

Tran Gia Quan

# PRIVATE CLOUD ENVIRONMENT and its utilization in a real-world scenario

Bachelor's thesis  
Information Technology

May 2017



South-Eastern Finland  
University of Applied Sciences

<b>Author (authors)</b>	<b>Degree</b>	<b>Time</b>
Tran Gia Quan	Information Technology	May 2017
<b>Title</b>		
Private cloud environment and its utilization in a real-world scenario		54 pages 0 pages of appendices
<b>Commissioned by</b>		
South-Eastern Finland University of Applied Sciences		
<b>Supervisor</b>		
Matti Juutilainen		
<b>Abstract</b>		
<p>The goal of my thesis, which was a continuation and expansion from my previous project, was to implement a private cloud system based on the Microsoft System Center tools. At the base, there was a virtualization infrastructure with three main components: computing hosts, storage providers and a flexible, reconfigurable network fabric controlled by Virtual Machine Manager. The environment had a web interface provided by Microsoft Azure Pack, based on the old portal of Microsoft Azure. This interface would simplify the view on the system and the process of provisioning virtual machines as well as other resources for students; at the same time, it would help system administrators and teachers manage student usage more efficiently through plans and subscriptions, compared to providing a multi-tenant environment directly on Virtual Machine Manager.</p> <p>Another goal of this thesis was to enable cooperation with other degree programs and provide a platform for software development. The environment was equipped with on-demand virtual machine provision, website hosting that supports multiple modern web technologies as well as source control methods and custom SQL/MySQL databases. With this, any student in our school can start developing his/her own application anywhere on campus without wasting time setting up a necessary environment from scratch. Finally, because this environment would be a duplicate of the public Microsoft Azure service, I wanted to observe the usage of private cloud in campus activities and to make a comparison of the pros and cons between public and private services.</p>		
<b>Keywords</b>		
Cloud, virtualization, Windows Azure Pack, Microsoft System Center		

# CONTENTS

1	INTRODUCTION .....	5
2	CLOUD TECHNOLOGY OVERVIEW .....	6
2.1	What is a cloud? .....	6
2.2	How are clouds categorized?.....	7
2.3	Why are private clouds needed? .....	8
2.4	Microsoft's private cloud solution: Azure Pack.....	9
2.5	Advantages of Microsoft's solution .....	9
3	THEORETICAL PART .....	10
3.1	Operating a blade server .....	11
3.1.1	Oracle's ILOM (Integrated Lights Out Management) .....	11
3.1.2	Problem with newer Java updates on old ILOM firmware versions.....	11
3.2	Necessary Microsoft's technologies.....	12
3.2.1	Active Directory Federation Service.....	12
3.2.2	System Center .....	13
3.2.3	SMB file shares.....	14
3.3	System Architecture.....	15
3.3.1	General view on the whole system .....	15
3.3.2	Azure Pack core management.....	16
3.3.3	Virtual Machine Cloud module .....	17
3.3.4	Website module .....	18
3.3.5	Tenant SQL and MySQL modules .....	19
3.4	Considerations for a stable and robust system .....	19
3.4.1	IP addressing scheme .....	20
3.4.2	Bandwidth problem and NIC teaming .....	20
3.4.3	Firewall .....	20
3.4.4	Automatic Virtual Machine Activation (AVMA) for Windows VMs running on Windows Server hosts .....	21
3.4.5	Pros and cons of using free Hyper-V Server nodes.....	21
3.4.6	Management and controlling components as virtual instances.....	22
4	PRACTICAL PART .....	23
4.1	Detailed planning .....	23
4.2	Building physical servers/Provisioning virtual servers.....	26

4.2.1	Preparing a Windows Server 2012 R2 disk image.....	26
4.2.2	Managing virtual servers.....	26
4.2.3	Hyper-V hosts.....	27
4.2.4	Storage servers.....	27
4.2.5	Other physical servers.....	28
4.3	Deploying Windows Server and necessary roles/features.....	28
4.3.1	Storage servers' provision changes during deploying different module.....	29
4.4	Deploying Windows Azure Pack core management.....	31
4.5	Deploying Virtual Machine Cloud module.....	35
4.5.1	Preparing a managed Hyper-V environment.....	35
4.5.2	Installing Service Provider Foundation.....	36
4.6	Deploying Website module.....	38
4.6.1	Preparation.....	38
4.6.2	Deployment.....	39
4.7	Deploying tenant SQL and MySQL modules.....	43
5	OPERATING AND UTILIZING THE COMPLETED SYSTEM.....	45
5.1	Administrators' viewpoint.....	45
5.1.1	Additional set up for Virtual Machine Cloud.....	45
5.1.2	Plans.....	50
5.2	Users' viewpoint.....	52
6	FURTHER OBSERVATIONS.....	54
6.1	The need for redundancy.....	54
6.2	The need for automation.....	55
6.3	Enhancing the network security and performance.....	55
6.4	Certificate management.....	56
6.5	Potential for development.....	57
7	CONCLUSIONS.....	58
	REFERENCES.....	59

## 1 INTRODUCTION

If you are a developer, you know that setting up an environment for a new project is a tedious task that can take hours. And for system operators and administrators, their job is no easier. Even with automated tools, they still need to manually deal with every request of provisioning virtual machines (VM) for developers. If they run out of resources, they also need to manually add more servers, install an operating system and necessary software. One can manage a couple of tens of servers, but when the number grows to hundreds and even thousands, the traditional approach is simply not feasible anymore.

Another problem is money. To some business, computing power is something they don't need at all time. For example, a restaurant's reservation system is idle most of the time, but becomes busy during dinner time and even more during holidays. For such cases, investing in on-premise servers with enough power to handle peak traffic but only for a short duration is a waste.

During the last decade, there have been several companies that began to offer computing-on-demand service, starting with Amazon and their Elastic Compute Cloud (Amazon Web Services Inc. 2006). They developed their own solutions and technologies to cope with the daily problem of every administrator, but on a "hyperscale" that has never existed before. Some of those solutions are later released to the public or made into consumer products, so that any organization can use them to create a more efficient computing solution for themselves. We can name a few of them: Windows Azure Pack (WAP), which represents Microsoft's experience with their own Azure public service; or Kubernetes, which is the result of Google's 15 years of experience of running containers (Burns et al. 2016). Since then, cloud technologies have been developed at a very fast pace and warmly embraced by everyone, users and administrators alike, as a solution for the future.

The aim of this study is to test the feasibility of cloud technologies in a private environment with general usage pattern. The work contains 3 main parts:

- Theoretical part: explain the theories and mechanism behind the technologies that are used in the work.
- Practical part: implement the technologies in a real-world scenario.
- Observation part: observe, find the missing pieces in the implementation and propose the necessary improvements.

## **2 CLOUD TECHNOLOGY OVERVIEW**

This part will give readers an overview of the cloud technology and Microsoft's solution.

### **2.1 What is a cloud?**

“Cloud” is a term used to describe systems that provide services to end users without them having to know or understand the underlying infrastructure. Moreover, the system, once properly set up, can operate autonomously without intervention from administrators and provide service to users on request. As defined by Mell and Grance (2011), there are “five essential characteristics” of a cloud system:

- *On-demand self-service*: Services can be provisioned without the need for administrators' intervention.
- *Broad network access*: Services are served over a networked connection. Thus, they allow users to access them from any device/client.
- *Resource pooling*: Resources from the provider are pooled together and can be allocated to users or deallocated dynamically according to their needs.

- *Rapid elasticity*: From the viewpoint of users their services can scale inward/outward to suit their demands, with the system's capabilities virtually unlimited.
- *Measured service*: The system can automatically control and optimize its resources.

Once a system achieves all these criteria, it can be categorized as a cloud service regardless of its scale in the beginning, as it can grow and expand seamlessly to suit the organization's needs later.

## 2.2 How are clouds categorized?

In the same document from NIST, Mell and Grance (2011) also suggested two ways to classify cloud services: based on the service model or deployment model.

Service model: this model is based on the final products that the cloud provides to customers such as the following:

- *Infrastructure-as-a-service (IaaS)*: Users are provided with raw computing capabilities and resources such as storage, processing power, network, etc.
- *Platform-as-a-service (PaaS)*: Users are provided with suitable environments (usually with frameworks, libraries...) to deploy their own applications.
- *Software-as-a-service (SaaS)*: Users are provided with complete, ready-to-use applications.

Deployment model: This model is based on the identity of customers that use the cloud as follow:

- *Public cloud*: Services are open to public usage and provided from the provider's datacenter,

- *Private cloud*: Services are exclusively available for private usage within an organization, can be from a provider's datacenter or on premise.
- *Community cloud*: Services are only available to a group of organizations.
- *Hybrid cloud*: Services can be provided from two or more distinct cloud models (public, private or community) which are connected to allow application or data portability among them.

In this study, I will focus on the private cloud model.

### **2.3 Why are private clouds needed?**

If we are talking about the breadth of Microsoft's or Amazon's service catalog, or the reliability of their infrastructures, public cloud services can satisfy most organizations' requirements. Even Dropbox (Metz 2016) and Netflix (Amazon Web Services Inc. 2016) are using third-party cloud service instead of building their own datacenters; and many other use cases can justify the reasonableness of choosing public clouds over building on premise datacenters. However, there are many more factors to the equation than just cost and convenience.

Many concern about their data's safety, and they want to keep their customers' financial and health data as close as possible, most favorably in their datacenters; while others simply need a private development environment for their products (Ibm.com 2012). In the second case, although their infrastructures are usually based on one or more open standards/platforms for compatibility, the solution also needs to be customized, sometimes so far that it is impractical or impossible to perform on public cloud. Either way, there are demands of building private environments that can scale easily whenever necessary, and we call them "private clouds".



## 2.4 Microsoft's private cloud solution: Azure Pack

Microsoft's answer to the demands of a private cloud platform is called Azure Pack, a bundle of software that runs on Windows Server. It mimics the interface of Microsoft's public cloud platform Azure, thus giving users the same experience they have with Microsoft's public Azure. Like its public counterpart, Azure Pack also demonstrates all five characteristics of a cloud service.

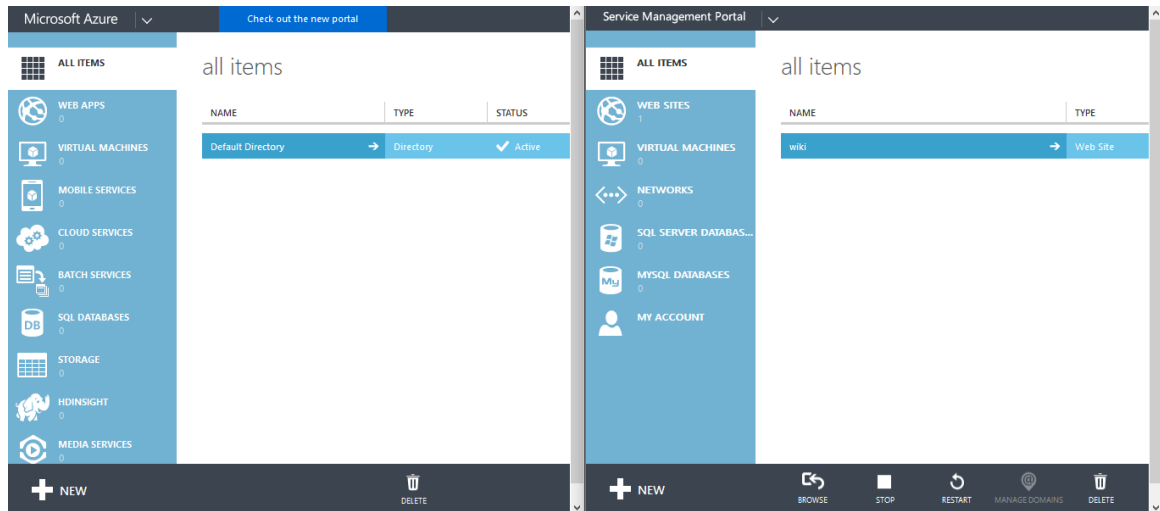


Figure 1: Public Azure's (left) and Azure Pack's (right) offering services

A full deployment of Azure Pack consists of several services that range from IaaS to PaaS to provide virtual machines, website hosting and hosted databases.

## 2.5 Advantages of Microsoft's solution

There are many solutions to the problem of building a private cloud such as OpenStack, CloudStack, OpenNebula, and of course Microsoft's Azure Pack. However, I find that there are many advantages in deploying Microsoft's solution over using the others.

One of them is the current popularity of the existing Microsoft's based infrastructure. Although there is no publicized research about the market of directory services, many professionals in the field agree that more than 90% of

Fortune 1 000 organizations are using Active Directory, which is provided along with Windows Server (Bhargava 2015). Microsoft also claimed that over 50% of companies in the Fortune 500 have already been using Windows Azure (Martin 2013). Therefore, there are increasing demands for employing private clouds that can both satisfy the requirements of performance and security of the said organizations and provide an environment for development which is compatible with public Azure infrastructures.

Azure Pack is a software bundle provided by Microsoft that allows organizations to deploy an Azure-like cloud on their own infrastructures and provides both Azure-compatible IaaS (Virtual Machine service) and PaaS (Website service). This cloud is based on and tightly integrates with Microsoft's technologies such as Active Directory, System Center and SQL Server.

There are also other solutions to deploying a private cloud, for example, OpenStack, CloudStack and OpenNebula. While I will not discuss their respective strengths and weaknesses in detail within the scope of this thesis, using Azure Pack certainly has a big benefit over the others: it can take advantage of the existing Microsoft infrastructures in each organization, like Active Directory and license agreements for various Microsoft software packages. Therefore, this is the best choice for organizations that have locked on using Microsoft's solutions.

### **3 THEORETICAL PART**

This part covers the theoretical aspect of my thesis, including the hardware and software architecture of the system and other necessary planning to make the system stable and robust. However, within the limit of this thesis, I will not discuss redundancy or high availability of the whole system, but only how to make the system run stably under normal conditions.

### **3.1 Operating a blade server**

Blade servers are the optimal choice for virtualization servers for the reasons listed below. They, for example:

- have centralized, remote management solutions,
- provide more power while using less space compared to traditional rack servers,
- scale well and easily when the environment needs more computing resources.

This section focuses on the operating procedure of Oracle blade servers, which are used in the practical part of this thesis.

#### **3.1.1 Oracle's ILOM (Integrated Lights Out Management)**

ILOM is Oracle's solution for remote management bundled with their Sun Blade chassis (Oracle.com 2017). It provides information on all the components of the chassis such as PSUs, power inputs, fans and so on as well as blades that are currently plugged into the chassis, including networking and computing blades. It also allows users to remotely control blades, for example, by changing a blade's power state, setting its boot sequence or directly interacting with a blade through a console session to compensate for the system's lack of video output.

The management interface can be accessed in two ways: either from a console session or from a web session. The console connection is essential for making initial configurations such as setting IP address/netmask for the management network which is used to access the web session later. The web interface offers a wider range of available configurations and controls.

#### **3.1.2 Problem with newer Java updates on old ILOM firmware versions**

Old firmware versions of Oracle ILOM come with a certificate which uses the obsolete SSLv3 protocol. Unfortunately, due to the disclosure of the “Poodle” vulnerability, Oracle has disabled SSLv3, weak cryptographic algorithms and the usage of small key size in Java (Oracle.com 2016), which is necessary for various functions of ILOM, such as console session and remote disk image mounting. The recommended solutions are either to upgrade the ILOM firmware to a new version or to add a new certificate that uses a valid algorithm. However, while being considered insecure, in a private and controlled environment users can also re-enable SSLv3 in Java settings.

In later versions of Java, this approach was not adequate, as there were still errors while processing the certificate even when SSLv3 was enabled, and the Java application for remote controlling would be denied from running. If the certificate cannot be replaced, it’s advised to disable certificate checking and to allow any application to run after a prompt in Java settings.

## **3.2 Necessary Microsoft’s technologies**

This part explains some technologies from Microsoft that will be used in the later parts of this thesis, as Azure Pack is heavily dependent on them. They include Active Directory Federation Service, System Center and SMB file share.

### **3.2.1 Active Directory Federation Service**

Active Directory Federation Service (ADFS) provides users with single sign-on capability across boundaries between organizations. It’s usually used in conjunction with Active Directory Directory Service as an identity provider to provide authentication service to applications from both inside and outside organizations (Msdn.microsoft.com 2017).

ADFS uses a claim-based mechanism to authenticate users in which a user with needs to access resources from an outside organization is authenticated inside

their own organization instead. Their organization then sends a claim in the form of a token with details about the user, such as permissions which the other organization trusts. The users will now be granted access to the outside organization's resources (Msdn.microsoft.com 2017).

### **3.2.2 System Center**

System Center (SC) is a software package provided by Microsoft that enables enhanced control over corporate assets (software, hardware, services), including monitoring, provisioning, configuring, protecting and automating/granting self-service capabilities. According to Microsoft, to manage that wide range of assets, SC is equipped with several components, such as:

- Operations Manager to monitor devices, services and operations.
- Configuration Manager to manage compliance settings and deliver services to devices efficiently with scalability.
- Virtual Machine Manager to manage virtualized datacenters and private clouds.
- Orchestrator to manage workflows.
- Data Protection Manager to manage backups.
- Service Manager to manage services.
- App Controller to configure, deploy and manage virtual machines and services across clouds in a self-service manner.
- Endpoint Protection to protect against malware.

Several years ago, SC (which was called System Management Server then) was just a collection of separate tools that ran independently with no cooperation and they usually conflicted with others and caused problems. However, after five to eight years and four to five generations, the ability to work together with other tools in SC has been greatly improved. They are also sold together as one license, not as separate products, and SC has since become a cost-effective solution in the eyes of corporations as they mostly have already had a Microsoft Enterprise

License Agreement and are entitled to some licenses of SC (Amaris & Yardeni 2012). It does not mean that they need to install every component, in fact they only need to install what they need while retaining the right to use the rest of the bundle. And SC is a solution provided by Microsoft, and therefore it is tightly bound to Microsoft's infrastructure, particularly to Windows Server, Active Directory and SQL Server. Usually, different components in SC are installed on separated servers to ensure good performance.

Within the scope of this thesis, Virtual Machine Manager is used to manage the Virtual Machine Cloud of Azure Pack. It is equipped with abilities to:

- manage resources (computing power, memory, storage, network) across Hyper-V hosts in the cluster.
- manage common resources (templates, libraries) on dedicated servers.
- manage local and remote (from Azure) virtual machines.
- distribute shared resources (such as storage) and automatically balance workload across hosts.
- create and assign self-service capabilities to users.
- automate the process of deploying workload with templates.

Another tool from SC that is also used in this thesis is Orchestrator, more specifically the Service Provider Foundation which is a part of the Orchestrator.

### **3.2.3 SMB file shares**

Since Windows Server 2012, SMB 3.0 file shares can be used as storage for Hyper-V hosts, including configuration files, disk images and snapshots (Microsoft TechNet 2016). This change brings forth a new storage solution for small clusters, without having to install an expensive and complicated SAN system. This solution also has many other advantages over SAN, such as independence of layer 2 implementations (SMB is a layer 7 protocol) and the abundance of bandwidth (more bandwidth can be added with link aggregation). File shares can be created

on volumes with redundancy integrated without knowing either the inner working of the volumes or whether it's software- or hardware-based RAID. This presents a unified interface to and lessen the number of configurations for end users.

### **3.3 System Architecture**

In this part, I will explain the architecture of the cloud system which will be implemented in this work, including its general deployment model and its individual components.

#### **3.3.1 General view on the whole system**

For my thesis, I chose a variation of minimal distributed deployment architecture provided by Microsoft TechNet (2016), as shown in Figure 2. The figure gives the distribution of services across multiple servers, both core and optional services. However, for simplicity, load balancers were removed and each component was only installed on one server (either physical or virtual). SQL Server was also only installed on one server instead of a failover cluster.

## Windows Azure Pack suggested minimal deployment architecture

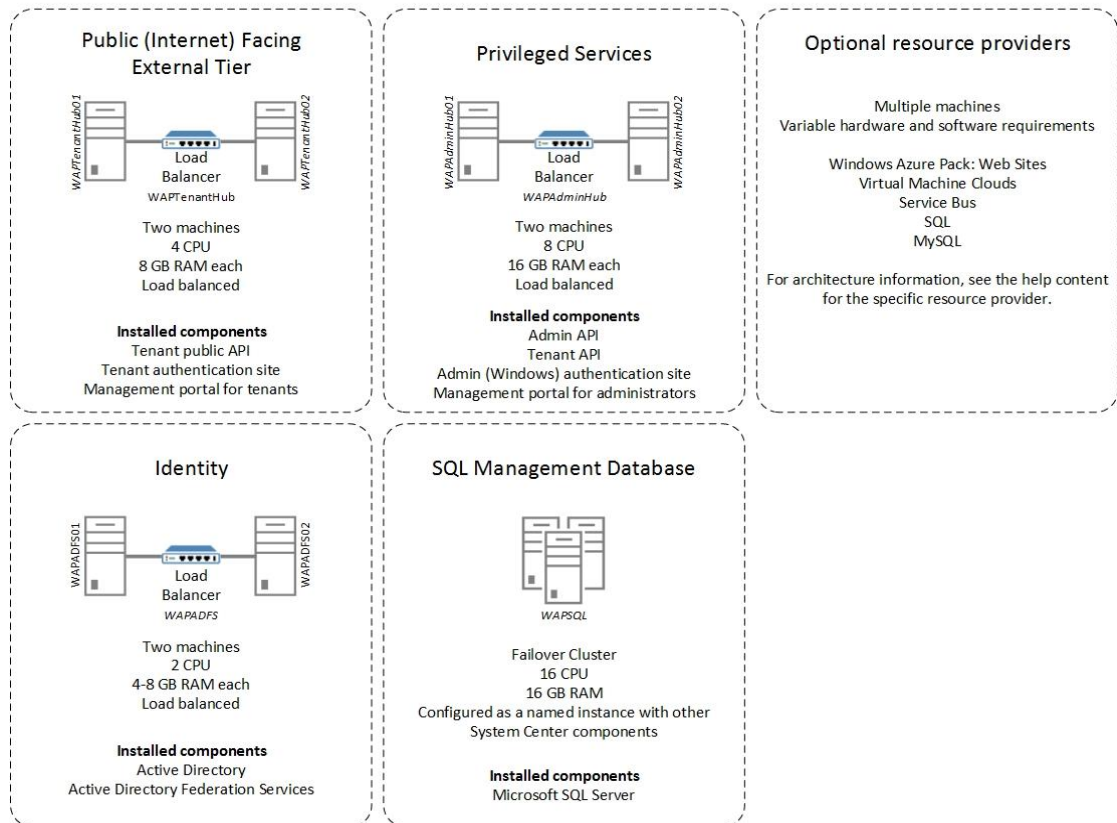


Figure 2: Azure Pack minimal distributed deployment architecture (source: Microsoft TechNet)

Generally, the whole system can be broken down into two parts: the core management components, which include portals, authentication sites and service management API; and various optional components that bring actual functionality to the system. The portals act as front-end interface for users and administrators to interact with the underlying system. Requests initiated from the portals are translated into API calls by the Service Management API components, then sent to intended endpoints, which can be the Virtual Machine Cloud service, Website service or Tenant SQL service.

### 3.3.2 Azure Pack core management

The Azure Pack's core management consists of three components: portals, service management API and authentication sites.



There are two different portals: tenants' portal and administrators' portal. Tenants' portal is a hub for users to get access to their services and manage their own resources. Administrators' portal is where system operators get an overview of how the system is running and configure various services.

Service management API delivers users' and administrators' requests from the portals to underlying service modules. Part of the tenant APIs is exposed publicly so that users can interact with the system more freely by directly calling the APIs instead of going through the portals.

Authentication sites provide authentication service for users who need access to the portals. By default, tenant authentication site uses ASP.NET Membership Provider and admin authentication site uses Windows Authentication, but both can be configured to use an existing Active Directory Federation Service (Microsoft TechNet 2016).

### **3.3.3 Virtual Machine Cloud module**

This module leverages an existing Hyper-V environment controlled by System Center Virtual Machine Manager to facilitate an IaaS cloud that supports Windows and Linux virtual machines.

On the lowest level, there are virtualization servers that run on Windows Server 2012 R2 Datacenter edition with Hyper-V role and storage servers which provides SMB file shares as remote storage. Virtual Machine Manager connects all servers together, manage them from one centralized interface and provision resources on demand according per server's capability. It also handles the creation and management of networks (either physical or virtual).

As shown in the picture below, Azure Pack uses Virtual Machine Manager as the backend for its Virtual Machine Cloud. To connect to the backend, it uses Service Provider Foundation, which is part of System Center Orchestrator. Service

Provider Foundation exposes a list of API that Azure Pack leverages for its service. From the figure, you can also see the similarities between the architecture of Microsoft's public Azure service and WAP's in deploying VMs.

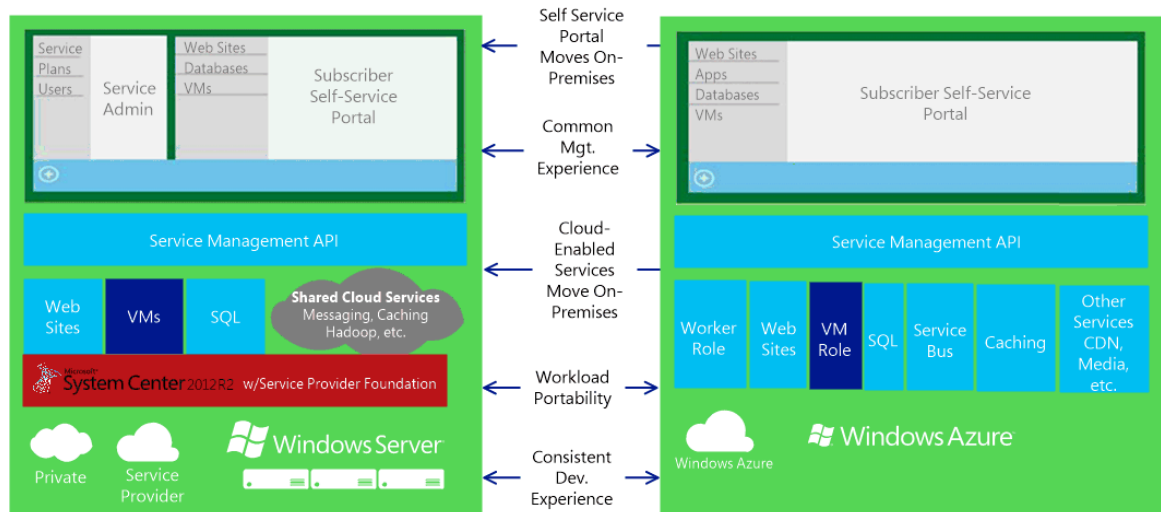


Figure 3: Comparison between WAP's Virtual Machine Cloud (left)'s and public Azure (right)'s architecture

### 3.3.4 Website module

This module provides a PaaS environment with multi-tenant web hosting service. It supports several languages such as JavaScript, PHP, ASP.NET and source control tools to automate the process of deploying websites/web applications.

According to TechNet (2013), Website module requires multiple servers for different roles, as shown in the figure below:

- Controller: controls the whole cluster internally.
- Management Server: exposes a set of REST APIs to allow management from outside the cluster.
- Web Worker: processes web requests from clients.
- Front End: accepts requests from clients, routes requests to web worker servers and returns response to clients.
- File Server: stores all content from every website on the system.

- Publisher: facilitate content publishing to the service through FTP or other protocols.

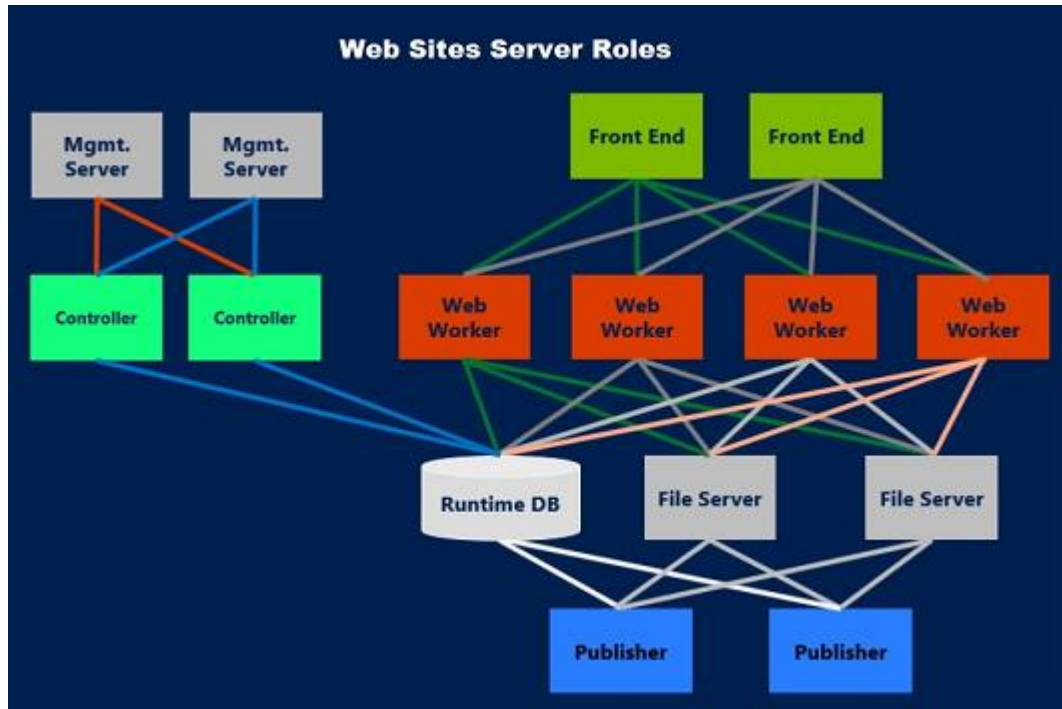


Figure 4: Server roles for website module (source: Microsoft TechNet)

Additionally, this module also requires a SQL database to hold management data and optionally databases for tenant usage. These databases can share the same SQL server with other system services.

### 3.3.5 Tenant SQL and MySQL modules

These modules allow users to create and use either SQL Server or MySQL database with Website service, or for personal purposes.

## 3.4 Considerations for a stable and robust system

Within the scope of this thesis, I did not implement any redundancy feature that allow failover or high availability, so the main aim is to make any piece of

infrastructure involved as stable as possible and can run autonomously without much intervention from administrators.

#### **3.4.1 IP addressing scheme**

Currently, all servers, either physical or virtual, are manually assigned an IP from a flat /21 subnet, more specifically from 172.16.0.64 to 172.16.0.95; and all traffic also goes on the same network, regardless it is management traffic or storage traffic. This can work in a testing/small environment, but as the environment grows and expands, there should be a more efficient scheme, for example, having separated networks and subnet for each type of traffic. The details, including detailed addressing and network topology, will be presented in Section 4.1.

#### **3.4.2 Bandwidth problem and NIC teaming**

Even with a gigabit switch, the theoretical transfer rate between hosts can only reach a bit more than 125MB/s. This is apparently not enough in a busy environment, especially during VMs' startup when operating systems load information from disk image files on storage servers into memories on Hyper-V servers.

Windows Server 2012 R2 provides built-in connections aggregating feature called NIC teaming. This feature allows two or more NIC on the same server to work together as one unified NIC in without concerning about the switch's compatibility (McIllece 2016), brings both redundancy and improvement in speed and reliability for inbound and outbound connections. This feature is especially useful when remote storage is used in the cluster as it can greatly improve transfer rate between storage servers and Hyper-V servers. Moreover, it will be a simple task to add more bandwidth to suit future's growth just by adding more connection to the existing team.

#### **3.4.3 Firewall**

There are several services on each server that need to be accessed from remote hosts. As a security measure, there should be firewall enabled on each host that only allows designated remote hosts to connect to pre-defined ports in production phase. However, during development phase, firewall can temporarily be disabled.

#### **3.4.4 Automatic Virtual Machine Activation (AVMA) for Windows VMs running on Windows Server hosts**

Per Windows Server 2012 R2 Licensing Datasheet (2013), a license for Datacenter edition comes with the right for unlimited virtual instances of Windows Server, so it's a great choice for infrastructure servers as well as Hyper-V servers. In addition to that, once a server is activated with a valid key, every VM running on Hyper-V on that host will automatically be activated during boot time, if it was installed using one of the generic keys listed on TechNet (2016). The number of VMs that can be activated on a host corresponds to the edition of Windows Server that was installed and activated on that server: 1 for Essentials edition, 2 for Standard edition and unlimited for Datacenter edition.

#### **3.4.5 Pros and cons of using free Hyper-V Server nodes**

In addition to using Windows Server 2012 R2 Datacenter edition on virtualization hosts, Microsoft also provides a free hypervisor: Hyper-V Server 2012 R2. This hypervisor is in fact a scaled-down version of Windows Server 2012 R2 with only the Hyper-V role enabled. During deploying my environment, I also tested Hyper-V Server and noted down some pros and cons of this solution as follows.

Pros:

- It is free, suitable for installing Linux VMs.
- It is lightweight, as both GUI and other roles are removed.
- It allows remote management from familiar tools like Microsoft Management Console or System Center Virtual Machine Manager.

Cons:

- It does not come with any license, so Windows VMs installed on Hyper-V Server must have individual licenses.
- There is no way to create loopback devices, which are software-based network adapters, thus prevent creation of tenant custom network (this point will be explained in more details in Section 5.1.1).

For reasons stated above, unless there are spare network adapters on the server, Hyper-V Server has limited use.

#### **3.4.6 Management and controlling components as virtual instances**

Aside from the main infrastructure servers like virtualization or storage servers, other components (such as Virtual Machine Manager, administrators'/tenants' portal and API, federation service and Websites' components) can be installed as virtual instances on a central server. This approach has several advantages:

- It decreases the number of physical servers used and utilize each server better.
- Some components support scaling up to process more workload, and with this approach we can simply add more instances from templates.
- It is easy to backup and redeploy in case of system failure.

Although this approach also creates single points of failure, it has proved itself useful in a case of system disk failure. Although the whole server that contains components for Websites module went down because of a failed system disk, the recovery process only took minimal effort, as reinstalling Windows Server, making minimal configurations and relaunching the virtual instances which are located on another disk array. This approach is apparently more preferable than having to reconfigure a failed service from scratch.

## 4 PRACTICAL PART

In this part, I will implement a WAP cluster with all of its components and optional modules: core management components, Virtual Machine Cloud module, Website module and SQL Server/MySQL module.

### 4.1 Detailed planning

I use eight physical servers for this system, four of them are blade servers from Sun Microsystems and the other four are custom-built servers.

The whole system belongs to a local Windows domain named *CLOUD.itlab.mamk.fi* with its own DNS server which is hosted on the domain controller, except for the MySQL server and two physical hosts for virtual servers that run management components. All servers run Windows Server 2012 R2, either the Datacenter or Standard edition, except for the MySQL server.

The detailed network topology and IP addressing is described in the following image and tables:

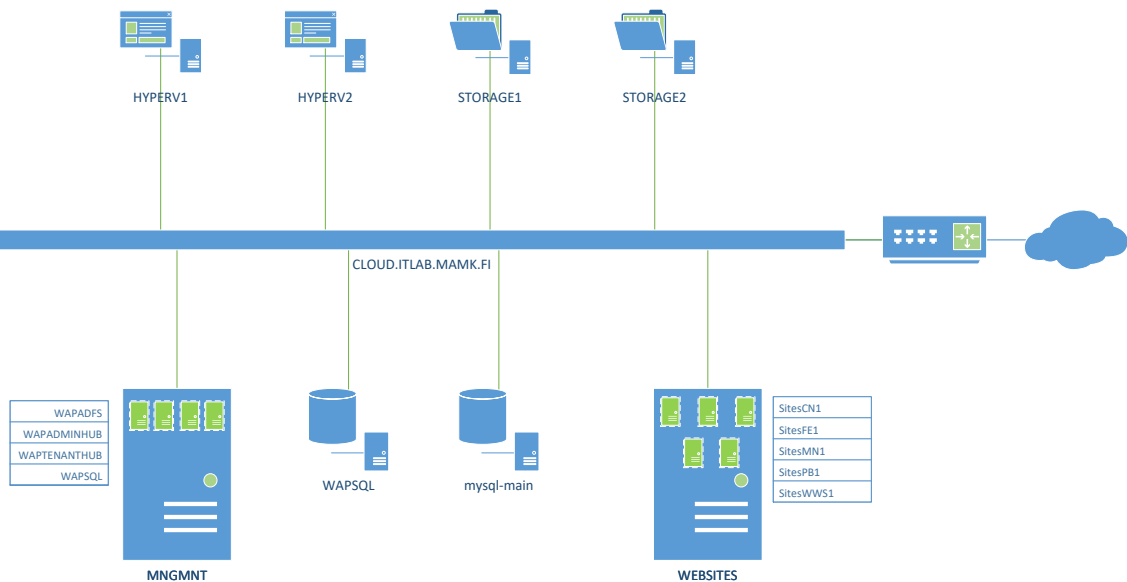


Figure 5: Physical implementation of the system

Table 1: Physical specification of physical and virtual servers

Server	Device	CPU	RAM	Disk
WAPSQL	Blade server 1	2x Xeon E5450	64GB	4x 73GB
MNGMNT	Blade server 2	2x Xeon E5450	64GB	4x 73GB
WAPADFS	Virtual server	1 virtual processor	4GB	1x 40GB
WAPAdminHub	Virtual server	4 virtual processors	8GB	1x 40GB
WAPTenantHub	Virtual server	2 virtual processors	4GB	1x 40GB
VMM	Virtual server	1 virtual processor	4GB	1x 40GB
HYPERV1	Custom-built tower	2x Xeon E5-2620	128GB	1x 250GB
HYPERV2	Custom-built tower	2x Xeon E5-2620	112GB	1x 250GB
STORAGE1	Custom-built tower	Core i3-2100	16GB	1x 240GB SSD 5x 3TB
STORAGE2	Custom-built tower	Core2Duo E7500	8GB	1x 500GB 3x 3TB
WEBSITES	Blade server 4	2x Xeon E5450	64GB	4x 73GB
SitesCN1	Virtual server	1 virtual processor	2GB	1x 40GB
SitesFE1	Virtual server	1 virtual processor	4GB	1x 40GB
SitesMN1	Virtual server	1 virtual processor	4GB	1x 40GB
SitesPB1	Virtual server	4 virtual processors	4GB	1x 40GB
SitesWWS1	Virtual server	1 virtual processor	8GB	1x 40GB
mysql-main	Blade server 6	2x Xeon E5450	64GB	2x 73GB

Note: Virtual servers denoted with blue are hosted on MNGMNT. Those denoted with red are hosted on WEBSITES.

All virtual servers' memory can be dynamically scaled up to meet the demand.



The IP range is 172.16.0.64-172.16.0 with the subnet mask 255.255.248.0, which is a part of the MB3 network used in XAMK's IT department's classes. This guarantees access for students in MB building in Mikkeli campus with proper DNS server configuration.

Table 2: operating system version and IP address allocation for each server

Server	IP address	Teamed connection?	Domain-joined?	Operating system
MNGMNT	172.16.0.66	Yes, from .64 and .65	No	Windows Server 2012 R2 Datacenter
WAPSQL	172.16.0.67	No	Yes	Windows Server 2012 R2 Datacenter
WAPADFS	172.16.0.68	No	Yes	Windows Server 2012 R2 Datacenter
WAPAdminHub	172.16.0.69	No	Yes	Windows Server 2012 R2 Datacenter
WAPTenantHub	172.16.0.70	No	Yes	Windows Server 2012 R2 Datacenter
WEBSITES	172.16.0.71	Yes, from .77 and .78	No	Windows Server 2012 R2 Datacenter
VMM	172.16.0.72	No	Yes	Windows Server 2012 R2 Datacenter
HYPERV1	172.16.0.73	No	Yes	Windows Server 2012 R2 Datacenter
HYPERV2	172.16.0.74	No	Yes	Windows Server 2012 R2 Datacenter
STORAGE1	172.16.0.75	No	Yes	Windows Server 2012 R2 Standard
STORAGE2	172.16.0.76	No	Yes	Windows Server 2012 R2 Standard
SitesCN1	172.16.0.79	No	Yes	Windows Server 2012 R2 Datacenter
SitesFE1	172.16.0.80	No	Yes	Windows Server 2012 R2 Datacenter
SitesMN1	172.16.0.81	No	Yes	Windows Server 2012 R2 Datacenter
SitesPB1	172.16.0.82	No	Yes	Windows Server 2012 R2 Datacenter
SitesWWS1	172.16.0.83	No	Yes	Windows Server 2012 R2 Datacenter
mysql-main	172.16.0.84	No	No	Ubuntu Server 14.04

## **4.2 Building physical servers/Provisioning virtual servers**

The cluster makes use of both physical servers and virtual servers. Each of them has distinctive characteristics, and are therefore suitable for different tasks.

### **4.2.1 Preparing a Windows Server 2012 R2 disk image**

All virtual servers are installed with Windows Server 2012 R2 Datacenter, which is activated through AVMA. To save the time and to avoid doing the same installation and configuration procedure multiple times, I just install it once and generalize it with sysprep, a tool provided by Microsoft, to remove any computer-specific information from the image. After being prepared with sysprep, the image can now be copied and used in multiple virtual servers. These servers only need to be configured a few settings like a computer name, username and a password before being ready for usage. This process can save a lot of time compared to installing Windows for each virtual server individually.

### **4.2.2 Managing virtual servers**

Two blade servers are allocated to host management components for the cluster. Both have the same CPU configuration (Dual-socket Intel Xeon E5450) and RAM amount (64GB), but different disk configuration due to their different priorities. The first blade, named MNGMNT, hosts core components of the whole cluster: Active Directory Directory Service and Federation Server, Admin and Tenant internal API, Tenant public API, portals and authentication sites; therefore, it is configured with four disks divided into two RAID array: the first array, configured in RAID-1 mode, is for the hypervisor, and the second array, configured in RAID-0 mode, is storage for VMs. The other blade, named WEBSITES, hosts management components for the Website and has four disks which are divided into one independent disk for the hypervisor and three disks configured into a RAID-0 array for VM storage. The two blades are partitioned as such, because first, MNGMNT cannot tolerate downtime, as it will take the whole cluster offline, while WEBSITES can sustain some

downtime without affecting any other module, and second, WEBSITES hosts more VMs, and therefore it needs more storage.

The hypervisor is Windows Server 2012 R2 Datacenter with Hyper-V role, installed manually on the blade through the remote control console of Oracle's ILOM.

### **4.2.3 Hyper-V hosts**

There are two virtualization hosts: HYPERV1 and HYPERV2. They are equipped with powerful CPUs and high amount of RAM, but with minimum local storages which are just enough for the OS, because their role is just providing computing power. The actual VMs are stored in remote storages. Both are actual tower servers, with their hardware being server-grade such as dual-socket motherboard, EEC RAM.

### **4.2.4 Storage servers**

In contrast to the two virtualization servers, two storage servers are built completely from scratch using commodity hardware. Their cases, motherboards, CPUs and RAM sticks are all taken from normal computers in the lab.

The first server is fit with five 3TB SATA disks, with one SSD in the PCI slot that acts as both system disk and cache for the storage pool. The second server uses a normal 500GB disk as a system disk and three 3TB SATA disks for the storage pool.

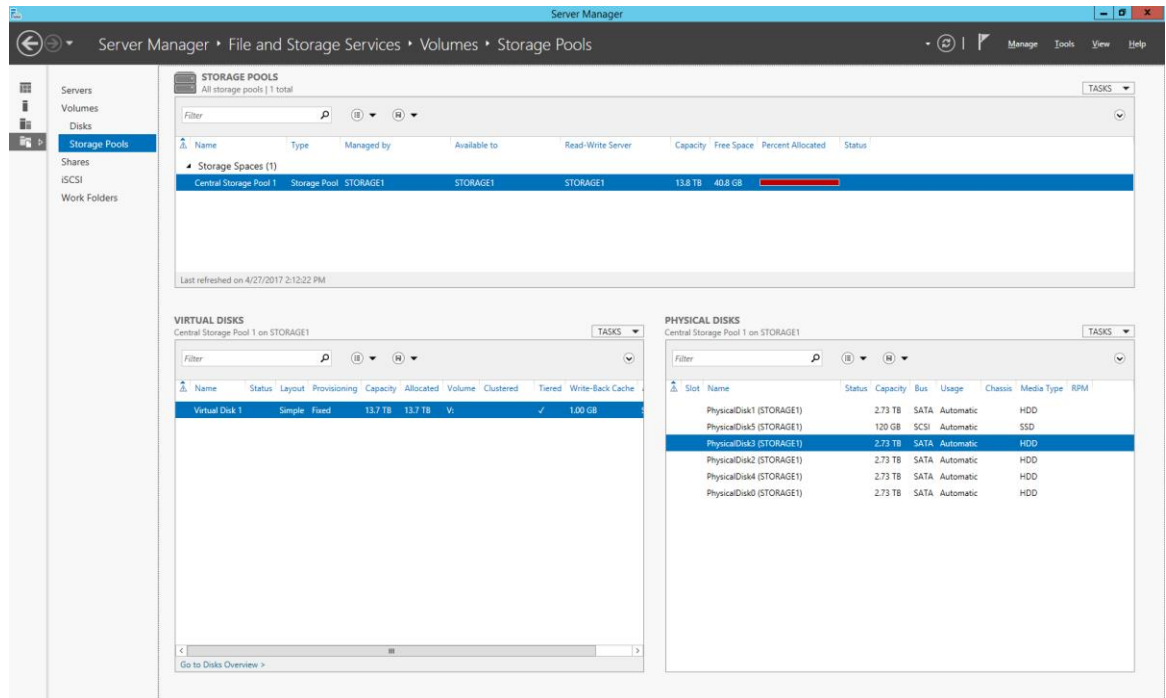


Figure 6: Physical, virtual disks and storage pools on STORAGE1

#### 4.2.5 Other physical servers

The two database servers, WAPSQL and mysql-main, are installed with Windows Server 2012 R2 and Ubuntu Server 14.04, respectively. They are hosted on two blades servers, blade 1 and blade 6.

#### 4.3 Deploying Windows Server and necessary roles/features

Except for two storage servers which use Windows Server 2012 R2 Standard, all other servers are activated with Datacenter edition keys. After that, the following things are done on all servers:

- Setting a proper server name according to the plan
- Joining the server to the domain (if applicable)
- Enabling remote desktop
- Reconfiguring the local administrator account to prevent its password from expiring

- Disabling the firewall if necessary
- Deploying necessary roles and features

On WAPSQL, Microsoft SQL Server 2012 SP2 is installed. It hosts several SQL instances for different services: WAP, Federation Service and many more. The process of deploying new instances as well as configuring them (for example, for different types of authentication) will not be discussed within the scope of this thesis.

Name	State	Start Mode	Log On As	Process ID	Service Type
SQL Server (ADFS)	Running	Automatic		1184	SQL Server
SQL Server (SCVMM)	Running	Automatic		1200	SQL Server
SQL Server (SPF)	Running	Automatic		1388	SQL Server
SQL Server (TENANTSQL)	Running	Automatic		1760	SQL Server
SQL Server (WAP)	Running	Automatic		2004	SQL Server
SQL Server (WEBSITES)	Running	Automatic		2260	SQL Server

Figure 7: List of SQL instances (with logged on username redacted)

On mysql-main, MySQL 5.5 is installed. It hosts a MySQL instance for tenants' usage. Like SQL Server, the process of deploying and managing MySQL will not be discussed. There are four servers with the Hyper-V role: MNGMNT, WEBSITES, HYPERV1, HYPERV2. Among them, the first two are not managed by the domain but instead managed by a local user. The latter two will join the domain as part of the VMM cluster. Two servers, STORAGE1 and STORAGE2, run File and Storage Services which are installed by default with Windows Server 2012 R2.

Among the virtual servers, WAPADFS is the only one with distinctive roles installed. It's the domain controller with Active Directory Directory Service and Federation Service installed. Federation Service requires a SQL instance for its own use, which is hosted on WAPSQL (WAPSQL\ADFS).

#### 4.3.1 Storage servers' provision changes during deploying different module

At the beginning of the thesis, the two storage servers were only intended to be used as remote storage for Virtual Machine Cloud module, with one being the

normal storage without redundancy, and the other being the redundant storage running on software-based RAID-5. However, with the addition of Website module, there is the need for storage for this module too. With software-based storage pool and virtual disk, provisioning layout can be changed quickly and easily; for example, on STORAGE2 I shrank the size of the redundant virtual disk to make space for one more simple virtual disk; thus, sophisticated layouts can be used on commodity hardware without the need for dedicated hardware like RAID controller.

Tasks related to storage can be executed either from the GUI with Server Manager, or from the command line with PowerShell. In fact, some effects can only be achieved by using PowerShell, for example changing a physical disk's media type from HDD to SSD.

The screenshot displays the Server Manager interface for storage management. It is divided into three main sections: Storage Pools, Virtual Disks, and Physical Disks.

**STORAGE POOLS**  
 All storage pools | 1 total

Name	Type	Managed by	Available to	Read-Write Server	Capacity	Free Space	Percent Allocated	Status
Central Storage Pool 2	Storage Pool	STORAGE2	STORAGE2	STORAGE2	8.18 TB	1.00 GB	<div style="width: 100%; height: 10px; background-color: red;"></div>	

Last refreshed on 5/4/2017 9:57:12 AM

**VIRTUAL DISKS**  
 Central Storage Pool 2 on STORAGE2

Name	Status	Layout	Provisioning	Capacity	Allocated	Volume	Clu
Website Storage		Simple	Fixed	2.40 TB	2.40 TB	W:	
Redundant Central Storage		Parity	Fixed	3.85 TB	3.85 TB	T:	

**PHYSICAL DISKS**  
 Central Storage Pool 2 on STORAGE2

Name	Status	Capacity	Bus	Usage	Chassis	Media
PhysicalDisk3 (STORAGE2)		2.73 TB	SATA	Automatic		HDD
PhysicalDisk2 (STORAGE2)		2.73 TB	SATA	Automatic		HDD
PhysicalDisk1 (STORAGE2)		2.73 TB	SATA	Automatic		HDD

Figure 8: Different disk layouts in STORAGE2's Server Manager

#### 4.4 Deploying Windows Azure Pack core management

The core management module of WAP consists of APIs, authentication sites and portals. They are divided between two servers: WAPAdminHub and WAPTenantHub.

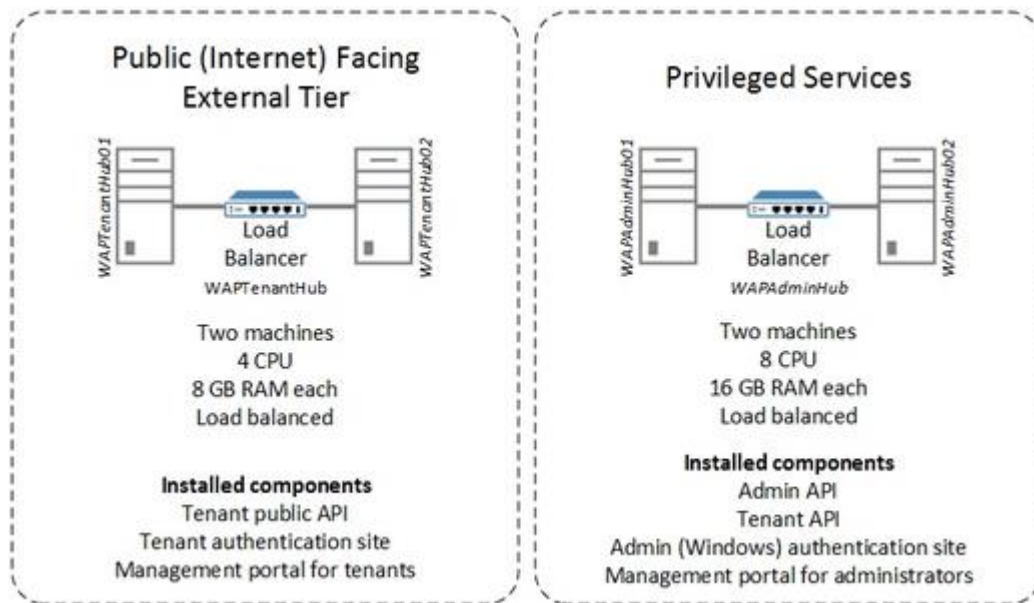


Figure 9: Modules in WAP core management

Web Platform Installer (WPI) provides a quick and easy way to install components related to Microsoft Web Platform, including WAP components. The installation process consists of adding required components to list, accepting the terms and conditions and installing. The recommended order of installing is APIs, portals and authentication sites.

After installing each component, a configuration page (shown in Figure 10) will open inside your browser. Here you can configure the connection to a SQL instance that holds the data for WAP (here I used WAPSQLWAP). This instance should be the same for all components that belongs to WAP core management.

SERVICE MANAGEMENT SETUP ✕

## Database Server Setup

**Database Server**

Please specify the SQL Server that you would like to use for the Service Management databases. Please use the same SQL Server instance for configuring the Service Management Admin, Tenant and Tenant Public APIs, Admin Site and Tenant Site.

**SERVER NAME**

**AUTHENTICATION TYPE**

SQL Server Authentication ▼

**DATABASE SERVER ADMIN USERNAME** **DATABASE SERVER ADMIN PASSWORD**

**Configuration Store**

Please provide a passphrase below that will be used to store and retrieve secrets from the configuration store. The same passphrase needs to be used in all machines on this deployment. Note that if the configuration store does not exist yet, the passphrase is always valid.

**PASSPHRASE**

 ?

→

Figure 10: Configuring database connection

Figures 11 and 12 show the components that need to be installed on each server:

	Snine Cloud Security for Azure Pack: Admin Site Extension	11/16/2015	Installed
	Windows Azure Pack: Admin API	11/1/2016	Installed
	Windows Azure Pack: Admin Authentication Site	11/1/2016	Installed
	Windows Azure Pack: Tenant API	11/1/2016	Installed
	Cloud Cruiser for Windows Azure Pack: Admin Site Extension	2/6/2015	Installed
	Windows Azure Pack: Admin Site	11/1/2016	Installed
	Windows Azure Pack: SQL Server Extension	11/1/2016	Installed
	Windows Azure Pack: MySQL Extension	11/1/2016	Installed

Figure 11: Components installed on WAPAdminHub








	Windows Azure Pack: Tenant Site	11/1/2016	Installed
	5nine Cloud Security for Azure Pack: Tenant Site Extension	11/16/2015	Installed
	Windows Azure Pack: Tenant Authentication Site	11/1/2016	Installed
	Cloud Cruiser for Windows Azure Pack: Tenant Site Extension	2/6/2015	Installed
	Windows Azure Pack: Tenant Public API	11/1/2016	Installed

Figure 12: Components installed on WAPTenantHub

After installing and configuring the database connection, WAP core management module is now ready, with the authentication sites using Windows authentication for administrators' portal and ASP.net membership provider for tenants' portal. However, since we have a domain with all the users, it will be convenient to use the domain's Federation Service as the identity provider and Directory Service as the identity source for the cluster.

According to the guide on TechNet (2013), there are three required steps to enable using Directory Service as the identity provider:

- Configure the management portals to trust ADFS. This step will tell the portals to rely on ADFS as the identity provider.
- Configure the tenant authentication site to trust ADFS as the identity provider. This also implies that admin authentication site trusts ADFS by default.
- Configure ADFS to trust the management portals. This step will tell ADFS that the management portals are trusted relying parties as well as configure the designated identity source for those relying parties.

In the last step, by default ADFS is set to use Active Directory as the identity source for the administrators' portal and ASP.net membership provider, which is the original identity provider for tenants' portal, as the identity source for tenants' portal. To make it easier to manage users, it's preferable to set the identity source of tenants' portal to Active Directory too. This can be achieved by manually editing

the provided script ("C:\Program Files\Management Service\MgmtSvc-PowerShellAPI\Samples\Authentication\Configure-Adfs.ps1") on line 90:

```

84 | Add-AdfsRelyingPartyTrust `
85 |     -Enabled $true `
86 |     -Name $tenantRelyingPartyName `
87 |     -MetadataUrl $tenantRelyingPartyMetadataEndpoint `
88 |     -EnableJWT $true `
89 |     -AllowedClientTypes None `
90 |     -ClaimsProviderName $identityProviderName `
91 |     -IssuanceTransformRules ([System.String]::Concat($transformationRules)) `
92 |     -IssuanceAuthorizationRules ([System.String]::Concat($issuanceRules)) `
93 |     -ImpersonationAuthorizationRules ([System.String]::Concat($impersonationRules))

84 | Add-AdfsRelyingPartyTrust `
85 |     -Enabled $true `
86 |     -Name $tenantRelyingPartyName `
87 |     -MetadataUrl $tenantRelyingPartyMetadataEndpoint `
88 |     -EnableJWT $true `
89 |     -AllowedClientTypes None `
90 |     -ClaimsProviderName 'Active Directory' `
91 |     -IssuanceTransformRules ([System.String]::Concat($transformationRules)) `
92 |     -IssuanceAuthorizationRules ([System.String]::Concat($issuanceRules)) `
93 |     -ImpersonationAuthorizationRules ([System.String]::Concat($impersonationRules))

```

Figure 13: Change in the script: old (above) and new (below)

After this, when an administrator or a user needs to access a portal, they will be redirected to the Federation Service sign in page:

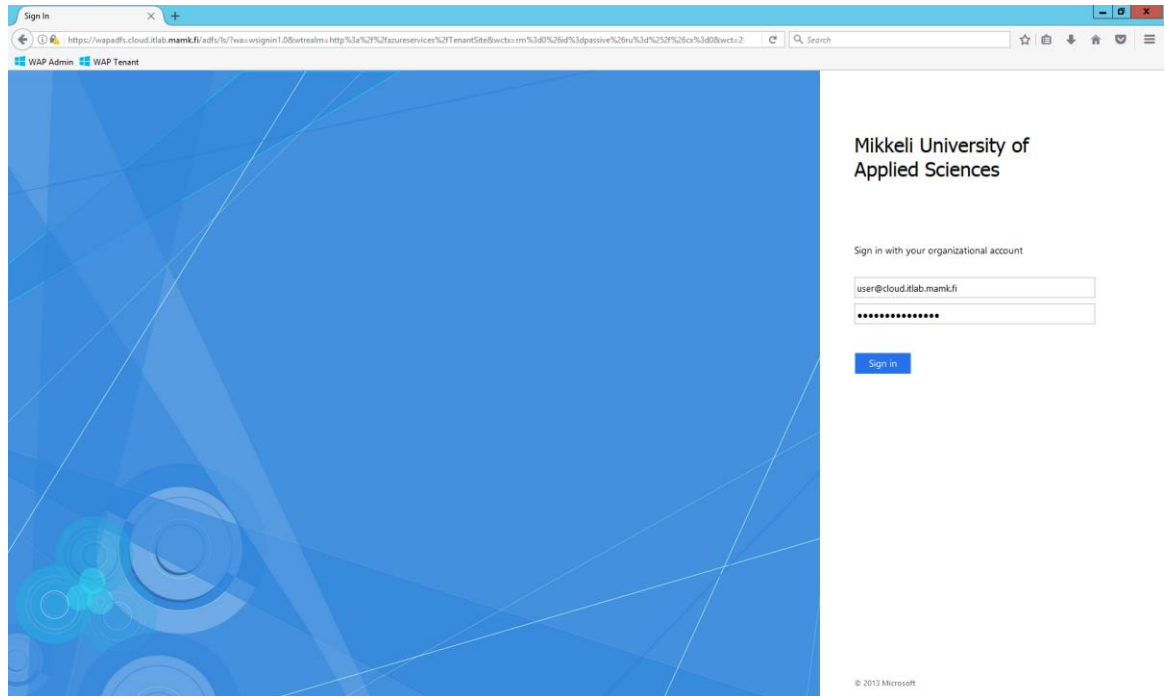


Figure 14: Federation Service sign in page

## **4.5 Deploying Virtual Machine Cloud module**

Virtual Machine Cloud is the focus of this system, with the ability to deploy virtual machines based on the existing templates on demand.

### **4.5.1 Preparing a managed Hyper-V environment**

The core of Virtual Machine Cloud is a Hyper-V environment managed through Virtual Machine Manager. It consists of:

- virtualization servers: HYPERV1 and HYPERV2.
- storage servers: STORAGE1 and STORAGE2.
- management server: VMM

A cluster managed by Virtual Machine Manager can also provision computing power (virtual machine) on-demand with great versatility, for example, creating new VM from disk image, disk template, or from scratch (with console connection). It can also manage networking and storage within the cluster. However, a user can only work with Virtual Machine Manager if they have access to a Virtual Machine Manager console, which is heavyweight and resource-intensive. Therefore, a system with only Virtual Machine Manager cannot be counted as a true “cloud” as it cannot be easily accessed remotely.

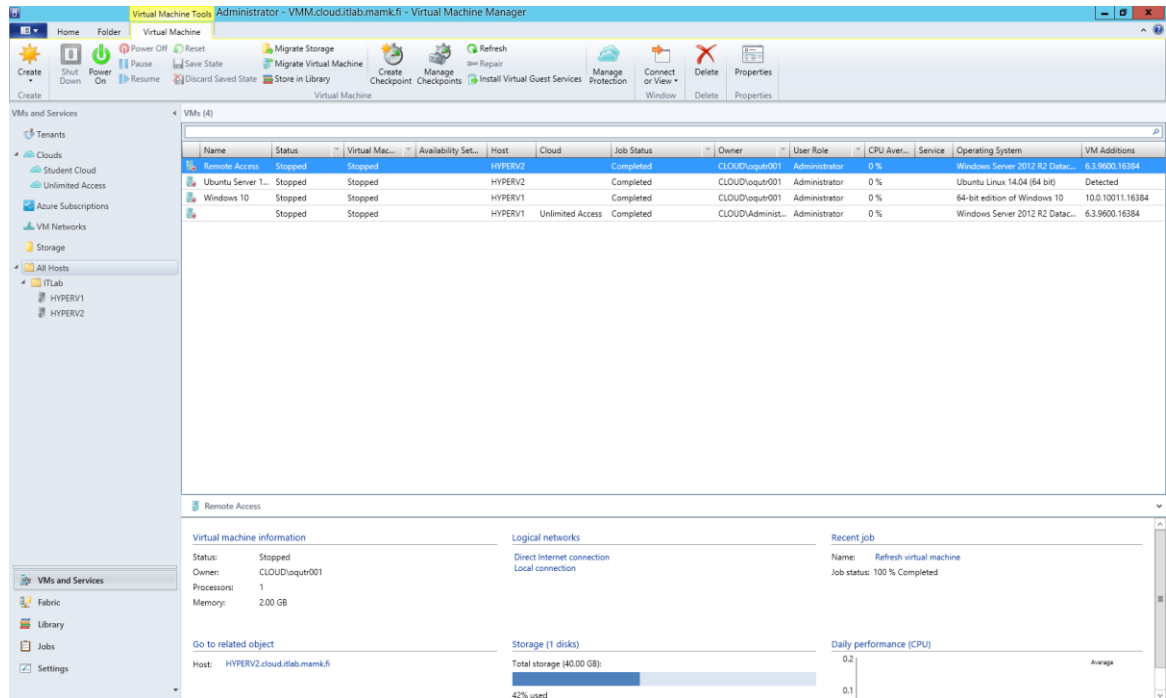


Figure 15: Virtual Machine Manager console

To prepare it for a true “cloud” experience, the existing cluster must be equipped with the following:

- VM networks for tenants to use directly or logical networks on which tenants can create their own VM networks (virtual networks in WAP).
- VM templates and hardware profiles, which are disk images from which tenants can deploy their own VM instances.
- a library share/server to hold VM templates and hardware profile. Optionally images sharing on the library server can be configured to prevent items in the library from being copied every time an instance is created from it.
- a “cloud” created from host groups in virtual machine manager to which logical networks and library servers/shares are associated.

#### 4.5.2 Installing Service Provider Foundation

Service Provider Foundation (SPF) is the middle layer that facilitates communication between Azure Pack core management and Virtual Machine Manager to provide virtual machine service to tenants. In this deployment, SPF is installed on VMM using the System Center Orchestrator installer. During the installation process the following actions are required:

- Specifying the database instance for SPF (in this case, WAPSQL\SPF).
- Specifying a name and port for the SPF endpoint .
- Specifying the service account for and accounts that will have access to the SPF Admin web service, Provider web service, VMM web service and Usage web service.

After the installation, there are several checks that need to be done to verify the the service account's credentials are put into correct local groups on the server. The service account must also be added to Virtual Machine Manager as an administrator.

Finally, the SPF endpoint must be registered in the administrators' portal so that WAP can recognize the Virtual Machine Cloud. The credentials of the service account specified above are needed to register successfully.

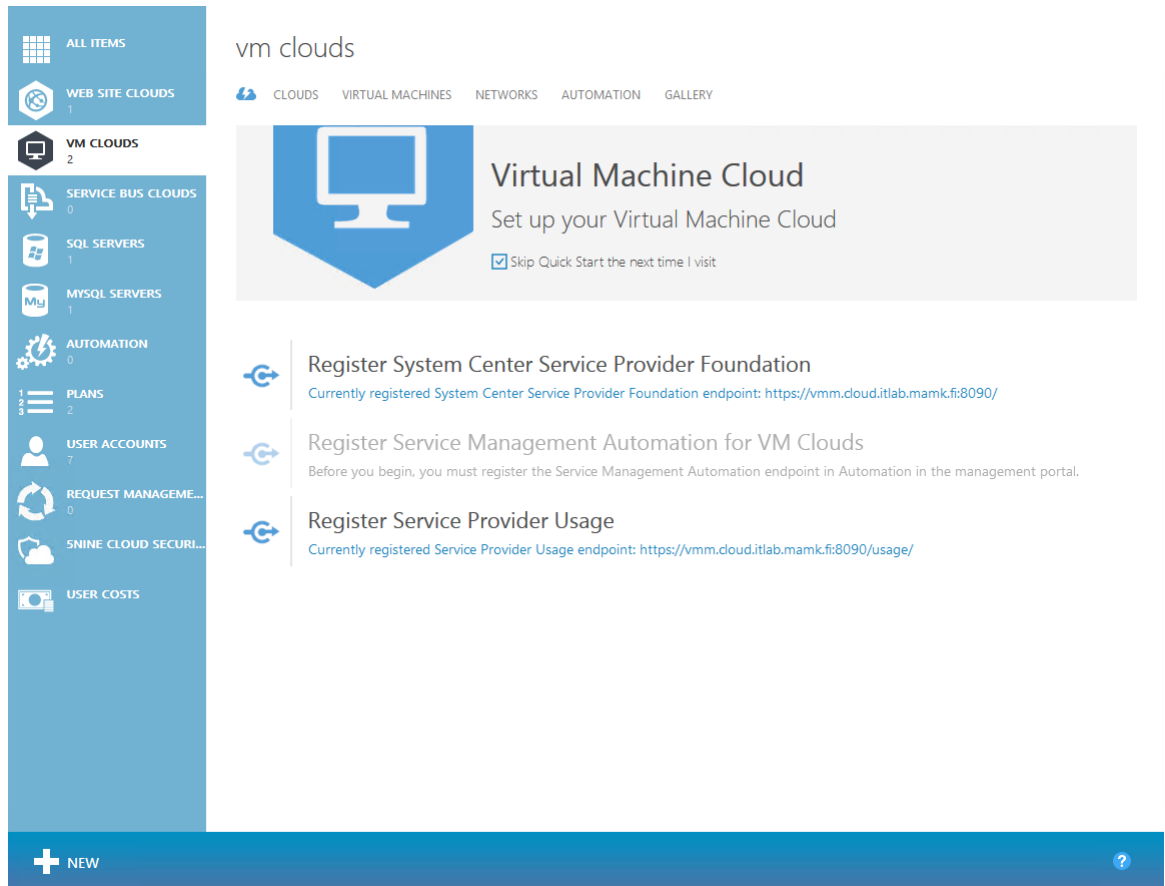


Figure 16: SPF endpoint registered in the administrators' portal

## 4.6 Deploying Website module

Most of the implementation in this section follows the guide on TechNet (2015), however there are some modifications such as reduced number of roles deployed.

### 4.6.1 Preparation

A full deployment of Website module requires servers for seven roles plus some more for redundancy. However, in my implementation, I only deploy six roles; five of which are deployed on provisioned virtual servers on blade 6 as mentioned in Section 4.1. The breakdown of the roles is as follows:

- Controller: installed on SiteCN1
- Management: installed on SitesMN1

- Shared Web Worker: shared among all tenants, installed on SitesWWS1
- Reserved Web Worker: available to be reserved and used exclusively by privileged tenants; not installed
- Front End: installed on SitesFE1
- Publisher: installed on SitesPB1
- File Server: co-exists on STORAGE2 with its own virtual disk based on the storage pool available on the server (refer to Section 4.3.1)

This module needs access to three different SQL instances:

- Service Management API database: This is the database that holds configuration data of WAP core management (in this case WAPSQL\WAP).
- Website Runtime Database: This database holds runtime data for Website module (in this case WAPSQL\WEBSITES).
- Application Database: This database allows tenant websites to have database functionality (in this case WAPSQL\TENANTSQL).

All servers and database instances are already prepared in the previous sections. The capacity and naming of the servers were decided based on the recommendations from TechNet's (2015) guide with several considerations to fit the situation.

The file server provides storage to the system in the form of a file share. Some configurations are needed for the module to be able to access the share with its own service users. These configurations won't interfere with other roles of STORAGE2.

#### **4.6.2 Deployment**

The first step is to install the controller which is performed on SitesCN1 through WPI.

Name	Released	Install
Windows Azure Pack: Websites Update Rollup 9	1/25/2016	Installed

Figure 17: Component(s) to install on SitesCN1

This component should be installed locally in the same way as other components. Many dependencies are also installed along. They are software that are necessary to the operation of Website module such as Python, PHP, etc.

After the installation, there will be Web Cloud Management Console on SitesCN1.

From there, the configuration goes in the following steps:

- Setting this server as a primary controller as we are creating new Websites Cloud.
- Setting the controller type and file server type.
- Entering details for database instances.
- Setting a DNS suffix for the farm (in this case *cloud.itlab.mamk.fi*).
- Entering credentials for various roles and functions in the deployment.
- Choosing a server to act as a file server (STORAGE2) and a server to act as a management server (SitesMN1). After this step, the controller will start configuring these two servers first. When it finishes, start Web Farm Controller Service.
- Adding more servers for the remaining roles. When all the necessary roles have already been configured and marked as "Ready", the farm has been successfully provisioned.

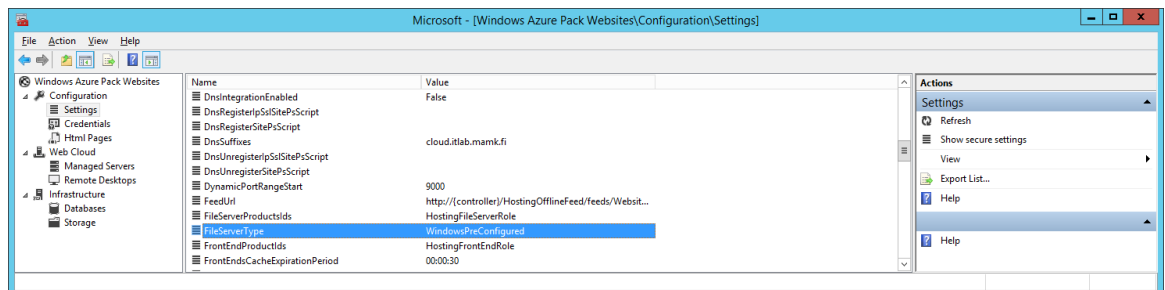


Figure 18: Some settings in Web Cloud Management Console



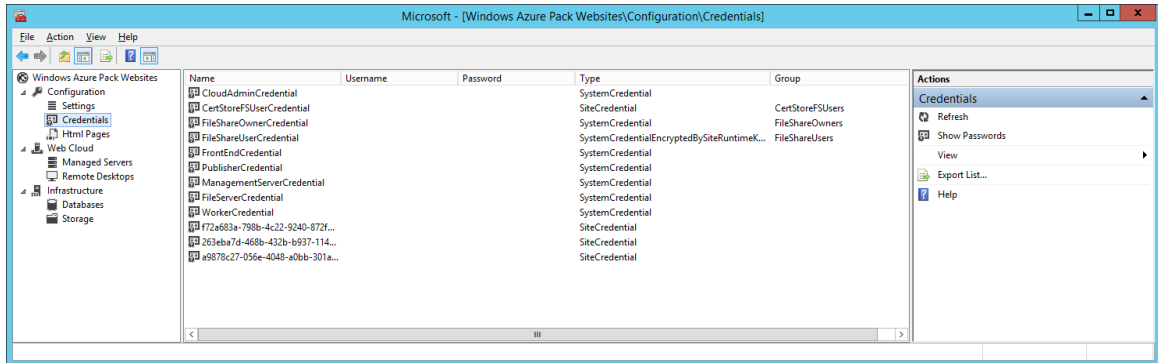


Figure 19: Credential management in the console (usernames and passwords redacted)

Servers provisioned by the Web Cloud Management Console can also be managed directly through the console (using Remote Desktop Protocol).

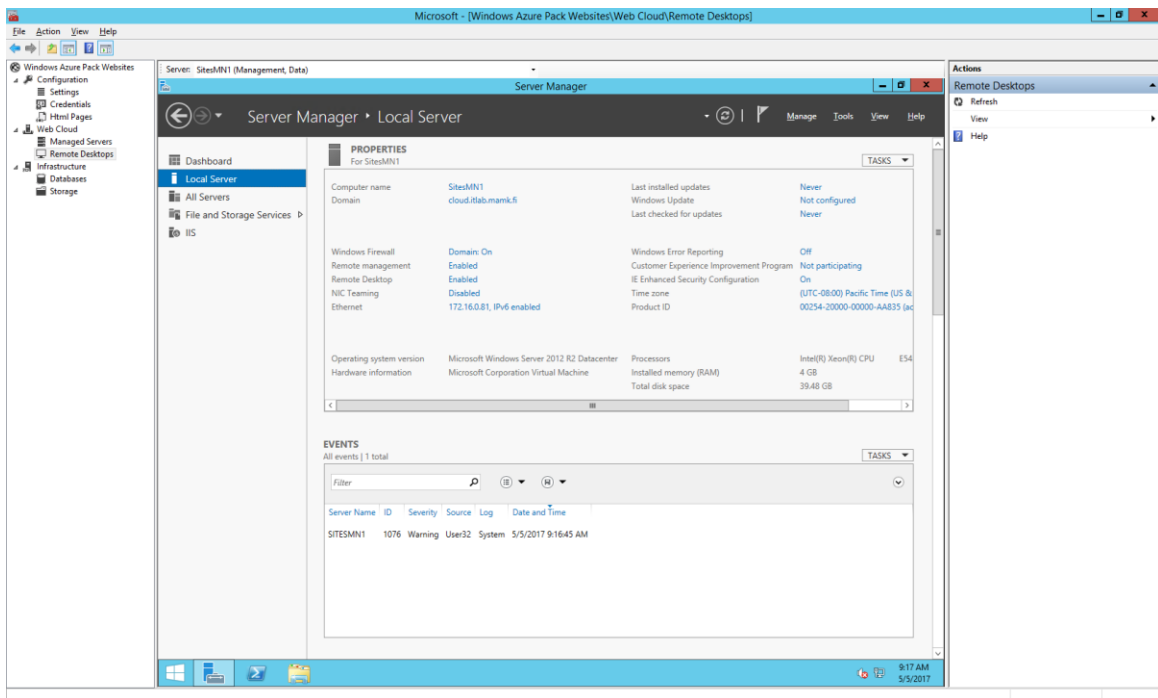


Figure 20: Manage servers inside the console

The operational log of servers in the farm can also be tracked directly from the console. This makes managing a large number of servers easier since the log does not need to be checked from each individual server.

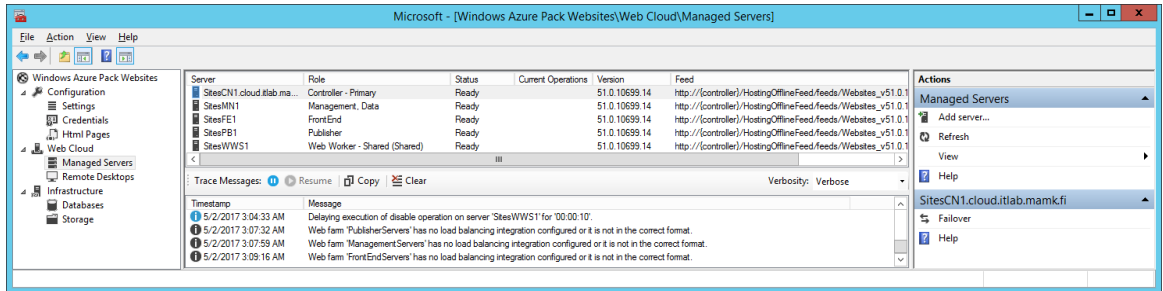


Figure 21: The console's "Trace messages"

The newly created Websites Cloud must be registered in the administrators' portal using the management server's (SitesMN1) address and credentials. At this point, the Website module can also be managed from the administrators' portal. It allows administrators to have a quick summary of system utilization, manage server roles, modify some configuration and credentials, list and delete websites running on the system.

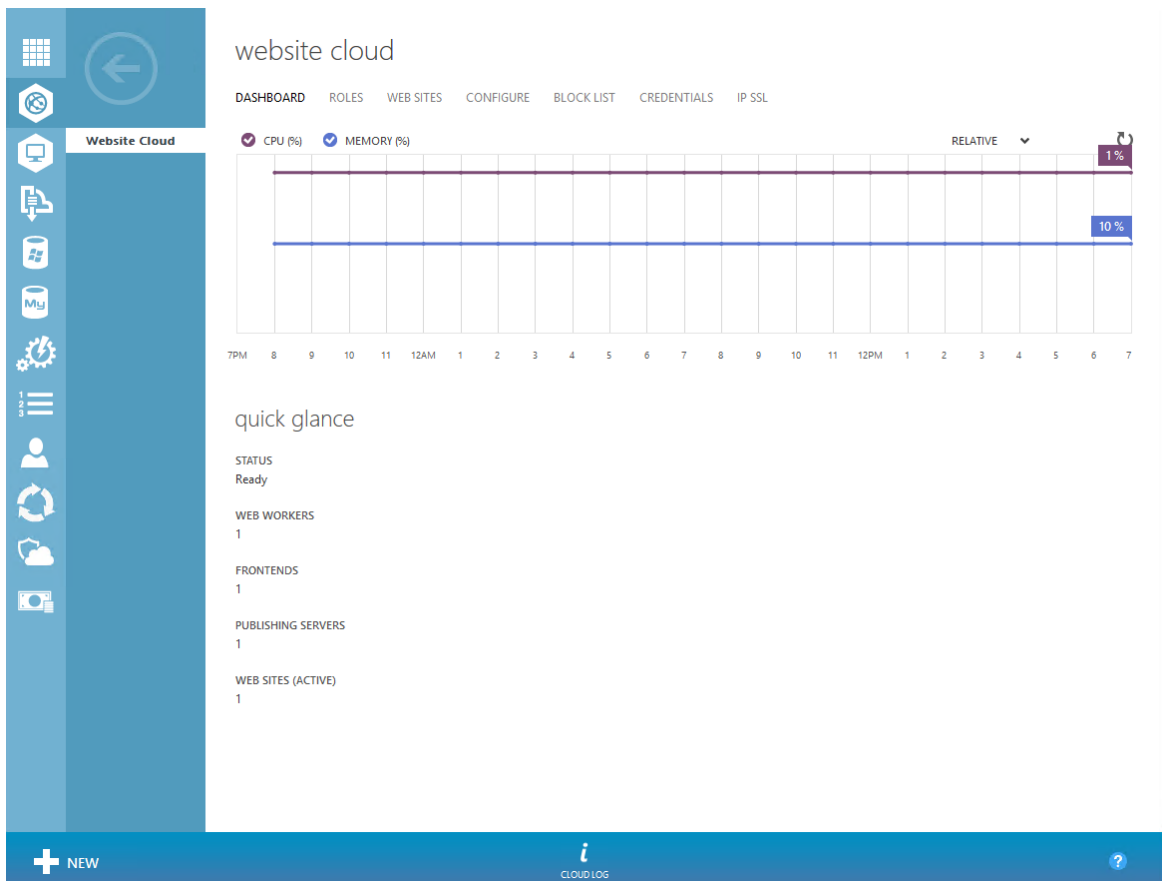
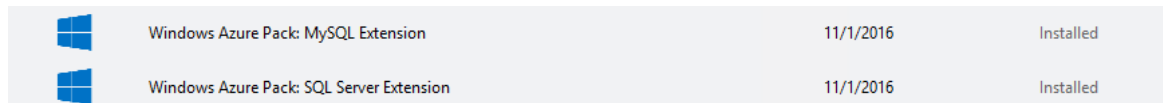


Figure 22: Management of Website module through administrators' portal

## 4.7 Deploying tenant SQL and MySQL modules

For WAP to be able to connect to SQL Server and MySQL instances, first resource providers for their respective type of instance must be installed. Microsoft provides these components through WIP.





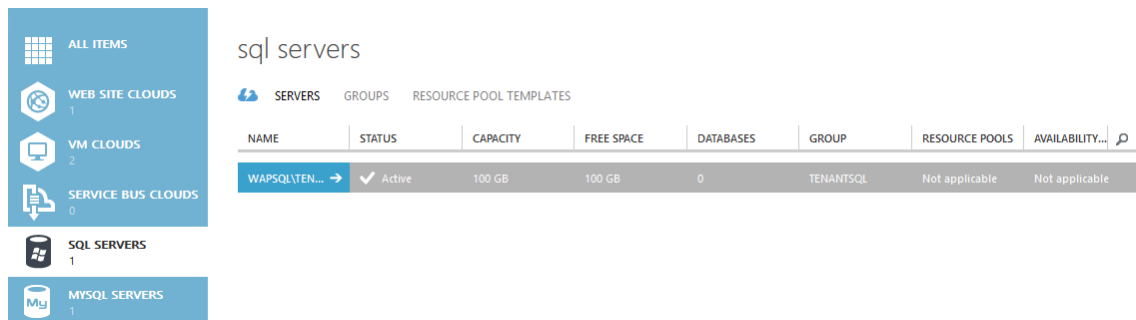
	Windows Azure Pack: MySQL Extension	11/1/2016	Installed
	Windows Azure Pack: SQL Server Extension	11/1/2016	Installed

Figure 23: Resource providers for SQL Server and MySQL

Both providers are installed on WAPAdminHub and the procedure is the same as with other components. The database that should be used here is the database that was used during the installation of the core management components (in this case, WAPSQL\WAP). After finishing the configuration, SQL Server and MySQL modules will appear in the administrators' portal.



sql servers								
SERVERS    GROUPS    RESOURCE POOL TEMPLATES								
NAME	STATUS	CAPACITY	FREE SPACE	DATABASES	GROUP	RESOURCE POOLS	AVAILABILITY...	
WAPSQL\TEN...	Active	100 GB	100 GB	0	TENANTSQL	Not applicable	Not applicable	

Figure 24: Summary of available SQL Server instances

To add a new SQL instance for tenants' usage, an existing instance with username and password for SQL Server authentication is needed. In this case I used WAPSQL\TENANTSQL. After that, each instance can be set with a limit on its serving capacity, as well as added to groups of instances.

NAME	STATUS	CAPACITY(GB)	FREE SPACE(GB)	DATABASE COUNT	GROUP
172.16.0.84	Active	50	49.8	1	Main

Figure 25: Summary of available MySQL instances

To add a new MySQL instance, we need its server name (or IP address) and a pair of username and password with administrator right on that instance. After that we can set its limit or add it to groups in the same way as with SQL Server instances.

TechNet's guide recommends using MySQL Windows 5.1 for instances, which is installed through WPI, however I find it difficult to work with MySQL on Windows due to the lack of tools, for example the *mysql* console command and other configuration files; therefore, in my thesis, a MySQL instance on Ubuntu Server is used instead.

From the administrators' portal, administrators can check on every instance that was registered on the system for a summary of its usage as well as list and delete databases on each instance. For a SQL Server instance, its capacity limit can also be adjusted.

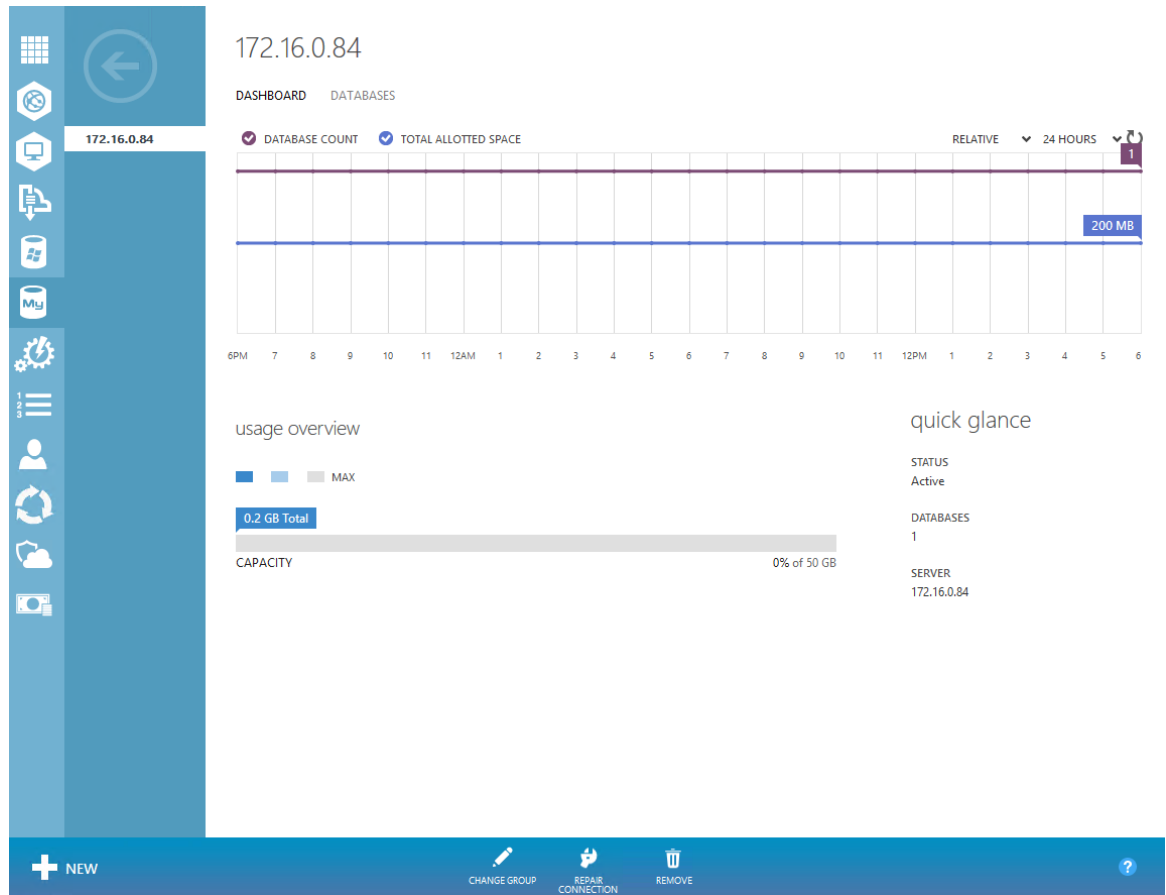


Figure 26: Dashboard of the MySQL instance

## 5 OPERATING AND UTILIZING THE COMPLETED SYSTEM

This section will explain how administrators and tenants can get the most out of the system.

### 5.1 Administrators' viewpoint

The system has now been successfully set up, and most administrative tasks can be done from the administrators' portal. However, there are still some configurations that need to be done directly on the servers.

#### 5.1.1 Additional set up for Virtual Machine Cloud

After the SPF endpoint has been registered, each "cloud" created inside Virtual Machine Manager will be shown as a cloud in administrators' portal. From there,

administrators can monitor the status of each cloud, list and delete virtual machines and custom networks on the system.

The top part of the image shows the administrators' portal with a sidebar on the left containing categories like ALL ITEMS, WEB SITE CLOUDS, VM CLOUDS, SERVICE BUS CLOUDS, SQL SERVERS, and MYSQL SERVERS. The main area displays a table of cloud configurations.

NAME	STATUS	VIRTUAL MACHINES	CORES	MEMORY (MB)	STORAGE (GB)
vmm.cloud.itlab.mam...	Ready	1 of unlimited	4 of unlimited	1048576 of unlimited	1064 of unlimited
Student Cloud	Ready	0 of unlimited	0 of unlimited	0 of unlimited	0 of unlimited
Unlimited Access	Ready	1 of unlimited	4 of unlimited	1048576 of unlimited	1064 of unlimited

The bottom part of the image shows the Virtual Machine Manager interface. The left sidebar shows 'VMs and Services' with 'VMs (1)' selected. The main area displays a table of virtual machines.

Name	Status	Virtual Mac...	Availability Set...	Host	Cloud	Job Status	Owner
	Stopped	Stopped		HYPERV1	Unlimited Access	Completed	CLOUD\Administ...

Figure 27: Clouds in administrators' portal (top) and clouds in Virtual Machine Manager (bottom)

However, in contrast to with Virtual Machine Manager which provides a broad range of methods and options to provision a virtual machine, with WAP tenants can only deploy virtual machines from pre-defined template which utilize one or more disk images and pre-defined size. Those templates are called "gallery items" in WAP, and they are provided by Microsoft through Web Platform Installer (with a custom feed).

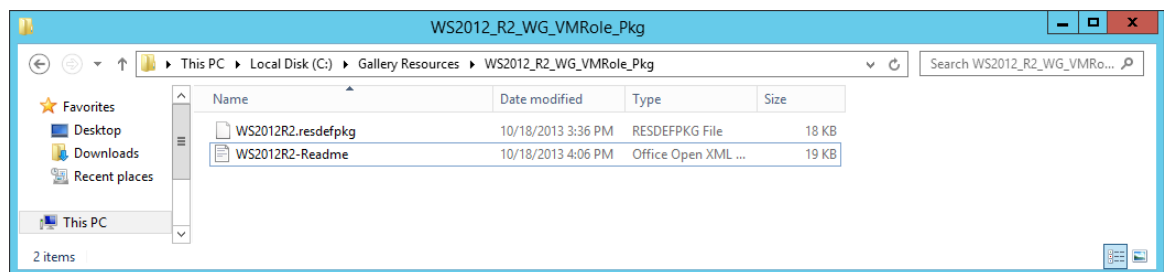


Figure 28: A gallery item downloaded

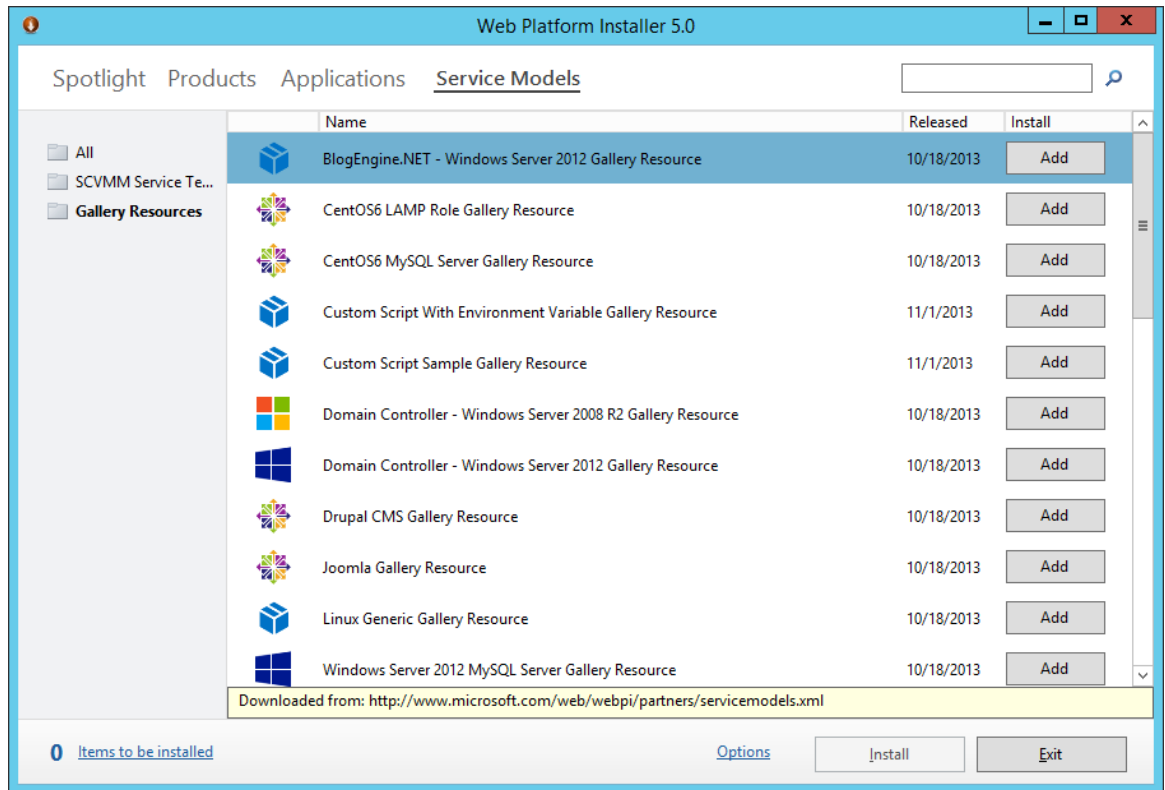


Figure 29: Gallery Resources in WPI

With each gallery item downloaded, you will get a folder with several files, one with *resdefpkg* extension, possibly one with *resextpkg* extension and one document file that explains how to use the item. The one with *resextpkg* extension is imported into Virtual Machine Manager using PowerShell, the one with *resdefpkg* extension is imported into the administrators' portal. Each gallery item will require some existing resources (for example, disk images) from the Virtual Machine Manager library that was associated with each cloud to have tags and other metadata set to designated values (which are listed in the enclosed document). For example, the item "Windows Server 2012 R2" requires a disk image with following metadata:

Operating System	Use one of the following: <ul style="list-style-type: none"> <li>Windows Server 2012 R2 Datacenter</li> <li>Windows Server 2012 R2 Standard</li> <li>Windows Server 2012 R2 Essentials</li> </ul>
Familyname	Consider the following values for Familyname: <ul style="list-style-type: none"> <li>Windows Server 2012 R2 Datacenter</li> <li>Windows Server 2012 R2 Standard</li> <li>Windows Server 2012 R2 Essentials</li> </ul>
Tags	Add all of the following tags: <ul style="list-style-type: none"> <li>WindowsServer2012</li> <li>R2</li> </ul>

Figure 30: Metadata for the Windows Server 2012 R2 disk (taken from the gallery item package for Windows Server 2012 R2)

These metadata can be set either in Virtual Machine Manager console or using PowerShell.

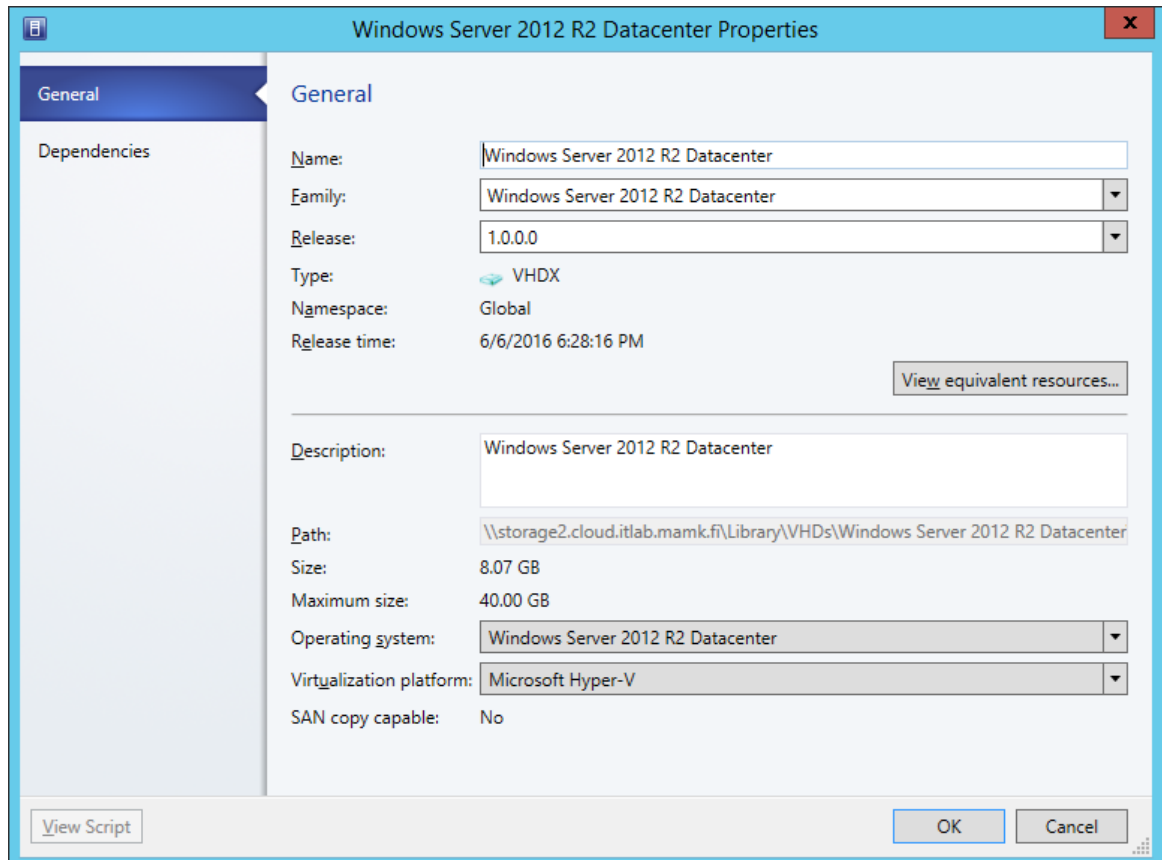


Figure 31: Setting metadata in Virtual Machine Manager



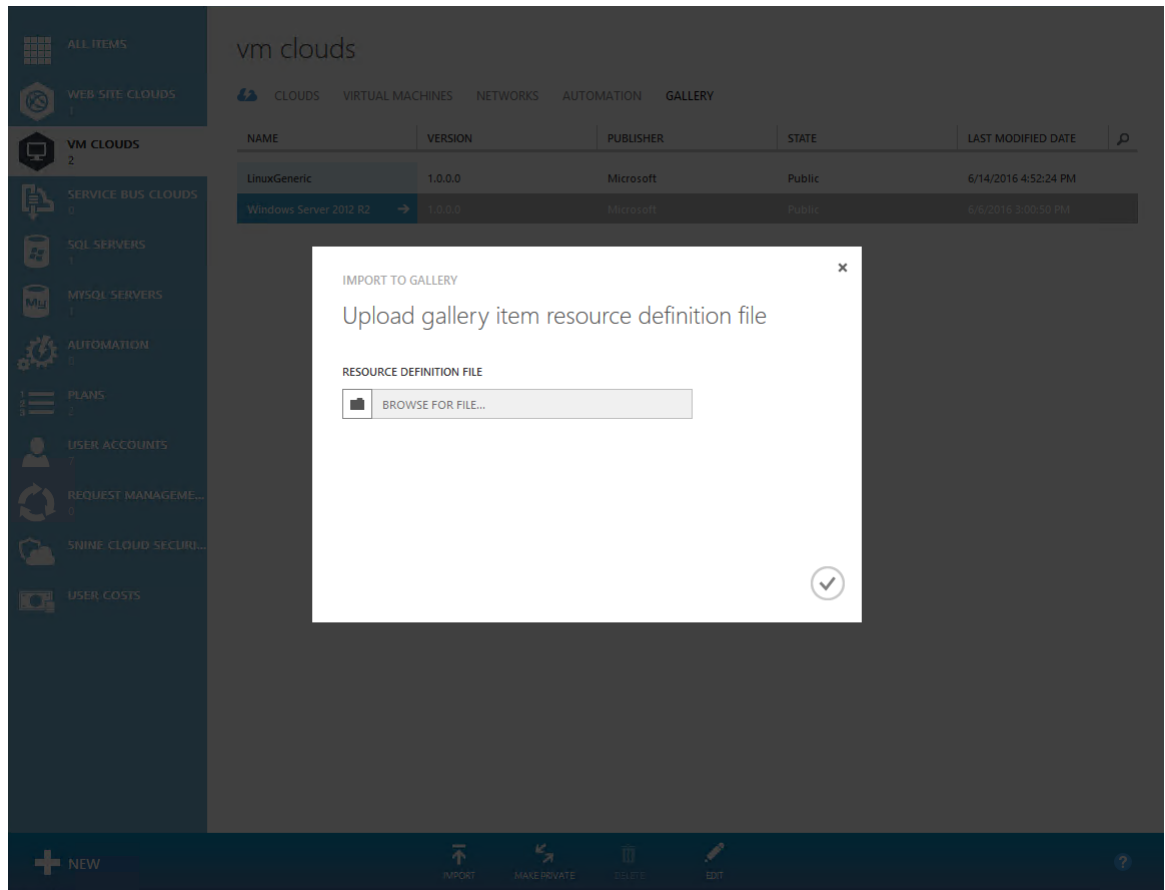


Figure 32: Importing a gallery item through administrators' portal

After importing and setting metadata for relevant resources managed by Virtual Machine Manager that gallery item is now ready to be used by tenants.

If a cloud is associated with a logical network, any tenant with access to that cloud can create a custom virtual network based on that logical network. However, for VM to be able to connect to that virtual network, any host in that cloud must also have a physical adapter associated with that logical network. In my case, due to the lack of network adapter, I used Microsoft KM-TEST Loopback Adapter for this purpose. On the free Hyper-V Server, there is not enough facility to create a new loopback adapter. Therefore, I did not use Hyper-V Server as hypervisors for virtualization nodes.

Optionally, administrators can also set up remote console for System Center, so that tenants can initiate a remote console to their VMs through tenants' portal.

### 5.1.2 Plans

The next step for administrators is to create plans that tenants can subscribe to. A plan can (but not necessarily) consists of access to:

- an instance of Websites Cloud
- an instance of Virtual Machine Cloud
- one or more SQL Server groups
- one or more MySQL server groups

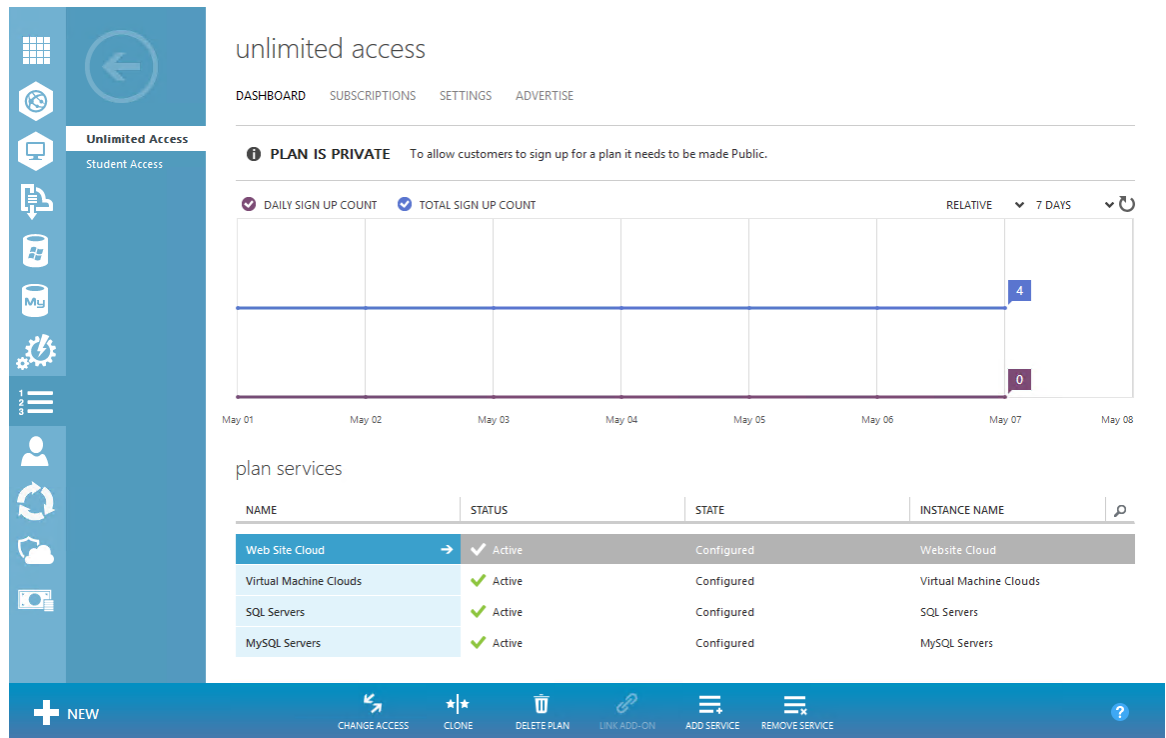


Figure 33: Overview of a plan

From the portal, administrators can set a plan to private (an administrator must enroll tenants to the plan) or public (tenants can subscribe themselves), list and delete subscriptions on a plan. Besides a plan's main services, administrators can create add-ons which can be subscribed to after a plan to receive additional services.

For each service, administrators can set the limit (or quota) that each tenant under that plan can use. Therefore, any Virtual Machine Cloud has two layers of limit: the

first one, set when created in Virtual Machine Manager, dictates the overall size of the whole cloud; and the second one, set in administrators' portal, dictates how much of that cloud each tenant can use.

The screenshot displays the configuration for a 'basic' plan. Under the 'usage limit' section, the following table summarizes the resource limits and settings:

RESOURCES	AVAILABLE	USE ALL AVAILABLE	USAGE LIMIT
VIRTUAL MACHINES	UNLIMITED	<input checked="" type="checkbox"/>	Unlimited
CORES	UNLIMITED	<input checked="" type="checkbox"/>	Unlimited
RAM (MB)	UNLIMITED	<input checked="" type="checkbox"/>	Unlimited
STORAGE (GB)	UNLIMITED	<input checked="" type="checkbox"/>	Unlimited

Figure 34: An example of limits on Virtual Machine Cloud in a plan

Another thing that administrators need to pay attention to when setting limits for Virtual Machine Cloud in a plan is that a gallery item will not work properly with that plan if that cloud's associated library doesn't contain resources that the gallery item requires (see Section 5.1.1).

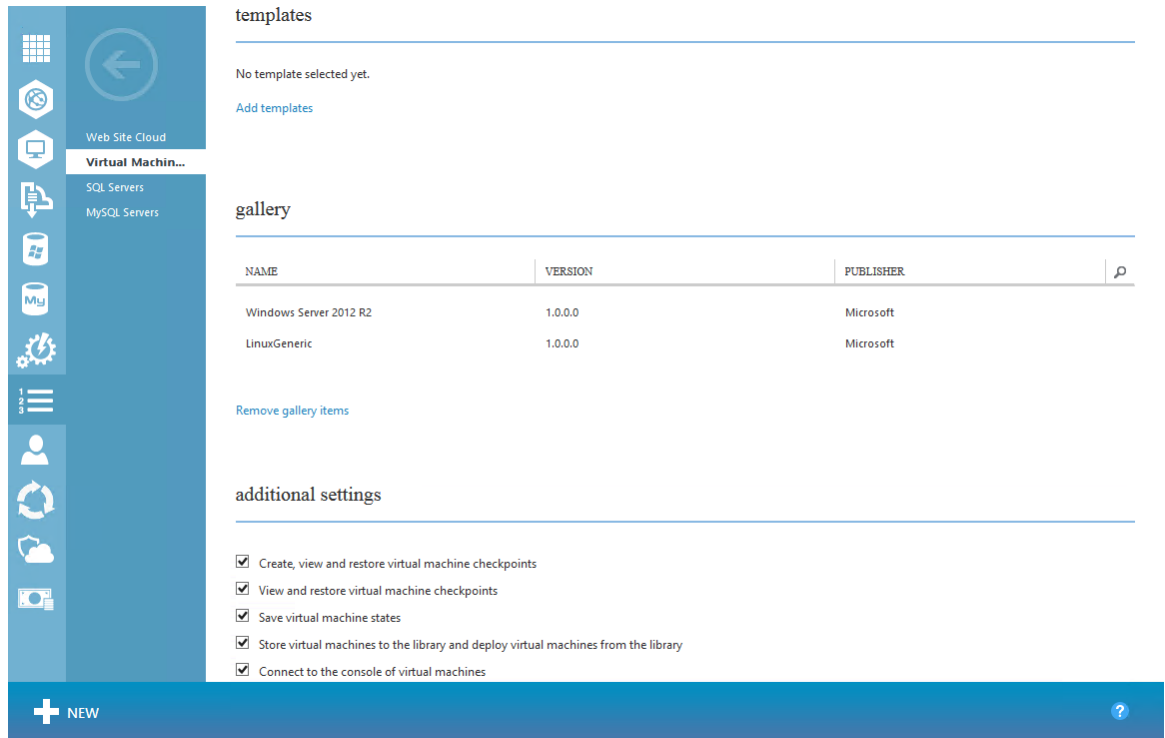


Figure 35: Selecting gallery items for Virtual Machine Cloud in a plan

## 5.2 Users' viewpoint

With all the core management components in place, the workflow for any user is as following:

- The user's domain account is created in Directory Service by an administrator
- The user accesses the tenants' portal at <https://waptenanthub.cloud.itlab.mamk.fi:30081/> or the administrators' portal at <https://wapadminhub.cloud.itlab.mamk.fi:30091/>
- The user gets redirected to Federation Service sign in page
- The user enters their own domain credential with the name in the form of *domain-account-name@cloud.itlab.mamk.fi*
- The user gets redirected back to the intended portal (figure 36)

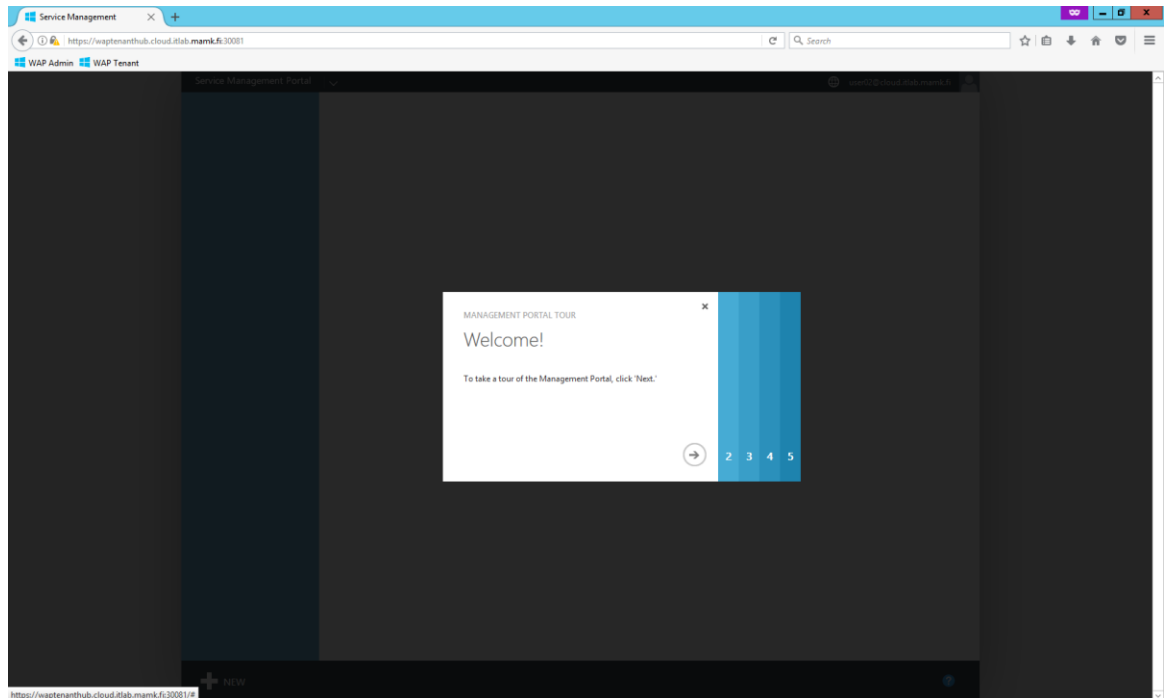


Figure 36: Users' first experience with the portal

After that, a tenant can either be enrolled to a plan by an administrator or enroll themselves to a public plan. The panel on the left of the tenants' portal shows the list of services that tenant has access to, as in figure 37. From there, tenants can deploy their own resources within the limit on their subscription without intervention from administrators.

all items				
NAME	TYPE	STATUS	SUBSCRIPTION	
wiki	Web Site	Running	Unlimited Access	

Figure 37: Tenants' portal with services

## 6 FURTHER OBSERVATIONS

The cluster was left running under observation for over a year. During that period, the system has shown many weaknesses in both technologies and designs as well as potential for improvement. These are discussed in the following sections, starting with redundancy.

### 6.1 The need for redundancy

During the observation period, the cluster has gone down several times for various reasons: system disk failure, network failure and even power failure. That is because it was built with little to no redundancy at all: each service runs on only one server without spare or load balancer, while only some physical servers come with redundancy for system data (all of them are blade servers with a built-in RAID controller). Images for virtual servers are only protected by snapshots taken inside

Hyper-V Manager on each virtualization server. Therefore, each time the cluster encountered a failure, it took a lot of time to find the broken component, replace and to reinstall it. This has a negative impact on the whole system, as the more it grows, the higher the possibility of breaking down is, the longer the downtime become, and the more complicated the troubleshooting process is.

Some redundancy measures that can be taken are as follows:

- Deploying one service on more than one server and use load balancer.
- Using RAID-1 configuration on every server.
- Taking regular backup/snapshot.
- Using teamed/aggregated connections and backup switches/routers for network infrastructure.
- Using two or more power supply for the system.

In order to implement all of these measures, there must be changes in the designs of servers, networks and support infrastructures like electricity.

## **6.2 The need for automation**

The measures mentioned in the previous section are not part of the original WAP, and therefore they are not managed and automated by WAP. As the system grows, these tasks become harder to do manually. Therefore, a certain amount of automation must be built into them. In addition to that, there should also be a monitoring system in place to check on every aspect of the system and warn of any potential problem, so that administrators can act early and accordingly before anything bad happens.

## **6.3 Enhancing the network security and performance**

Right now, the same network and subnet is used for all purposes in the cluster except for users' custom networks, and that's a bad practice with negative

consequences on both security and performance. For example, a rogue user can attempt to access the management data stream, or a file transfer across hosts can potentially slow down the whole network. Ideally, physical networks and subnets should be separated for the following purposes:

- Management/private network: This could be used for communication among servers and for administrators to do administrative tasks. All servers are connected to this network and servers that require access to external networks or the internet should access them through a gateway on this network.
- Storage network: This could be used for traffic between virtualization servers and storage servers, as well as migration traffic among virtualization servers. This network should be completely isolated from other networks.
- User public networks: These networks provide access to external networks or the internet to every users. Due to the way Hyper-V works, all virtualization servers should be connected to these networks.

Users can also create virtual networks that only the one who created has access to. These networks are also logically isolated from each other.

#### **6.4 Certificate management**

Across the deployment, I always use self-signed and self-generated certificates as well as disable certificate verification in every component; and that's not a good practice in a production environment. There are at least two cases where the lack of proper certificate management creates errors in the system:

- When I created a certificate for the remote console function for System Center, a temporary certificate according to the guide from Technet (2016) didn't work. I had to create a separate CA, added the CA's root certificate to HYPERV1's and HYPERV2's trusted store and to generate a certificate



with the same specifications from that CA. However, that's just a temporary CA and neither the official CA for the system nor trusted by any CA chain.

- The certificate generated by ADFS expired after one year, and that made the portals show error 500 when authenticated through ADFS. Commands had to be run on WAPAdminHub and WAPTenantHub to recognize the new ADFS certificate and trust ADFS again.

In a production environment, all certificates should be issued from a trusted CA in the organization.

## **6.5 Potential for development**

The main purpose of WAP is to create a private cloud environment that mimics some of the public Azure cloud's functions to help enterprises have a consistent experience across their hybrid cloud solution. However, with the development of its public counterpart, WAP now cannot provide an adequate environment to match, and therefore becomes obsolete. While it can serve as a good environment for general purposes or academic purposes, Microsoft is preparing another Azure-based solution for private cloud: Microsoft Azure Stack (Azure.microsoft.com, 2017). Azure Stack reflects better the experience that users get with the public Azure, especially the new portal instead of the old dashboard, as well as provide much more Azure services from one's own datacenter than the current three (Virtual Machine Cloud, Website and SQL/MySQL).

In this next generation of Azure-based private cloud, Microsoft has a different approach: server vendors will provide servers with Azure Stack integrated, and this makes the deployment much easier, and more use case scenarios become feasible. For example, on oceanic research ships where both power and bandwidth are limited while the amount of data generated is huge, a deployment of several servers as pre-processors can help reduce the amount of data transmitted while having the agility in processing power according to demand.

## 7 CONCLUSIONS

With the advent of new service models such as serverless computing and solid enhancements in security, public cloud is gaining popularity. However private cloud in general is also exploring new service models like managed container orchestrator and even “serverless” computing apart from virtual machine, which is the most traditional method of computing power provisioning. Vendors are also giving new approaches to private cloud, such as managed on-premise cloud in the form of a turnkey solution where vendors deliver the “cloud” to customers’ datacenter in a package with both hardware and software tightly integrated. Deployment is becoming easier, and even management can be delegated to vendors. To organizations that want to do most of the work by themselves, there are still platforms that allow them to build a system with high scalability and security.

Those evaluations are also true in the specific case of Microsoft’s solution. Besides the popularity of Microsoft Azure and other Microsoft enterprise technology in big organizations, Microsoft is also giving customers new services as well as developing the next generation of the Azure private cloud.

Throughout this project, I got acquainted with the working principle of various cloud models, especially those of private clouds. By building the whole cluster from scratch, it also gives me insights into multiple aspects of a cloud, for example security, performance, management, etc as well as methods to improve them in both software and hardware. I also learned about many technologies from Microsoft and other vendors that proved useful in this project and my subsequent projects.

In conclusion, the future of private cloud is still promising and it still stays a technology that worth investing in; more specifically Microsoft’s next-generation Azure Stack is a strong contender among private cloud solutions.

## REFERENCES

Amaris, C. and Yardeni, G. 2012. *Microsoft System center 2012 unleashed*. Indianapolis, Ind.: Sams Pub.

Amazon Web Services, Inc. 2006. *Announcing Amazon Elastic Compute Cloud (Amazon EC2) - beta*. WWW page. <https://aws.amazon.com/about-aws/whats-new/2006/08/24/announcing-amazon-elastic-compute-cloud-amazon-ec2---beta/>. Updated on 24 August 2006. Referred 29 December 2016.

Amazon Web Services, Inc. 2016. *Netflix Case Study – Amazon Web Services (AWS)*. WWW page. <https://aws.amazon.com/solutions/case-studies/netflix/>. No update information. Referred 22 October 2016.

Azure.microsoft.com 2017. *Azure Stack – Azure On-premises*. WWW page. <https://azure.microsoft.com/en-us/overview/azure-stack/>. No update information. Referred 30 April 2017.

Bhargava, R. 2015. *LDAP vs Active Directory vs JumpCloud: which is Best? - JumpCloud*. WWW page. JumpCloud. <https://jumpcloud.com/blog/ldap-vs-active-directory/>. Updated on 26 January 2015. Referred 12 October 2016.

Burns, B., Grant, B., Oppenheimer, D., Brewer, E. and Wilkes, J. 2016. Borg, Omega, and Kubernetes. *Queue*, 14(1), 70-93.

Ibm.com 2012. *Advantages and options of private cloud computing*. WWW page. <https://www.ibm.com/developerworks/rational/library/private-cloud-advantages-options/>. Updated on 17 April 2012. Referred 13 May 2017.

Martin, S. 2013. *50 Percent of Fortune 500 Using Windows Azure*. WWW page. <https://azure.microsoft.com/en-in/blog/50-percent-of-fortune-500-using-windows-azure/>. Updated on 14 June 2013. Referred 12 October 2016.

McIllece, J. 2016. *Windows Server 2012 R2 NIC Teaming User Guide*. PDF file. <https://gallery.technet.microsoft.com/windows-server-2012-r2-nic-85aa1318>.

Updated on 17 December 2016. Referred 28 December 2016.

Mell, P. and Grance, T. 2011. *The NIST definition of cloud computing*. PDF file. <http://dx.doi.org/10.6028/NIST.SP.800-145>. Updated on September 2011.

Referred 23 October 2016.

Metz, C. 2016. *The Epic Story of Dropbox's Exodus From the Amazon Cloud Empire*. WWW page. <https://www.wired.com/2016/03/epic-story-dropboxs-exodus-amazon-cloud-empire/>. Updated on 14 March 2016. Referred 22 October 2016.

Microsoft Cloud Platform 2017. *System Center 2016*. WWW page. <https://www.microsoft.com/en-us/cloud-platform/system-center>. No update information. Referred 13 May 2017.

Microsoft.com 2016. *System Center 2012 R2 Components*. WWW page. <https://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/Components.aspx>. No update information. Referred 21 March 2016.

Msdn.microsoft.com 2017. *Active Directory Federation Services*. WWW page. <https://msdn.microsoft.com/en-us/library/bb897402.aspx>. No update information. Referred 13 May 2017.

Msdn.microsoft.com 2017. *An Introduction to Claims*. WWW page. <https://msdn.microsoft.com/en-us/library/ff359101.aspx>. No update information. Referred 13 May 2017.

Oracle.com 2016. *CVE-2014-3566 - Instructions to Mitigate the SSL v3.0 Vulnerability (aka "Poodle Attack") in Java SE*. WWW page.

<http://www.oracle.com/technetwork/java/javase/documentation/cve-2014-3566-2342133.html>. No update information. Referred 19 September 2016.

Oracle.com 2017. *Oracle Integrated Lights Out Manager*. WWW page. <http://www.oracle.com/technetwork/server-storage/servermgmt/tech/integrated-lights-out-manager/ilom-362784.html>. No update information. Referred 13 May 2017.

Technet.microsoft.com 2013. *Configure Active Directory Federation Services for Windows Azure Pack*. WWW page. <https://technet.microsoft.com/en-us/library/dn296436.aspx>. Updated on 17 October 2013. Referred 13 May 2017.

Technet.microsoft.com 2013. *Install the authentication sites*. WWW page. <https://technet.microsoft.com/en-us/library/dn457760.aspx>. Updated on 17 October 2013. Referred 29 December 2016.

Technet.microsoft.com 2015. *Deploy Windows Azure Pack: Web Sites*. WWW page. <https://technet.microsoft.com/en-us/library/dn457745.aspx>. Updated on 1 June 2015. Referred 1 May 2017.

Technet.microsoft.com 2016. *Automatic Virtual Machine Activation*. WWW page. [https://technet.microsoft.com/en-us/library/dn303421\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn303421(v=ws.11).aspx). Updated on 5 September 2016. Referred 28 December 2016.

Technet.microsoft.com 2016. *How to Assign SMB 3.0 File Shares to Hyper-V Hosts and Clusters in VMM*. WWW page. <https://technet.microsoft.com/en-us/library/jj614620.aspx>. Updated 13 May 2016. Referred 20 March 2016.

Technet.microsoft.com 2016. *Remote Console in System Center 2012 R2*. WWW page. [https://technet.microsoft.com/en-us/library/dn469415\(v=sc.12\).aspx](https://technet.microsoft.com/en-us/library/dn469415(v=sc.12).aspx). Updated on 13 May 2016. Referred 7 May 2017.

Technet.microsoft.com 2016. *Windows Azure Pack architecture*. WWW page. <https://technet.microsoft.com/en-us/library/dn296433.aspx>. Updated on 30 September 2016. Referred 28 December 2016.

*Windows Server 2012 R2 Licensing Datasheet 2013*. PDF file. [http://download.microsoft.com/download/F/3/9/F39124F7-0177-463C-8A08-582463F96C9D/Windows\\_Server\\_2012\\_R2\\_Licensing\\_Datasheet.pdf](http://download.microsoft.com/download/F/3/9/F39124F7-0177-463C-8A08-582463F96C9D/Windows_Server_2012_R2_Licensing_Datasheet.pdf). No update information. Referred 28 December 2016.