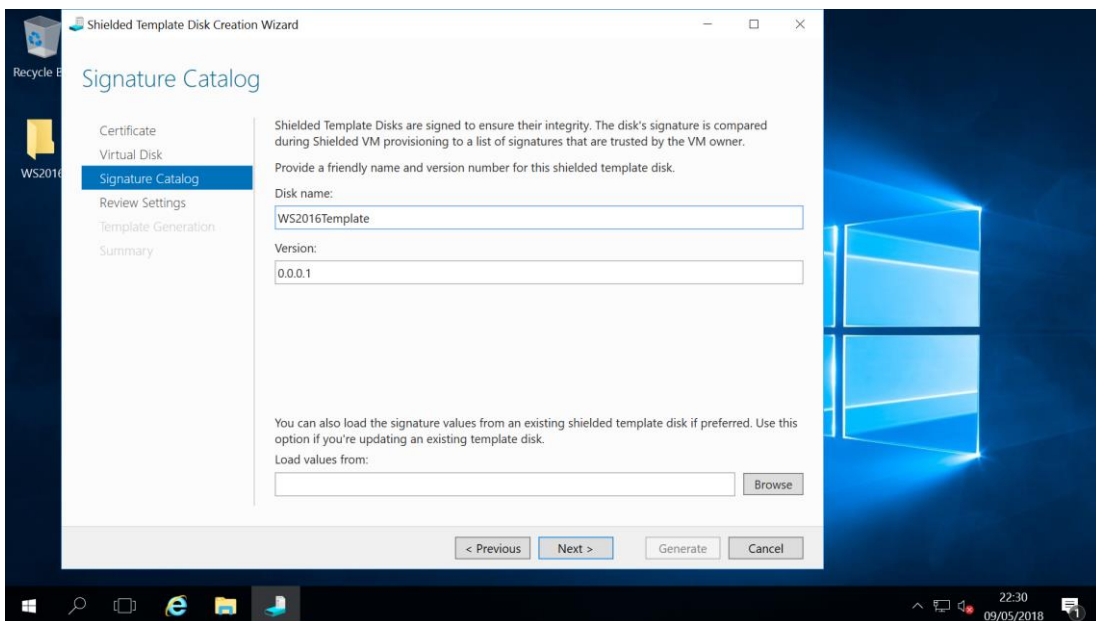
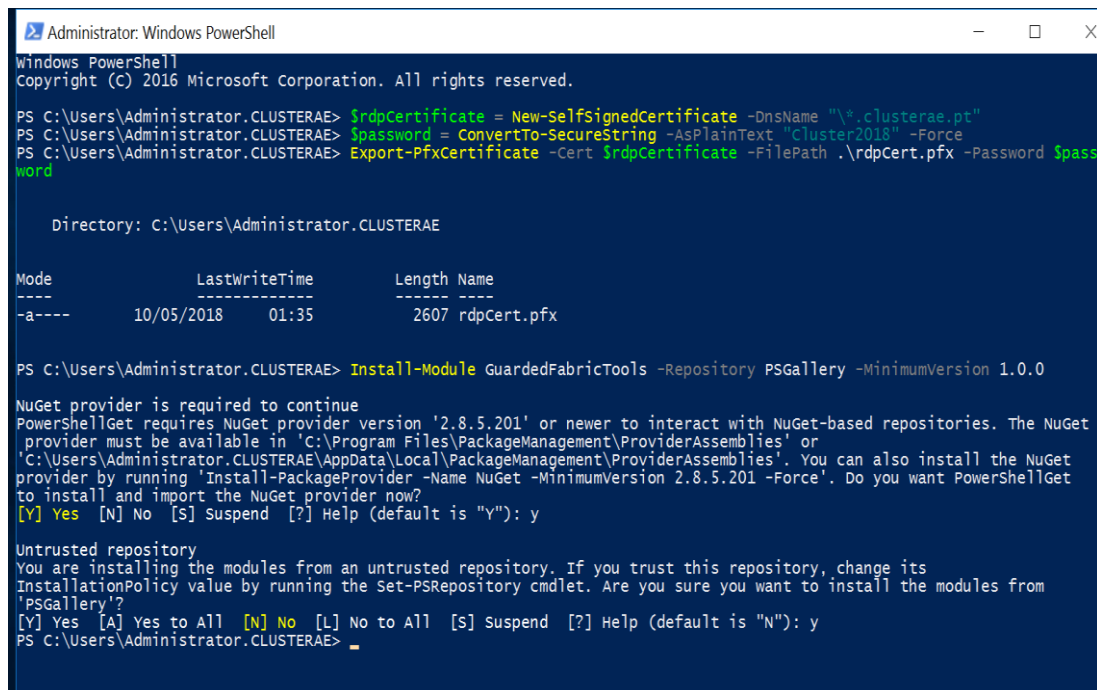


Figure 3.25: Shielded template disk creation wizard.

It is possible to create a Linux template disk as well, but in this project, only a Windows template disk has been created.

Creation of the Shielding data file

The concept of shielded data has already been discussed in section 2.3.5. Steps to create the Shielded Data file are shown in the figures below:



```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.CLUSTERAE> $rdpCertificate = New-SelfSignedCertificate -DnsName "*.clusterae.pt"
PS C:\Users\Administrator.CLUSTERAE> $password = ConvertTo-SecureString "cluster2018" -Force
PS C:\Users\Administrator.CLUSTERAE> Export-PfxCertificate -Cert $rdpCertificate -FilePath .\rdpCert.pfx -Password $password

Directory: C:\Users\Administrator.CLUSTERAE

Mode                LastWriteTime         Length Name
----                -
-a----            10/05/2018   01:35           2607 rdpCert.pfx

PS C:\Users\Administrator.CLUSTERAE> Install-Module GuardedFabricTools -Repository PSGallery -MinimumVersion 1.0.0

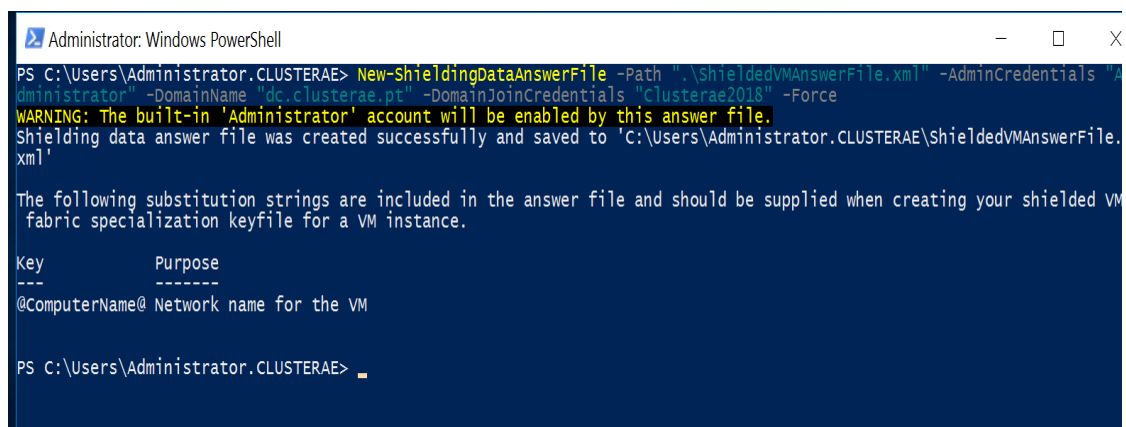
NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\Administrator.CLUSTERAE\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet
provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet
to install and import the NuGet provider now?
[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): y
PS C:\Users\Administrator.CLUSTERAE>

```

Figure 3.26: Obtain a certificate for a remote desktop and installation of a guarded fabric tools.

Figure 3.26 shows the commands to obtain the certificate for Remote Desktop Connection. They have been created because the tenants are only able to connect to their shielded VMs using Remote Desktop Connection or can connect even using other remote management tools.



```

Administrator: Windows PowerShell

PS C:\Users\Administrator.CLUSTERAE> New-ShieldingDataAnswerFile -Path ".\ShieldedVMAnswerFile.xml" -AdminCredentials "Administrator" -DomainName "dc.clusterae.pt" -DomainJoinCredentials "Clusterae2018" -Force
WARNING: The built-in 'Administrator' account will be enabled by this answer file.
Shielding data answer file was created successfully and saved to 'C:\Users\Administrator.CLUSTERAE\ShieldedVMAnswerFile.xml'

The following substitution strings are included in the answer file and should be supplied when creating your shielded VM
fabric specialization keyfile for a VM instance.

Key           Purpose
----           -
@ComputerName@ Network name for the VM

PS C:\Users\Administrator.CLUSTERAE>

```

Figure 3.27: Command to create a shielding answer file.

The last component in the shielding data files is related to the guardian of a VM and the owner. Guardians are used to designate both the guarded fabric and the owner of a shielded VM on which it is authorized to run [20]. Figure 3.28 shows the command to obtain the guardian metadata directly From the HGS of the infrastructure. The out file is “*ShieldedGuardian.xml*”.

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-HgsServer

Name                Value
----                -
AttestationOperationMode AD
AttestationUrl      {http://testehgs.shielded.com/Attestation}
KeyProtectionUrl    {http://testehgs.shielded.com/KeyProtection}

PS C:\Users\Administrator> Invoke-WebRequest "http://testehgs.shielded.com/KeyProtection/service/metadata/2014-07/metadata.xml" -OutFile .\shieldedGuardian.xml
PS C:\Users\Administrator>
```

Figure 3.28: Selected trusted fabric.

Shielded data file has been generated on “Shielding Data File Wizard”. In addition, to designate an existing owner guardian, for example, the appropriate guardian in the fabric has been selected.

Deployment of Shielded VM using the Windows Power Shell

According to Microsoft [20], it is possible to deploy the Shielded virtual machines in 4 ways: i) using the Power Shell, ii) using Windows Azure Pack, iii) using VMM and iv) Shield an existing VM. In this work, the Shielded VMs have been deployed using the Windows power shell. The command to create a new Shielded virtual machine in the Guarded Host is shown below:

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.CLUSTERAE> New-ShieldedVM -Name "EvaldoShieldedVM" -TemplateDiskPath "C:\VirtualDisk1.vhdx" -ShieldingDataFilePath "C:\temp\cluster\cluster.pdk" -wait
```

Figure 3.29: Command to create a new shielded virtual machine.

When the VM finishes provisioning, it will enter the OS-specific specialization period, and then it will be ready for use. The VM should be connected to a valid network for remote connect

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures using PowerShell RDP or SSH [20]. The creation of the Shielded VM differs only slightly from the creation of regular virtual machines. With a simple command in Windows PowerShell we can create, naming just the Shielded VM “EvaldoShieldedVM”, the path of the disk template and the path where the shielded data was saved (where it contains all the necessary security information for the protection of the Virtual Machine).

3.5 Conclusions

In this chapter, the proposed architecture for the project test bed has been illustrated: the architecture for the high availability environment of the regular virtual machines and the environment for the implementation of Shielded VMs.

A failover cluster in Windows Server 2016 using Hyper-V as the Hypervisor for the High availability of the regular VMs has been implemented. The Storage Server has been configured with FreeNas.

A Guarded Fabric has also been deployed and the Shielded VM has been implemented. The Host Guardian Service has been deployed, the creation of Self-Signed Certificates for HGS, the initialization of the HGS using the Admin-Trusted Attestation, the configuration of the Fabric DNs resolution were made, the Guarded host has been deployed and finally the Shielded VM has been deployed.

Chapter 4

Experiments and Results

4.1 Introduction

After the implementation of the failover cluster with regular VMs and shielded VMs, the next step is the evaluation of the performance implications for the use of regular virtual machines versus shielded virtual machines. This chapter, describes the experiments performed over the environment and the analysis of the obtained results.

4.2 Performance Metrics

4.2.1 Benchmarking

A Benchmarking program has been used to obtain the results performance due to the use of regular VMs and shielded VMs. Novabench [28], was the chosen program due to its simplicity and effectiveness. This software tests the performance of computer components and attribute proprietary scores, where higher scores correspond to better performance. The components the Benchmark test are the following ones [28]:

- **CPU (Central Processing Unit):** allows Novabench to evaluate general CPU performance while controlling memory performance and other variable.
- **GPU (Graphic Processing Unit):** the graphics tests are designed to run on most graphics cards and integrated graphics. If the system graphics capabilities do not meet the test requirement, the test is skipped and a score of 0 is given.
- **RAM (Random Access Memory):** evaluates the system memory transfer performance. RAM speed is measure in MB/s (Megabyte/seconds).
- **Disk:** this test measure direct, write speeds and sequential disk read of solid state or hard disk drive where the OS is installed on. Write Speed and Reed Speed is measure in MB/s.

The Novabench score has no upper limit, which means the higher the score, the better performance.

4.2.2 Virtual Machines

To measure the performance of the regular VM over the failover cluster created in Windows Server 2016, a set of experiences has been conducted. The hosts of the virtual machines were servers with Intel Core i7-770 CPU running at 3.6 GHz and 16 GB memory from Dell Brand, which run a 64-bit Windows Server 2016 Datacenter edition. Hyper-V 2016 is chosen as the Hypervisor for the native virtualization. The VMs have installed the Windows Server 2016 Datacenter edition and have 3 GB memory.

4.2.3 Shielded virtual machines

Shielded VMs may be seen as protected virtual machines. After the entire shielded VM creation process, detailed in chapter 3, some tests were performed to evaluate the performance. The guarded host of the shielded virtual machines was installed on a Server with Intel Core i7-770 CPU running at 3.6 GHz and 16 GB memory from the Dell Brand, which run a 64-bit Windows Server 2016 Datacenter edition. Hyper-V 2016 is chosen as the Hypervisor for the native virtualization. The shielded VM have 3-GB memory and have installed the Windows Server 2016 Datacenter edition. The metrics used for evaluation the shielded VMs were the same ones used to evaluate the performance of regular virtual machine: VCPU (Virtual Central Processing Unit), RAM and writing speed (Disk).

4.3 Virtual Machine Workloads

The first Workload used to measure the performance of virtual machines and shielded virtual machines consists of the following: after the virtual machine has been connected, several programs were opened, at the same time an 8-GB file transfer was executed while a video was reproducing as well. After realizing that the programs are all running, the Benchmark is turned on to measure the performance of both virtual machine and shielded virtual machine.

The second workload was based on the execution of a script in Windows PowerShell ISE, which looped 9 million times (9000000) to create a multiplication table.

4.4 Performance Evaluation Using the First Workload

Performance of the Virtual Machines using Novabench

A set of experiments has been made in virtual machines in order to evaluate its performance in terms of VCPU, RAM and writing speed. The experiments that were made consisted of putting the first workload of processing in the virtual machine to evaluate its performance.

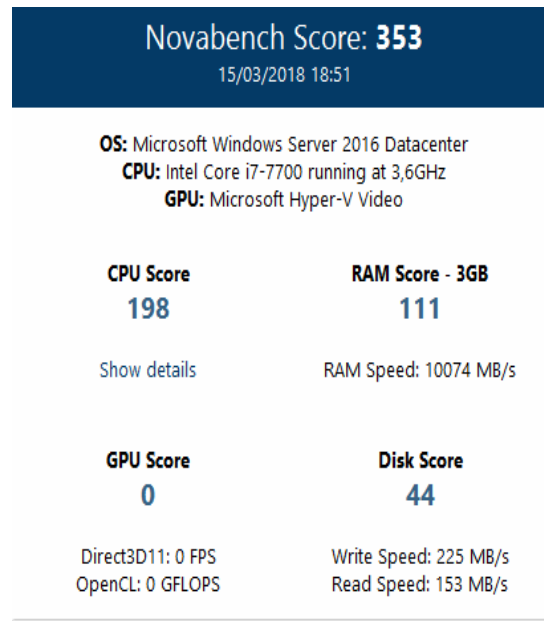


Figure 4.1: Regular virtual machine performance evaluation.

Figure 4.1 shows the performance evaluation of the regular VMs using the above infrastructure. The CPU had a Score of 198, while the RAM had a Score of 111, in which its speed was 10074 MB/s. The disk score had a score of 44 and the write speed was 225 MB/s and Read Speed was 153 MB/s. The overall performance score of the virtual machine was 353 as shown in figure 4.1. Several other tests and experiments have been done, and the average performance score of the virtual machines ranged from 320 to 400.

Performance of the Shielded virtual machines using Novabench

Experiments made were the same as those made with regular virtual machines with the same process. The results provided by the Benchmark are shown in figure 4.2.

As shown in figure 4.2, after the performed tests, the same workload sequence previously submitted to the virtual machine has been submitted to the shielded VM leading to a score of 314. This results was obtained using Novabench Benchmark.

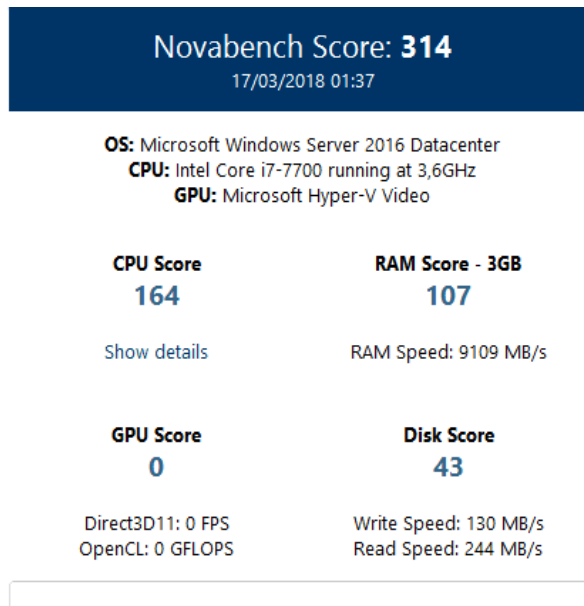


Figure 4.2: Shielded virtual machine performance rating.

Performance Comparison between Virtual Machines and Shielded virtual machines

Figure 4.3 summarizes the performance results of VCPU, RAM and Disk Written for both virtual machines and shielded virtual machine. Several experiments and tests have been made and the results varied based on the amount of workload submitted both to virtual machines and shielded virtual machines.

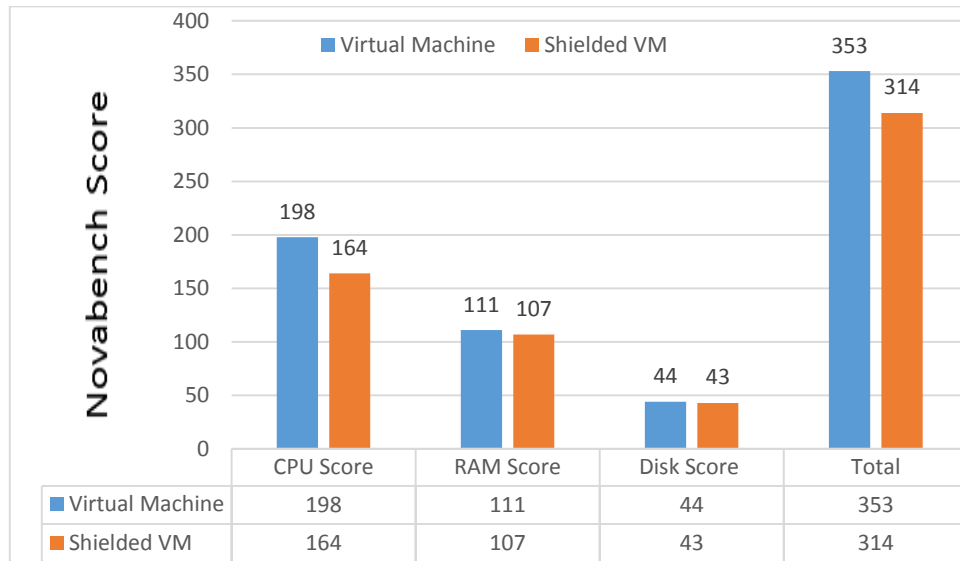


Figure 4.3: Shielded virtual machine versus virtual machine performance rating.

As shown in figure 4.3, with the same workload submitted for the virtual machine and the Shielded VM in terms of CPU the difference was small. The virtual Machine had a Score of 198 and the shielded VM had a Score of 164. In terms of RAM, the VM had a Score of 111 and the Shielded VM had a Score of 107, being small the difference between the two machines. Regarding the Disk Score, the virtual machine had a Score of 44 and the Shielded VM had a score of 43, which are very close. In total, according to this experience, the virtual machine had a score of 353 and the shielded VM had a Score of 314, being the performance of regular virtual machines better than the performance of the shielded VM.

Figure 4.4 shows a brief resume about the performance of the Memory (Disk) between virtual machines and shielded virtual machines. The first section represents RAM Speed measure in MB/s, the second section represents the Write Speed of the disk and the third section represents the Read Speed. This figure illustrates the performance of Disk for the virtual machine and the shielded virtual machine by running the Benchmark on disk. As may be seen in this figure the virtual machine has better performance than the shielded virtual machine.

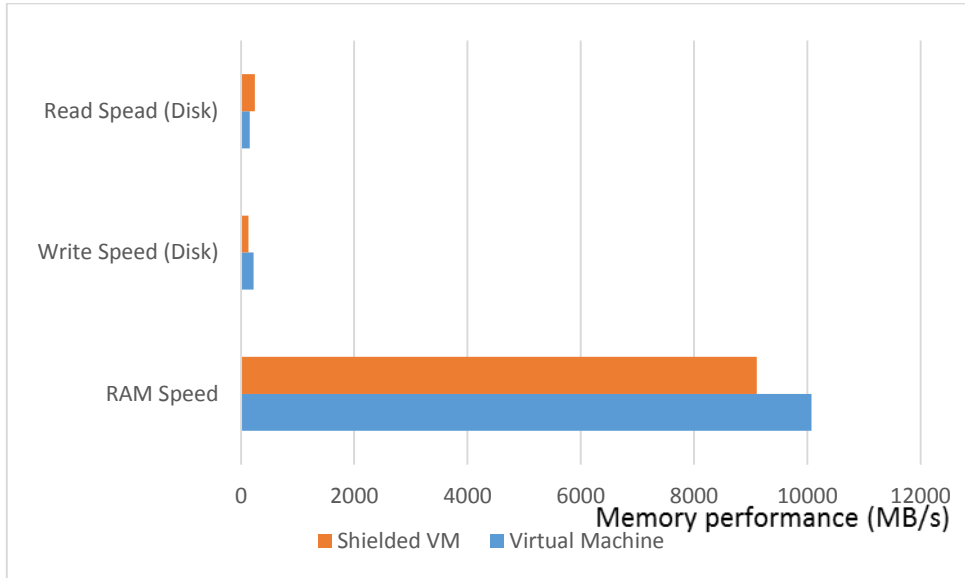


Figure 4.4: Memory performance between virtual machines and shielded VM.

Time do Install a New SO

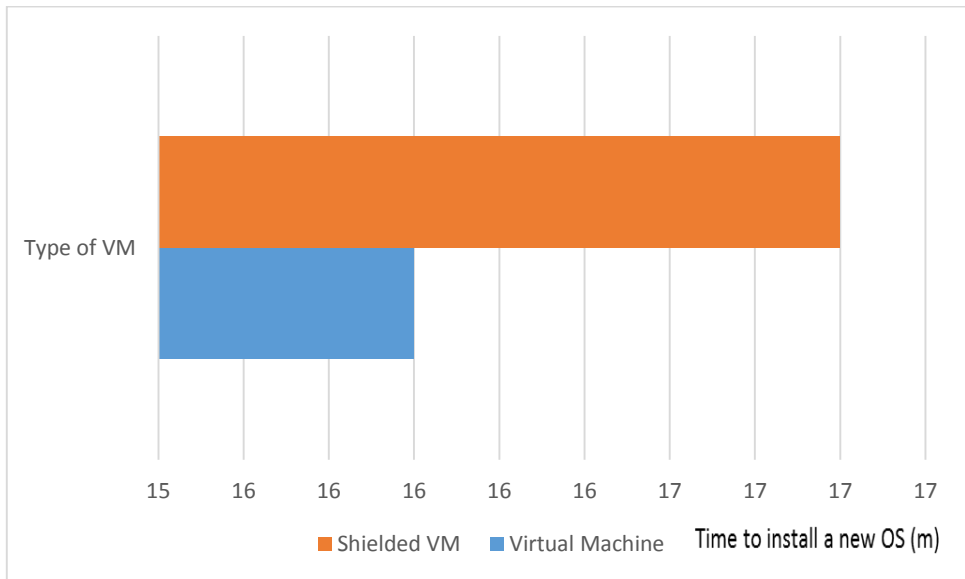


Figure 4.5: Time to install an Operating System.

Figure 4.5 shows the minimum time required to install Windows Server 2016, both in a virtual machine and in a shielded virtual machine. As may be seen in this figure, the minimum time

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures required for the installation of an operating system in virtual machines is 16 minutes and 8 seconds while the shielded VM requires 17 minutes and 5 seconds for the same operation.

Time to Boot

Figure 4.6 shows the minimum time required to boot a Windows Server 2016, both in a virtual machine and in a shielded virtual machine. This figure shows that the average time to boot for a machine, whether regular or shielded is 40 seconds according to the experiment carried out.

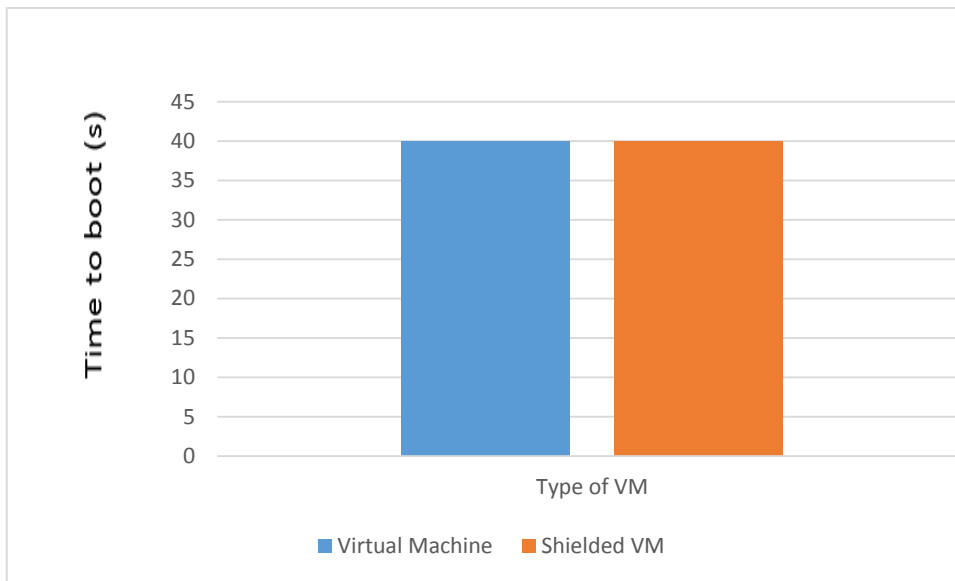


Figure 4.6: Boot time of shielded VM and virtual machine.

To the best of our knowledge, there are no published works comparing the performance of virtual machines and Shielded virtual machines. Most of the reported works made comparisons among different hypervisors or between host and VM.

Table 4.1: Summary of the performance results.

	Virtual Machine	Shielded virtual machine
CPU Score	198	164
RAM Score	111	107
Disk Score	44	43
RAM Speed (MB/s)	10074	9109
Write Speed (MB/s)	225	130
Read Speed (MB/s)	153	244
Installation of OS (m)	16	17
Time to Boot (s)	40	40

Table 4.1 shows the Summary of the performance results for the performed tests.

4.5 Performance Evaluation Using the Second Workload

For this evaluation, the workload was the execution of a script in Windows PowerShell ISE, which looped 9 million times (9000000) to create a multiplication table. For this test, the results in terms of runtime are presented in table 4.2.

Table 4.2: Script runtime comparison

Type of VM	Script runtime
Virtual Machine	23 min, 38s
Shielded virtual machine	23 min, 52s

According to the table 4.2, the shielded virtual machine took more time to finish the execution of the script, but it may also be observed that the difference is small (14 s).

During the execution of the Script, one may also observe through Windows Resource Monitor the performance of CPU and Memory. The performance of CPU is shown in the table 4.3.

Table 4.3: CPU performance for the script execution.

Type of VM	Threads	CPU (%)	Average (%)
Virtual Machine	20	98	97,81
Shielded V.M	20	98	97,85

According to the results show in table 4.3, the number of activity threads in the process according to the Windows Resource monitor was 20. The CPU presents in the table indicates the percentage of CPU consumed on the process. Moreover, the Average indicates the percentage consuming by the process. The results show that there is a similar CPU consumption between virtual machines and shielded virtual machines for the execution of the script.

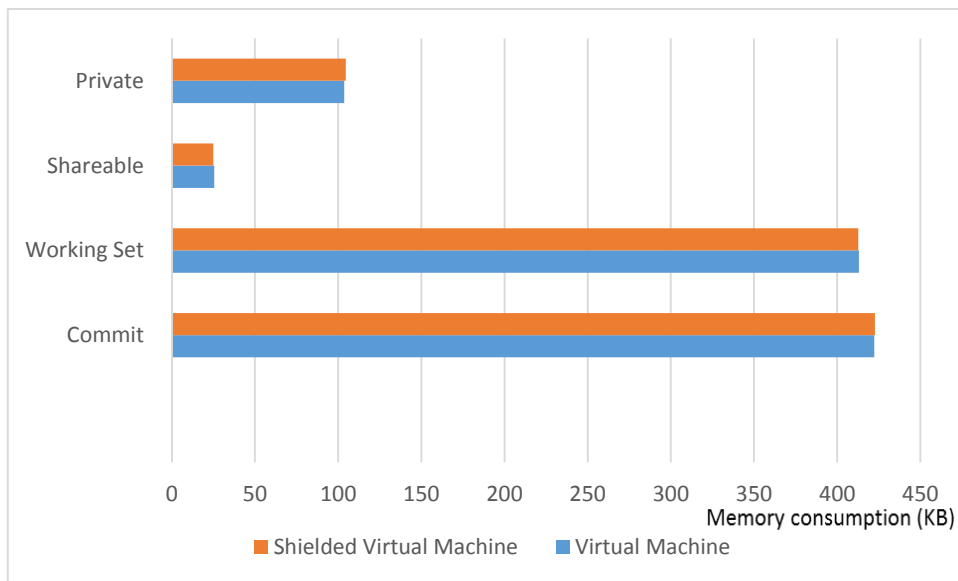


Figure 4.7: Comparison of memory consumption between virtual machine and shielded virtual machine.

Figure 4.7 shows a brief resume regarding the performance of the Memory consumption between virtual machines and shielded virtual machines during the execution of the script. The Commit variable represents the amount of virtual memory reserved by the operating system for the process in Kilobytes (KB). Working Set represents the amount of physical memory

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures currently in use by the process in KB. Shareable represents the amount of physical memory in use in the process that can be shared with other process in KB. Private represents the amount of physical memory currently in use in the process that cannot be used by other process. According to this figure, we may see that there is also a similar performance between virtual machines and shielded virtual machines.

4.6 Conclusions

Based on the results obtained in the project, and by the study we did between VM and Shielded VM we can consider that the virtual machines had better performance in relation to the Shielded VM. However, the results also show that the difference was very small, which leads us to conclude that the protection that the Shielded VM has does not affect its normal performance compared to the virtual machines. In terms of cost and benefits, companies are more likely to do some resistance to deploy or upgrade their virtualized environments to Shielded VMs because they require a larger infrastructure for their proper operation than regular VMs. If the idea of virtualization is cost reduction, we think that the implementation of Shielded virtual machine would be more expensive for the company since in terms of performance the Regular Virtual Machine have better performance as shown the results obtained in this project.

In a general way, controlling access to VMs is a problem that unfortunately all the Hypervisors have. VMware vSphere, KVM and Hyper-V all share the same security problems. The new HGS in Windows Server 2016 Hyper-V with its Shielded VMs studied in this dissertation give a unique solution to the problem of securing VMs from all unauthorized access. Although the configuration of the HGS is very complex, it allows restricting access to the VMs to only running on trusted Hosts (Guarded Host), as well as prevents unauthorized admins and malware from compromising the VM [26]. Shielded VMs allows restricting access to the VMs to only running on trusted Hosts, as well as prevents unauthorized admins and malware from compromising the VM.

The regular VMs performed slightly better than shielded VMs, because of the new elements that appear for the configuration of an environment of Shielded virtual machines such as Host Guardian Service and Guarded Host.

Chapter 5

Conclusions and Future Works

5.1 Main Conclusions

With this work, researchers and any professionals of the area, and with particular interest in virtualization, can have access to the process of creating and implementing a high availability environment for Virtual Machines in a Datacenter. They will also have access to the complete process of Deploying Shielded virtual machines with Host Guardian Service. The Shielded virtual machines have been implemented through Admin-trusted attestation, which designates hosts that should be designated as guarded hosts in Active Directory to decrypt and start shielded VMs.

One of the major contributions of this work is that we can find in the same work both processes, the Implementation of a failover cluster in Windows Server 2016 Hyper-v and the Deployment of a Guarded Fabric and Shielded VM through Admin-trusted attestation.

It has been observed that Virtual machines had better performance in relation to the Shielded VM. However, the results also show that the difference was very small, which leads us to conclude that the protection that the Shielded VM has does not affect its normal performance compared to the regular virtual machines. We think that the implementation of Shielded virtual machine would be more expensive for the companies because of the amount of equipment needed compared to normal virtual machines.

It has also been observed that the new HGS in Windows Server 2016 Hyper-V with its Shielded VMs studied in this dissertation give a unique solution to the problem of securing VMs from all unauthorized access. Although the configuration of the HGS is very complex, it allows restricting access to the VMs to only running on trusted Hosts as well as prevents unauthorized admins and malware from compromising the VM.

The main objective of this dissertation was to specify and implement a failover cluster with native virtualization at the hardware level that includes virtual machines versus shielded virtual machines in order to study the performance implications for the use of virtual machines versus shielded virtual machines in high availability infrastructure. Throughout this work and at the end of the implementation of the bed test and the experimental tests, the objective has been achieved.

Throughout our work, we had some limitations in terms of infrastructure, since it was not enough to integrate regular virtual machines and Shielded virtual machines in the same high availability environment, and we also had time limitation for making more tests, since we first had to configure the high availability environment of the virtual machines and then we had to

Performance Implications For the Use of VMs vs Shielded VMs in High Availability Virtualized Infrastructures
reconfigure the same devices to configure the Guarded Fabric and the Shielded virtual machines.

5.2 Directions for Future Work

As future work, it is suggested:

- Deploy Shielded VMs with TPM-trusted attestation mode (Hardware based) for testing the hardware level security
- Make experiments with live migration of Shielded VM and Virtual Machines and measure their performance;
- Perform tests and experiences in real production environments.

References

- [1] “Microsoft | Windows Server Blog | A closer look at shielded VMs in Windows Server 2016.” [Online]. Available: <https://blogs.technet.microsoft.com/windowsserver/2016/05/10/a-closer-look-at-shielded-vm-in-windows-server-2016/>. [Accessed: 05-Dec-2017].
- [2] “VMware - Official Site.” [Online]. Available: <https://www.vmware.com/>. [Accessed: 19-Jun-2018].
- [3] “KVM.” [Online]. Available: https://www.linux-kvm.org/page/Main_Page. [Accessed: 19-Jun-2018].
- [4] “The Xen Project, the powerful open source industry standard for virtualization.” [Online]. Available: <https://www.xenproject.org/>. [Accessed: 19-Jun-2018].
- [5] “Rogue sysadmins the target of Microsoft’s new ‘Shielded VM’ security • The Register.” [Online]. Available: https://www.theregister.co.uk/2016/10/21/shielded_vm/. [Accessed: 05-Dec-2017].
- [6] B. Li, “Front cover Introduction to Windows Server 2016 Shielded VMs Introduces the new Shield Virtual,” 2016.
- [7] V. K. Manik and D. Arora, “Performance Comparison of Commercial VMM : ESXI, XEN, Hyper-V & KVM,” *2016 3rd Int. Conf. Comput. Sustain. Glob. Dev.*, pp. 1771-1775, 2016.
- [8] P. Sheinidashtegol and M. Galloway, “Performance impact of DDoS attacks on three virtual machine hypervisors,” *Proc. - 2017 IEEE Int. Conf. Cloud Eng. IC2E 2017*, pp. 204-214, 2017.
- [9] D. R. Tobergte and S. Curtis, *Distributed and Cloud Computing*, vol. 53, no. 9. 2013.
- [10] “What is virtual machine (VM)? - Definition from WhatIs.com.” [Online]. Available: <http://searchservirtualization.techtarget.com/definition/virtual-machine>. [Accessed: 30-Nov-2017].
- [11] H. Aissaoui-Mehrez, P. Urien, and G. Pujolle, “Implementation Software to Secure Virtual Machines with Remote Grid of Secure Elements,” in *2014 IEEE Military Communications Conference*, 2014, pp. 282-287.
- [12] D. Vogel, “The Benefits and Challenges of Virtual Machine Hosting - Datapipe

- Blog.” [Online]. Available:
<https://www.datapipe.com/blog/2014/04/23/benefits-challenges-virtual-machine-hosting/>. [Accessed: 21-Dec-2017].
- [13] S. Bigelow, “Benefits of VMs include workload mobility and fast duplication.” [Online]. Available:
<http://searchservvirtualization.techtarget.com/tip/Understanding-the-benefits-of-a-virtual-machine>. [Accessed: 21-Dec-2017].
- [14] R. Natário, “Networks and Servers: Failover Clustering (I).” [Online]. Available:
<http://networksandservers.blogspot.pt/2011/04/failover-clustering-i.html>. [Accessed: 01-Feb-2018].
- [15] J. Gerend, “Failover Clustering | Microsoft Docs.” [Online]. Available:
<https://docs.microsoft.com/en-us/windows-server/failover-clustering/failover-clustering-overview>. [Accessed: 01-Feb-2018].
- [16] N. M. Maharjan, “Implementing Failover Clustering with Windows Server 2016 Hyper-V - MS Server Pro.” [Online]. Available:
<http://www.mserverpro.com/implementing-failover-clustering-windows-server-2016-hyper-v/>. [Accessed: 01-Feb-2018].
- [17] M. E. Elsaid and C. Meinel, “Multiple virtual machines live migration performance modelling - VMware vMotion based study,” *Proc. - 2016 IEEE Int. Conf. Cloud Eng. IC2E 2016 Co-located with 1st IEEE Int. Conf. Internet-of-Things Des. Implementation, IoTDI 2016*, vol. 04, pp. 212-213, 2016.
- [18] J. Gu *et al.*, “Secure Live Migration of SGX Enclaves on Untrusted Cloud,” *Proc. - 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Networks, DSN 2017*, pp. 225-236, 2017.
- [19] T. Overview, *Introducing Windows Server*. 2012.
- [20] Microsoft, “Virtualization Guarded Fabric and Shielded VMs Hyper-V,” 2016.
- [21] V. Apolinario, “What are Shielded VMs in Windows Server 2016 Hyper-V? - Datacenter and Private Cloud Security Blog.” [Online]. Available:
<https://blogs.technet.microsoft.com/datacentersecurity/2016/03/14/windows-server-2016-shielded-vms-protecting-tenant-secrets/>. [Accessed: 04-Feb-2018].
- [22] “Create a Windows shielded VM template disk | Microsoft Docs.” [Online]. Available: <https://docs.microsoft.com/en-us/windows-server/virtualization/guarded-fabric-shielded-vm/guarded-fabric-create-a-shielded-vm-template>. [Accessed: 05-Dec-2017].

- [23] VMware, *vSphere Web Services SDK*. .
- [24] B. Lee, “Hyper-V Cluster Setup 1 of 3: Configuration, Network Planning.” [Online]. Available: <https://www.nakivo.com/blog/hyper-v-cluster-setup-host-configuration/>. [Accessed: 18-Apr-2018].
- [25] “1. Introduction – FreeNAS®11.1-U4 User Guide Table of Contents.” [Online]. Available: <https://doc.freenas.org/11/intro.html#new-features-in-release>. [Accessed: 18-Apr-2018].
- [26] M. Otey, “Shield Hyper-V with Microsoft’s Host Guardian Service -- Redmondmag.com.” [Online]. Available: <https://redmondmag.com/Articles/2016/11/01/HyperV-Lockdown.aspx?Page=1>. [Accessed: 23-Apr-2018].
- [27] B. Lee, “Hyper-V Cluster Setup 3 of 3: Creation, Shared Volume.”
- [28] Novabench, “Novabench - Documentation - Getting Started.” [Online]. Available: <https://novabench.com/docs/getting-started>. [Accessed: 30-May-2018].

