

Airidas Svobunas

# IMPLEMENTING A PRIVATE CLOUD WITH MICROSOFT SYSTEM CENTER 2016 IN A VIRTUAL LAB ENVIRON- MENT

Bachelor's Thesis  
Information Technology

2017



South-Eastern Finland  
University of Applied Sciences

<b>Author (authors)</b>  Airidas Svobunas	<b>Degree</b>  Bachelor of Information Technology	<b>Time</b>  May 2017
<b>Title</b>  Implementing a private cloud with System Center 2016 in a virtual lab environment		59 pages
<b>Commissioned by</b>  South-Eastern University of Applied Sciences		
<b>Supervisor</b>  Matti Juutilainen		
<b>Abstract</b>  <p>The objective of this thesis was to create a private cloud with Microsoft System Center 2016. The practical part was implemented in a virtual lab environment. Additional software such as Microsoft Azure Pack: Portal and API Express was used for end users to interact with the private cloud over a web browser.</p> <p>A private cloud environment consists of four virtual machines, where every of it has a specific role in the environment. Domain Controller is responsible for Active Directory, DNS, DHCP, SQL, SAN and SC VMM. RemoteDG is a server that has Remote Desktop Gateway feature installed. While rest of last two virtual machines (Hyper-V01 and Hyper-V02) are Hyper-V servers and configured to work as a failover cluster to provide high availability.</p> <p>The main findings of the study were to implement a private cloud with System Center 2016 in a virtual lab environment. The study showed that in order to implement a private cloud the knowledge of cloud computing, networking and <i>fabric</i> was required (where <i>fabric</i> implies a private cloud resources such as network, storage, servers and clusters). This private cloud was successfully implemented in a virtual lab environment.</p>		
<b>Keywords</b>  Windows Server 2016, System Center 2016, cloud computing, private cloud		

# CONTENTS

1	INTRODUCTION .....	5
2	VIRTUALIZATION AND CLOUD COMPUTING .....	6
2.1	What is virtualization? .....	6
2.2	What is cloud computing? .....	9
2.3	Virtualization in cloud computing .....	12
2.4	Cloud service models .....	13
2.5	Cloud types.....	15
2.6	Private cloud creation and management alternatives .....	18
2.7	Microsoft System Center 2016.....	19
2.8	Microsoft System Center 2016 Virtual Machine Manager.....	20
3	DESIGNING A PRIVATE CLOUD .....	22
3.1	Network .....	22
3.2	Servers .....	23
3.3	Storage.....	27
3.4	Clusters .....	28
4	INSTALLATION AND CONFIGURATION.....	29
4.1	Operating system installation.....	30
4.2	Microsoft network service installation and configuration .....	31
4.3	Preparing the environment for System Center Virtual Machine Manager .....	32
4.4	Installing System Center Virtual Machine Manager .....	35
5	BUILDING THE PRIVATE CLOUD WITH SYSTEM CENTER VIRTUAL MACHINE MANAGER.....	36
5.1	Adding VMCluster to the host group .....	37
5.2	Allocating host reserves.....	37
5.3	Storage classification.....	38

5.4	Creating a logical network .....	39
5.5	Creating a virtual network .....	41
5.6	Assigning resources to the Service Network .....	42
5.7	Creating a cloud.....	43
5.8	Building a hardware profile .....	45
5.9	Creating a guest OS profile .....	45
5.10	Building a VM template.....	46
5.11	Deploying Windows Azure Pack: Portal and API Express .....	47
5.12	Connecting System Center Virtual Machine Manager to the Windows Azure Pack portal	48
5.13	Creating a new subscription plan and adding end users .....	49
5.14	Creating certificates .....	49
6	RESULTS AND ANALYSIS .....	52
6.1	The administrator's experience in the Windows Azure Pack portal and in the System Center Virtual Machine Manager console .....	52
6.2	The end users' experience in the Windows Azure Pack portal .....	53
7	CONCLUSIONS .....	56
	REFERENCES .....	57

## 1 INTRODUCTION

A few decades back, there was no email, the internet or telecommunications. However, today massively huge amounts of information are flying through every person via email, the internet and other IT technologies. In the 21<sup>st</sup> century the internet is prevailing and it is the main technology not only for communication, but also for providing services. In addition, technology such as cloud computing has become very popular in the past few years.

The cloud itself is a term which describes network elements that provide services, from the user point of view. Because of this, cloud computing is a technology based on the internet that provides shared computer resources over the network for end users. Cloud types such as private, public or hybrid offer flexibility for consumers to support their business needs in the best way. Also, cloud computing includes virtualization. For example, nowadays computers are so powerful that one physical computer can run virtual machines that act like physical ones. Moreover, virtual machines have been implemented in clouds that allow optimization and flexibility. From this view point, how can organizations, companies or developers have the job done faster and easier using this approach? How quickly can they release their software for testing their product on different platforms without buying machines with powerful hardware for each worker?

The aim for this thesis is to answer these questions by creating a private cloud where the end users could reach an organization's private cloud by sitting in their office and running a virtual machine on a private cloud instead on their work computer. End users will interact with a private cloud by using the user interface (UI) via the web browser. But before all this, the most important task is to understand what a private cloud is, how it works, what services it needs to run and how to implement it. I am planning to start the practical part in the following order: First, I install and configure required servers (DC, DNS, SQL, SAN, RDG and SC VMM). Then, I start to implement a private cloud. Finally, set up the web browser and configure remote access to allow end users to connect to virtual machines. Everything will be installed and tested in a virtual lab environment.

## 2 VIRTUALIZATION AND CLOUD COMPUTING

This chapter deals with technologies such as virtualization and cloud computing. The role of virtualization in cloud computing takes a very important part in optimizing devices' workload as well as energy efficiency in data centers. Also, cloud types and service models allow deploying automatization over the internet as well as running software and enabling a self-service feature. This chapter also discusses management tool alternatives for a private cloud creation. Finally, the end of the chapter takes a closer look at the System Center suite.

### 2.1 What is virtualization?

Virtualization is technology which allows making virtualized hardware, both input and output devices as well as operating systems. For example, servers, personal computers, storage or operating systems can be virtualized, but they act as they would be physically real. This technology allows running several or even tens of virtual machines in a one physical server. To run a virtual machine, a virtualization layer and a hypervisor software are required. Today, hardware-assisted virtualization technology helps to increase optimization and enables excellent performance in order to create virtual machines and to run them together with a hypervisor software. A hypervisor (Virtual Machine Monitor or VMM) is software responsible for hosting and managing virtual machines on a physical one (also known as a *host*). There are two types of hypervisor: native or bare-metal type, where virtualization is running directly on top of hardware, and hosted hypervisor, where software is running on top of the operating system.

In addition, according to VMware (2007, 6), hardware-assisted virtualization enables running new instructions with the new CPU execution mode under the *Ring 0* layer with a new root mode (see Figure 1). Vendors such as Intel (Intel-V technology) or AMD (AMD-V technology) include this type of virtualization technology in their CPUs released in 2006 so forth. As Figure 1 shows, the guest OS is directly running on *Ring 0* layer, and user requests are directly running on the *Ring 3* layer, and this enables no collapse and no errors between root and non-root modes in order to run virtualization with the best performance and optimization.

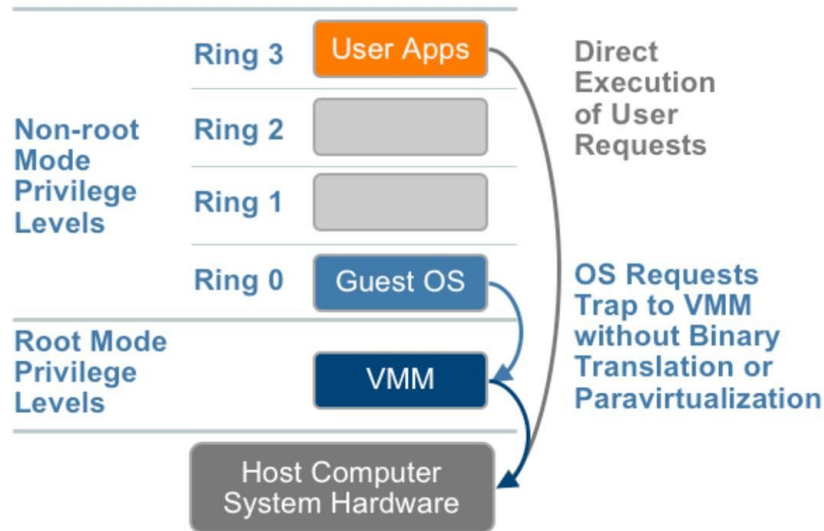


Figure 1. Hardware-assisted virtualization (VMware 2007, 6)

To run virtualization in a physical machine, it is not enough to virtualize the CPU only. There is another component required for virtualization – memory. Every modern x86 CPU includes the memory management unit (MMU) and the translation lookaside buffer (TLB) for optimizing the virtual memory performance. In order to run a virtual machine, another level of the memory virtualization is required. The MMU has to be virtualized in order to support the guest OS (virtualized operating system). Since every time the physical memory is translating addresses between the virtual and the physical memory, the TLB technology is used to avoid two level access (see Figure 2). When the guest OS makes some changes from the virtual memory to the physical memory, the VMM updates a shadow page table for synchronization. (VMware 2007, 6.)

The following figure shows the memory virtualization in a shadow page table. The red line in Figure 2 shows that the VMM uses the TLB hardware to map the virtual memory directly to the physical memory to avoid two-level translation on every access. Thus, the performance of the virtual memory is enhanced.

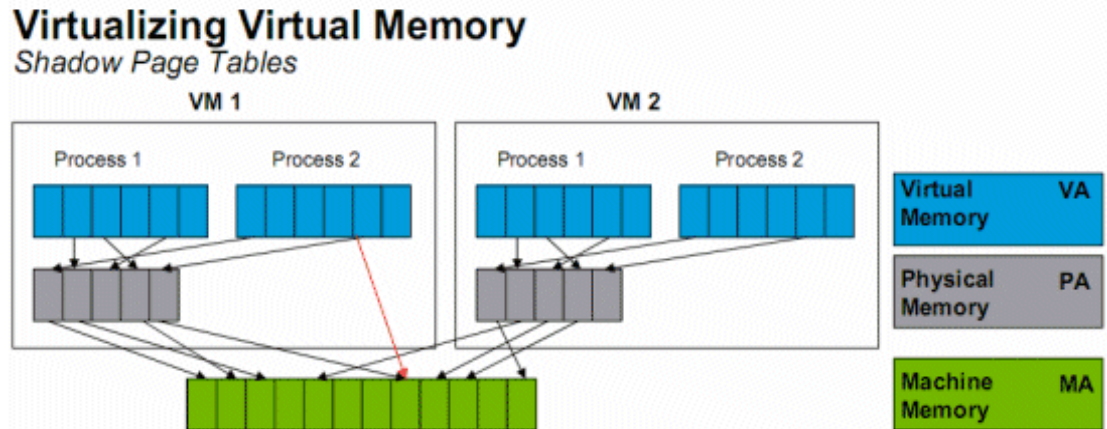


Figure 2. Virtualizing Virtual Memory (VMware 2007, 7)

The last major component in virtualization is the device and I/O virtualization. This includes sharing the hardware and handling the routing of I/O requests between virtual machines and physical ones. Often, software based I/O in virtualization is full of features and the simple management. This includes, for example, the networking where virtual NICs (Network Interface Card) and switches can be created without any effect on the real physical network infrastructure and bandwidth. A single hardware component can be split into few virtual devices. For example, a single NIC can be virtualized into few virtual NICs. This step is achieved with a hypervisor software which is virtualizing the physical hardware and creating each virtual machine with a specific group of standard virtual devices. They emulate the well-known hardware and communicate with the physical hardware by translating virtual machine requests to the system hardware. (VMware 2007, 7.)

There is also the ability to run a virtualization layer inside a virtual machine, and this technology is called nested virtualization. The first level virtualization is running on the typical hardware and called *Level 0* or *L0*. For the first level virtualization layer, VMware Workstation Player hypervisor will be used in the practical part of this thesis and will run the whole system required for a private cloud implementation. The following Figure 3 shows the nested virtualization scheme for this practical part.



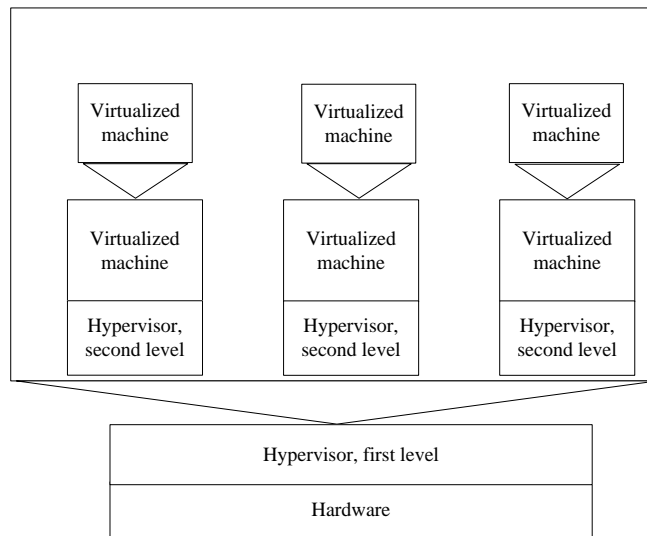


Figure 3. Nested virtualization scheme

The second level, or *Level 1* or *L1* virtualization would be running inside the first level virtualization layer. The second level virtualization could be running a hypervisor such as Hyper-V or KVM (kernel-based virtual machine). In this scenario, for the second virtualization layer, Hyper-V is selected. In fact, the host is running a standard unmodified operating system such as Windows, Linux or MAC OS X. One or several virtual machines can be created and running at the same time. The virtualization application is responsible for managing virtual machines – starting, stopping, restarting or pausing them including the essential control of physical machine resources of the individual virtual machine.

## 2.2 What is cloud computing?

To begin with, cloud computing is quite young technology. According to Levitt et al. (2009, 2), in the 1990s, it came as a very simple idea – computers could become as easy to access as power grid line are accessing homes. Later, in 1999 Salesforce.com introduced a pattern where some applications were delivered via a simple website. From this view point cloud computing started to grow. Big companies such as Amazon or Google began to use their own services based on cloud computing. After the success of Google Docs, cloud computing became popular around the world for personal use, e.g. keeping personal files in the clouds. This also deals with probabilities of losing personal data. Indeed, accessing the personal data from anywhere in the world at any time using any device

which supports a web browser has become very easy. And for security reasons, only authorized access is allowed where only the user who knows his login can access the data.

This technology allows companies as well as end users to access their personal data which is stored in clouds. When they access the data they actually access the cloud itself where personal data is stored. This is called the client-server model, where the client is the end user that is requesting services, and the server is where specific service, data or application is located. Clients are communicating with servers via the internet, where the client is sending specific requests to the server, and then the server responds to the client in order to receive the specific data. The server side topology begins with firewalls and ends with clustering (servers) (see Figure 4). Technology like firewall ensures security to help keep users' data safe. It is essential to have strong network security in data centers where cloud computing servers are located. In addition, clustering is a technology which enables optimization in virtualization and redundancy between critical devices such as network routers, switches or servers and ensure high availability and load balancing where specific data or application could be accessed 24/7.

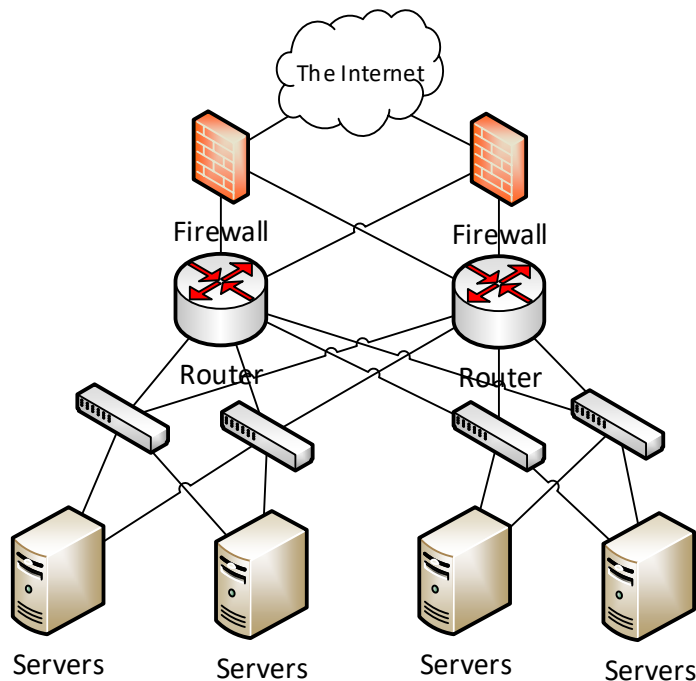


Figure 4. Simple data centers network's topology

Cloud computing allows accessing and using applications via the internet. Consumers usually access cloud computing using a web browser, although there is a possibility to use specific mobile apps or client applications installed on the computer. According to Kelvin (2014), this is called *Front End*. This part consists only of the client side network infrastructure (network devices and computers) and applications. While *Back End* is a cloud part where end users are accessing to. The following Figure 5 shows the architecture of cloud computing where end users are communicating with clouds via the internet.

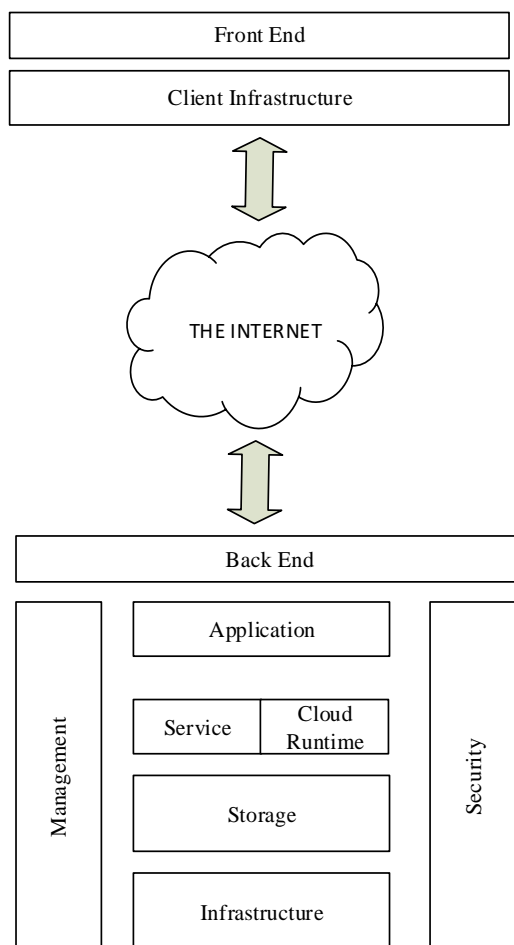


Figure 5. Cloud computing architecture

Cloud computing consists of a big data storage, security, services, servers, applications etc. In order to keep end users' data safe, it is important to ensure security in both physical and network parts. High availability, load balancing and integrity between cluster nodes should be also improved. (Kelvin 2014.)

### 2.3 Virtualization in cloud computing

Virtualization and cloud computing enables and optimize workload management, automation and self-service, and at the same time allows for end users to use services such as email, deploy virtual machines or keep backup copies in the cloud. Virtualization is a technology which is manipulating the hardware, whereas cloud computing offers services from that manipulation. According to Swathi et al. (2014, 5–6), a virtualization can be applied very broadly including storage, network, memory, OSes and applications. A virtualization offers the best management, enables automatization and security, where all virtual machines are separated and isolated from each other. This allows creating and deploying virtual machines without any interaction between different users' virtual machines even if those were created on the same physical host. Also, the hardware management is more optimized for virtual machine, for example, adding additional hardware component requires less time and money. Thus, for example, developers can run few virtual machines in the cloud for deployment or testing of their product which they about to release.

Another example, where virtualization can help to reduce the management time, money and at the same time to increase high availability in cloud computing is a recover in case there was a natural disaster. Nowadays, often phenomenon is natural disasters, which can lead data centers into losing electricity. Sometimes, even, servers are required to be updated in order to gain strong security patches (especially, in Windows systems). According to Arab (2017, 1), first, solution such as live migration can help reduce time and cost in case there is a catastrophe or any other situation that creates collapse of devices' in the data center. Second, live migration offers fast move of the virtual machine from the one physical server to the another. Third, live migration allow for system administrators to optimize system load or save power by completely shutting down servers. Practically, the purposes of the virtual machine live migration are numerous.

A hypervisor in data centers for cloud computing is an important component to manage and deploy virtual machines. This option allows to have 20 or 30 virtual machines running inside the one physical host. Virtualization in data centers, will

reduce not only business cost and management time, but also reduce amount of racks which follows more space in the data center. Thus, this optimize efficiency in the data center and reduce heat in the building as well as taxes of cooling process. (Hess 2011.)

Virtualization also can have server pools and with this option could bring virtualized infrastructure using the advanced management software such as Microsoft System Center. This implies that instead of running several virtual machines on a single physical server this could distribute physical resources among several physical servers, networking or storage. The following Figure 6 illustrates a virtual infrastructure scheme.

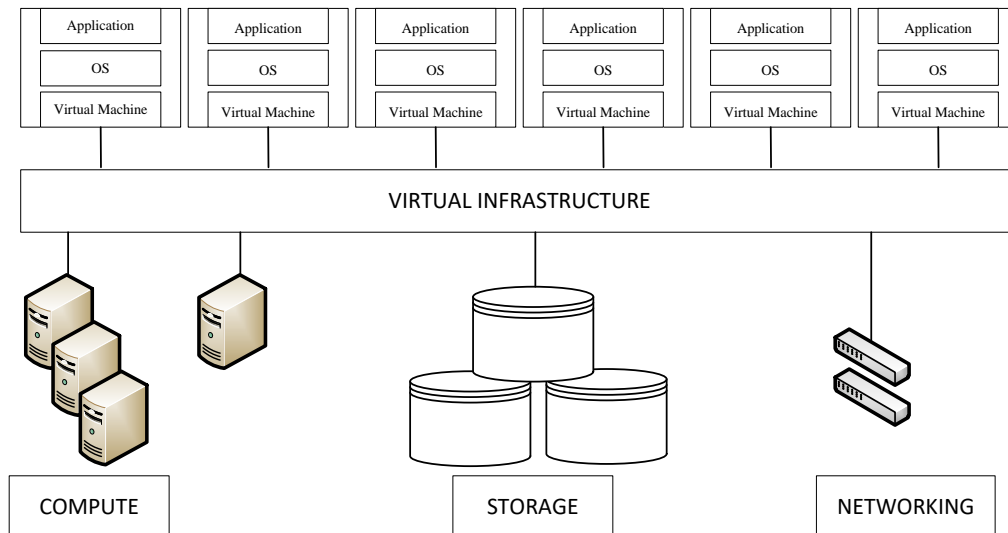


Figure 6. A virtual infrastructure scheme

It would act as a one big system and bring benefits such as scalability, flexibility and load balancing. Thus, helps increasing devices' uptime, improve disaster recovery or isolate applications. Also, the cost of business is reduced too by maintaining the whole infrastructure.

## 2.4 Cloud service models

A cloud can interact in various of ways with end users for providing services. Essentially, there are three main cloud computing service models: SaaS (*Software-*

as-a-Service), PaaS (*Platform-as-a-Service*) and IaaS (*Infrastructure-as-a-Service*). Each model provides different services and has different resources management. The following Figure 7 shows the management of resources in cloud computing service models.

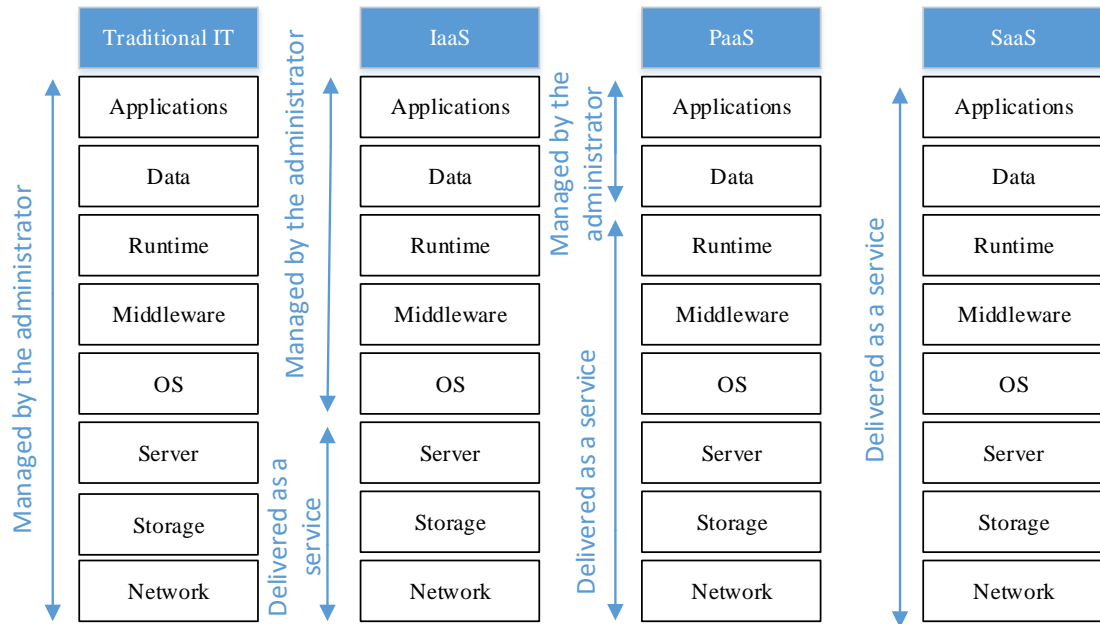


Figure 7. Cloud service models

**Software-as-a-Service** – It can be defined as a software deployed over the internet (see Figure 7, p. 14). End users usually access these services using a web browser and it is hosted on the service provider cloud. Customers themselves do not need to buy any hardware to deploy this application. According to Kepes (2017), the customer does not need to care about software installation or infrastructure that supports the application, making this cloud service simple for end users. In fact, customers do not gain any other permissions to change any infrastructure-related information but only use the service. Payment is very simple – pay as much as the customer works with the application. The example of this cloud service model would be Google Apps or storage cloud providers like Dropbox. Big players in the market such as Amazon AWS and Microsoft Azure also provide these services.

**Platform-as-a-Service** – Is a service more dedicated for developers. According to Kepes (2017), PaaS brings benefits like creating new web applications without the complexity of maintaining data and infrastructure between them. Repositories

are required to store their applications in service providers' cloud, where all other components are hosted there too. Customers usually access PaaS services via a website, but there is also possibility to use it within the application such as *Microsoft Visual Studio*. Also, customers gain important tools and programming languages together with the APIs (Application programming interface) needed to create and develop their own applications. Like in SaaS, customers do not need to care about configurations or infrastructure related information such as network, storage, servers and thus, brings benefits for costumers to focus more on the application development goal (see Figure 7, p. 14). This way the application itself should be created, developed and tested much more faster than in the traditional way. Examples of this service would be Microsoft Azure, Google App Engine or Amazon AWS.

*Infrastructure-as-a-Service* – Is a cloud computing infrastructure provided over the internet (see Figure 7, p. 14). Customers again do not need to take care of resources or infrastructure of the cloud service as well as the management and maintenance of these resources in leading to easy usage of the service itself for customers. The cloud providers are responsible for this part. According to Kepes (2017), customers can create new infrastructure without buying any new hardware which can reduce money and time usage in the business. This implies that customers have direct access to servers and storage and also gains much higher availability and security of their bought resources. Also, if needed customers can create their own virtual data centers similar to traditional ones. This could be implemented without planning any of the physical hardware which sometimes can bring lots of problems if planned reckless since all resources are hosted in the service provider's cloud. Customers pay for only for what they are using. Thus, providers specify hour cost. Providers of this service would be NaviSite, exoscale or again, Microsoft Azure or Amazon AWS.

## **2.5 Cloud types**

IT services in our days are very common and required in order to support business with the best optimization. According to Howell (2015), the other matter in this field is that IT is growing and changing very quickly, which sometimes can be

problematic for the small business. In fact, the small business is often forced to upgrade their IT equipment, because it does not meet business needs and because of this, it usually leads to downtime. For example, the hardware has become too slow or the technology is no longer supported, i.e. outdated, or because security hardly decreased. Moreover, these changes require big money investment and a lot of working hours. Cloud computing types can help reduce all these problems and at the same time increase flexibility and save cost. Today, there are three common cloud types: public cloud, private cloud and combination of both – hybrid cloud.

Public cloud – As the word ‘public’ explains this cloud type can be accessed by everyone where customers can leverage resources for their own use. According to Maitland (2010), a public cloud is connected through the public internet for anyone to leverage. In business, this type of cloud is very common for providing services for others. In general, public clouds are cheaper compared to a private cloud because they are using shared infrastructure. However, public clouds are used for the application development and testing or for email purposes. Today some of the biggest public cloud providers in the market are Amazon AWS and Rackspace.

Private cloud – This type of cloud can only be accessed by the organization members. Behind the scenes of management, the responsibility comes to the private organization itself, a third party or to a teamwork. Before implementing a private cloud, it is important to ensure that data center has proper security in both network and physical parts. In fact, it is an automated and scalable environment running on organization’s own servers and behind its own firewall. According to Maitland (2010), a private cloud can be connected for end users through the private line or the public internet when the internal network is created for best security purposes. This implies that end users can access a private cloud via the public internet without accessing the organization’s private network itself. A private cloud is a choice of an organization itself and often keeps private and important data or highly sensitive applications as well as the huge data analysis. Also, a pri-



vate cloud can be implemented for employees to give them a “public cloud experience” where everything is set up in a controlled environment. Private cloud technology will be used in this thesis for end users to access the virtual machine resources.

Hybrid cloud – According to Maitland (2010), this cloud type is a combination of both private and public cloud types. A hybrid cloud architecture starts from the private cloud traffic and bursts to the public cloud environment whether the load is heavy or the traffic is high. A public cloud can be used for additional capacity or as a cloud bursting (see Figure 8) where an application could be running privately but if there are any extra resource pools needed, then could be borrowed from a public cloud.

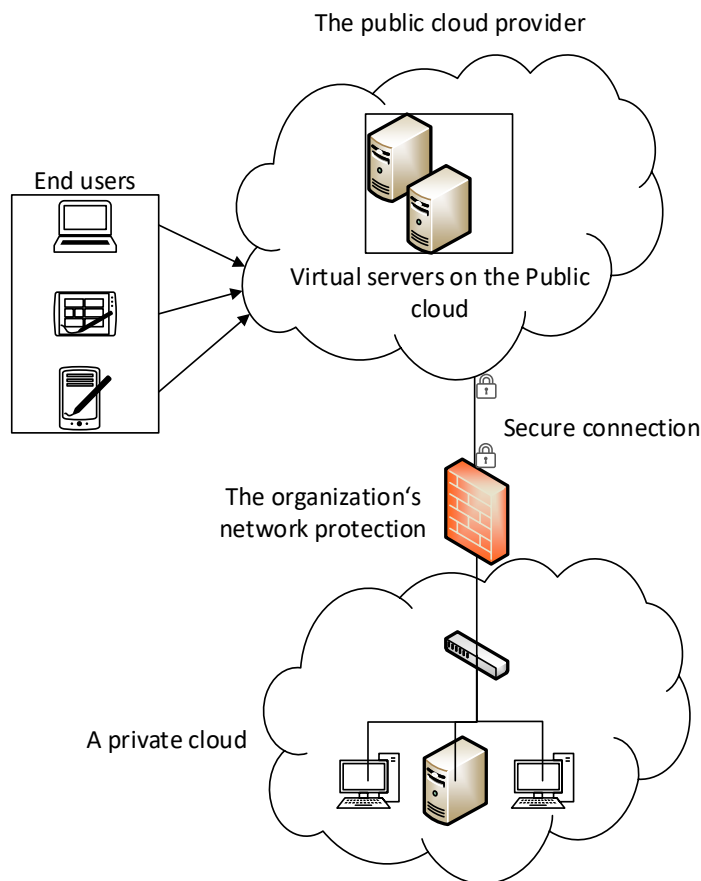


Figure 8. Cloud bursting scheme

But mostly, there are some services that must be kept private and some services like email can be outsourced. In general, the connection between a private and a

public cloud is secured and encrypted with technology such as VPN (Virtual Private Network) in case of cloud bursting. In addition, the SSL (Secure Socket Layer) can also be used to secure the connection between the cloud and the end user when using a web browser.

## **2.6 Private cloud creation and management alternatives**

Today, in the market, there are various of tools for creating and managing a private cloud. Choosing a right tool to create and manage a private cloud is quite hard decision because of few considerations which must be taken into an account: the management, the compatibility with existent infrastructure, security and cost. IT administrators should always keep in their mind that a private cloud software should work with the virtualization layer for providing hardware resources and allow administrators to manage the environment with the user interface. Diversity of open-source software can lead to reckless decisions because of necessary features lack. There should be answered lots of questions, scaled pros and cons to choose the best product based on the business needs. A few examples of software for creating and managing a private cloud in the market currently exists:

*VMware vCloud Suite Private Cloud* – Is a commercial use product. VMware is currently leader in the market of virtualization. vCloud suite comes in three different licenses: standard, advanced and enterprise. This product offers powerful server virtualization, disaster recovery automation, management and other features which are necessary for a private cloud environment. (Kirsch, 2015.)

*OpenStack Private Cloud* - This is one of the most popular cloud computing options for creating and managing the cloud environment in the today's market. This is a free license software based on Linux and has capabilities to manage network and storage. This is a limited feature tool and do not have its own hypervisor, for example, like Microsoft and VMware does. For this option, it can be used with VMware ESXi or Microsoft Hyper-V. However, mostly it is used with KVM which is also a free license hypervisor. (Kirsch, 2015.)

But for this thesis, to implement a private cloud, Microsoft System Center 2016 Virtual Machine Manager (SC VMM) was chosen because of the following reasons:

- Compatibility with Microsoft product such as Hyper-V;
- Compatibility with Windows Azure Pack as well as Service Provider Foundation for the self-service management;
- Capability to create and manage logical and virtual networks;
- Capability to store necessary files into the Library;
- Capability to manage large amounts of virtual machines.

Microsoft System Center 2016 Virtual Machine Manager has much more features helping to create, manage and deploy virtual machines in the cloud environment. The following two chapters define Microsoft System Center 2016 suite including Virtual Machine Manager. Also, these two chapters define arguments why this suite was selected.

## **2.7 Microsoft System Center 2016**

Microsoft System Center 2016 is a suite that enables the data center's management, helps to develop the modern business and empower to support end users. More concentrating on the cloud management for both a private cloud as well as a public cloud. On the other hand, connecting System Center 2016 suite to the Microsoft Azure cloud would bring the best support for a hybrid cloud. According to CFreemanwa (2017), this suite includes following components and each of them has a specific role in the data center's environment and can help improve its management and optimization:

Data Protection Manager – Is more dedicated for the data protection. This tool allows to implement backup and recovery solutions. One of new features in System Center 2016 Data Protection Manager allows using shielded VMs backup where it assists to protect VMs from tampering and data thefts.

Orchestrator – Handles the automatization infrastructure. Using Runbook Designer, can help improve automatization processes and operations in the data center environment. System Center 2016 Orchestrator allows extending its libraries with an integration pack and the Orchestrator Integration Toolkit features, if needed.

Operations Manager – Provides monitoring of the data center infrastructure, helps to ensure performance and availability of main applications. This also applies to comprehensive monitoring of both private and public clouds. The new Windows Server 2016 Nano Server can also be monitored with System Center 2016 Operations Manager.

Service Manager – It is more self-service tool where can help for users themselves to track tasks in their environment. This tool can be accessed through knowledge base. System Center 2016 Service Manager performance was improved to handle more simultaneous client connections within the environment.

Virtual Machine Manager – In this thesis, more is concentrated in this component in order to create a private cloud, deploy and manage virtual machines inside it. System Center 2016 Virtual Machine Manager is now updated including storage, networking and security new features to help configure and manage the environment across on-premises and the Azure cloud experience. Eventually, this component allows configuring and managing data centers' components as single *fabric*.

## **2.8 Microsoft System Center 2016 Virtual Machine Manager**

In 2010, Microsoft released Virtual Machine Manager Self Service Portal 2.0 (SCVMMSSP 2.0) which is a part of the System Center product. At first, this sub-product was not widely adopted, but Microsoft later announced that there is more to come from System Center Virtual Machine Manager. This approach drove Microsoft into a private cloud. (Finn et al. 2012, 14.)

Often, IT administrators have lots of virtual machines in their cloud environment, and this involves another challenge the management. There is many a hypervisor software which is best to use with small amounts of virtual machines. For example, a Hyper-V hypervisor allows creating, deploying and managing virtual machines, but it is not practical to use it alone in larger environments concentrating more on virtual machines' management. This approach can lead to losing the administrator's own control of virtual machines' environment and to the process known as *virtual machine sprawl*. Combining Hyper-V together with System Center Virtual Machine Manager (SC VMM) could optimize the management of virtual machines.

According to Finn et al. (2012, 19–20), System Center Virtual Machine Manager allows configuring and managing virtualization hosts, infrastructure resources, creating and deploying as well as managing a huge number of virtual machines, and services for a private cloud. These resources include network, servers and clusters, and storage which are considered and defined as *fabric* from where a private cloud can be managed and deployed. This System Center suite product combines a private cloud infrastructure and resources into one place and allows managing following components:

*Fabric management* – In order to optimize a private cloud, it is important to manage whole *fabric*. System Center Virtual Machine Manager enables private cloud components to be managed in one place. Other vendor hypervisor such as VMware's vSphere or XenServer also can be managed within System Center Virtual Machine Manager.

*Resource management* – Libraries is one of Virtual Machine Manager features which allows creating virtual machine templates, virtual machine profiles or scripts. Dynamic optimization allows to dynamically load balance virtual machines and workload across the whole virtualization infrastructure. It can help to optimize power output resources in the data center's environment to consolidate virtualized workloads into a less host servers.

*Cloud management* – This tool allows to manage the cloud itself. The administrator can delegate permissions for end users, set quota parameters in a private cloud as well as create policies.

### **3 DESIGNING A PRIVATE CLOUD**

Before starting to implement a private cloud, it is important to understand how to build it. A private cloud requires lots of choices to be made and brings features such as an automatization, flexibility and self-service. Virtual machines, user interaction or controlled environment in a private cloud is a last part job. Before these, it is important to have implemented *fabric* components. However, it is essential task to understand major building blocks in order to implement a private cloud.

#### **3.1 Network**

First major component of *fabric* is a network. In the real world, it is important for administrator to check that every physical device like a switch or a router is in the right place that creates the Local-Area-Network (LAN), which joins all computers to the same network, and connects them to the Wide-Area-Network (WAN), where geographical areas are connected together, before implementing a private cloud. For proper work *fabric* requires network services. Every network service is vital and if one of them fails this can lead to the unreachable private cloud.

The network can be divided into several subnets for security purposes. For example, whole IPv4 network such as 192.168.163.0/24 (where /24 is a mask written in the CIDR standard) has place for 254 devices to be added into the network. In fact, it has 256 free IP addresses, but the first and the last numbers are reserved for the network address and broadcasting. On the other hand, connectivity to the public internet requires public IP addresses.

In addition, the network administrator can set virtual LANs also known as VLANs. They can be configured on a switch, a router or any other network equipment that

supports this technology including virtual networking. The main idea of VLAN is to enhance the security by isolating devices' ports to not allow to see each other. In other words, different users can be isolated from each other to protect their data. This includes, for example, broadcasting if devices' ports are isolated the data that has been broadcasted cannot be seen by the same device port i.e. the data will not be forwarded between isolated ports.

### **3.2 Servers**

Depending on how big a private cloud can be, required software can be installed on the same server but best practices and requirements for scalability, flexibility or high availability points that they must be installed in separate servers or virtual machines. It is important to consider, if one of components fail for some time what consequences will be. There are a lots of components and network services that are required for a Microsoft private cloud environment in order to work properly and smoothly. Following describes Microsoft environment network services.

Domain Name System (DNS) – Is a network service more helpful for humans than computers. The idea of DNS is to convert names to IP addresses. This way is easier to remember the website's name than IP address.

Dynamic Host Configuration Protocol (DHCP) – Is a network protocol which is useful tool for the administrator. For every computer, for the communication on the network, IP address is required. Dynamic Host Configuration Protocol assigns IP address dynamically to every computer on the network. IP addresses are stored inside pools. In order to activate DHCP pool, host machine must be a member of a domain.

Active Directory (AD) – This network service component is required for forests or domains. In most corporations where Active Directory is implemented, employees can login with their own credentials to every computer on the same network. This is essential difference between the local and the network account. When Active Directory is installed the administrator can choose to provision that machine as a

domain controller (DC). Domain controller is responsible for the whole domain itself and stores information related with it. According to Microsoft (2014), by default, the first domain controller machine stores the global catalog file. This file is responsible for often accessible objects on the network for communication needs between them. In addition, forests are used with Active Directory. It is a logical division in the Active Directory's network. These forests sit on the top of the structure and shares common resources such as global catalog files or directory configurations.

SQL server (a database server) – A database is a component where specific information is stored. Virtual Machine Manager requires a database to store libraries and other components. SQL server can be reached over the network and communicate with other software and services or if needed, also, can be installed locally.

In addition, Remote Desktop Services with the Remote Desktop Gateway feature is required for the remote connection for the end user. It allows for authorized remote users to connect to resources on the internal network that supports the Remote Desktop client. This way the remote user is accessing resources to the separated internal corporate's network. When the remote user requests to connect to the virtual machine, the RDP file is automatically generated and downloaded to the client's computer. The RDP file includes all the necessary information to successfully establish the remote connection session between the remote computer and the destination computer. (Microsoft 2017.)

According to Finn et al. (2012, 34), the most important component when building a private cloud is the System Center Virtual Machine Manager management server. This component is responsible for communicating with the SQL Server as well as store and retrieve required configuration and performance information about different *fabric* resources. It also responsible for communicating with library servers, monitoring jobs, starting and stopping services as well as communicating with other System Center components. And it comes with System Center Virtual Machine Manager console in a GUI edition and is built on top of command shell –



PowerShell (see Figure 9). These core components such as management, database and library servers are recommended to be installed in separated servers to provide scalability, flexibility and high availability.

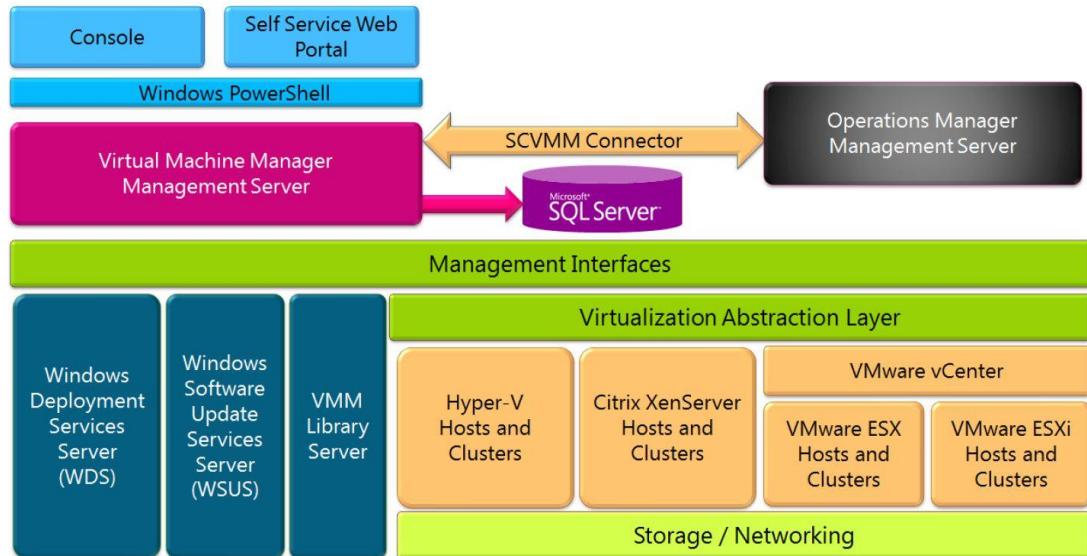


Figure 9. Microsoft System Center Virtual Machine Manager architecture (Finn et al. 2012,34)

The System Center Virtual Machine Manager database server is a Microsoft SQL Server database which should be installed by recommendations in the separate server or a cluster to provide high availability. It is also can be installed on a virtual machine. According to Rayne-wiselman (2016), this core component is required and must be available before System Center Virtual Machine Manager should be installed.

The System Center Virtual Machine Manager library provides all resources needed to support the cloud, whether they are stored in library shares or a SQL database. It stores files such as .iso images, virtual machine templates or PowerShell scripts. In some cases, when virtual machines are not in use, they also can be stored in the library. Indeed, it is a resource to effectively deploy a private cloud. (Finn et al. 2012, 37.)

For end users, the self-service portal is required to interact with a private cloud and use its resources. In this case, Windows Azure Pack: Portal and API Express is used. They can create, deploy or manage their own virtual machines in the

controlled environment. Indeed, it is a good choice to install this component into the machine that hosts Internet Information Service (IIS) which is responsible for webpage hosting and management. (Finn et al. 2012, 37.)

In the real world situation, it is important to have an appropriate number of servers for proper load balance and high availability. Some components by recommendation should not be installed together with each other, but the practical part of this thesis will be implemented in a virtual lab environment and there are no requirements for load balance or high availability, and also, resources are limited. Therefore, the following Figure 10 shows the architecture of a private cloud virtual servers for this practical part.

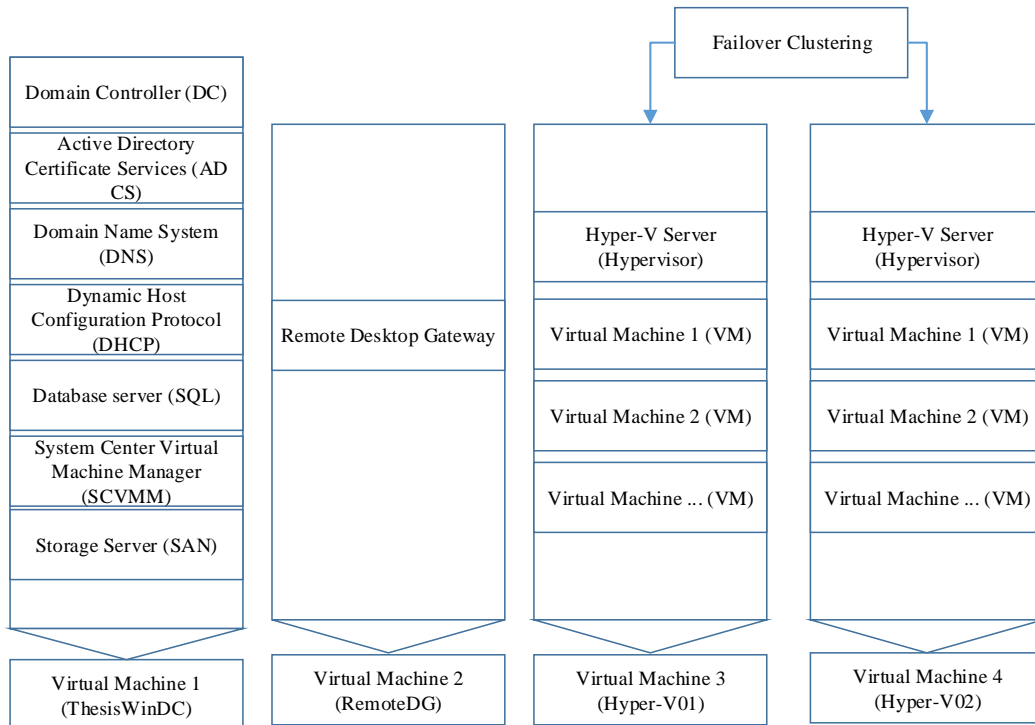


Figure 10. The private cloud architecture for this practical part

Virtual machine 1 (Domain Controller) consists of the control management. This machine will be responsible for a domain controller, DNS and DHCP network services. In the real world situation, it is recommended to have a separate database server and redundancy of it. Since this thesis practical part is not a high availability consideration, it will be installed together with all the other control systems including storage (SAN). Virtual machine 2 (RemoteDG) will be responsible for the

Remote Desktop Gateway feature and will authenticate end users for the remote connection to virtual machines. While virtual machine 3 (Hyper-V01) and virtual machine 4 (Hyper-V02) will be responsible for storing virtual machines and will have the Hyper-V role installed. They will be configured to work as a failover cluster and provide high availability for virtual machines.

### **3.3 Storage**

Next major building block is storage. In order to implement a private cloud, it is a major task to have a network storage which offers the storage capacity. The organization itself with a private cloud storage also have benefits for keeping corporate's data in one place as well as share it.

Existence of various storage types (HDD, SSD) can sometimes perplex consumers. According to Finn et al. (2012, 140–142), in the cloud environment it is important to keep consumers always with instructions, i.e. inform them about every step they are about to make by experiencing with the user interface. Notes about storage classification like Gold Storage, Silver Storage or Bronze Storage can be helpful for consumers which could be administrators or regular users. Terms like this can tell a useful information about storage, e.g. Gold Storage can be understood as a high availability storage, while Silver and Bronze storages can be defined as a medium or low availability storage and could be used for testing purposes only.

For this purpose, Storage Area Network (SAN) will be used as a private cloud storage. The key of SAN is to connect network storage to computers and assign disks as local. SAN allows I/O with block level data storage over the network. This technology is quite expensive because requires the fiber channel and the fiber equipment like fiber HBAs (Host Bus Adapter) and fiber switches. But on the other hand, it provides high availability and scalability. However, further development of SAN is now allowing to implement this technology over the traditional network which is called an IP SAN (See Figure 11). Figure 11 illustrates the traditional network with its traditional equipment such as a network switch and cabling system.

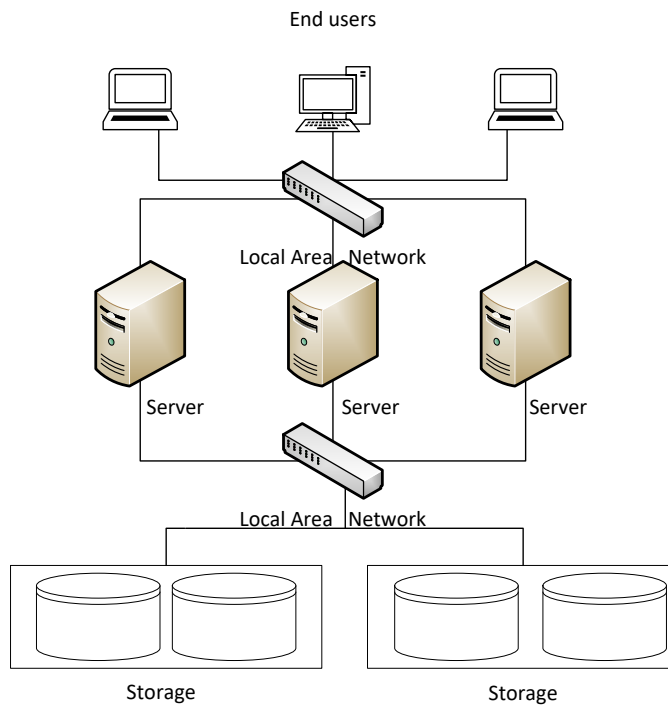


Figure 11. An IP SAN infrastructure

This technology allows to use the same regular network for block level I/O that can reduce company's cost for implementing such a technology without the fiber channel. IP SAN supports iSCSI (Internet Small Computer System Interface) protocol which is built on top of SCSI that is encapsulating SCSI commands over the network and sending TCP/IP packets from the remote server (also known as a initiator) to the destination computer (also known as a target) and vice versa. By this approach computers can "understand" SAN storage capacity and use it locally.

### 3.4 Clusters

A computer cluster is a technology which forms a group of several machines and allows them to work together. To form a group of machines, they must be as close as possible including hardware and software components. Microsoft fail-over cluster allows to form a cluster that provides high availability and scalability in the environment. To communicate with each other, computers (or also known as nodes) should use the separate network called heartbeating. Thus, they "talk" with each other to provide high availability as well as scalability. In addition,

quorum storage (or quorum disk) is needed to store cluster configurations or also can be understood as a database. Quorum disk stores information that allows to understand clusters which node is in alive state and thus decide which node should take priorities to provide high availability on specific roles, for example, on highly available virtual machines. To provide high availability, cluster nodes use a Cluster Shared Volume (CSV) to store resources in the shared storage and in case one of the nodes failed the other one still can reach the same data.

Clusters are usually used for high availability, load balancing and compute. High availability clusters working together in order to achieve redundancy and fault-tolerance in different sites, for example. If one of these sites are down for some reasons, the other one still can provide services for end users. Thus, bring benefits for business not to lose business finance. When clusters working as a load balance they are sharing resources between each other and working as a single machine. For example, Network Load Balance (NLB) is a software-based clustering feature to keep balance of network. This feature must be installed on all machines in order to work properly because it calculates the load and decides in which node new request should be accepted. Eventually, clustering in the technology of compute, enables to provide all features mentioned above and also, enables to share pools of configurable computing resources such as network, storage or servers. Moreover, empowering this together with an automatization, compute allows to provisioning and releasing services with minimal management effort. (Sadashiv & Kumar 2011, 1–2.)

#### **4 INSTALLATION AND CONFIGURATION**

This chapter deals with the practical part of this thesis. The very first thing after creating virtual machines in the *Level 0* virtualization layer, is to install the guest OS - Windows Server - on all virtual machines. Then, configure required services, and also, to install additional software and all prerequisites. Finally, start the installation of System Center Virtual Machine Manager.

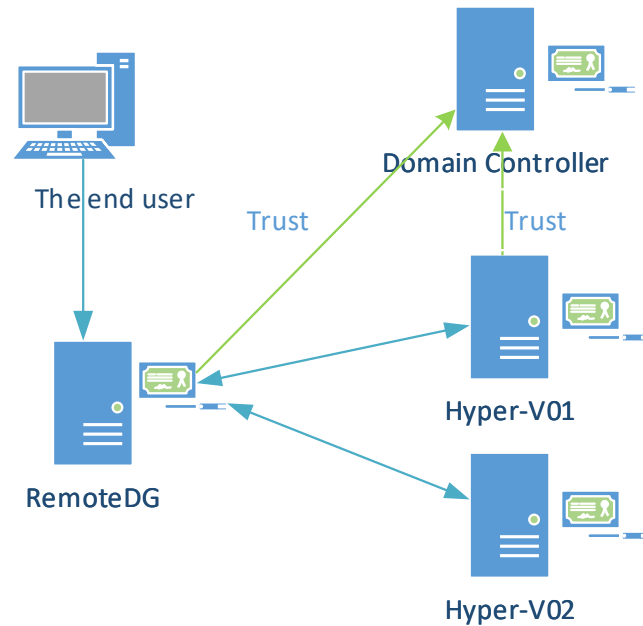


Figure 12. Servers topology in the practical part

The figure above illustrates the topology which must to be followed in order to connect to the virtual machine in *Level 1* virtualization layer using Connect Console. The end user connects to the Windows Azure Pack portal via a web browser. Then, the RDP file will be generated and downloaded to the end user's computer. To continue, Domain Controller determines the resources, and if the authentication succeeded via RemoteDG server, it allows to connect to the virtual machine over Remote Desktop Connection. One thing to observe is that near Domain Controller, Hyper-V hosts and RemoteDG servers are attached certificates which means that the relationship between these servers is trusted and secure.

#### 4.1 Operating system installation

Firstly, I created three virtual machines in the *Level 0* virtualization layer with the following parameters: For Domain Controller I assigned 2 CPU cores and 6 GB of RAM, for Hyper-V01 and for Hyper-V02 the same 2 CPU cores and 2.3 GB of RAM for each. Then, for Domain Controller I created additional HDDs for iSCSI and Library VMs as well as for a private cloud storage which will be assigned later. In addition, I created one more virtual machine and named it RemoteDG.

This virtual machine will be responsible for the Remote Desktop Gateway feature and for allowing end users to connect to virtual machines securely after the RDP file is generated. This machine will authenticate if end users are able to connect from Windows Azure Pack to Virtual Machine Manager server via the Remote Desktop Gateway server to virtual machines.

Secondly, I started Windows Server 2016 operating system installation. I used local disks for storing the operating system, although I could use iSCSI for e.g. Hyper-V01 and Hyper-V02 servers, but I rejected this option since during the implementation all these servers will be constantly powered on and off. All these Guest OSes are installed under the evaluation mode, which means that operating systems are downloaded directly from Microsoft and verified, but can only be used for testing purposes. Finally, after operating systems' installations are completed, the next part will be continued only with the Domain Controller server and the setup of Active Directory. When this machine is configured properly, all other machines will be joined to the same domain and assigned other additional properties.

#### **4.2 Microsoft network service installation and configuration**

To promote this server to a domain controller, I first installed the role known as Active Directory Domain Services. Then, I assigned new forest with the following name xamkthesis.lt (which will be my domain name for this thesis). This server will also be the DNS server and store global catalog (GC). As a result, Domain Controller is configured with the new forest.

The next network services are DNS and DHCP servers. To install both these network services, I added roles to the Domain Controller server such as DNS server and DHCP server. After these roles were installed, I configured xamkthesis.lt zone. In addition, I added a forward lookup zone and a reverse lookup zone for proper DNS work. They both work together to solve IP addresses from names to numbers where a forward lookup zone stores name host records (the A) and a reverse lookup zone is responsible for converting the in-addr.arpa (inverse address) addresses to domain names. The DHCP role is a bit different and can be

installed only after the Active Directory Domain Services role is installed because it requires domain administrator commitment (authorization). Therefore, a new scope was created with the following parameters shown in the Table 1 and Table 2.

Table 1 DHCP server automatically assigned values for every new client on the same subnet

Number	Parameters	Values
1.	Network mask	255.255.255.0
2.	Gateway	192.168.163.5
3.	Preferred DNS server	192.168.163.5

Table 2 IP addresses' distribution from DHCP server

Network Service	IP addresses starts from	IP addresses ends with
DHCP	192.168.163.50	192.168.163.75

After that, I installed and configured iSCSI. Virtual disks are stored in the Domain Controller HDD, while in a production environment this setup should not be considered but for a virtual lab environment this should not bring any complications. Due to this, I created three virtual disks for failover clustering. One for a private cloud provider (SMI-S WMI), another for the additional cluster shared storage and the last one a quorum disk. First two disks will be used as a Cluster Shared Volume to provide high availability of the *Level 1* virtualization layer virtual machines.

### 4.3 Preparing the environment for System Center Virtual Machine Manager

Before starting the SQL Server 2016 installation, I additionally installed Native Client used for the x64 architecture and Command Line Utilities x64. These, additional software, are required for SQL Server 2016 to run smoothly. I chose to install SQL Server 2016, but System Center Virtual Machine Manager 2016 also supports SQL Server 2012 SP2 and SQL Server 2014. This SQL Server 2016 is also installed under the evaluation mode the same as Windows Server 2016. When the setup file was launched and the installation's wizard appeared, the most important part was to select required features which are SQL Database En-



engine Services and Reporting Services – Native (see Figure 13). In addition, I created an SQL Server network account for security reasons and assigned it when the installation's wizard asked to specify an SQL services account. In the wizard's following page under Authentication Mode I assigned a built-in administrator account. When all the required information was gathered and after the installation successfully installed SQL Server 2016, in addition, I installed SQL Server Management Tools (SSMS) for proper SQL Server management over the UI.

During the SQL Server installation, I created System Management container inside System container under Active Directory. Then, I set full permissions for the System Center Virtual Machine Manager administrator. This container will be used for System Center Virtual Machine Manager because it needs permissions to write the specific data to Active Directory.

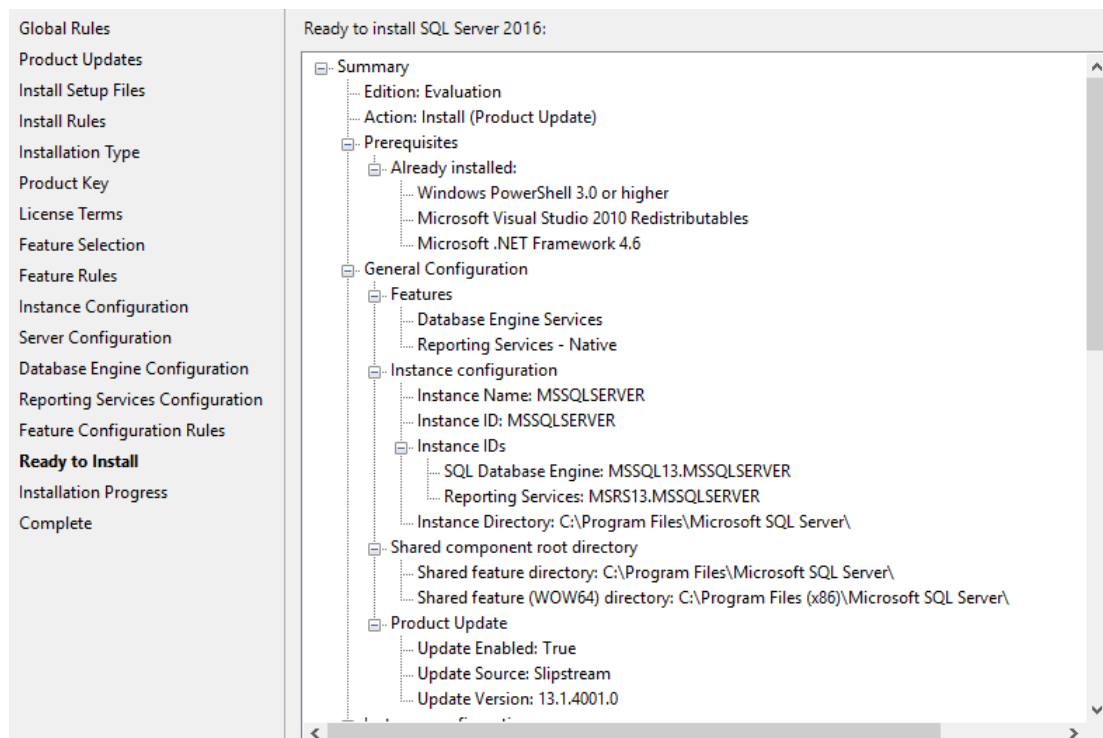


Figure 13. SQL Server 2016 summary page

When required server roles are installed and configured, further steps are additional software. System Center Virtual Machine Manager requires Windows 10 Assessment and Deployment Kit (ADK) with Deployment Tools and Windows Pre-installation Environment (Windows PE) features (see Figure 14).

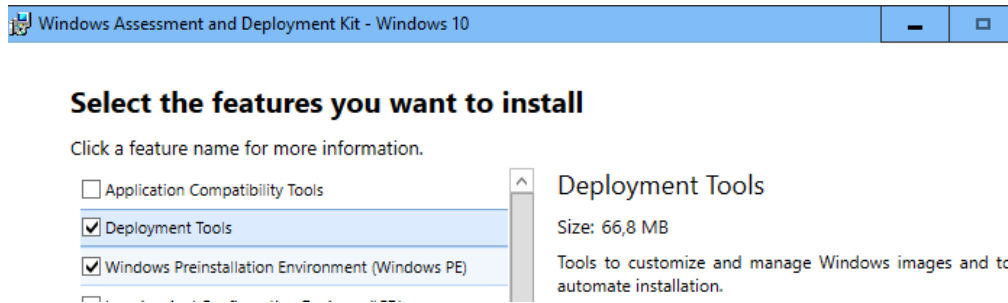


Figure 14. Windows Assessment and Deployment Kit features page

In order to allow creating virtual machines on the *Level 1* virtualization layer, I installed Hyper-V role inside both Hyper-V01 and Hyper-V02 servers and restarted the destination computers to apply new changes. To continue with, the configuration of failover clustering should be also set in case if one of the server fails the other one could provide same services for high availability. To start with failover clustering, first I need to ensure that both Hyper-V01 and Hyper-V02 servers are considered to be as failover clustering nodes. Firstly, I installed Microsoft Failover feature in both servers and started the Validate Configuration feature to ensure that both servers could work as a one system (see Figure 15). One thing to observe is that in the figure below, under the storage's description, it says Not Applicable. This means that storage is working properly and is already in a failover cluster (tests was made after a failover cluster was created).

#### Results by Category

Name	Result Summary	Description
<a href="#">Cluster Configuration</a>		Success
<a href="#">Hyper-V Configuration</a>		Success
<a href="#">Inventory</a>		Success
<a href="#">Network</a>		Success
<a href="#">Storage</a>		Not Applicable
<a href="#">System Configuration</a>		Success

Figure 15. Validate Configuration feature's results by category

Once tests passed, then I created a failover cluster of Hyper-V01 and Hyper-V02 servers. I launched the Create Cluster wizard and added two earlier mentioned nodes. Then, I assigned cluster name (VMCluster) and IP address

(192.168.163.12). I deselected Add all eligible storage to the cluster, because I want to do it manually (see Figure 16).

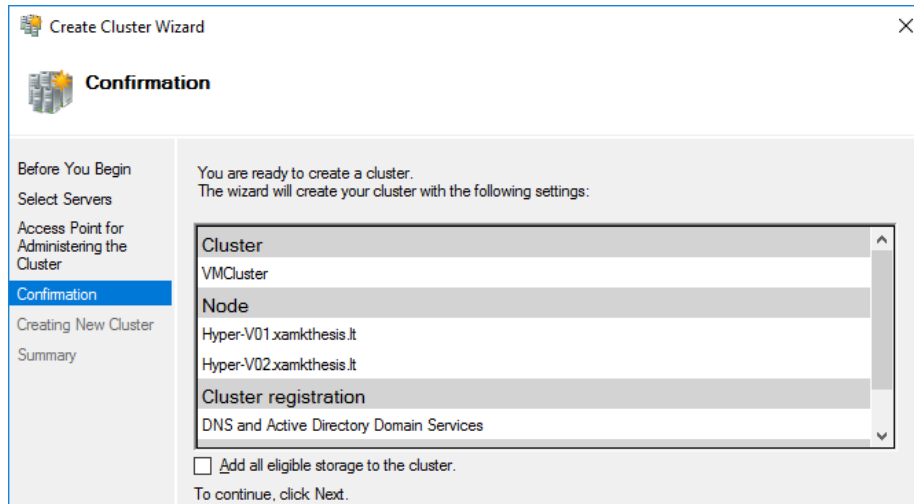


Figure 16. Create Cluster Wizard confirmation page

When cluster was created, then I added Cluster Shared Volume and assigned a Disk Witness in the Quorum. I could create new role and assigned it to provide high availability of virtual machines but this step will be done when private cloud will be implemented. The failover clustering is ready to provide highly available virtual machines.

#### 4.4 Installing System Center Virtual Machine Manager

Once all prerequisites are installed and configured, then System Center Virtual Machine Manager installation can be started. I chose to install VMM management server and VMM console (see Figure 17). These options installed required services for proper work of System Center Virtual Machine Manager as well as console for management of hosts. Again, this product is installed under the evaluation mode. When the installation wizard appeared and once all registration information is gathered and license agreement are accepted, then configuration steps must be set up to proceed. On the wizard's Database configuration screen, I entered earlier created SQL server name and entered required credentials. I left default for the instance name and for the new database name, the installation will create it automatically. Then, the installation's wizard asked to configure services and distributed key management. I added the System Center Virtual Machine

Manager administrator and entered its credentials. Thereafter, I specified a share Library for Virtual Machine Manager which I created in the separate Domain Controller's HDD. When the installation summary page appeared (see Figure 17), the installation of System Center Virtual Machine Manager 2016 started.

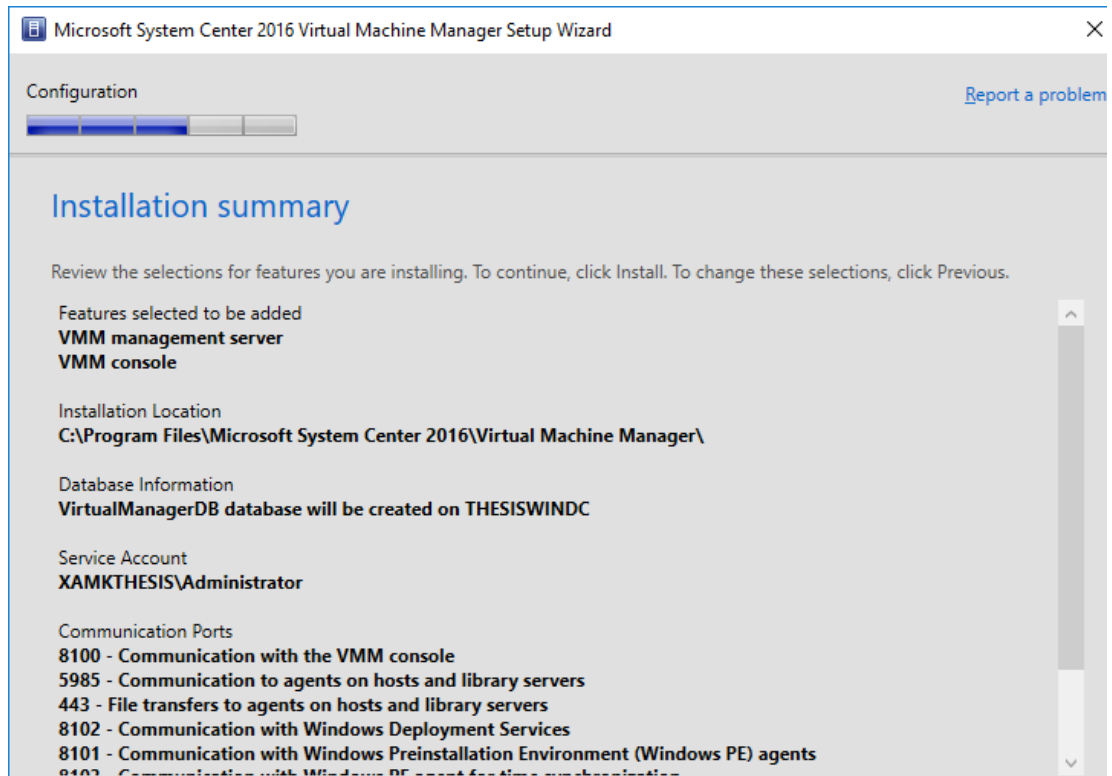


Figure 17. Microsoft System Center 2016 Virtual Machine Manager installation summary page

Once the installation is finished, the environment for a private cloud was set up successfully. The next part is to start implementing the private cloud. Due to this, the next step is to add Hyper-V hosts to the host group and enable the management of them over the System Center Virtual Machine Manager console.

## 5 BUILDING THE PRIVATE CLOUD WITH SYSTEM CENTER VIRTUAL MACHINE MANAGER

This chapter describes the private cloud creation. Every step in this process is described in as detailed as possible. When the private cloud will be created, then the experience of the end user as well as the administrator over a web browser will be discussed, too.

## 5.1 Adding VMCluster to the host group

The very first step is to add Hyper-V hosts to the host group. At this point, it is a cluster consisting of two nodes Hyper-V01 and Hyper-V02 (see Figure 18). This step is required, because when adding hosts to the host group, the wizard installs an agent and other necessary features for proper communication between System Center Virtual Machine Manager and hosts, or in other words it enables the management of Hyper-V hosts over the System Center Virtual Machine Manager console.

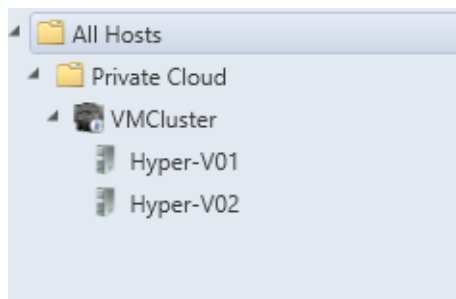


Figure 18. Hosts added to the host group over the SC VMM console

In addition, I created the Private Cloud group and dragged newly added hosts to this group. This step later allows configuring host reserves by setting hosts' resources to optimize heavy workload of the Private Cloud group.

## 5.2 Allocating host reserves

Specifying host reserves is an important step. Host reserves are hosts' resources used for guest operating systems. Administrator can specify these based on his company's needs to allocate proper hosts' resources. If resources' limit is reached, it then return an error for a host and stops all jobs, if any was started. The following Figure 19 illustrates host reserves for the Private Cloud host group.

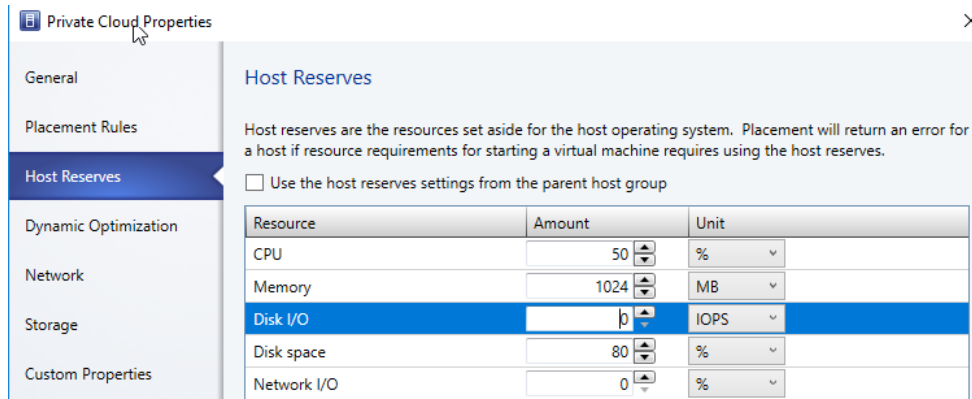


Figure 19. Host reserves parameters

As Figure 19 shows, resources' limitations, such as CPU, memory, disk space and network I/O can be set in order to optimize hosts' workload. Since this is a virtual lab environment I still set host reserves for Hyper-V01 and Hyper-V02 hosts in order to optimize workload. In case of the virtual machine migration of the *Level 1* virtualization layer, hosts should also have additional free resources.

### 5.3 Storage classification

Storage classification allows defining what type of disks will be used for virtual machines. As Figure 20 shows, Bronze Storage is defined as iSCSI, Silver Storage – FC (fiber channel) and Gold Storage is defined as SSD. This step allows keeping things well understood and not to misunderstand the whole system. The next step is to assign physical storage to storage classifications.

Name	Type	Size	Available Capacity	Assigned	Description
Bronze Sto...	Classification	0 GB	0 GB		iSCSI storage
Gold Stora...	Classification	0 GB	0 GB		SSD
Silver Stora...	Classification	0 GB	0 GB		Fibre Channel con...

Figure 20. Storage classification in the Library workspace

To assign physical storage, I opened the Add Storage Devices wizard which allows adding physical storage and assign it to storage classifications. The first

step is to specify provider type. In most cases, it can be a third-party storage provider, but in this case I use my own storage based on iSCSI from the Domain Controller server.

Name	Management Address	Arrays	Status	Provider Type
192.168.163.5	ThesisWinDC.xamkthesis.lt	ThesisWinDC	Responding	SMI-S WMI

Figure 21. Storage providers in the Library workspace

As Figure 21 shows, I then selected SMI-S WMI storage provider which supports iSCSI - based target server. And the final step for the physical storage assign is to set Bronze Storage as the storage classification for newly added physical storage and then I added this storage to the Private Cloud group.

#### 5.4 Creating a logical network

After the storage is assigned, the next step is to create a logical network. A logical network will be used for Hyper-V hosts and this logical network should represent the real physical network (IP addresses). I named this logical network as a Service Network. During the logical network creation I enabled an option to Allow new VM networks created on this logical network to use network virtualization (see Figure 22) which allows later to virtualize it and use it for virtual machines of the *Level 1* virtualization layer. Then, in the Network Site section I assigned this logical network to the Private Cloud group and inserted IP subnet with the following information: 192.168.163.0/24 (where /24 is a subnet mask written in the CIDR).

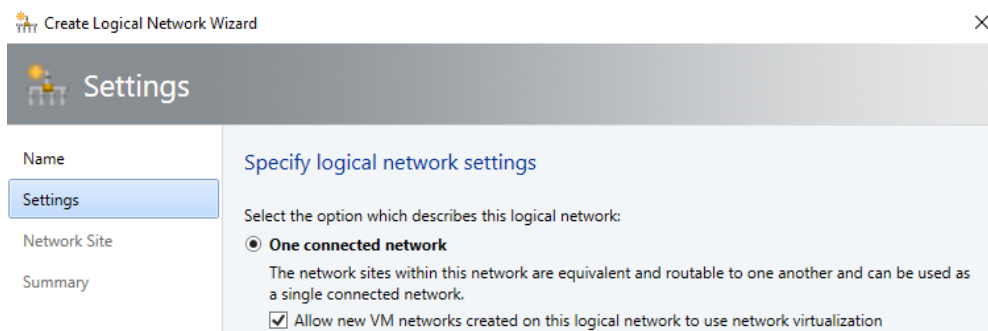


Figure 22. A logical network settings page

To continue, the next step is to create an IP address pool for VMs. This address pool will be used for VMs to automatically assign IP address to each VM that is created on the network site. I a network site already created as well as IP subnet. As Figure 23 shows, I entered an IP address range with the following information: IP range starts from 192.168.163.76 and ends with 192.168.163.100.

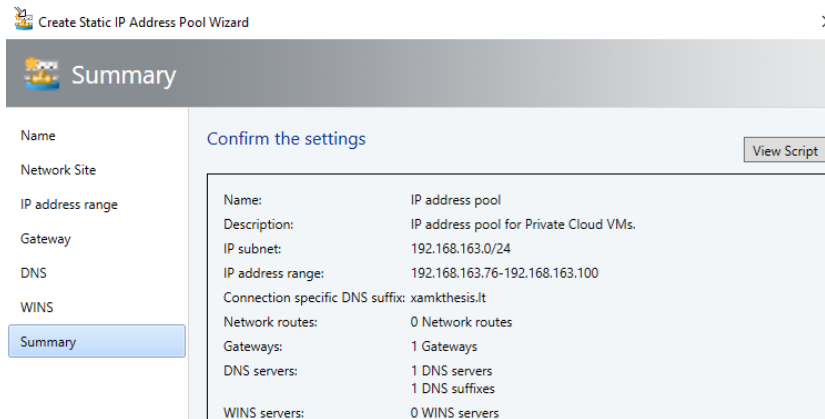


Figure 23. Create Static IP Address Pool Wizard summary page

Also, I provided a gateway by entering 192.168.163.5. I specified the DNS server which is 192.168.163.5 and DNS suffix xamkthesis.lt. After the logical network was created, the next step was to create an uplink port profiles. They allow creating additional virtual adapters connected to physical hosts. In addition, I created the port classification and named it Service Network classification. It allows identifying Service Network objects.

Then, I created a logical switch with the Team uplink mode and named it Logical Switch for SN. This mode allows using this logical switch for several physical hosts. In addition, I assigned port classifications in the Virtual Port section such as low, medium and high bandwidth as well as Service Network classification created earlier. Virtual ports allow using resources of hosts. I set the default for the low bandwidth and this applies when the virtual network adapter will be used, the low bandwidth will be used as a default. Now I can create virtual network adapters (vNICs) that allow connecting a virtual machine to the Virtual Machine Networks. The following figure shows dependencies of this logical switch.



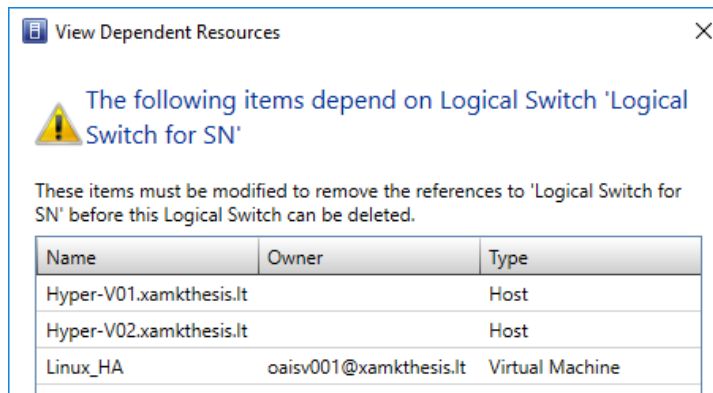


Figure 24. Dependent resources of the Logical Switch for SN

This Figure 24 was made after the private cloud was implemented. As Figure 24 shows that dependent resources of Logical Switch for SN are both Hyper-V hosts and virtual machine Linux\_HA. Logical Switch for SN is assigned to both Hyper-V hosts. Linux\_HA virtual machine sits on the Hyper-V01 server and by default is connected to this Logical Switch for SN switch.

## 5.5 Creating a virtual network

There is an option to isolate all virtual machines from virtual and logical networks. This step can be achieved with the virtual routing domain traffic to isolate them. Therefore, the first step after a logical network was created, inside VM Networks under Library workspace, I created new VM network and named it Virtual Machine Network (see Figure 25).

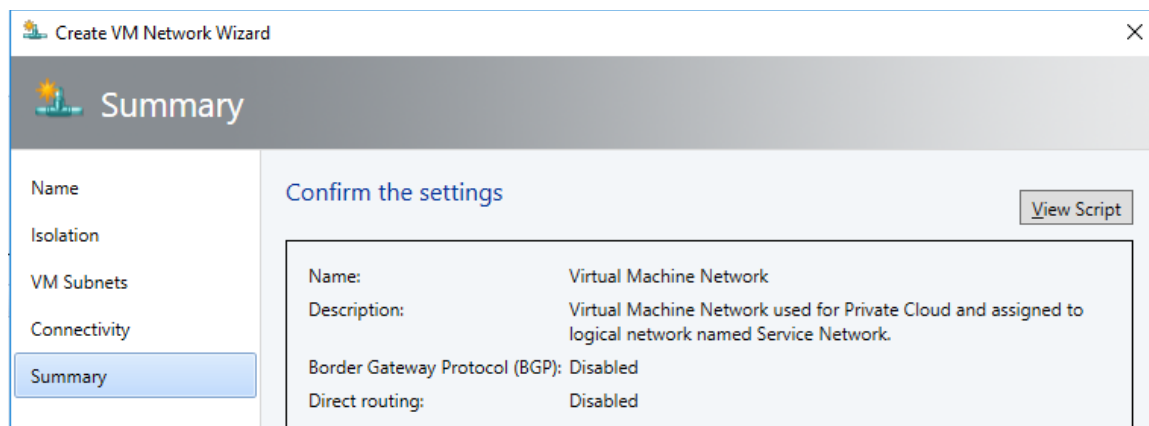


Figure 25. The Create VM Network Wizard summary page

I chose to isolate this network using Hyper-V network virtualization and selected IPv4 protocol. I specified VM subnet 192.168.163.0/24 with the CIDR notation. This VM network allows virtualizing the IP subnet by disabling direct routing to the logical network. On the other hand, I created a virtual machine network without any isolation and named it Virtual Machine Networks. This implies that the virtual machine network has full access to a logical network. This may be harmful, because end users can reach physical network via virtual machines, but since this is a lab environment, it really has no impact.

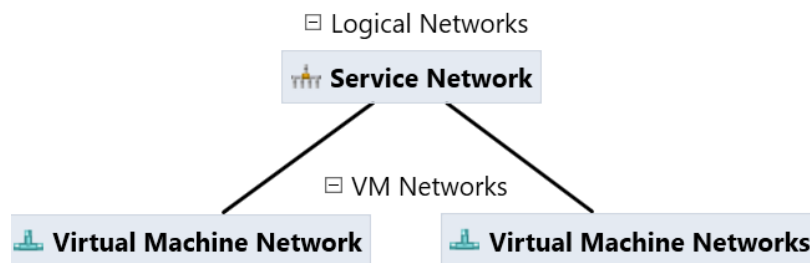


Figure 26. Network topology in System Center Virtual Machine Manager

As Figure 26 shows, both virtual networks are connected to a logical network. When creating the virtual network with isolation, in order that network to work as expected, the administrator must first create additional pool inside the virtual network without isolation. This implies, since the virtual network is isolated, then it can't get any DHCP information from the DHCP server.

## 5.6 Assigning resources to the Service Network

Now I need to assign Service Network for the host group. I added additional NIC for both nodes because one NIC will be used for the proper Hyper-V communication with the System Center Virtual Machine Manager server (management network) and with other features such as Microsoft Failover clustering, and another NIC will be used for a Private Cloud connection which is a logical switch and VM networks (placement network).

## 5.7 Creating a cloud

So far I created resources such as network, storage and computing. Now it is time to combine them into one single object called a private cloud. To do this, I launched the Create Cloud Wizard and firstly the wizard asked to enter the name for a private cloud and I named it Private Cloud. In System Center Virtual Machine Manager 2016 there is option to enable shielded VM support. This implies for additional security by encrypting the disk and state of virtual machines and only specific administrators can access it. But in this practical part, I chose not to support this feature on this private cloud. Then, I assigned already created resources which are located in the Private Cloud group. The following Figure 27 shows port classifications for this private cloud and each port is briefly explained in the figure's description field.

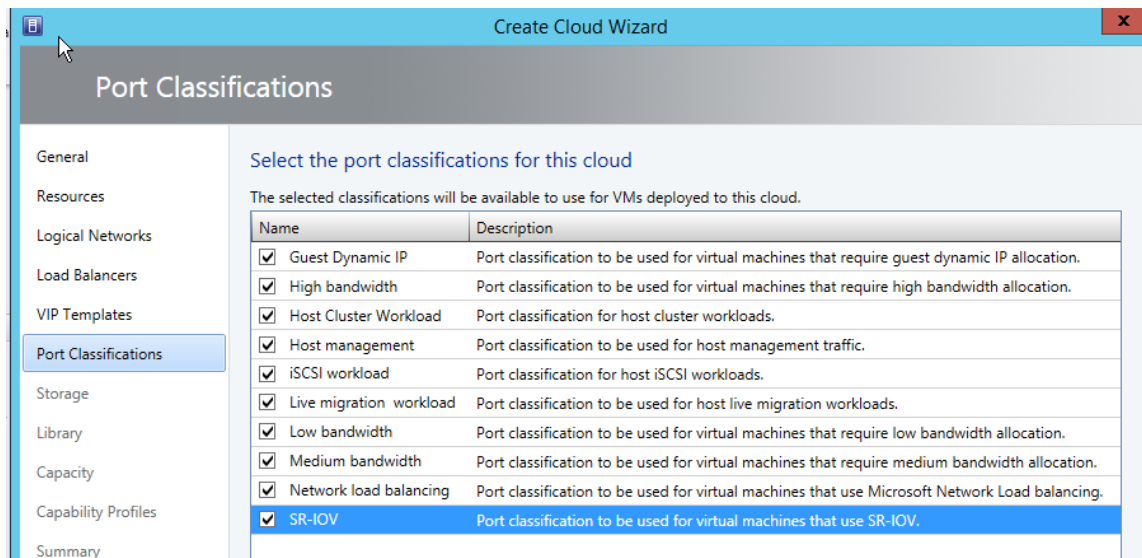


Figure 27. Create Cloud Wizard Port Classifications page

Thereafter, I specified read-only library shares which I created during the installation of System Center Virtual Machine Manager. As Figure 28 shows, the cloud capacity and specified limitation options allow setting the capacity in the different hardware component. Since this is a lab environment and hosts do not have that much CPUs, I used the maximum capacity. While the other components I limited for the workload optimization. After that in the Capability Profiles page, I selected the Hyper-V profile as this allows me to build the *fabric* capability profiles for Microsoft Hyper-V profiles.

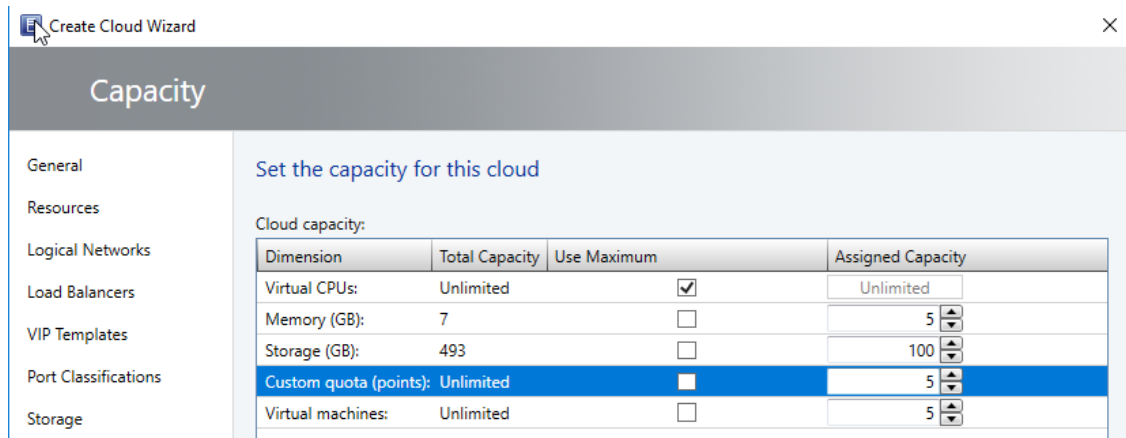


Figure 28. Create Cloud Wizard Capacity page

When all required information was specified and gathered, the summary page of this wizard appeared (see Figure 29). As Figure 29 shows, the following information will be used for the Private Cloud creation. One thing to observe, for example, in the storage section there is Remote Storage. This storage defines Microsoft Failover clustering storage which is iSCSI based. The summary page also shows replication groups, but since I have implemented cluster consisting of two nodes, I did not added any replication groups.

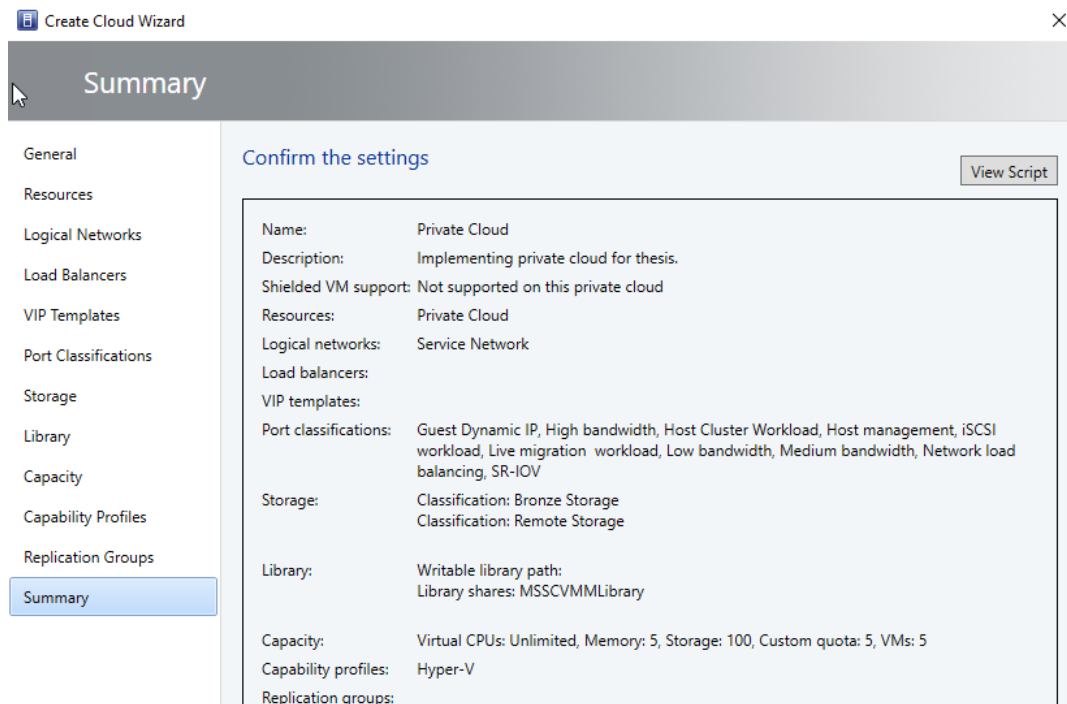


Figure 29. Create Cloud Wizard summary page

At this point, a private cloud was created but it is just a collection of resources (storage, network and computing). The aim is now to make this cloud self-provision that end users could interact with it and use virtual machine templates without any administrator's touch, or in other words the whole process should be automated.

### **5.8 Building a hardware profile**

After a cloud was created, the next part is to start implementing end users' self-provision steps. Firstly, I created a hardware profile which defines resources for each template. The point of a hardware profile is to make everything less problematic and more automated. If, e.g. the administrator needs to create tens of same virtual machines it would be wasting of time to do it manually. Or allow creating virtual machines for those who don't understand it. It makes everything simpler and again, automated. All profiles are stored inside Library workspace of System Center Virtual Machine Manager.

I chose to create a hardware profile for both Linux as well as Windows platforms. A hardware profile can be, for example, any Linux distribution or any Windows system version. Here, I assigned compatibility for Hyper-V, assigned 512MB of RAM for Linux, specified the x86 architecture and connected this hardware profile to the Virtual Machine Networks. For Windows, I assigned 1 GB of RAM, also specified the same x86 architecture and connected this template to the Virtual Machine Networks. Both hardware profiles were made that virtual machines to be highly available. It is beyond this hardware profile to assign the storage.

### **5.9 Creating a guest OS profile**

The main purpose of a guest OS profile is to create same virtual machines with same roles or features. Also, all virtual machines can be joined to the same domain or have the same administrator account. This also can be set up with a guest OS profile.

Profiles (3)		
Name	Type	Owner
Linux guest profile	Guest OS Profile	XAMKTHESIS\Administrator
Guest OS profile for Windows 7	Guest OS Profile	XAMKTHESIS\Administrator
Guest OS profile for Windows 8	Guest OS Profile	XAMKTHESIS\Administrator

FIGURE 30. SC VMM guest OS profiles stored in the VMM Library

To continue, I created few guest OS profiles for both Linux and Windows (see Figure 30). For this purpose, I specified Windows 7 OS and for another Windows 8. Also, specified administrator accounts.

### 5.10 Building a VM template

Creating a VM template additionally allow specifying the virtual hard disk (VHD). There are few options when choosing virtual hard disks stored in the library and here I specified Blank Disk – Large.vhd for Windows and Blank Disk – Small.vhd for Linux. The ending of .vhd stands for virtual hard disk and it is a file format which represents the virtual machine's hard drive. Then, I assigned both hardware and guest OS profiles to these VM templates shown in Figure 31.

Templates (4)				
Name	Release	Type	Owner	Status
Linux template		VM Template	XAMKTHESIS\Administrator	OK
VM template for Windows 7		VM Template	XAMKTHESIS\Administrator	OK
linux-self-service		VM Template	XAMKTHESIS\Administrator	OK
VM template for Windows 8		VM Template	XAMKTHESIS\Administrator	OK

Figure 31. VM templates stored in the SC VMM Library

As all profiles was created, the next step was to deploy the Windows Azure Pack portal. In addition, System Center 2016 Service Provider Foundation was also required. Then, connecting the private cloud to this portal and creating subscription plans, creating certificates to define trusted relationship between servers and finally testing the whole environment.

### 5.11 Deploying Windows Azure Pack: Portal and API Express

Windows Azure Pack: Portal and API Express is the self-service management portal allowing to manage clouds over a web browser. This tool also allows to enabling self-service and automation for end users in order to create virtual machines inside clouds.

Another software to mention is System Center 2016 Service Provider Foundation. This software allows exposing OData web services which interacts with System Center Virtual Machine Manager. Due to this, the administrator can design and implement self-service portals. In addition, this software installation media can be found inside System Center 2016 Orchestrator. (Microsoft 2016a)

To install the Windows Azure Pack portal, first I need to install IIS Server on the Domain Controller server. I selected the following additional features for IIS server: Management OData IIS Extension and HTTP activation. Also, I added management tools and basic authentication as well as Windows authentication. Thereafter, additionally installed WFC Data Services 5.0 and started the installation of Service Provider Foundation. For proper communication, I left the default name of the website which is SPF and the port number 8090 (see Figure 32). This port will be used for the communication with the portal and System Center Virtual Machine Manager server. Then, I configured self-signed certificate. The following Figure 32 shows the summary page before the installation of Service Provider Foundation began.

In addition, I created new account for Service Provider Foundation services with the following name: spf\_sa and added this user to the administrators group. Due to this, I specified this new service account to run services such as admin web, provider web, VMM web and usage web. Then, from Microsoft/web I downloaded Web Platform Installer and via it installed Windows Azure Pack: Portal and API Express.

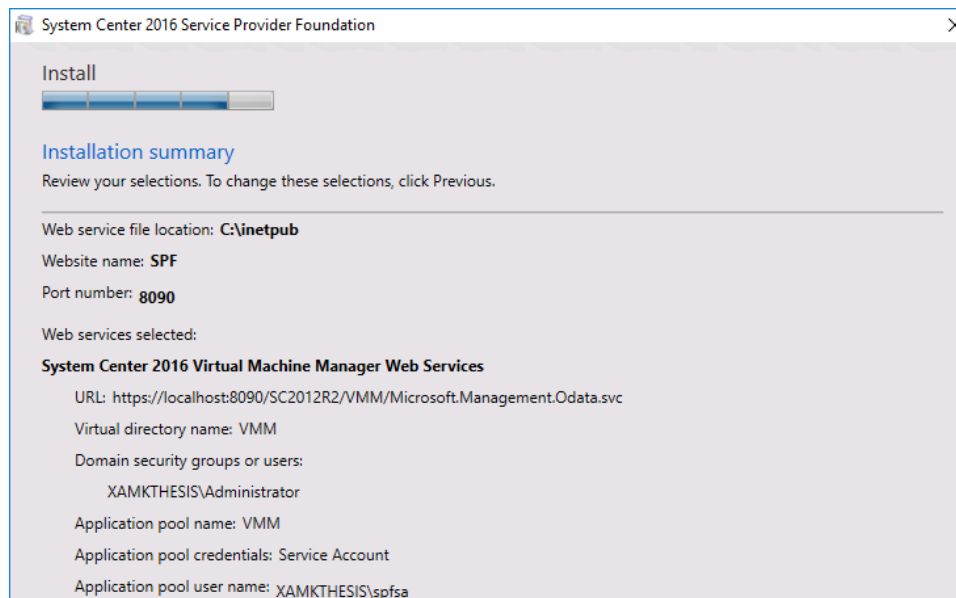


Figure 32. System Center 2016 Service Provider Foundation's summary page

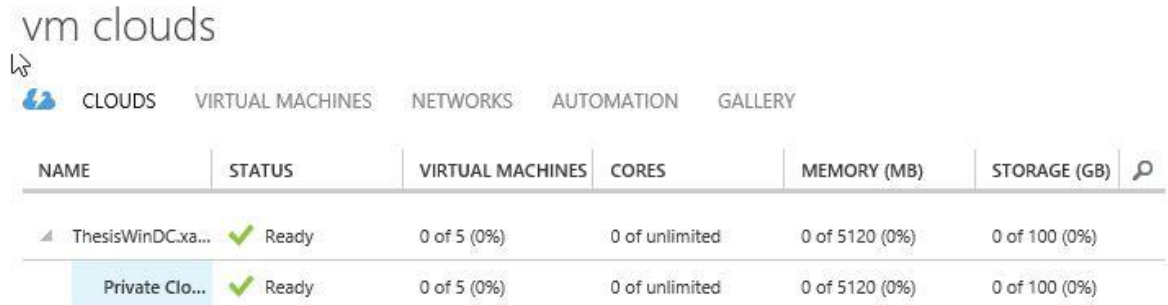
After the installation was finished, Internet Explorer was opened with the following URL <https://localhost:30101/> and informed that right now I am using self-signed certificate which can be harmful. In a production environment there should be set additional certificate server or bought official ones. Still, I continued to the website by clicking continue to this website (not recommended). From this point view, the portal requires additional configuration to continue. I specified the database server name and its administrator credentials. Due to this, I entered ThesisWinDC.xamkthesis.It as a database server's FQDN (fully qualified domain name) and XAMKTHESIS\Administrator as a windows user and specified passphrase: XamkSchool1. After that, additional features started to configure itself and when this step was done, the Windows Azure Pack portal was ready to use.

## 5.12 Connecting System Center Virtual Machine Manager to the Windows Azure Pack portal

When connecting System Center Virtual Machine Manager to the Windows Azure Pack portal it is required to specify FQDN of the System Center Virtual Machine Manager server. Due to this, I specified ThesisWinDC.xamkthesis.It and optionally specified the 8100 port. According to Hornbeck (2013), it is also important to set the correct network accounts for the proper communication between all the



components such as IIS, SQL and VMM. As Figure 33 shows, VM clouds was successfully added to the portal by saying its status Ready. Since this cloud was newly added, there are no virtual machines running and no resources using so far.



NAME	STATUS	VIRTUAL MACHINES	CORES	MEMORY (MB)	STORAGE (GB)
ThesisWinDC.xa...	Ready	0 of 5 (0%)	0 of unlimited	0 of 5120 (0%)	0 of 100 (0%)
Private Clo...	Ready	0 of 5 (0%)	0 of unlimited	0 of 5120 (0%)	0 of 100 (0%)

Figure 33. VM clouds in the self-service portal

Additionally, I created SQL user and named it spf to add the database to the portal and allowing the connection between latter and SQL Server. This user must be created under the SQL authentication mode because only this mode is supported by the Windows Azure Pack portal.

### 5.13 Creating a new subscription plan and adding end users

In order to allow end users to sign in to the SC VMM console via a web browser, I first have to create a plan where all users could subscribe to it or in other words sign up. I created a new plan and named it Tenants Plan and added Virtual Machines as a clouds feature. Then, I assigned ThesisWinDC.xamkthesis.It server as a VMM management server and a Private Cloud as a virtual machine cloud. In addition, I added networks, hardware profiles, templates and specified additional settings to allow anyone who will subscribe to this plan to use those settings. Finally, I published the plan and now I could create end users who could use the self-service portal.

### 5.14 Creating certificates

In order to create a trust relationship between several machines, certificates are used for this purpose. When the client connects to the remote machine, the

server and information are identified by certificates. When the certificate is installed in the client's machine, the information between the client and remote machine is considered as secure.

Each certificate request is processed by the specific set of rules and each certificate can have various number of extensions that regulates the user. For example, application policies give an essential ability to define which certificate is used for the specific purpose. Also, they are called Enhanced Key Usage. (Microsoft, 2008) Certificates must be encrypted using the specific hash algorithms. Cryptographic hash functions are based on mathematical operations that are easy to compute but significantly harder to reverse. For example, SHA-256 hash algorithm uses 256-bit digest and encrypts the information with quite long hash value which is considered as secure.

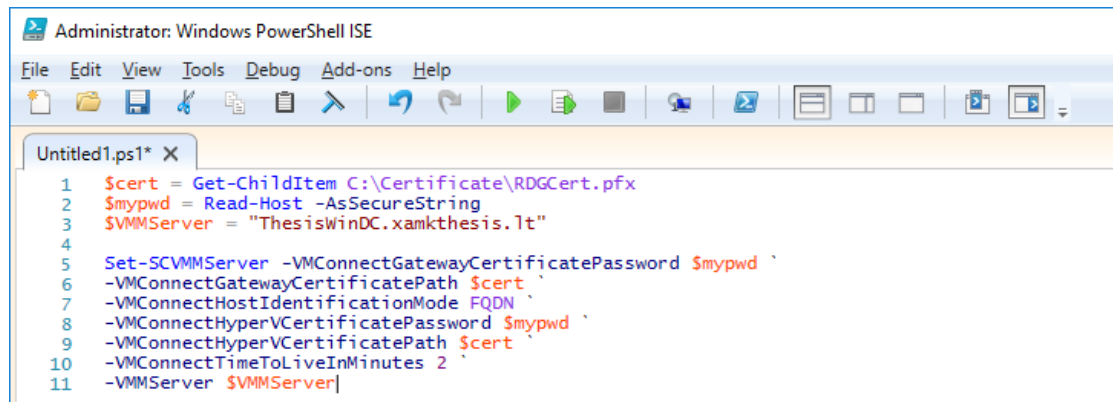
In addition, private and public keys can be used to create more secure sessions. For example, to ensure the confidentiality when the private key is used to encrypt the data, the private key is used for decrypting it. In this scenario, only the host has the private key while the public key is disseminated widely. Tokens are used to authenticate access to virtual machines and supply a token, because Hyper-V host uses tokens for allowing access for the end user.

With this said, I defined a certificate template for the trust relationship. The trusted relationship will be created between Domain Controller, RemoteDG and both Hyper-V01 and Hyper-V02 hosts (see Figure 12, p. 29). Certificates created for the trust relationship must have the following properties: It must include Enhanced Key Usage (EKU), support the SHA-256 hash algorithm and have the 2048-bit key length. Because of these requirements, I created the certificate at Active Directory Certificate Services and named it Remote Desktop Connection.

The next step is to issue this certificate for the trust relationship between Domain Controller, Hyper-V hosts and RemoteDG servers. I created a certificate request (CSR) for Certificate Authority (CA) which in my case is the Domain Controller server. This request will generate the certificate itself. In the certificate request, I

must include the Remote Desktop Gateway server name, key length, hash algorithm, key usage, the client's authentication OID and also set the exportable private key.

With the request created, I generated the certificate and verified it. Furthermore, I submitted the certificate request to the Certificate Authority (Domain Controller). When the certificate request was submitted, the very last step was to export the trusted certificate as a PFX file, because later I will import it to the Virtual Machine Manager management server database. According to Microsoft (2016b), to import a PFX file to the Virtual Machine Manager management server database, I ran the script bellow in the PowerShell:



```

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1* X
1 $cert = Get-ChildItem C:\Certificate\RDGCert.pfx
2 $mypwd = Read-Host -AsSecureString
3 $VMMServer = "ThisisWinDC.xamkthesis.lt"
4
5 Set-SCVMMServer -VMConnectGatewayCertificatePassword $mypwd `
6 -VMConnectGatewayCertificatePath $cert `
7 -VMConnectHostIdentificationMode FQDN `
8 -VMConnectHyperVCertificatePassword $mypwd `
9 -VMConnectHyperVCertificatePath $cert `
10 -VMConnectTimeToLiveInMinutes 2 `
11 -VMMServer $VMMServer|
  
```

Figure 34. PowerShell script that allows importing certificates to the SC VMM management server database

This script firstly gets the required information about the certificate, its password (which was required when the certificate was imported) and the Virtual Machine Manager server itself. When the required information is gathered, further commands can be issued. This script sets the tokens' lifetime by identifying host server by its FQDN name which later will be included, when the RDP file will be generated for end users.

For the Remote Desktop Gateway server, I again requested and installed a new SSL Web server certificate in the Certificate Authority and assigned it for the Remote Desktop Gateway server by importing it. This step is required for the Remote Desktop Gateway server to encrypt the RDP session. Finally, I registered

the Remote Desktop Gateway server in the Windows Azure Pack admin's portal. Eventually, end users now can use Remote Console.

## 6 RESULTS AND ANALYSIS

This chapter describes the domain built-in administrator's as well as the end user's experience using the Windows Azure Pack portal. It provides a deeper look at what kind of management abilities the administrator has in both System Center Virtual Machine Manager console and in the Windows Azure Pack portal. And what kind of experience is for the end user when he is creating virtual machines and remotely connecting to them.

### 6.1 The administrator's experience in the Windows Azure Pack portal and in the System Center Virtual Machine Manager console

The administrator has the ability to use the Windows Azure Pack portal for management purposes. As a result, the administrator can connect VM clouds as shown in the figure (Figure 33, p. 48), create and manage subscription plans, VM templates, VM networks and more. Also, the administrator can create users as well as suspend them, if needed, and in addition create SQL databases.

USER	STATUS	SUBSCRIPTIONS	ENROLLMENT DATE
test@xamkthesis.it	Active	1	4/4/2017 12:08:06 PM
oaisv001@xamkthesis.it	Active	1	4/4/2017 12:28:58 PM

Figure 35. Users' account page in Service Management Portal

The figure above presents end users which can be seen by the domain built-in administrator. The figure shows, that I am currently logged in as a XAMKTHE-SIS\Administrator and with this I can see users, their status, subscriptions as well

as enrolment dates. In the figure's left side column can also be seen created VM clouds, SQL servers and subscription plans.

The domain built-in administrator (the System Center Virtual Machine Manager administrator) is capable of using the console of latter product. It has additional features in the VMs and Services workspace (see figure 36) to create, manage and deploy clouds or virtual machines. Within the same workspace can also be created or managed VM networks. In the Fabric workspace, the administrator can add and manage hosts, host groups, infrastructure such as library, update or VMM servers. Also, the domain built-in administrator can create and manage networks and storage. The Library workspace allows storing additional information needed for clouds such as VM templates, hardware profiles, guest OS profiles or other libraries such as storing ISO files.

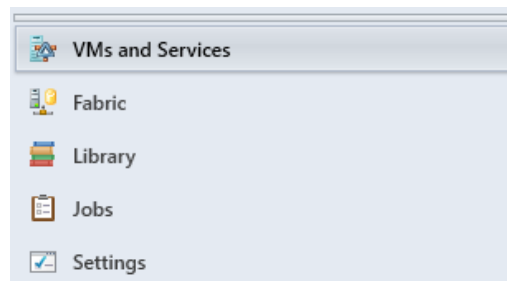


Figure 36. Microsoft System Center 2016 Virtual Machine Manager workspaces

The Jobs workspace includes all the information related with states of currently running jobs. The domain built-in administrator has the ability to check the history of jobs within the specific period of time. The last workspace that administrator has in the System Center Virtual Machine Manager console is Settings. This workspace allows managing all information related with the security. Also, the domain built-in administrator can create and manage user roles and run as accounts (which are used for accessing other hosts).

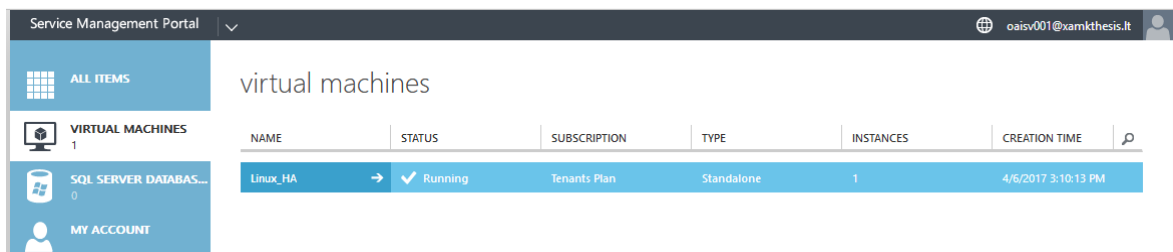
## 6.2 The end users' experience in the Windows Azure Pack portal

In addition, end users can also sign up by themselves by opening the following link <https://localhost:30081/#Workspaces/All/dashboard> in a web browser. An error appears about the website's security certificate. Nonetheless, I continued to

this website which is not recommended due to security reasons, but again, this is a lab environment. Eventually, after the page is loaded, I can login or sign up as the end user. To sign up, I have to specify the email address and enter the password. Once I signed up, I gained the welcome message and a tutorial for using the portal. The next thing to do is to add a subscription plan. I selected Tenants Plan created earlier. Finally, the end user can log in to the website and use the resources of the private cloud.

End users are able to create two types of virtual machines which are the virtual machine role and standalone virtual machine. The main difference between these two types is that standalone VM allows installing an operating system and directly maps a template to the virtual machine. The virtual machine role is acting in a bit different way using the Service Template engine by allowing to install an operating system with an application inside it. Or in other words, the end user can customize the deployment wizard.

Currently I am logged in as oaisv001@xamkthesis.it. From the menu at the left side, I chose virtual machines option, then the standalone virtual machine option and finally, the quick create option. In order to create a virtual machine, I have to specify the name, template and administrator's account password. Due to this, I named this virtual machine Linux\_HA (where HA means that this virtual machine is highly available) and chose linux-self-service template (see Figure 37).



NAME	STATUS	SUBSCRIPTION	TYPE	INSTANCES	CREATION TIME
Linux_HA	Running	Tenants Plan	Standalone	1	4/6/2017 3:10:13 PM

Figure 37. The virtual machine successfully created and running

To verify that the virtual machine was created successfully, the following two figures illustrates running virtual machine inside the VMCluster role as well as in the VMM console. As Figure 38 shows, the Linux\_HA virtual machine is running in

the Hyper-V01 node and is highly available, while the Figure 39 shows that the owner of this virtual machine is oaisv001@xamkthesis.lt.

Name	Status	Type	Owner Node	Priority
SCVMM Linux_HA Resources	Running	Virtual Machine	Hyper-V01	Medium

Figure 38. Virtual machine in VMCluster roles

Name	Status	Virtual...	Host	Cloud	Job Status	Owner
Linux_HA	Running	Running	Hyper-V01	Private Cloud	Completed	oaisv001@xamkthesis.lt

Figure 39. Virtual machine in the VMM console

When the virtual machine is created and running, the final step is to connect to it over the Connect Console. When ready, the RDP file will be downloaded from the Hyper-V host and the session will be started (see Figure 40).

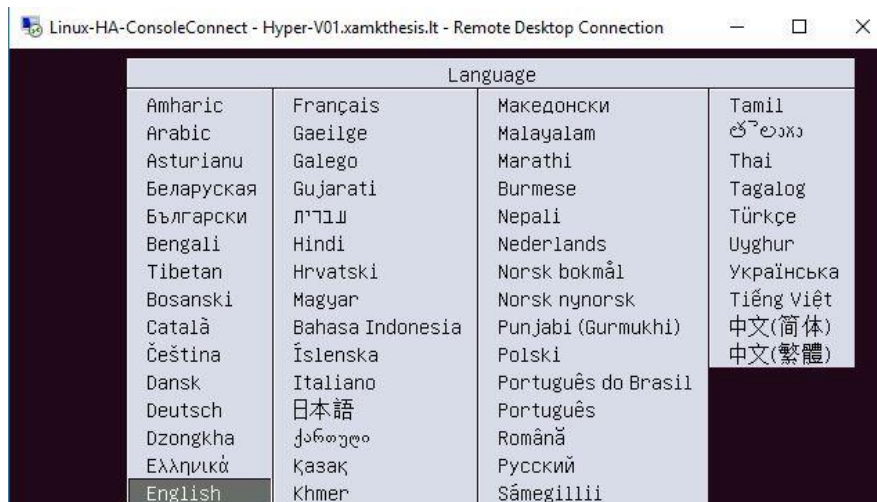


Figure 40. Connect Console page view

As Figure 40 illustrates, the connection between client's computer and the Hyper-V01 server was successfully established. The end user can successfully connect to the virtual machine using Connect Console over the Remote Desktop Connection feature. The figure above also shows the Linux installation process.

## 7 CONCLUSIONS

The objective of this thesis was to create a private cloud with Microsoft System Center 2016. The practical part of this thesis was to implement a private cloud in a virtual lab environment. The study showed that implementation of a private cloud requires knowledge of cloud computing, networking and *fabric* where *fabric* implies a private cloud resources such as network, storage, servers and clusters. Servers such as Domain Controller, RemoteDG and both Hyper-V as well as services like DNS, SQL, SAN, RDG and SC VMM itself was successfully set up in order to run a private cloud smoothly. Also, the private cloud itself was created and running successfully. Additional software such as Microsoft Azure Pack was used for end users to interact with a private cloud over a web browser.

The theoretical part showed that cloud computing is a growing technology and today mainly used in a regular basis. A private cloud has variable sets of advantages while implemented in the organization's data center that has invested in their hardware. Furthermore, a private cloud can be connected to a hybrid cloud to extend its abilities.

The main findings of the study were to implement a private cloud with System Center 2016 in a virtual lab environment. This private cloud is now ready to be implemented in a real production environment. In the future, the real third party certificates could be issued to ensure security or an automation tool implemented such as Microsoft System Center Orchestrator to build an IT process automation to automate creation, monitoring and deployment of virtual machines in a private cloud environment.



## REFERENCES

Arab, B. H. 2017. Virtual Machines Live Migration. PDF document. Available at: [https://www.researchgate.net/profile/Heni\\_Ben\\_Arab2/publication/273574310\\_Virtual\\_Machines\\_Live\\_Migration/links/5505c7750cf231de07778450.pdf](https://www.researchgate.net/profile/Heni_Ben_Arab2/publication/273574310_Virtual_Machines_Live_Migration/links/5505c7750cf231de07778450.pdf) [Accessed 28 January 2017].

CFreemanwa. 2017. System Center 2016. WWW document. Updated 15 February 2017. Available at: <https://technet.microsoft.com/en-us/system-center-docs/system-center> [Accessed 16 February 2017].

Finn, A., Vredevoort, H., Lownds, P. & Flynn, D. 2012. Microsoft Private Cloud Computing. Wiley, New Jersey.

Hess, K. 2011. Five Good Reasons to Create a Virtual Infrastructure. WWW document. Available at: <http://www.zdnet.com/article/five-good-reasons-to-create-a-virtual-infrastructure/> [Accessed 9 February 2017].

Hornbeck, J. C. 2013. System Center: Virtual Machine Manager Engineering Blog. Blog. Available at: <https://blogs.technet.microsoft.com/scvmm/2013/11/12/general-troubleshooting-list-for-windows-azure-pack-wap-and-spf-integration/> [Accessed 27 March 2017].

Howell, D. 2015. How often should your business update its tech?. WWW document. Available at: <http://www.techradar.com/news/world-of-tech/management/how-often-should-your-business-update-its-tech-1301140/2> [Accessed 17 February 2017].

Kelvin. 2014. Basic Overview on Cloud Computing. WWW document. Available at: <https://www.hostdepartment.com/blog/2014/08/05/cloud-computing/> [Accessed 12 February 2017].

Kepes, B. 2017. Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS. WWW document. Available at: <https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/> [Accessed 31 January 2017].

Kirsch, B. 2015. 5 Private Cloud Providers Compared. WWW document. Available at: <http://www.tomsitpro.com/articles/private-cloud-providers-comparison,2-899.html> [Accessed 1 February 2017].

Levitt, Raymond E., Fry, C., Greene, S. & Kaftan, C. 2009. Salesforce.com: The Development Dilemma. PDF document. Available at: <https://gpc.stanford.edu/sites/default/files/salesforce.comcasestudy.pdf> [Accessed 28 January 2017].

Maitland J. 2010. Cloud Computing Models: Public vs. Private vs. Hybrid. WWW document. Available at: <http://searchcloudcomputing.techtarget.com/video/Cloud-computing-models-Public-vs-private-vs-hybrid/> [Accessed 31 January 2017].

Microsoft. 2008. Administering Certificate Templates. WWW document. Available at: [https://technet.microsoft.com/en-us/library/cc725621\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc725621(v=ws.10).aspx) [Accessed 12 April 2017].

Microsoft. 2014. Domain Controller Roles. WWW document. Available at: [https://technet.microsoft.com/en-us/library/cc786438\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc786438(v=ws.10).aspx) [Accessed 12 January 2017].

Microsoft. 2016a. Service Provider Foundation. WWW document. Available at: [https://technet.microsoft.com/en-us/library/jj642895\(v=sc.12\).aspx](https://technet.microsoft.com/en-us/library/jj642895(v=sc.12).aspx) [Accessed 06 April 2017].

Microsoft. 2016b. Remote Console in System Center 2012 R2. Available at: [https://technet.microsoft.com/en-us/library/dn469415\(v=sc.12\).aspx](https://technet.microsoft.com/en-us/library/dn469415(v=sc.12).aspx) [Accessed 01 April 2017].

Microsoft. 2017. Overview of Remote Desktop Services. WWW document. Available at: [https://technet.microsoft.com/en-us/library/cc731150\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc731150(v=ws.11).aspx) [Accessed 07 April 2017].

Rayne-wiselman. 2016. Plan VMM installation. WWW document. Updated 12 July 2016. Available at: <https://technet.microsoft.com/en-us/system-center-docs/vmm/plan/plan-install> [Accessed 10 January 2017].

Sadashiv, N. & Kumar, S. M D. 2011. Cluster, Grid and Cloud Computing: A Detailed Comparison. PDF document. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.465.8919&rep=rep1&type=pdf> [Accessed 17 February 2017].

Swathi, T., Srikanth, K. & Reddy Raghuntah, S. 2014. Virtualization in Cloud Computing. WWW document. Available at: [http://s3.amazonaws.com/academia.edu.documents/33782483/V3I5201499a.pdf?AWSAccessKeyId=AKIAI-WOWYYGZ2Y53UL3A&Expires=1490639071&Signature=h%2FJIGS-rCbHgfyt9yWVQlnAVj20I%3D&response-content-disposition=inline%3B%20filename%3DVIRTUALIZATION\\_IN\\_CLOUD\\_COMPUTING.pdf](http://s3.amazonaws.com/academia.edu.documents/33782483/V3I5201499a.pdf?AWSAccessKeyId=AKIAI-WOWYYGZ2Y53UL3A&Expires=1490639071&Signature=h%2FJIGS-rCbHgfyt9yWVQlnAVj20I%3D&response-content-disposition=inline%3B%20filename%3DVIRTUALIZATION_IN_CLOUD_COMPUTING.pdf) [Accessed 12 January 2017].

VMware. 2007. Understanding Full Virtualization, Paravirtualization, and Hardware Assist. PDF document. Available at: [https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/VMware\\_paravirtualization.pdf](https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/techpaper/VMware_paravirtualization.pdf) [Accessed 12 January 2017].