A taxonomy of virtualization technologies

Master's thesis

Delft University of Technology
Faculty of Systems Engineering Policy Analysis & Management

August, 2010
Paulus Kampert
1175998

TU Delft
Delft University of Technology

Atos Origin

Preface

This thesis has been written as part of the Master Thesis Project (spm5910). This is the final course from the master programme Systems Engineering, Policy Analysis & Management (SEPAM), educated by Delft University of Technology at the Faculty of Technology, Policy and Management. This thesis is the product of six months of intensive work in order to obtain the Master degree. This research project provides an overview of the different types of virtualization technologies and virtualization trends. A taxonomy model has been developed that demonstrates the various layers of a virtual server architecture and virtualization domains in a structured way.

Special thanks go to my supervisors. My effort would be useless without the priceless support from them. First, I would like to thank my professor Jan van Berg for his advice, support, time and effort for pushing me in the right direction. I am truly grateful. I would also like to thank my first supervisor Sietse Overbeek for frequently directing and commenting on my research. His advice and feedback was very constructive. Many thanks go to my external supervisor Joris Haverkort for his tremendous support and efforts. He made me feel right at home at Atos Origin and helped me a lot through the course of this research project. Especially, the lectures on virtualization technologies and his positive feedback gave me a better understanding of virtualization. Also, thanks go to Jeroen Klompenhouwer (operations manager at Atos Origin), who introduced me to Joris Haverkort and gave me the opportunity to do my graduation project at Atos Origin. I would also like to thank Stephan Lukosch for his feedback, which helped me to be more precise.

Furthermore, I would like to thank the persons interviewed from Atos Origin, Mick Symonds, Jacco van Hoorn, Gerard Scheuierman and Joris Haverkort. Likewise, my gratitude goes to the persons from the virtualization vendors, Michel Roth (Quest Software), Jan Willem Lammers (VMware), Robert-Jan Ponsen (Citrix) and Robert Bakker (Microsoft). Orchestrating a meeting with the interviewees was not always easy and specials thanks go my supervisor Joris Haverkort from Atos Origin, who assisted me during the whole interview process and helped me find the right persons for the interviews. It was a pleasure working on this topic, although not also easy due to virtualization being a very broad concept. Through the course of the research I picked up so much information on the topic virtualization that it was sometimes difficult to determine what to include in the report and in how much detail.

Paulus Kampert
August, 2010

Graduation committee

Professor	: Dr. ir. J. van den Berg (Section of ICT)
First supervisor	: Dr. S. Overbeek (Section of ICT)
Second supervisor	: Dr. S.G. Lukosch (Section Systems Engineering)
External supervisor	: Dhr. J. Haverkort (Product manager at Atos Origin)

Management summary

The past decennium virtualization technologies have emerged in the IT world. In this period, many IT companies shifted their attention towards virtualization. Whereas competition increased, many IT companies started to develop their own virtualization technologies that have led to the development of many different types of virtualization technologies. Contemporary organizations have access to a swiftly expanding selection of computing, storage and networking technologies than ever before.

However, the increasing number of virtualization technologies from virtualization vendors have made is difficult to keep track of all the types of virtualization technologies. Furthermore, in the current body of literature there is a lot of technical information about a specific virtualization technology, but there no clear overview of all the different types of virtualization technologies. Also, for virtualization service provider Atos Origin, it is imperative to keep track of the latest developments in virtualization technologies to stay competitive. Due to the many developments by virtualization vendors, Atos Origin wants to have an overview of the virtualization domains and trends. In this report, the following research question is answered:

Which trends in virtualization technologies can be identified and how can they be structured?

The goal of this research projects is to design a structured overview of virtualization technologies and at the same time identify the virtualization trends. To answer the main research question, a taxonomy model has been made that provides a structured overview of the virtualization domains. The research methods that have been used can be characterized as Design Science Research (DSR). The data collection consisted of literature papers, documents from Atos Origin, presentations from events and interviews with experts from Atos Origin and virtualization vendors, VMware, Citrix, Microsoft and Quest Software. Also, during the course of the research project, the case study research method has been used to evaluate the taxonomy model and to identify the virtualization trends.

In the analysis phase of the research, it became apparent that there are many types of virtualization technologies that can be categorized into several virtualization domains. Also, many virtualization technologies still have to mature and are accompanied with many challenges, in particular management and security. At this point of the research, a taxonomy model was made to structure the different types of virtualization technologies. Subsequently, the taxonomy model was evaluated by using the case study research method where at the same time trends in virtualization technologies were identified.

The case study provided a lot of constructive remarks on the taxonomy model and information about the main virtualization trends. The overall findings of the virtualization trends indicated that desktop virtualization and management technologies are becoming very popular and have received much attention by virtualization vendors. Reasons for its popularity are the need by organizations for seeking new flexible and easier methods of offering work places and the limited functionalities of traditional management tools for virtual environments that have hinder successful management. The case study showed that there are many issues regarding management of virtual environments, such as configuration management and capacity management. Also, it showed that the main business reasons for virtualization are in particular cost savings. New management tools are being developed that must

tackle many of the virtualization challenges, thereby reducing the complexity of controlling virtual environments, which can also lead to additional cost savings. Furthermore, security has become more critical to address, because virtualization has brought new security challenges. Security technologies for virtualization are currently receiving more attention by virtualization vendors and better virtualization aware security technologies are expected to make their appearance very soon.

However, the remarks made by the virtualization experts on the taxonomy model led to a revision of the first taxonomy model. While the first taxonomy did provide an overview of the different types of virtualization technologies, it lacked to show the relations and dependencies between the virtualization domains. Also, not all virtualization domains were shown clearly. Therefore, a new taxonomy model was designed using a layered approach that was able to structure the virtualization domains in such a way that it illustrates their relations as well as their dependencies. The taxonomy model demonstrates the various layers of a virtual server architecture and virtualization domains in a structured way.

Finally, for Atos Origin the following recommendations were made based on the findings of this research project:

- Desktop virtualization is expected to continue and increase its growth significantly in the years to come. However, combining desktop virtualization with application virtualization and user state virtualization hold interesting business opportunities. Application virtualization is currently offered as a separate service. Combining this service with desktop virtualization and user state virtualization allows for a better desktop service offering. This combination is also called the three layered approach and is different from standard VDI solutions.

- Interesting developments are happening for virtualization security technologies. Keep an eye out for new virtual security appliances, as it can help providing better security solutions to the customer.

- New management tools for virtualization tackle a lot of management issues and hold interesting business opportunities. These management tools can offer clients better control of their virtual IT environment and can be provided via a new virtualization management service.

Table of contents

1. Introduction 1

1.1 Research problem 2

1.2 Research questions 3

1.3 Research methodology 3

2. Conceptualization 6

2.1 Definition of virtualization 6

2.2 Role of virtualization in data centers 7

2.3 Summary and outlook 8

3. Analysis: Part I 9

3.1 Virtualization domains 9

3.2. Virtualization domains of Atos Origin 22

3.3 Summary and outlook 23

4. Analysis: Part II 25

4.1 Virtualization journey 25

4.2 Virtualization challenges: two examples 26

4.3 Current developments 28

4.4 Summary and outlook 31

5. Taxonomy model of virtualization technologies 33

5.1 Modeling Language 33

5.2 Taxonomy model 33

5.3 Summary and outlook 38

6. Evaluation using case study method 40

6.1 Case Study 40

6.2 Case 1: internal group 41

6.3 Case 2: external group 43
6.4 Conclusion of case studies 44
6.5 Quality of Case study 46
6.6 Summary and outlook 47
7. Revised taxonomy model of virtualization domains 48
7.1 Layers of the taxonomy model 49
7.2 Conclusions 51
8. Reflection 52
9. Conclusions & Recommendations 53
9.1 Conclusions 53
9.2 Recommendations for Atos Origin 55
Literature 58
Appendix A: History of virtualization 66
Appendix B: Terminology 68
Appendix C: Benefits and challenges of virtualization 71
Appendix D Case study interviews 79

1. Introduction

Contemporary organizations have access to massive amounts of computing technologies. A remarkable recent trend is the advent of virtualization technologies. While the origins of virtualization go way back to the large mainframe period, virtualization has been reintroduced to servers, desktop computers and many other IT devices of today [1]. The reintroduction of virtualization received much interest and many IT companies shifted their attention towards virtualization [1]. Whereas competition increased, IT companies eagerly developed many new virtualization technologies, which have led to the development of many different types of virtualization technologies [2].

In general, virtualization attempts to reduce complexity by separating different layers of software and hardware. This enables an organization to interact with their IT resources in a more efficient way and allows for a much greater utilization. Therefore, virtualization technologies have rapidly become a standard piece of deployment in many IT organizations. An example of virtualization is depicted in figure 1. On the left a traditional IT infrastructure is depicted and on the right a new IT infrastructure is depicted that uses virtualization. An IT infrastructure can be seen as everything that supports the flow and processing of information such as the physical hardware that interconnects computers and users, plus the software that enables sending, receiving and management of information [3].

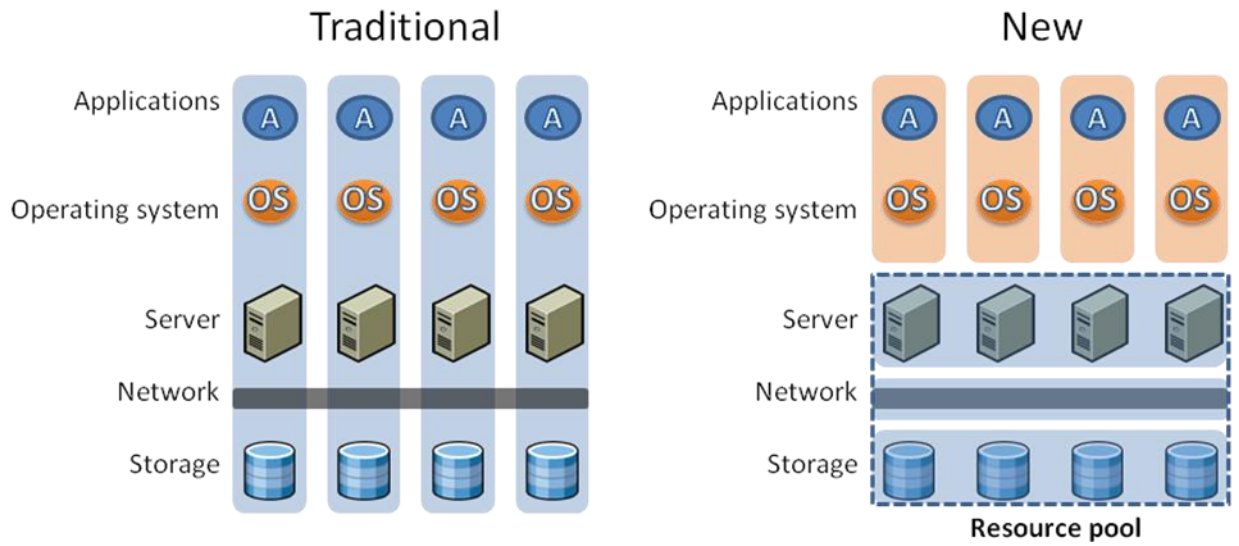

Figure 1 Traditional and new IT infrastructure

In figure 1, both IT infrastructures consist of a storage, network, server, operating system and application layer. In the traditional setting, all the components of one layer are connected to a single component of another layer. Each server is comprised of one operating system, a set of applications, a network and a storage device. The network connects the different servers and storage systems together and can also connect the server to other public IT infrastructures such as the internet or private IT infrastructures from other organizations.

On the left, the vertical blue pillars point out a specific type of configuration of applications, server, network and storage system. When there is a failure of a component in one of the layers, the

whole pillar is affected. For example, when there is a hardware failure in a server, the whole blue pillar becomes dysfunctional. Until the hardware failure is repaired the operating system and applications on that particular server are down.

On the right, the horizontal blue pillars display the new configuration of servers, network and storage that now function as a pool of resources. The software, marked by orange pillars, on top of the servers show that it is not tied to a specific server or hardware configuration. This means that if one server has become non-operational the applications can continue to function on another server in the resource pool.

The example of figure 1 shows a small portion of the many features of virtualization technologies [4]. There are many different virtualization technologies that concentrate on particular layers of the IT infrastructure that together enable the transformation of a traditional IT infrastructure into a virtual IT infrastructure. Currently, there are many virtualization vendors that offer the same kind of virtualization technologies, but use a different approach and implementation method underneath. Atos Origin, who is a virtualization service provider, uses virtualization technologies of different virtualization providers to provide suitable IT solutions according to the wishes of their clients, which are often large enterprises.

In the following sections the research of this master's thesis is described. In section 1.1, the research problem is explained, which leads to the research questions in section 1.2. The research method for answering the research questions is described in section 1.3.

1.1 Research problem

As was mentioned in the introduction, many IT companies entered the virtualization market. Furthermore, the growth of virtualization vendors has led to the development of many different virtualization technologies [2]. Possibilities of virtualization seem to be endless, seeing that new virtualization technologies keep on making their appearance [4]. This has made is difficult to keep track of all the types of virtualization technologies that are available. The current body of literature shows that there is a lot of technical information about a specific virtualization technology, but there no clear overview of virtualization technologies [5, 6, 7, 8, 9, 10].

Furthermore, for Atos Origin it is imperative to keep track of the latest developments in virtualization technologies to be competitive as a virtualization service provider [11]. Due to the many developments by virtualization vendors, Atos Origin wants to have an overview of the virtualization domains and trends. At the moment Atos Origin offers five types of virtualization services: server, desktop, application, storage and disaster recovery virtualization. However, other types of virtualization technologies might hold interesting business opportunities for Atos Origin.

The goal of this research is to design a model that illustrates the different virtualization domains. To do this, a taxonomy model is designed and evaluated in a valid way that provides a taxonomical classification of the virtualization technologies that also explicates the relations between the technologies. By taxonomy we mean "A model for naming and organizing things [...] into groups which share similar qualities" [12]. A taxonomy model is used, because it allows an overview of virtualization technologies to be presented in a visual and logical way. It can be used as a reference model to show the different types and layers of virtualization technologies, but also to indicate what virtualization technologies have become important, based on current trends.

1.2 Research questions

The research problem made it clear that one of the latest IT trends is the emergence of virtualization technologies. Much literature can be found about a certain virtualization technology, but there is no clear overview of the different virtualization technologies. Also, for Atos Origin it is considered to be very important to keep track of the latest trends, because new virtualization technologies can hold new business opportunities. Following the problem statement the main research question can be formulated as:

Which trends in virtualization technologies can be identified and how can they be structured?

To answer the main research question a taxonomy model has been made. The following sub questions have been posed that helped answering the main research question:

1) What virtualization technologies are currently available? (Chapter 3)
2) What are the current developments in virtualization technologies? (Chapter 4)
3) How can the virtualization technologies be structured? (Chapter 5,7)
4) What are the virtualization trends? (Chapter 6)

1.3 Research methodology

The research method that has been used to answer the main research question can be characterized as Design Science Research (DSR). DSR is a research method that is used for the development of artifacts to solve problems. Artifacts are objects made by humans. Generally, DSR focuses on creating and evaluating innovative artifacts that enable organizations to address important information-related tasks [13]. Design research is often applied to categories of artifacts including (but not limited to) algorithms, human and computer interfaces, design methodologies and languages [14]. The taxonomy model that has been developed in this research can be characterized as an artifact. In this case, the artifact presents a structured overview of virtualization technologies and their relations. The research process of a DSR commonly consists of formulating a design, conducting an experiment and evaluating results [15]. The research method DSR is used, because it is best suitable for this research. An artifact has been created with the purpose of solving the research problem that was addressed in section 1.1.

On the next page, the research process is depicted in figure 2. The research process is based on the design science research guidelines of Hevner (15). These DSR guidelines specifically describe the design, evaluation and results process of figure 1. The research process is made up of five phases of which the first two phases were added to the research process, because for the design of the taxonomy model preliminary steps were taken. These steps include an explanation of virtualization terms, concepts and an extensive research on virtualization technologies to provide the researcher a basic understanding of virtualization. The data collection consisted of literature papers, documents from Atos Origin, presentations from events and interviews with virtualization experts. The data has been used to create an overview and basic understanding of the different types of virtualization technologies, and are the input for the design of the taxonomy model. The output of the design has been used to answer the second part of the main research question. For the first part of the research question, interviews with experts from Atos Origin and virtualization vendors were used to evaluate the taxonomy model and to identify virtualization trends.

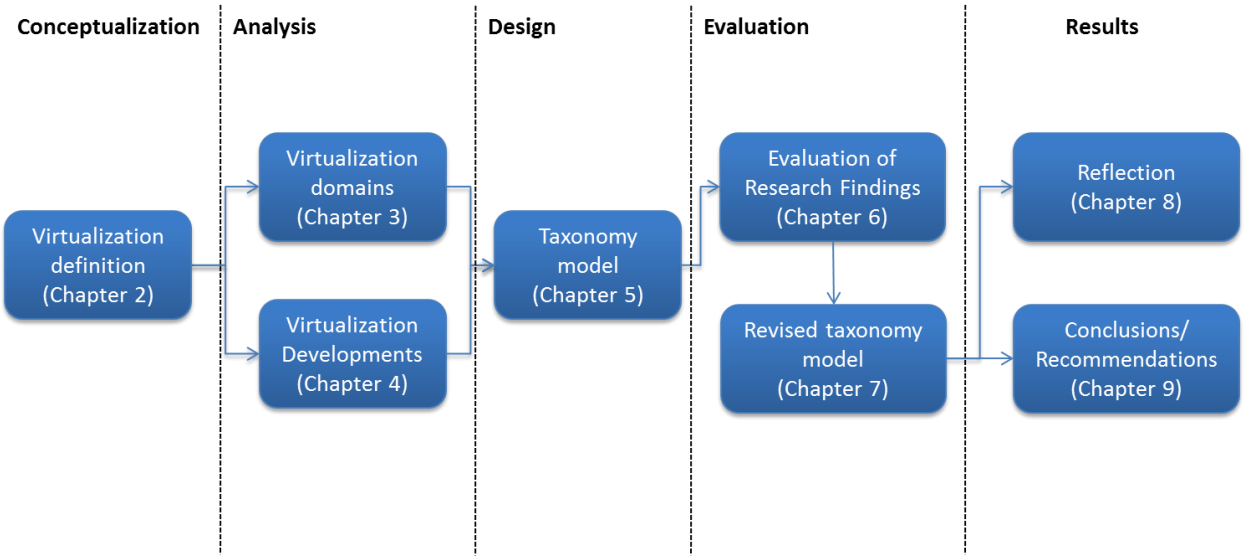

Figure 2 Research process based on Design Science Research [15]

In figure 2, a distinction can be made between five phases:

Phase 1: Conceptualization

In the conceptualization phase, the term "virtualization" is defined. Furthermore, a short introduction is given that elaborates on the role of virtualization in data centers and how the technologies are being used.

Phase 2: Analysis

The analysis phase consists of two parts: virtualization domains and current developments. In part I, the different domains of virtualization technologies are discussed in which the first research question is addressed. Also, during part I an overview has been made of the benefits and challenges of virtualization technologies of each domain. This part of the analysis can be found in Appendix C and serves as additional reading material that provides additional insight in virtualization technologies. In part II, the virtualization developments have been analyzed for new types of virtualization technologies. Information is used from papers, presentations and interviews. The results of part II led to the findings of additional virtualization technologies for the taxonomy model and hold the answer to the second research question.

Phase 3: Design

For the design phase, information from the analysis phase has been used as input for the taxonomy model. In the taxonomy model, the virtualization technologies have been structured. By structuring the virtualization technologies an overview is created of the different types of virtualization technologies. The third research question is addressed in the design phase.

Phase 4: Evaluation

After the design phase, the taxonomy model has been evaluated using the case study research method in which the findings of the previous phases were evaluated. In the validation phase, the taxonomy

model is evaluated by using two cases. In the first case, virtualization experts from Atos Origin have been interviewed and in the second case experts from well-known virtualization vendors. The case study has been used to evaluate and improve the taxonomy model, but also to identify virtualization trends. The results of the case study provided the answer of the fourth research question. Also, the validity of the case study was tested by applying several validity tests. Furthermore, the results of the evaluations have led to a revision of the taxonomy model of phase 3.

Phase 5: Results

In the last phase, a reflection is made on the course of the research. Also, conclusions have been drawn from the research results to answer the main research question. In the recommendations the conclusions are used to indicate and discuss business opportunities for Atos Origin.

2. Conceptualization

In section 2.1, a definition of virtualization is formulated that is used throughout the research project. Furthermore, a short notion is given about the similarities of virtualization with simulation and emulation. In section 2.2, the role of virtualization in data centers is discussed. The reason for this is to familiarize the researcher with the concept data center and create a basic understanding about the role of virtualization in data centers. Section 2.3 provides a summary of this chapter and an outlook on the following chapters.

2.1 Definition of virtualization

Virtualization may be a difficult term to grasp. If this is the case, background reading about the history of virtualization is recommended and can be found in appendix A. To understand more about the research environment, virtualization needs to be defined. However, defining virtualization is not an easy task, as there are different types of virtualization and a definition that would be adequate for all is not easy to achieve. Most definitions of virtualization often refer to a single type of virtualization, which is server virtualization. Singh [16] for example describes virtualization as a "framework or methodology for dividing the resources of a computer into multiple execution environments by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, quality of service, and many others". Similarly, Kiyanclar [17] describes virtualization as "the faithful reproduction of an entire architecture in software, which provides the illusion of a real machine to all software running above it".

Most of the definitions are correct if we only consider server virtualization. According to Ray [18], the term virtualization refers to technologies that are designed to provide a layer of abstraction between computer hardware systems and software running on them. Virtualization provides a logical view of looking at computing resources to simplify interaction with them. However, we think this definition is also incomplete as virtualization not only provides a layer of abstraction between hardware and software, but also between layers of software. An example is application virtualization, which is described in chapter 3. With application virtualization, there is an abstraction layer between the operating system and application. Therefore, for this research project we have adapted our own definition:

Definition: *Virtualization refers to technologies that are designed to provide a layer of abstraction between layers of hardware and software, as well as layers of software that enables a more simplified interaction with it.*

Terminology

The word "virtualization" in the definition above is American English. According to British English the word "virtualisation" should be used. In this research, American term is used, as it is the most commonly used version on the Internet and in the literature. Furthermore, many of the new terminology that is used to describe virtualization technologies can be confusing. Therefore, the meanings of common virtualization-related terms that are used throughout this research are described in Appendix A.

Simulation & Emulation

In the process of understanding and defining what virtualization is, one might think that virtualization is the same as simulation or emulation. Although virtualization has characteristics of both is not exactly and only simulation or emulation. Reading definitions such as those of Singh, as described above, it is understandable that the relation or connection of simulation and emulation with virtualization can be very difficult [16, 20]. Looking at what virtualization does, imitating the behavior of the 'real' thing, much resembles a simulation. Simulation and virtualization are very much intertwined and can be confusing. Looking at the definition [20], simulation is the imitation of the operation or features of one system using another system. It is pretending to be the other system. Virtualization is a technology that is about running virtual copies of servers, which is looks like pretending as well. The difference between the two is that simulation does not do the real thing, but creates a virtual object or representation of the real thing with that needs to behave likewise. Simulation requires a model of the virtual object in order to do anything, meaning that a virtual representation of the real object is needed [20]. Virtualization converts a server into a virtual server with the only difference that it is not just a virtual representation of the real object, but it is the real object. Therefore it is not just pretending to be the real object.

Emulation is a type of virtualization and part of server virtualization, which is discussed in chapter 3. Emulation comes from the verb "emulate", which means to imitate or reproduce. Therefore, computer emulation is when one system imitates or reproduces another system [21]. Server virtualization decouples the operating system and applications from the hardware layer below, which are called virtual machine. This virtual machine, which basically consists of an operating system and application(s), emulates hardware components by using a set of drivers. Drivers are a small piece of software that tells the operating system and applications how to communicate with the hardware [31]. It emulates its own hardware by looking at what hardware is available and creates its own virtual version of the hardware. This way, when hardware configuration changes are made or when there is a hardware failure the virtual machine is able to continue its operation on the same or another server without re-installing the operating system, applications and drivers.

2.2 Role of virtualization in data centers

Virtualization has become a major IT industry trend in data centers, storage systems and even personal computers (PCs) [22]. Data centers are facilities that household a large collection of computer systems and their associated components. They are also called server farms. Data centers are prone to a limited life span as computing demands increase in time. Therefore, organizations seek to optimize their data center to get to most out of their data center and hopefully increase their life span [23]. Virtualization technologies allow an organization to optimize their data center in terms of space, costs and management. For example, virtualization is often used reduce the number of servers by turning multiple servers into virtual machines and running them on one server. This is also known as server consolidation [24].

Considering the economic climate of the past years, virtualization is considered as the solution to lower capital and operating costs by reducing the number of servers. Data centers require significant amounts of computer hardware, power and cooling [23]. Virtualization technology impacts all these factors and that is why virtualization has become increasingly popular in data centers. However, the benefits and impacts of virtualization reach much further than cost savings. The benefits depend on the

kind of virtualization technology that is going to be used and if it's suited to the needs and goals of the organization [18].

A basic understanding of the different virtualization technologies is imperative for an organization to know which virtualization technologies are interesting for their data center and what they want to achieve. Optimizing a data center is considered to be a complex task in which virtualization technologies can have implications for every business area [25].

2.3 Summary and outlook

The definition that is used in this research states that virtualization provides a layer of abstraction between layers of hardware and software, as well as between layers of software that enables a more simplified interaction with it. Also, virtualization looks very similar to simulation and emulation. It has characteristics of both simulation and emulation, but is not one and the same. Furthermore, virtualization has become increasingly popular in data centers. Data centers are facilities that household large collections of computer systems and their associated components. Virtualization technologies have become very popular in data centers, because it holds many benefits for large collections of computer systems.

In the next chapter, different types of virtualization technologies are analyzed. The analysis phase consists of two parts. In part I, the different types and domains of virtualization technologies are described. In part II, the current developments have been analyzed to look for new types of virtualization technologies.

3. Analysis: Part I

In this chapter, the different types of virtualization technologies that can be found in literature have been explored. In section 3.1, virtualization technologies are categorized into five domains. The five domains are explained and described in sub sections 3.1.1 to 3.1.5. In section 3.2, the virtualization domains are explained that Atos Origin currently is active in. The chapter closes with a summary and an outlook on the next chapter.

3.1 Virtualization domains

In this chapter an overview has been made of virtualization technologies. The data collection in this chapter consists mainly of literature and documents from Atos Origin. In the following chapters, information from virtualization events and interviews are also used to examine the virtualization developments in which additional types of virtualization technologies have been found. Literature reveals that there are many different types of virtualization technologies that share a common area of interest [26, 27]. Hence, these different types of virtualization technologies have been categorized into domains. Each domain contains a group of technologies that share a common area of interest.

In this chapter, a distinction is made between five virtualization domains: server, application, desktop, storage and network virtualization. Each domain and their virtualization technologies are explained in the following sections. An attempt is made to use universal terms to describe the virtualization technologies. Virtualization vendors often use their own technical terms or name for certain virtualization technologies. This can be confusing. Hence, a general description of the virtualization technologies is given. More detailed descriptions of virtualization technologies require detailed information of virtualization products from virtualization vendors. Products of similar virtualization technologies of virtualization vendors are different underneath and an attempt to describe all the virtualization products from virtualization vendors is too extensive and not the goal of this research. However, an effort is made to provide the reader plenty of detailed information to understand the virtualization domains. In appendix B, an overview can be found with technical terms that are being used and provides a short explanation. In section 3.1.1 till 3.1.5, the virtualization domains, server, application, desktop, storage and network are described consecutively.

3.1.1 Server virtualization

Server virtualization is the main virtualization domain in which a (physical) server is converted into a virtual server. A physical server is often used term by virtualization vendors to describe the difference between a virtual server and a physical server [28]. The term physical server refers to the hardware that does the actual computing processing imposed by the software, such as operating system and applications. A virtual server cannot operate without a physical server. With server virtualization, multiple physical servers can be converted into virtual servers and be placed on one physical server, which is called the host. The virtual servers are called the guests. In figure 3, the difference between a traditional server architecture and virtual server architecture is shown.

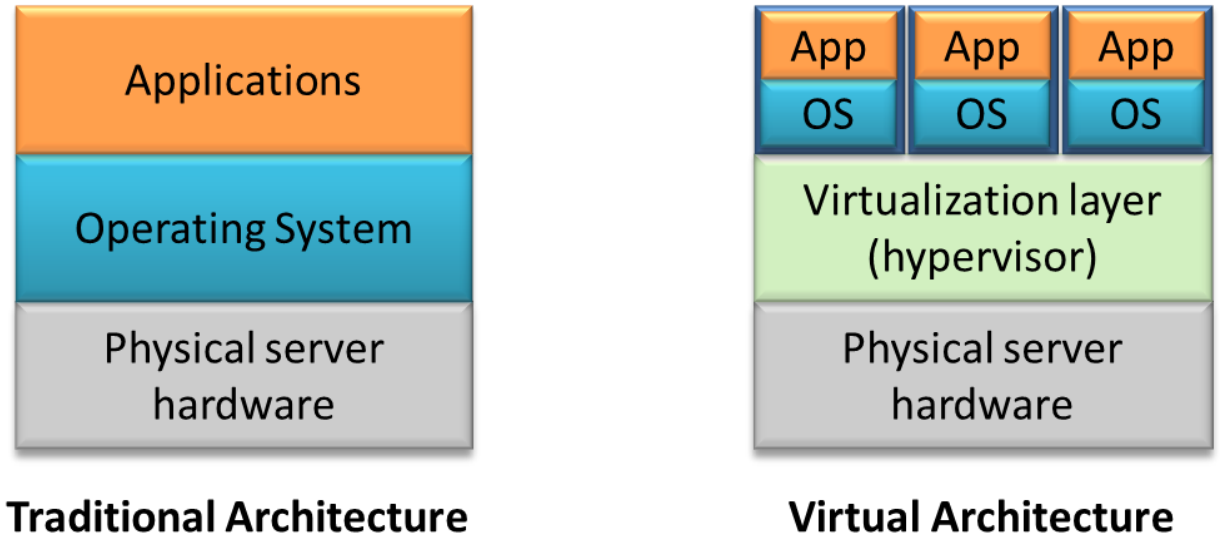

Figure 3 Traditional vs. Virtual, adapted from [33]

In figure 3, both the traditional and virtual architecture show their server architecture. On the bottom layer, both architectures are composed of a set of computing hardware such as a Central Processing Unit (CPU), memory, Network Interface Card (NIC) and a local hard disk. The hardware is placed inside a box or casing and is called a physical server on which software, an operating system (OS) and application(s), are installed on top. However, installing operating systems or applications on a traditional server architecture is very vulnerable to changes or failures on the hardware layer. Changes to the hardware configuration or hardware failures immediately result into an operating system malfunction, which means that the physical server need to be repaired with the same configuration of hardware or else requires a reinstallation of the operating system (OS) and applications.

With server virtualization, a virtualization layer is placed above the physical server hardware and beneath the operating system and application layers. The virtualization layer makes it possible to install multiple set or instances of operating system and applications on one physical server. Each set of operating system and applications functions similar to the traditional server architecture, with the difference of running multiple instances on a physical server instead of only one instance. Furthermore, the virtualization layer isolates each set or instance from each other, which makes it unaffected for failures or changes of other instances or hardware. All instances think that they are the only instance on the physical server. These instances are called virtual machines or virtual servers. As was shown in figure 1 of the introduction, server virtualization decouples software (OS and applications) from a particular set of hardware, which makes it independent of a specific configuration of hardware that is needed in order to function. This way, a virtual machine can operate on physical servers that use different hardware configurations underneath.

Another characteristic of server virtualization is that a traditional physical server with a specific configuration of an OS and applications can be converted into a virtual server or virtual machine [28]. Originally, Popek and Goldberg [29] defined virtual machines (VM) as an efficient, isolated duplication of a real machine. A real machine refers to a traditional server architecture with one only OS and

application(s). However, the use of virtual machines with server virtualization goes beyond the duplication of a real machine.

Virtual Machine

A virtual machine (VM) is the virtual representation of a physical server and composed of an operating system and one or more application(s). Throughout this research report, a virtual machine (VM) is represented in the following manner, depicted in figure 4.

Figure 4 Representations of a Virtual Machine (VM)

In figure 4, two representations are shown of a virtual machine (VM), which is either illustrated as a box with an OS and application icon or the abbreviation VM. A virtual machine is typically comprised of either a single file or a group of files that can be read and executed by the virtualization layer. Each virtual machine is a self-contained operating environment that behaves as if it is a separate computer. The different virtual machines are not aware of each other. The virtual machines are built in such a way that they are isolated, which means that they are unaware of other virtual machines being present on the same physical server [30].

A virtual machine uses emulation to imitate a complete set of hardware such as CPU, memory, NIC, etc. This is done by using a set of drivers that are compatible with different kinds or types of hardware. Drivers are a small piece of software that tells the operating system and applications how to communicate with the computer hardware [31]. The drivers are built in a virtual machine and can be used for different configurations of hardware. With these drivers a virtual machine generates a virtual version of the physical hardware and creates a virtual CPU, virtual memory, virtual Network Interface Controller (NIC) card, virtual hard disk and other types of hardware that might be needed. When a virtual machine is started or online, a certain amount of CPU processor capacity, memory and disk space is assigned automatically by the virtualization layer or hypervisor.

To implement a virtual machine, a virtualization layer is added to a physical server to support the desired architecture. By doing so, a VM can circumvent hardware compatibility and resource constraints [30]. This virtualization layer is often called hypervisor.

Hypervisor

A hypervisor, also known as the virtual machine monitor (VMM), is the host layer of software that enables multiple virtual machines or operating systems to operate on a single physical server [32]. There are two types of hypervisors called “Type 1” and “Type 2” [34]. Type 1 is a hypervisor that is installed directly on the hardware and is also called a “bare-metal” hypervisor. Type 1 hypervisors are positioned between the hardware and virtual machines. The hypervisor in figure 3 is a “bare metal” hypervisor. Type 1 hypervisors are dominantly used on the server market [34].

Type 2 is a hypervisor that is installed on top of an operating system and is also called “hosted”

hypervisor. In contrast to type 1, the hypervisor is placed above the operating system and not below the operating system or virtual machines. This allows for an additional operating system to be run in a virtual environment on top of an existing operating system. Hosted hypervisors can be used to run a different type of operating system on top of another operating system. For example, if a user with a Mac OS wants to run an application that is designed for Windows, he or she can run a Windows OS in a virtual environment on top of the Mac OS and vice versa [35]. In figure 5, both types of hypervisors are shown.

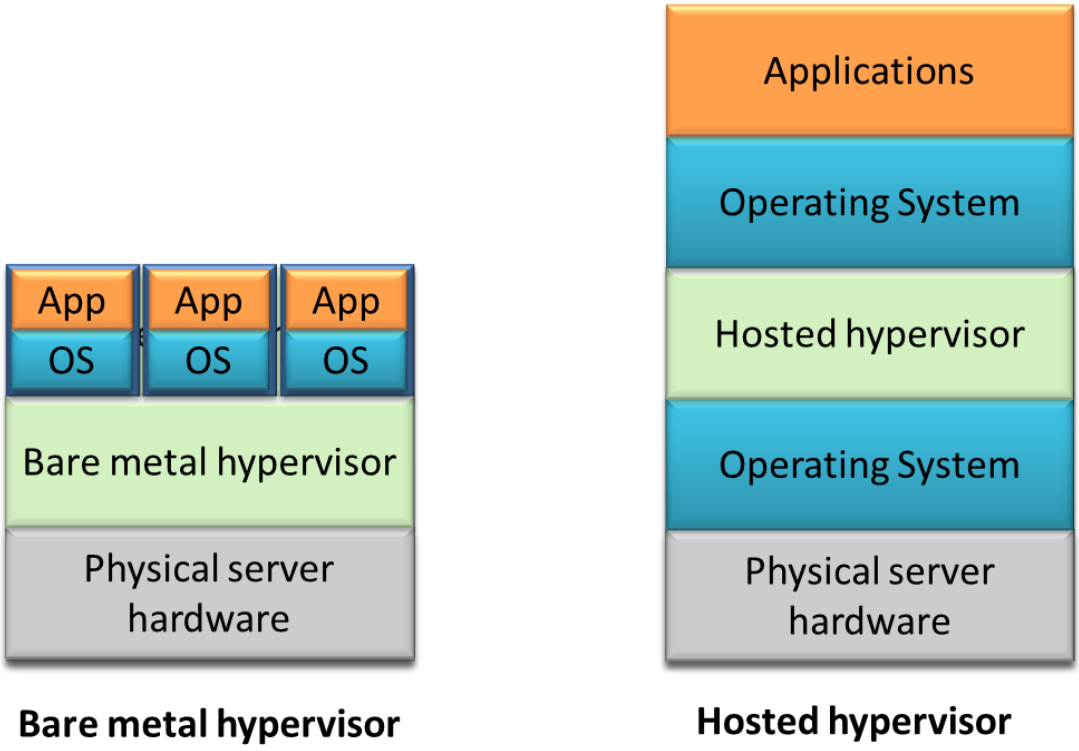

Figure 5 Bare metal and hosted hypervisor

In general hypervisors are directly responsible for hosting and managing virtual machines on the host or server [36]. The host is another name for the physical server and hypervisor. The virtual machines that run on the host are called guest VM or guest operating system [32]. Furthermore, a hypervisor provides a uniform view of the underlying hardware, which means that it can operate on hardware of different vendors. Hence, virtual machines can run on any available and supported computers, since the hypervisor isolates software from hardware [37]. System administrators, who maintain and operate a computer system and network, are also able to view their hardware as a pool of resources, which allows new functionalities that are described below.

Hypervisors are equipped with several different technologies, which vary depending on the virtualization vendor. However, there are some common technologies that are widely known and used by different virtualization vendors that bring out the features and benefits of server virtualization. The common features of hypervisors are “High Availability (HA)”, “Fault Tolerance”, “Live migration”, “Distributed Resource Scheduler (DRS) and Distributed Power Management (DPM) [38, 39]. The last two

are names that are specifically used by VMware, who was the first with these technologies. Since no other common name has been found in literature, the VMware terms are used.

High availability is a technology that continuously monitors all virtual machines running in the virtual resource pool, looking for a hardware failure [40]. The virtual resource pool is a set of resources or physical servers which run virtual machines. When a physical server fails the VM is automatically restarted on another server. This is depicted in figure 6.

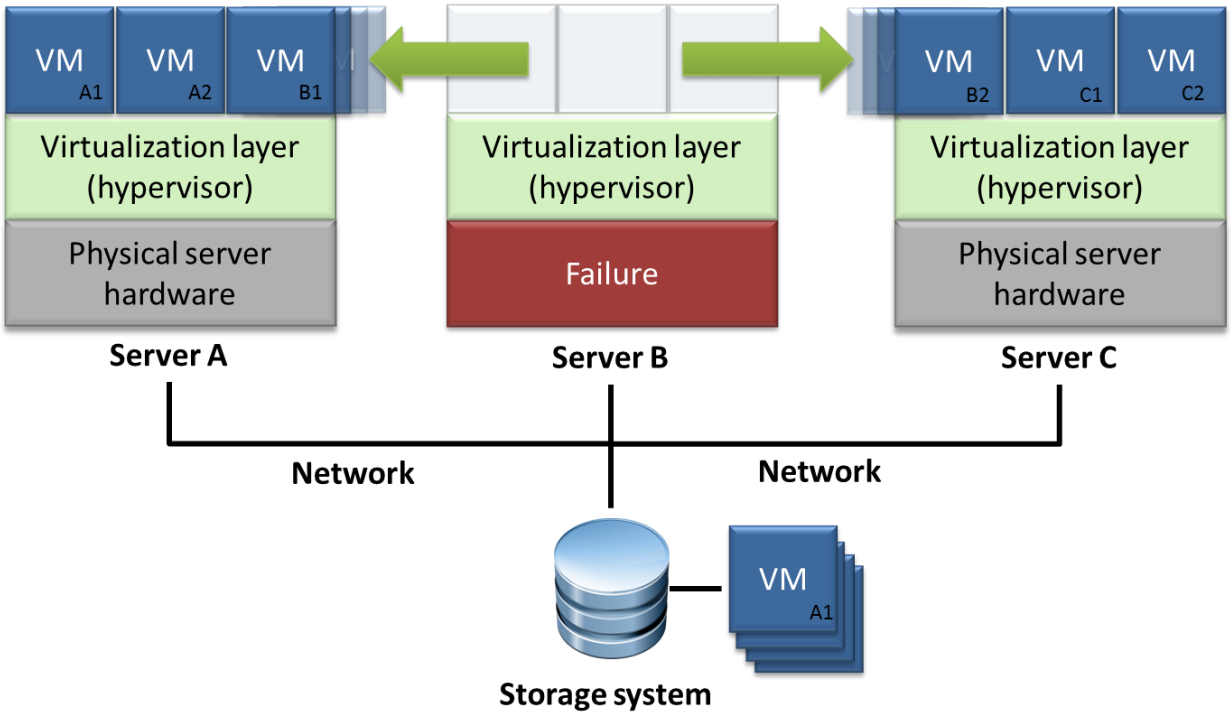

Figure 6 High Availability, adapted from [33]

In figure 6, there are three physical servers. When there is a failure in server B, the virtual machines B1 and B2 are restarted on server A and server C. This can be done, because images of the virtual machines are stored in the storage system, which the servers are connected to. However, depending on how active the user is, a hardware failure can lead to data loss. The current state of the VM is not saved, which means that the changes made by the user are not saved. There is only a "clean" backup image of the VM on the storage system. However, this problem is solved with fault tolerance (FT). Fault tolerance goes a step beyond high availability and runs an identical copy of the VM on another server. As a result, there will be no data loss or downtime. This is illustrated in figure 7.

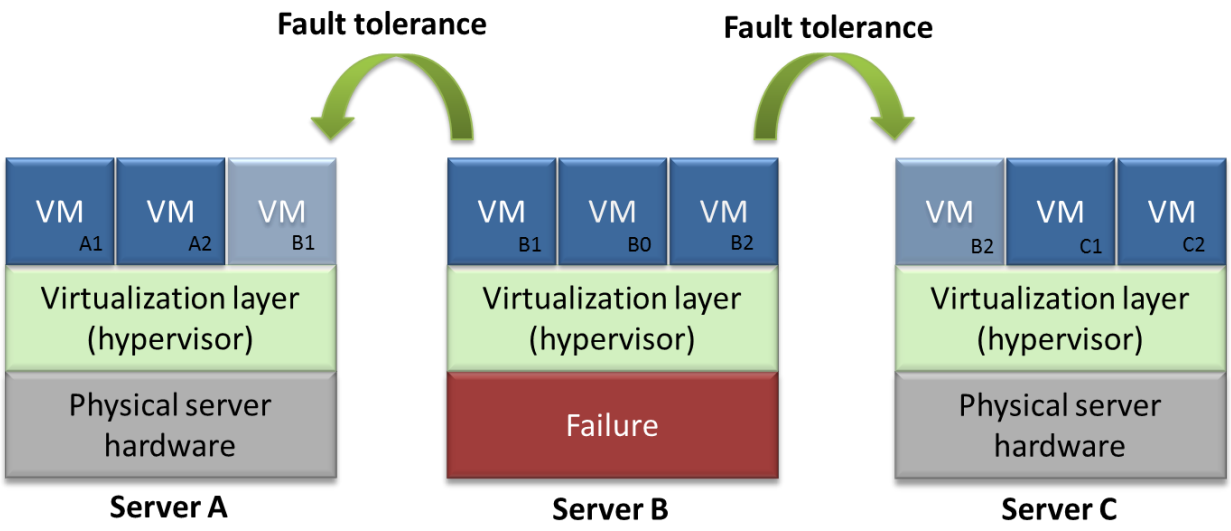

Figure 7 Fault Tolerance, adapted from [33]

In figure 7, fault tolerance is used for virtual machine B1 and B2. With fault tolerance copies of B1 and B2 will be run and maintained on a separate host or physical server in real-time. Every instruction of the primary VM will be executed on the secondary VM as well. When server B fails, B1 and B2 will continue on server A and C without any downtime. The technology to move virtual machines across different hosts or physical servers is called live migration. An example of a live migration is depicted below in figure 8.

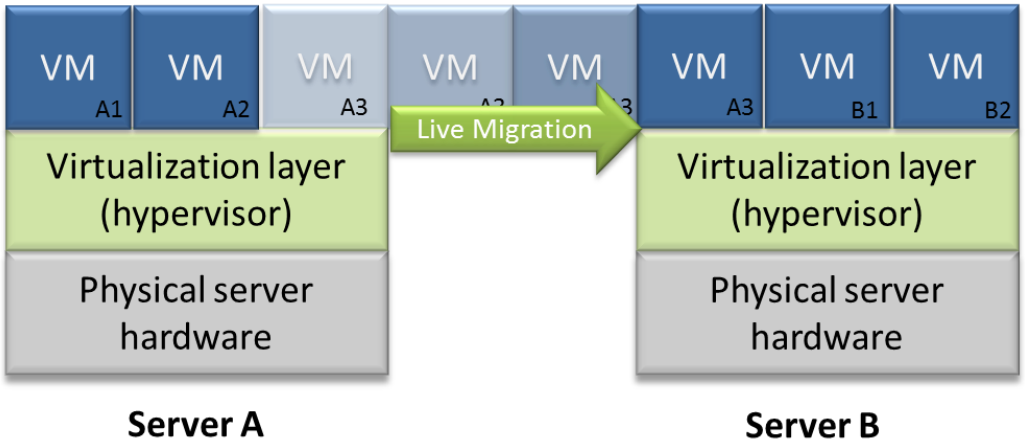

Figure 8 Live Migration, adapted from [33]

In figure 8, virtual machines are migrated or transferred from one host to another. Possible reasons for live migration can be that the workload of a server is becoming very high and as a precaution transfers VMs to another server, but also for server maintenance purposes. Workload is to the amount of processing that the computer has been given to do at a certain time. Because a virtual machine (VM) is hardware (configuration) independent, it is not dedicated to a single physical server or hardware configuration and can be moved from one server to another even when it is in operation. This makes it

possible to balance capacity across servers that will ensure that each virtual machine has access to appropriate resources in time. The technology to balance server capacity is called Distributed Resource Scheduler (DRS) or load balancing. The DRS continuously monitors utilization across physical servers and allocates available resources among the virtual machines, which can be based on pre-defined rules. Virtual machines with important business applications can be given higher priority and more resources will be made available for these virtual machines [39]. Furthermore, Distributed Power Management (DPM) is used to optimize power consumption in a data center. When virtual machines need fewer resources in evenings or weekends, the VMs of low utilized servers can be moved to other servers and are powered off. An example is depicted below in figure 9.

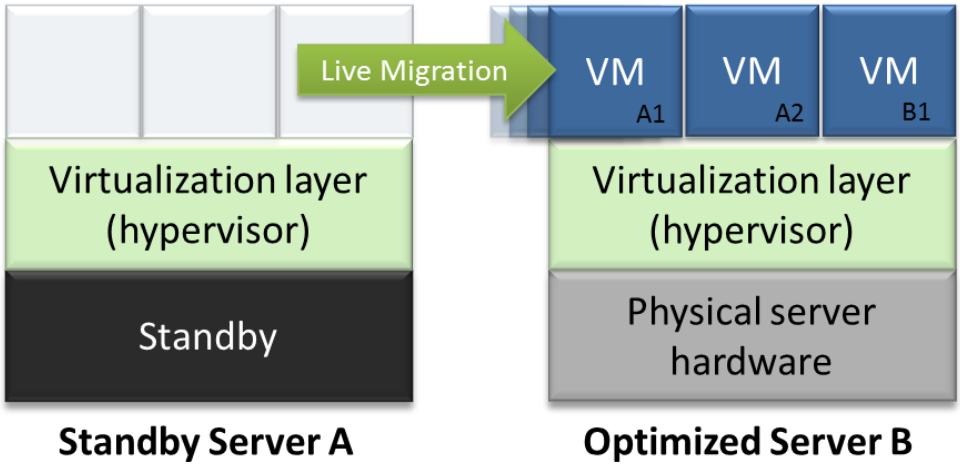

Figure 9 Distributed Power Management (DPM), adapted from [33]

In figure 9, the virtual machines of host A are migrated to host B to reduce power consumption and server A will be powered off. If virtual machine resource demands increase when users log into applications in to morning, DPM brings powered off hosts back online to ensure resource requirements are met [39].

Types of server virtualization

There are three different approaches to server virtualization: full virtualization, para-virtualization and OS partitioning [27].

With full virtualization, a hypervisor serves as the hardware abstraction layer and can host multiple virtual machines as was explained previously. The virtual machines are isolated from each other. Figures 3 to 7 are all examples of full virtualization.

With para-virtualization, specially modified operating system(s) are installed on top of the hypervisor to host multiple guest operating systems. One of the differences with full virtualization is that the guest operating systems are aware that they are running in a virtualized environment. Furthermore, device interaction with para-virtualization is very similar to the device interaction with full virtualization, because the virtual devices also rely on physical device drivers of the underlying host [41]. However, due to the fact that the operating system is modified, the hypervisor technology is more simplified, which allows for better performance achievement [32].

With OS partitioning, a common operating system (OS) on a physical server is divided into multiple isolated partitions. Each of them looks like a real server, from the point of view of the user. With OS partitioning a single OS is installed and provides its functionality to each of the partitions [42]. The difference is that full virtualization offers the possibility to run different operating systems on a physical server. With OS partitioning one type of operating system is used on the physical server.

3.1.2 Application virtualization

Application virtualization is comprised of technologies that isolate applications from the OS. With application virtualization, an application is packaged in a single executable or in a set of files that can be distributed independently from the operating system. There are different types of application virtualization of which two common types are sandbox application and application streaming.

Sandbox applications are completely isolated in what is called a “bubble”, where it is encapsulated from the underlying OS. No installation or additional driver installation is required, which eliminates dependency conflicts. All the operating system features required for application execution are already embedded in the executable file. While virtualized applications reside in isolated “sandboxes”, software can operate side-by-side without conflicts or modifications to the operating system. No application data or files are stored on the OS. Every time the user starts the application he or she gets a “clean” copy of the application as the executable file can be seen as an image of the application. Depending on the user rights that can be built in the application executable, user changes to the application can be allowed or disallowed. Furthermore, sandbox applications can be easily distributed through various means. For example via a server or on a simple USB stick [42].

Application streaming is a form of application virtualization where an application is divided into multiple packages. With application streaming, the application is stored on a central server and streamed towards the user location. Only the application data that is required will be streamed to the user [43]. For example, when a user wants to use an office program such as Word, the server will not stream the whole Office application. Only the application package with the Word application will be streamed to the user. Even the functionalities in Word are limited and packages with additional Word functionalities will only be sent when the user requests it. In figure 10, examples of application virtualization are illustrated. Applications are sandboxed and are stored on an USB stick or distributed via a central server. The grey boxes indicate physical servers on which virtual machines can be installed. The servers are connected to a storage system of which application packages can be streamed towards users. The bubbles around the sandbox applications indicate that they are isolated from other applications as well as the operating system.

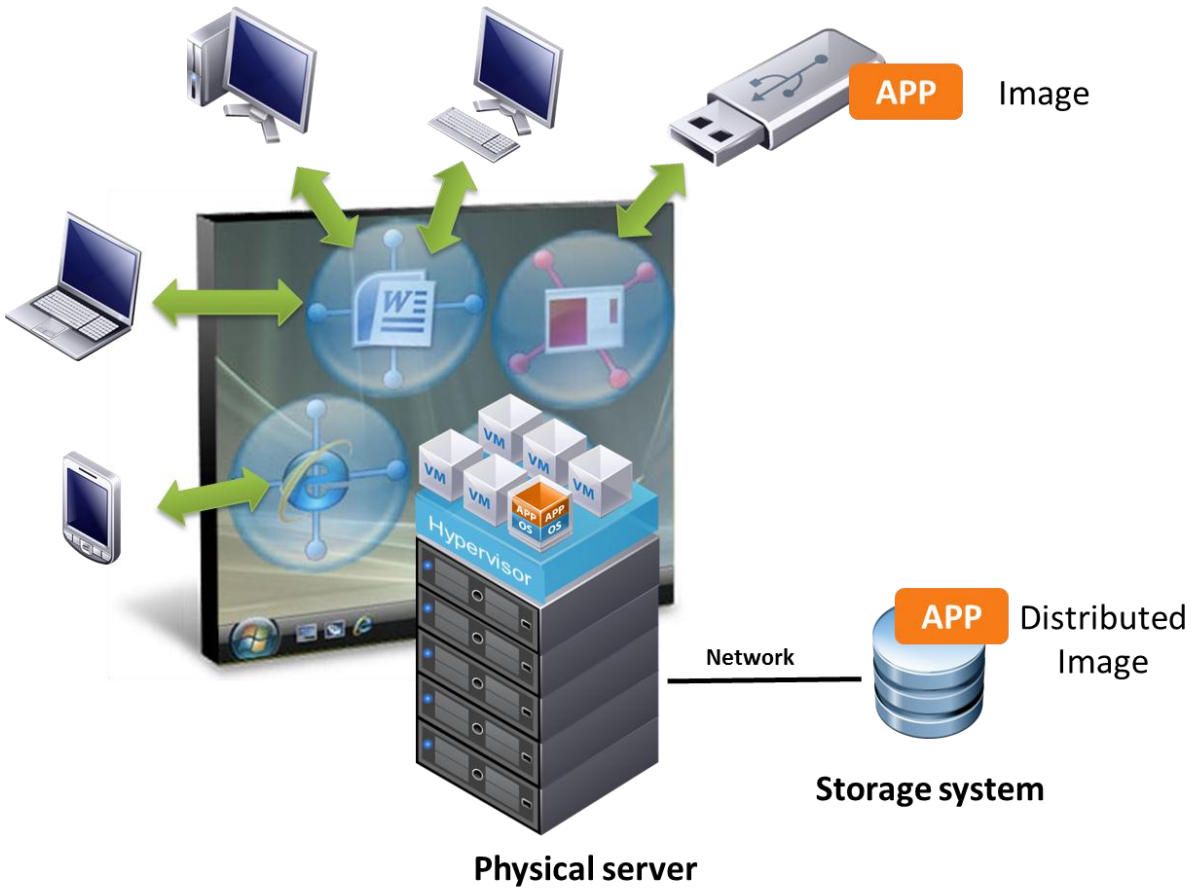

Figure 10 Examples of application virtualization, adapted from [33]

3.1.3 Desktop virtualization

Desktop virtualization is the separation of a desktop, consisting of an operating system, applications and user data, from the underlying endpoint. The endpoint is the computer device which is used to access the desktop. Desktop virtualization can be subdivided into two types: “Client side” and “Server side” [44]. With server side desktop virtualization, the end-user applications are executed remotely, on a central server, and streamed towards the endpoint via a Remote Display Protocol or other presentation and access virtualization technology. Controlling a desktop from a remote location is also called presentation or access virtualization, because the screen images are streamed from one location to another [45]. With client side desktop virtualization, the applications are executed at the endpoint, which is the user location, and presented locally on the user’s computer. In figure 11 below, different types of desktop virtualization are depicted.

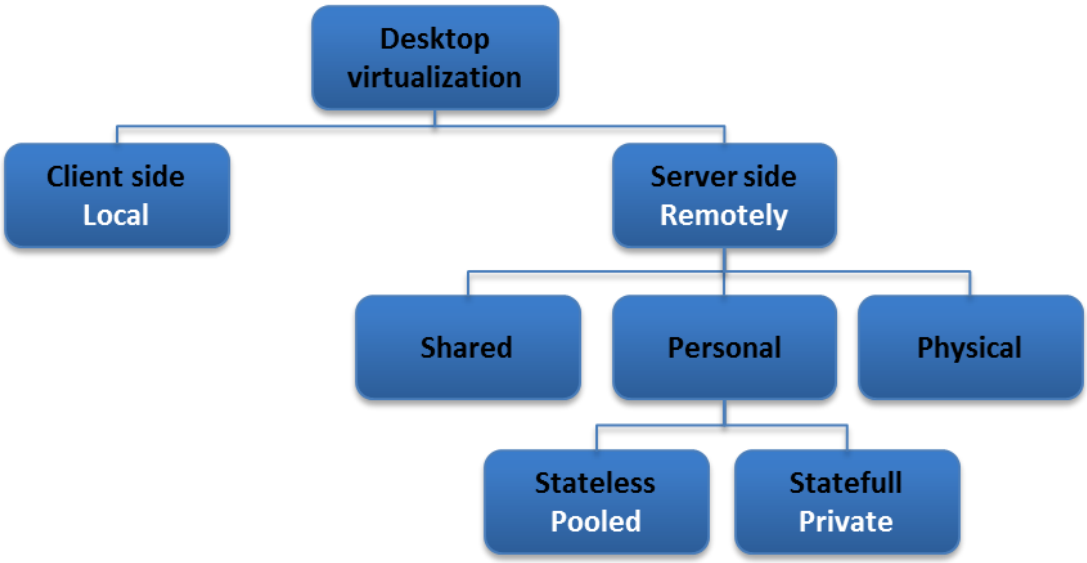

Figure 11 Types of desktop virtualization, adapted from [44]

Client side

Client-side desktop virtualization is a solution through which a desktop is executed locally at the user's location. For client-side desktop virtualization, type 1 or type 2 hypervisors can be used, which have been discussed in section 3.1.1.

Server side

Shared virtual desktops are a solution for gaining remote access to desktops and applications that are executed on a central server that usually located inside a data center. Access to the desktop or application is not restricted to a certain location or end-user equipment and the execution of the program takes place centrally on the server. The information appears on the client's screen via a remote display protocol. Every user has their own desktop session but shares the same operating system and applications with other users [44].

Personal virtual desktops are a solution for gaining remote access to desktops that are executed on a virtual machine in the datacenter. This type of desktop virtualization is also known as Virtual Desktop Infrastructure (VDI) and makes it possible to host large numbers of desktops. The desktops are virtual machines on a central server in a datacenter. VDI is the most common used desktop virtualization technology, which makes it possible to install entire desktops, including OS and applications and user profile on a remote server. Each user has their unique, personal and completely isolated desktop. Program execution, data processing and data storage take place centrally on the server. The information is displayed on the client's screen via a remote display protocol. Furthermore, virtual desktops lack graphic processing power. For this reason, virtual desktops can be enhanced by offering access to physical desktops with graphic processing power that are executed on a physical server in the data center. The physical desktops are equipped with additional graphic processing power and contain powerful Graphics Processing Units (GPU). The GPUs provide sufficient graphic processing power to execute multimedia, 2D/3D applications [44].

User state/profile virtualization

Stateless desktops refer to virtual desktops that remain 'clean' or 'stateless'. All desktop-related modifications, for example changes to applications by a user, are removed when the user logs off. However, user-specific settings that are recorded in the user profile can be stored and re-used. Stateful desktops refer to virtual desktops where the users have the freedom to install software and to make changes to his or her desktop. This is also called user state or profile virtualization. The adjustments will be maintained within the desktop, which is where the term 'stateful' is derived from. In addition to stateless desktops, stateful desktops allow the freedom to install software within the desktop. However, updating, upgrading and security are harder to manage than with stateless desktops. The impact on storage is also greater than stateless desktops as the users "state" need to be stored [44].

Example of desktop virtualization

In figure 12, an example of the most common form of desktop virtualization, Virtual Desktop Infrastructure (VDI) is illustrated.

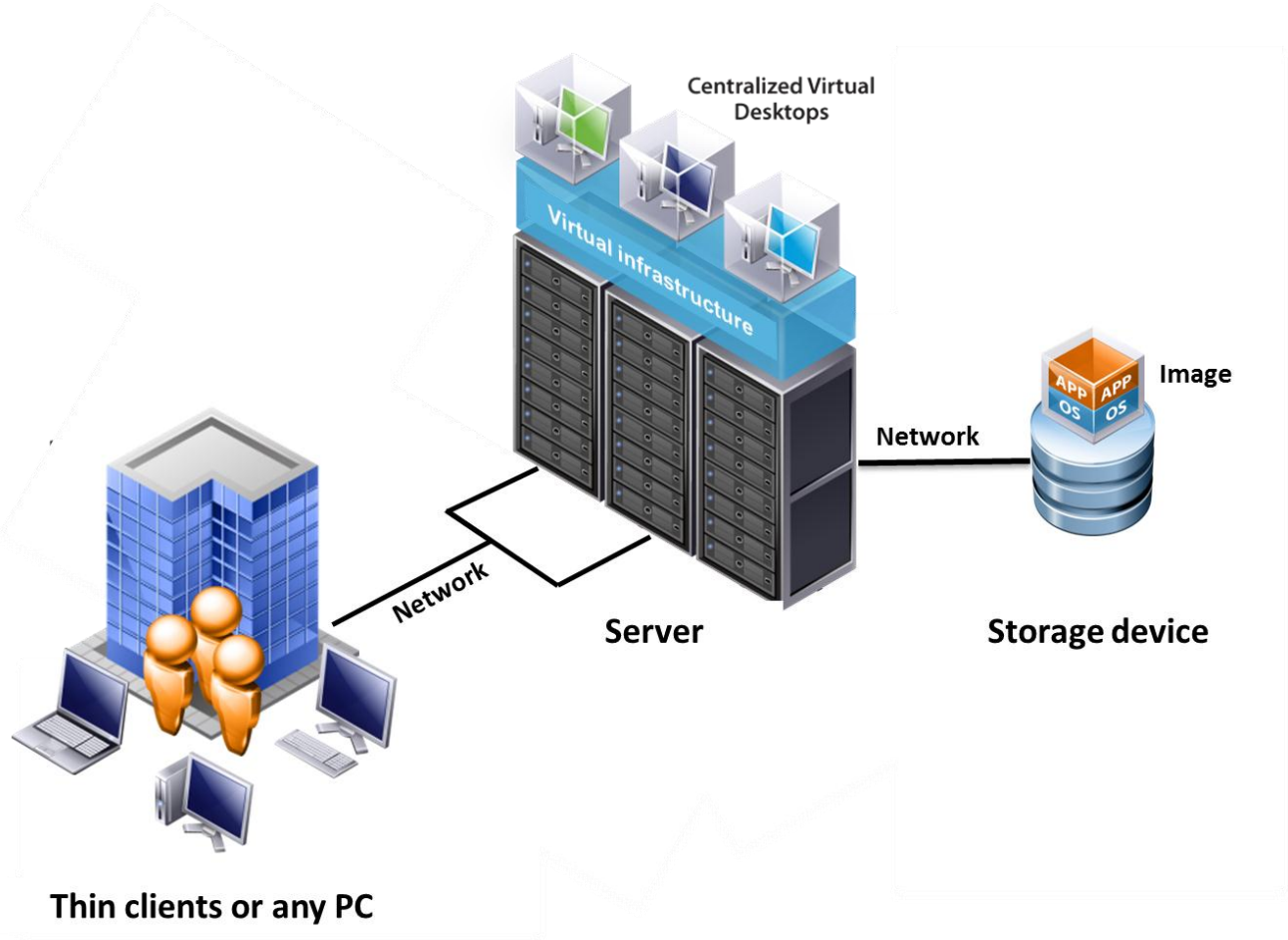

Figure 12 Example of Virtual Desktop Infrastructure (VDI), adapted from [33]

In figure 12, a central server is running multiple VMs with virtual desktops. In this setting, the desktop are executed from the central server and all the data processing is done by the server. When a user in

the office, shown on the left, wants to access his or her desktop, thin clients or any other computer devices can be used. A thin client is a small computer consisting of a limited set of hardware and is dependent on computing or data processing of the central server. For example, thin clients do not require a hard disk to process or store data, because this is done by the server. They only need to be able to run remote controlling software to interpret the data streaming into an image and display it on the screen of the user. Besides a thin client, users can access their desktop on any capable device such as notebook, personal computer, smart phone and PDA. It does not matter if the computer device has different hardware architectures or runs another operating system. Also, the example above shows only one of the many desktop virtualization implementations [46].

3.1.4 Storage virtualization

Storage virtualization is often used at locations with many storage systems. Storage virtualization is comprised of a set of technologies that create an abstraction layer between logical storage and physical storage systems [49]. Multiple storage devices in a network will be logically pooled into what appears to be a single storage device. The storage pool can be managed from a central console.

Storage virtualization technologies can be divided into two types: block virtualization and file virtualization [26]. Block virtualization focuses on creating virtual disks so that distributed storage networks appear as one (physical) storage system. An example is shown in figure 11. File virtualization creates a virtual file system of the storage devices in the network. It involves uniting multiple storage devices into a single logical pool of files. It keeps track of which files reside on which storage devices and maintains a global mapping of file locations.

Storage virtualization is commonly used in storage area networks (SAN) and is a form of block virtualization. The characteristics of SAN networks can be very complex in particular when there are many different types of storage systems and networks. Storage virtualization hides the physical complexity from applications and storage administrators, making it possible to manage it as a single resource. The management of storage devices can be very time-consuming when there are a huge number of storage devices in the network. Storage virtualization helps the storage administrator perform the tasks of backup, archiving, and recovery, by disguising the actual complexity of the SAN [47].

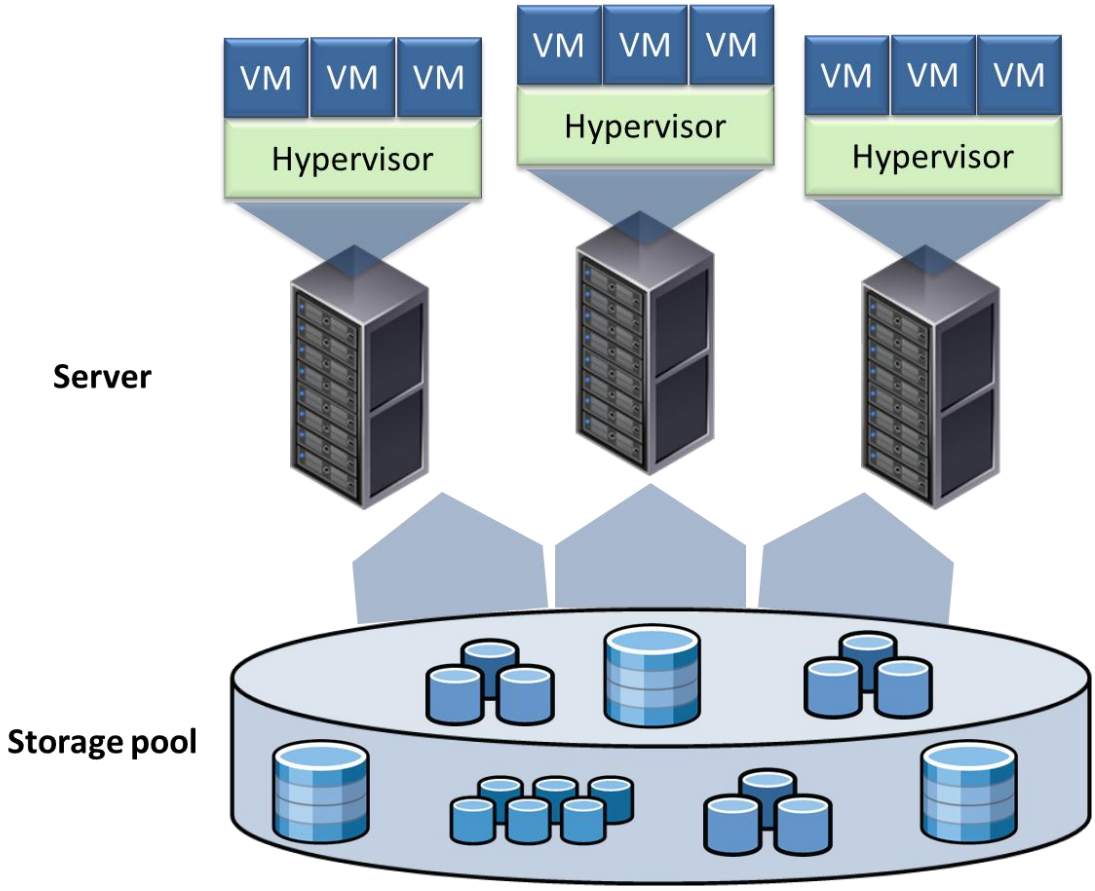

Figure 13 Storage Virtualization, adapted from [33]

In figure 13, the servers in the data center are not tied to a particular storage device, but have a storage pool at their disposal. The administrator can use a central console, which is placed inside on one of the servers and can be accessed remotely, to generate an overview of how much and what kind of data is stored on which storage system.

3.1.5 Network virtualization

Network virtualization is comprised of a set of technologies that hide the true complexity of the network and separates it into manageable parts. With network virtualization multiple networks can be combined into a single network, or a single network can be logically separated into multiple parts [48]. The currently known network virtualizations are Virtual LAN (VLAN), Virtual IP (VIP) and Virtual Private Network (VPN) [49]. VPN and VLAN are well-known, but network virtualization is still developing and other network virtualization technologies are expected to make their appearance in the near future [50].

Virtual LAN (VLAN) is a method of creating independent networks using a shared (physical) network. It is used to logically segment and control the interaction between different network segments [49]. A VLAN is a common feature in all modern Ethernet switches, allowing the creation of multiple virtual networks, which isolates each segment from the others. An Ethernet switch is a device that connects multiple network segments and enables network devices to communicate efficiently [51].

VLAN is a safe method of creating independent or isolated logical networks within a shared (physical) network. Devices in one isolated segment cannot communicate with devices of other segments even if they are connected to the same physical network [52].

Virtual IP (VIP) is an IP address that is not associated to a specific computer or network interface card (NIC), but is normally assigned to a network device that is in-path of the network traffic. Incoming packets are sent to the VIP but are redirected to the actual network interface of the receiving host or hosts. It is used in virtualization technologies such as High-Available and Load-Balancing, where multiple systems have a common application such as a VM, and they are able to receive the traffic as redirected by the network device. Virtual IP address eliminates a host's dependency upon individual network interfaces. If a computer or NIC fails the VIP address may still be available, because another NIC responds to the connection [49].

Virtual Private Network (VPN) is a private communication network that uses a public network, such as the Internet. The purpose of a VPN is to guarantee confidentiality on an unsecured network channel, from one geographical location to another. It is normally used as a means to enable remote employee home networks to connect to an organizations' network. This is normally done by using special software (for example: Cisco VPN Client), but after the connection is established, all the interaction with the other resources on the network is handled as if the computer was physically connected to the same network, although this depends of the way security policies are applied [49].

3.2. Virtualization domains of Atos Origin

In this research an overview has been made of the virtualization technologies, but also each virtualization technology is analyzed to see whether they are important for Atos Origin to take into consideration. The basis for this analysis is to first look at the virtualization technologies that Atos Origin currently offers. As a virtualization service provider Atos Origin offers five virtualization services in five virtualization domains [53]. These domains are server virtualization, desktop virtualization, application virtualization, storage virtualization and disaster recovery virtualization. The first four domains are well-known domains and have been described in section 3.1. However, the fifth virtualization domain is disaster recovery virtualization. Disaster recovery virtualization is a term that is used by Atos Origin in which virtualization technologies are used for recovery of IT infrastructures in case of a disaster.

Atos Origin provides IT infrastructure recovery for organizations who wants to take precautions when a disaster strikes, such as power failures, floods, earth quakes, etc. To provide disaster recovery, Atos Origin has multiple datacenters in distant locations at its disposal. Distance between the data center locations is very important, because a disaster might disrupt a large geographical area [54]. Disaster recovery requires the maintenance of an IT infrastructure in at least two separate data center locations. One location contains the IT infrastructure of the organization that supports the business and the second location contains the back-up or recovery IT infrastructure. This is depicted below in figure 14.

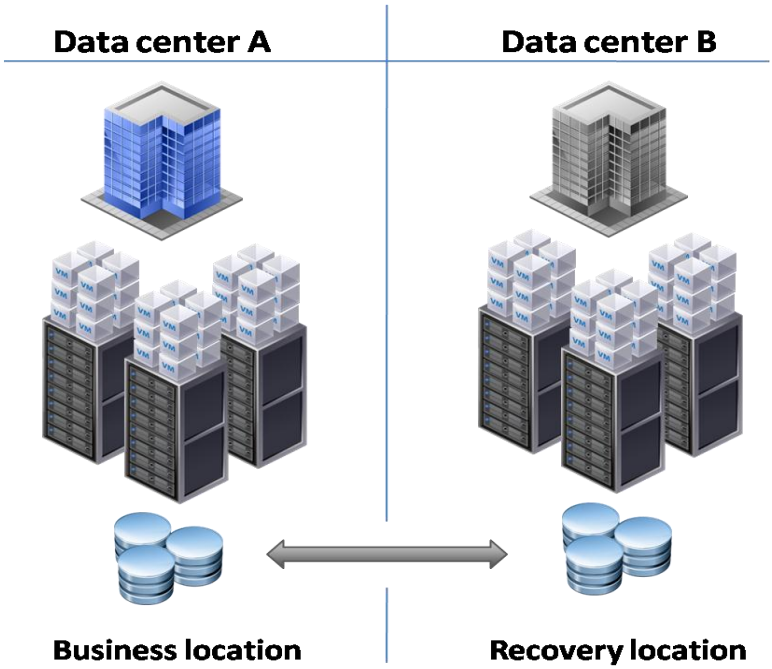

Figure 14 Disaster recovery, adapted from [33]

Deploying two separate IT infrastructures can be a very expensive and difficult task. Traditional methods require duplication of hardware, software and network configuration and installation. This can be very labor intensive to keep up to date, maintain and test, but also requires ongoing management. Virtualization technologies are used to make this process more simple and autonomous. For example, with server virtualization there is no need for installing or reconfiguring hardware for servers in case of a disaster. All the virtual machines that contain the organizations applications, databases, and more can be stored in separate storage systems. These data files can be recovered to any hardware without the need for changes, because virtual machines are hardware independent and can operate on other physical servers in the recovery location [55]. In figure 12, when a disaster takes place and data center A is not operational anymore, the VMs of data center A continue their operation on servers in data center B. However, this example shows an optimal situation where data center A is completely virtualized and a full backup of the VM's is made and stored in data center B.

3.3 Summary and outlook

In chapter 3, many different virtualization technologies were discussed. In short, a distinction can be made between five virtualization domains. The virtualization domains are server, application, desktop, network and storage virtualization. Each domain consists of a group of virtualization technologies that share a common area of interest. This answers the first sub question which stated:

- *What virtualization technologies are currently available?*

This chapter has discussed the virtualization technologies that can be found in literature. In the next chapter, the exploration for virtualization technologies continues by looking at the current developments. Also, certain issues will be discussed that have led to the developments of new

virtualization technologies. More types of virtualization technologies have been found in the next chapter that can be added to list of virtualization domains of this chapter.

Furthermore, in appendix C the benefits and challenges of the five virtualization domains have been described. Appendix C offers additional insight on the virtualization domains. Also, chapter 4 describes one of the main challenges of virtualization, which is the manageability of virtualization technologies.

4. Analysis: Part II

Part II of the analysis looks at the current virtualization developments. In this chapter information is gathered from, papers, interviews and presentations at a virtualization event. The virtualization event was held in Nijkerk. In this event, many virtualization companies were present, showing the latest challenges, products and developments regarding virtualization. The virtualization event was in particular focused on VMware virtualization products, because there were no presentations of main competitors Citrix and Microsoft. However, at the stands of the attendant companies, it was possible to get information of virtualization products from different virtualization vendors such as Citrix and Microsoft.

Section 4.1 begins with a short overview of the journey virtualization has made and is currently making. In section 4.2, two examples are given of virtualization challenges, which have led to the development of new virtualization technologies. The new developments are discussed in section 4.3. At the end of chapter 4, a summary is made of the research findings of the analysis phase and an outlook is given on what is to be expected in the following chapters.

4.1 Virtualization journey

Virtualization technologies on x86 platforms started with the idea of delivering full virtualization by creating virtual machines on x86 computers [80]. Virtualization made it possible to increase utilization of servers, which allowed organization to significantly reduce the number of (physical) servers. Virtualization has rapidly become a standard piece of deployment platform in IT organizations, because of the benefits in terms of capital cost reductions and operational benefits. The challenging economic climate of the recent years has made organizations to be more cautious about their budgets. Therefore, the majority of organizations started virtualization projects by focusing on server consolidation to reduce costs [81].

As virtualization technologies improved, organizations started to notice the additional benefits of virtualization such as high availability and allocating and re-allocating resources to applications when necessary [82]. From implementing virtualization only on small scale, the use of virtualization has started to also become more interesting for important business applications, due to capabilities like high availability. Important business applications are applications that are heavily used by an organization and require high amount resources to ascertain that enough resources available. Starting with servers, virtualization has rapidly become an important technology across all parts in IT infrastructures. Besides virtualization technologies for servers, it also expended towards storage, networks and desktops [83].

Many vendors entered the virtualization market, which caused a significant reduction in pricing of hypervisors. While some virtualization vendors focused on large organizations, others targeted small and midsized organizations with great success. The adoption of virtualization technologies by organizations are increasing, but the penetration of virtualization within organizations is still relatively low [84]. One of the reasons is that many organizations implemented virtualization on only a small portion of their IT infrastructure. A lot of large organizations started implementation of virtualization in small steps in contrast to smaller organizations that cover multiple steps at once [85]. Virtualization is still early in its life cycle and virtualization vendors are already talking about next steps, when all parts of the IT infrastructure are virtualized.

Virtualization technologies lead to more automation of IT infrastructure and lay the foundation for IT services and resources to be offered via the Internet as a metered service in a public or private cloud. Although there is not one agreed definition of what cloud exactly is, the idea behind it is that IT-related services are offered and provided via the Internet, with very limited if any commitments from either side, in terms of either volumes or quality, and payment by usage [86]. Cloud computing defines a shared (or private) environment, scalable up and down, and flexible, with easy entry and exit. Organizations can decide if they want to run their business application on their own private (internal) cloud or on a public (external) cloud. A private cloud is an IT infrastructure that is owned or leased by a single organization of which IT managers of an organization are fully in control and is well protected behind a firewall. A public cloud is a datacenter of an external organization, which is often called a cloud service provider that is offering IT services to general public or large industry group. A public cloud is a shared environment that can be used by multiple organizations where organizations pay for the amount of infrastructure they use. Depending on the demand, infrastructure usage can easily be scaled up and down [86].

However, for cloud services to take off on a large scale, virtualization still needs to mature and despite good progress virtualization technologies suffer from many issues and rolling out of virtualization on a large scale is complex. Currently, there are already cloud providers such as Google and Amazon. Google for example has a cloud service called App Engine, which basically allows users to run their web applications on Google's IT infrastructure. These are individual companies, that want to take a leading role in offering these cloud computing platforms and it is expected to take off rapidly [87]. Yet, much development still remains and recently virtualization vendors have shifted a lot of their attention towards easier management and new capabilities of virtualization technologies [81].

4.2 Virtualization challenges: two examples

There are still many issues with virtualization technologies. For instance, in traditional environments there are many tools that facilitate management and security for IT infrastructures. However, for virtual environments traditional management and security technologies are often not suitable. In appendix C, the main challenges are described for each virtualization domain.

Below two examples of virtualization challenges are given that were very apparent in the virtualization events [88, 89, 90], but also in literature papers and reports [18, 71, 73, 81, 96]. During this event, market leaders from the virtualization industry discussed the important challenges of today and the technologies that can be used to tackle these challenges [91]. Below, two examples are discussed regarding two important virtualization challenges: management and security.

4.2.1 Example 1: Management

Organizations that have adopted virtualization technologies are facing a number of management issues. Many organizations start with server consolidation in which the number of (physical) servers can be significantly reduced to smaller number of (physical) servers that are running multiple virtual servers. While the hardware can significantly be reduced, an organization still has to manage the large number of virtual servers. Furthermore, server virtualization allows organizations to easily deploy new virtual servers with the click of a mouse button. While having to manage less physical servers, a large number of virtual servers on top can become hard to manage. Server virtualization introduced a new issue,

called VM sprawl.

Virtualization has made server deployment very easy and organizations easily find themselves in the pitfall of VM sprawl [90]. Traditionally, if someone wants to deploy more servers there is a whole process of ordering hardware and procedures, but now IT administrators can deploy virtual servers with a click on the mouse. There is often the deception that virtual machines are free. However, the deployment of new virtual machines can lead to the requirement or purchase of additional hardware resources. Deploying a couple new virtual servers might not require additional resources, but in case of VM sprawl, the virtual environment is characterized by many redundant virtual machines that inefficiently use resources. This could lead to the purchase of more hardware, consisting of servers and storage, and possibly additional licensing cost. Also, while the virtual environment can be centrally managed more IT staff might be needed to address and solve the VM sprawl problem.

Another problem is the sharing of IT resources. As resources are shared, the applications and data of different departments of an organization can reside anywhere in the virtual environment. Different departments of an organization are often also reluctant of the idea on sharing resources with other departments and losing control of their own resources [85]. However, new development in management tools has addressed some of these problems and is discussed in section 4.3 below.

4.2.2 Example 2: Security

Whereas more and more physical servers are being virtualized, security issues associated with virtualization have become more critical to address. In fact, virtualization adds new challenges for organizations that require involvement of information security measures in initial stages of virtualization projects. According to MacDonald [92], most virtualized servers are being deployed insecurely. The reasons he addresses are the immaturity of tools, processes and the limited training of staff, resellers and consultants. Virtualization creates a dynamic environment that is difficult to secure [89]. Virtualization adds a new layer of software on a (physical) server and like any software that is written by a “human being” it can contain embedded and yet to be discovered vulnerabilities that may be exploitable [92]. When hackers get access to the virtualization layer, which contains the hypervisor, all the virtual machines could be compromised.

Furthermore, traditional security and management tools inside an OS are not aware or designed to access, scan or protect the virtualization layer. There are security tools for virtualization, called virtual security appliances. Virtual security appliances are security programs that are places inside VMs. The VM is packaged with an OS and security application, which can offer better performance, than installing security application in each VM, due to its dedicated approach. However, the security tools are still placed on top of the virtualization layer, which has its drawbacks, especially if the virtualization layer is compromised.

Another risk is the communication between virtual machines. Many virtual environments include the ability to create virtual networks and switches inside the host (or physical server) to enable virtual machines to communicate directly. This traffic is not visible to traditional physical network-based security protection devices as the traffic goes through a virtual network inside the host. Monitoring the traffic between virtual machines on the same server requires security measures placed inside the host. In table 1 below an overview is made of new security challenges that come with virtualization.

Table 1 Security Challenges, adapted from [89]

Virtualization security challenges
• **Inactive VMs**
• **VM awareness**
• **VM Sprawl**
• **Inter VM traffic**
• **Live Migration**

Inactive VMs are VMs that are offline and are placed on a server that is unused. Using traditional security measures that require daily updates, these VMs can become a security risk when they come online even after a small period of time [89]. VM awareness is about conventional security solutions that are not designed to be aware of VMs. Not all security solutions work correctly with virtualized environments [93]. Security measures can be taken in many different layers: network, application, OS and virtualization layer. Therefore, virtualized environments can be very complex. For instance, security solutions may not know or be able to scan all the traffic between VMs and different operating systems in the virtual network running on the same virtual network. Also, with the additional virtualization layer where the hypervisor is present, security solutions must also be able to scan and report vulnerabilities of this layer. Another security challenge is VM sprawl which has been discussed previously.

The security problem with VM sprawl is that security weaknesses can replicate quickly. For example, server virtualization offers the possibility to create templates of an existing VM to easily duplicate and roll out new virtual servers. When templates are being used to create new VMs and this template includes an application or OS with security vulnerabilities, all the VMs created from this template will be vulnerable. Keeping the virtual servers up to date with the latest security updates is one the challenges at the moment [89]. Inter-VM traffic is another challenge, because this traffic is not visible to network-based security protection devices of traditional physical network monitoring tools. With virtualization, virtual networks are used inside the host to enable VMS to communicate directly. Therefore, virtualization aware security measures need to be taken to enable monitoring of traffic in a virtual network. Furthermore, live migration enables VMs to travel from server to server. When a VM is safeguarded by a security policy that is different to the security policy on another server live migration can become a security challenge. Hence, it is important that security measures in one part of the network can be preserved on another part of the network. A possible solution is by addressing security policies inside a VM [89]. This live migration problem is one of the issues currently with cloud. Live migration of a VM from one cloud to another cloud must be safeguarded by security policies and standards [95].

4.3 Current developments

The following developments have received much attention by virtualization vendors. These are management tools, security tools and desktop virtualization. The developments are discussed consecutively in sections 4.3.1, 4.3.2 and 4.3.3 below.

4.3.1 Management tools

Many management and security issues of which some are described above have been identified by software vendors and resulted in the development of management and security tools. Surveys among organizations that adopted server virtualization show that the main challenge is the management of virtual environments [90, 96]. For traditional environments, there are many management tools that have matured over the years. In virtual environments similar management is required as traditional environments. However, many of the traditional management tools are insufficient for virtual environments. Reasons are limited functionalities of traditional management tools for virtual environments. Software vendors started to address this issue and currently several management tools have and are entering the virtualization market. Many of these management tools are still under development, but are expected to become available very soon [90]. In table 2 below, an overview is given of the different types of management tools.

Table 2 Types of Management Tools, adapted from [90]

Management Tools
• **Application performance monitoring**
• **Configuration management**
• **Cost control**
• **Capacity planning & monitoring**
• **Asset management**

Application performance monitoring

Application performance monitoring management tools can graphically map the virtual environment and are equipped with automated discovery of servers in both virtual and physical infrastructures. One of the main obstacles for managing application performance in virtual environments is the lack of visibility of the entire application transaction flow [93]. The performance management tool enables an organization to monitor and analyze the performance of the virtual infrastructure. It measures the latency experienced between application and end-users and can identify application performance bottlenecks. Furthermore, applications can be tested how they would perform in a virtualized environment, which can eliminate uncertainty about making critical business applications virtual.

Configuration management

Configuration management tools make it possible to track, report and share the configuration of virtual resources. In a situation where there are hundreds of virtual machines in one environment, error tracking and checking configuration compliance can become complex. Configuration management makes it possible to track configuration of virtual machines, analyze their configuration and check whether they comply with the standards determined by the organization. These management tools can

be used pro-actively to see how changes will impact the virtual environment in what way. For instance if an organization want add a new SAN storage, this management tool can show which virtual machines it will impact.

Cost control

Cost control is a way to account, monitor and report on costs that are associated with the virtual infrastructure. Different models can be used such as fixed, allocation based and utilization based pricing [90]. With fixed pricing, users or a group of users can be charged with a fixed price for the number of hardware resources they use. Allocation based pricing is a variable pricing method where users pay for the number of resources that are reserved for them. Utilization based pricing goes beyond allocation where users specially pay for the used processing power, internal memory, storage space, etc. A distinction can be made between variable components such as CPU, memory and storage usage and fixed components such as license and energy costs. Cost control management tools can schedule reports, which can be sent to users or end-users for billing purposes. The benefits of cost control are that it can bring insight in resource utilization of users and budget requirement for different departments of an organization and to determine where most of the costs are being made.

Capacity planning & monitoring

Capacity or resource planning management tools can be used to determine what resources have been used and are currently used. It can analyze, forecast and plan capacity of a datacenter or virtual environment. Unused capacity can be identified, but can also perform scenarios where the impact of effect of capacity changes can be tested. For example, an organization can test the impact on capacity of new additional servers with multiple virtual machines that might be needed for upcoming projects. Also an organization can make a forecast of when or in what scenarios they will run out of capacity.

Asset management

Asset management tools that can be used to analyze and track what assets an organization has in their IT environment. An asset can consist of hardware components, but also software such as applications, virtual machines etc.

4.3.2 Security tools for virtualization

Currently, virtualization technologies are developed that can offer security solutions from within the virtualization layer or hypervisor in contrast to virtual appliances located inside virtual machines. This new security technology is called an application program interface (API)-sharing program, which security vendors can use to develop their own security products for virtualized environments. By enabling security measures inside the hypervisor the security program is isolated from the servers running in virtual machines. This takes away the need to install security programs on the virtual servers itself. The virtual machines are protected by monitoring all the virtual components: CPU, memory, network and storage all goes through the hypervisor. It addresses the issue of conventional solutions by being aware of virtualization layer. The virtualization layer can make a map of the IT infrastructure and is able to scan and protect any VM in the network. Security updates can be done centrally and do not need to take place inside the servers. Also, virus scans often goes along with performance degradation, but now VMs can be scanned on servers where resources are sufficient and if not can be live migrated towards other

servers. This way, better performance can be gained than running virus scans inside servers [89]. The security program is still at an early stage, but might be a promising virtualization technology that can address and solve many of the security challenges of virtualization.

4.3.3 Offline Desktop virtualization

Delivering desktops from a datacenter as a managed service is an emerging technology that is expected to take off significantly in the coming years [94]. Distributed computing, which requires significant hardware capabilities at the location of the user, has been dominant for the past 15 to 20 years. At the moment, there is a tendency that is heading into the opposite direction where desktops are deployed from a central location. Desktop virtualization enables organizations to change standard PC deployments. Organizations that have previously purchased high volumes of expensive desktop PCs can now look for less-expensive computers, such as thin clients. While desktop hardware expenditure might drop, desktop virtualization requires the acquisition of significant server and network capabilities. Organizations can centralize user data and applications without changing or re-engineering their application for desktop virtualization.

Virtual desktops and applications offer the possibility for organizations to be more flexible and allow their employees to access their desktop from any place, any time with any device. However, there are factors that inhibit adoption of desktop virtualization. These factors are network latency issues, lack of proper management tools, inadequate application performance and high initial and additional costs that are associated with desktop virtualization [94]. Organizations that are adopting desktop virtualization often have other reasons than cost savings. The ability for employees to connect from everywhere and anything, offering a “new way of working”, is one of the main reasons for desktop virtualization. To access their desktop, employees need to have a continuous internet connection that allows the streaming of their desktop to their computing device. At the moment, an interesting development is the offline functionality. This way, employees can decide to copy their desktop from the remote server on their own computer and offers the possibility to continue their work without having an internet connection. However, for security reasons this functionality requires the user to connect to the remote server again after a short period of time for update reasons and to check the user authenticity [94].

4.4 Summary and outlook

Virtualization technologies have become popular with organizations initially because it allowed them the opportunity to save cost. More vendors saw business opportunities and entered the virtualization market. While server consolidation is the main motive or focus for organizations to start with virtualization to reduce capital spending, virtualization brings new challenges. The challenges experienced by organizations have led to the need of additional virtualization technologies. In section 4.3, the second research question is answered, which stated:

- *What are the current developments in virtualization technologies?*

The virtualization developments consist of developments in management tools, desktop virtualization technologies and new security tools. In chapter 5, the virtualization technologies of Part I and Part II

have been added together and used as input for the design of the taxonomy model. In chapter 6, the research findings and taxonomy model are evaluated.

5. Taxonomy model of virtualization technologies

In this chapter, a taxonomy model has been made that provides an overview of the different types of virtualization technologies. In section 5.1 the modeling language is explained that has been used to design the taxonomy model. In section 5.2, the taxonomy model is shown and divided in multiple parts. At the end of section 5.2, the taxonomy model is shown in full detail. The taxonomy model illustrates the main virtualization domains and their relation. Each domain is further divided into subtypes. Section 5.3 closes the chapter with a summary and outlook on the following chapter.

5.1 Modeling Language

In analysis part I and II many types of virtualization technologies have been discussed. In this chapter, a taxonomy model has been constructed that provides an overview of the virtualization technologies that were identified in the analysis phase. There are different ways and modeling languages to design a taxonomy model. However, a well-known standardized modeling language is used, called Unified Modeling Language (UML). UML offers a standardized way of visualizing objects and provides notifications to describe the different virtualization technologies and their relationships [97]. UML is used for this research, because it is a well-known standardized format and it is able to visualize the technological concepts and their relations in a suitable way. UML defines many different types of diagrams, which can be divided in two general sets: structural and behavioral diagrams [98].

Structure diagrams show the static structure of the model that is being designed. It focuses on the objects of a model, irrespective of time. The static structure is depicted by showing the object types in the model. Structure diagrams can also show the relationships among and between these objects. Behavior diagrams, as its name proclaims, are diagrams that capture the varieties of interaction and instantaneous states of objects within a model. As the name indicates, it attempts to track how the model behaves or acts in a real-world environment. The taxonomy model that has been made can be categorized as a structure diagram of which the system is a static overview and classification of the elements, which are in this case virtualization technologies. The specific structure diagram that is used to classify the object is called a class diagram. A class diagram describes the structure of the model by showing the models' objects as classes and relationships [98]. Hence, a class diagram is very appropriate to design the taxonomy model of this research.

5.2 Taxonomy model

In the analysis part I, it became apparent that virtualization technologies can be part of the same group of technologies. These groups were called domains. According to the first part of the analysis, there are five main domains in which virtualization technologies can be categorized. These are server, application, desktop, storage and network. In UML, the five domains are defined as objects that are called classes. In the second part of the analysis, two new types of virtualization technologies were introduced: management and security tools. Management and security tools are also added as classes in UML. They are comprised of a set of virtualization technologies that provide some form of management or security measures and must not be confused with other aspects of management and security, such as the making of policies and their execution.

When we look at the relations of the management class, the security class and the five domain classes, both management and security classes are associated with the five domain classes. For example, management technologies can have a relation with all domains as each domain can be managed. The same goes for security, where virtualization security technologies can be used to provide security for each domain. When we translate this relationship to UML, it can be visualized as follows.

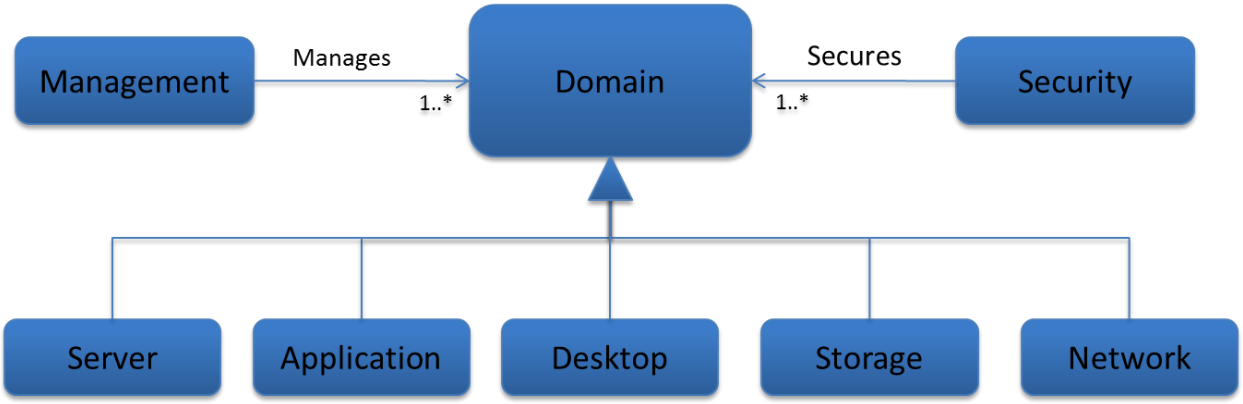

Figure 15 Taxonomy model

All objects in figure 15 are classes of which "domain" is a super class of the five domain classes: server, application, desktop, storage and network. A super class inherits the identical functionality of another class, which is in this case a domain type. The super class domain is put in between the classes to make the taxonomy model orderly. Without the super class domain, a line must be drawn from each domain to both the management class and security class, resulting in a web of lines between the classes. The bold arrow below the super class domain indicates the hierarchical relation of the classes with the super class "domain". The classes "management" and "security" both have a one-way relationship or association with the super class domain and is indicated by small arrows. Both arrows are labeled with one word and a multiplicity value indicator to describe their association. In this case, the association for management means that the class "management" manages one or more domains. The same applies for the security class, which means that security is related to one or more domains. In other words, this class diagram states that virtualization technologies for both management and security can be applied to 1 or more virtualization domains. However, each class of the taxonomy model can be further divided into a set of technologies. Starting with the domain classes, each class will be discussed in detail.

Server

Section 3.1.1 shows that server virtualization can be divided in 3 types or sub classes: para-virtualization, full virtualization and OS partitioning. Furthermore, full virtualization technologies can be divided into two more sub classes: "Type 1" and "Type 2" hypervisors. In figure 16, a detailed overview is depicted of the types of virtualization technologies of the server domain.

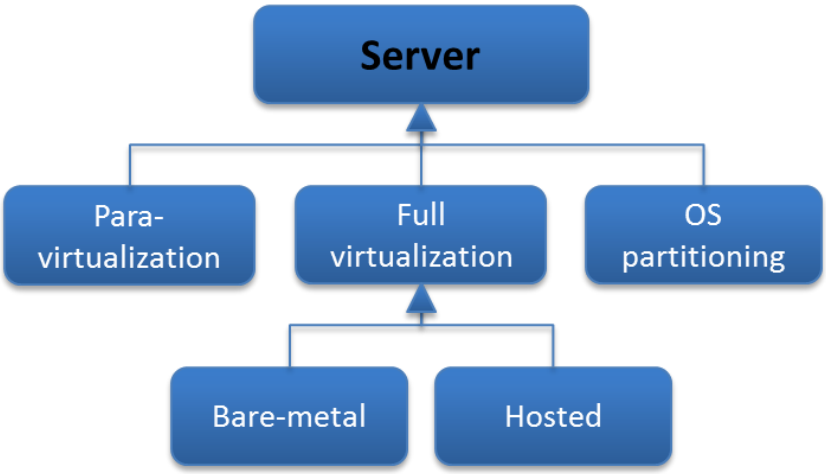

Figure 16 Server virtualization classes

Application

Section 3.1.2 describes two types of application virtualization technologies: sandbox and application streaming. This is shown in figure 17.

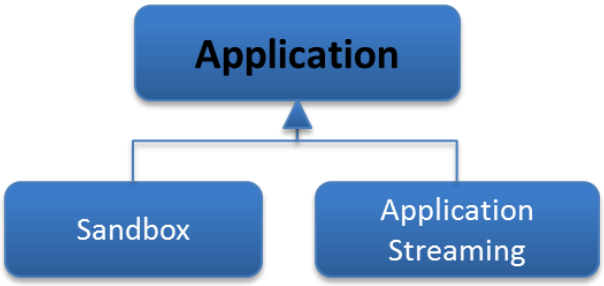

Figure 17 Application virtualization classes

Desktop virtualization

Section 3.1.3 describes two general types of desktop virtualization: client and server. Client desktop virtualization technologies are used to host virtual desktops (or virtual machines) locally on the clients' computer. Server desktop virtualization can be divided into two types: personal and shared. As explained in section 3.1.3, shared desktops refer to desktops that are shared among users and personal desktops refer to users having their own completely isolated desktop. Personal desktops can further be divided into virtual or physical. Physical desktops are equipped with additional graphic processing power for graphic intensive applications. In section 4.3, a new virtualization technology was introduced that allows a personal virtual desktop to become available offline. In figure 18 below, an overview of the desktop domain is depicted.

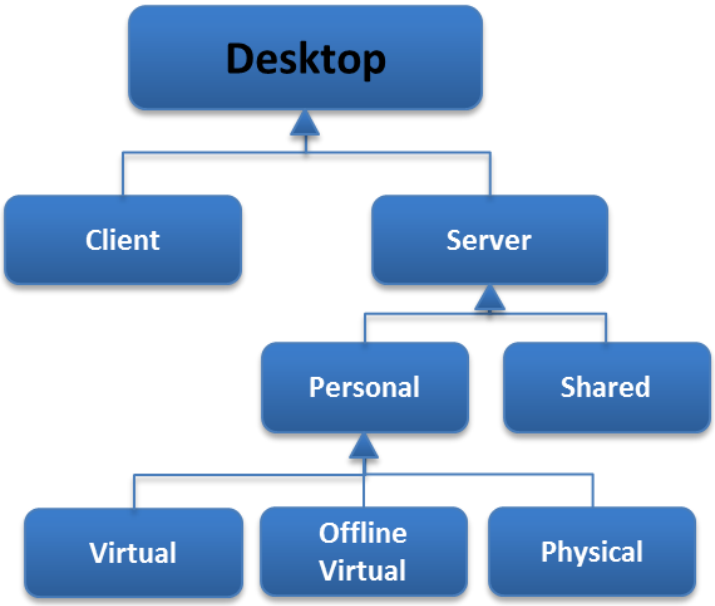

Figure 18 Desktop virtualization classes

Storage virtualization

Section 3.1.4 describes storage virtualization as the pooling of data from multiple storage devices. Examples of storage devices are storage attached network (SAN) and network attached storage (NAS). While storage virtualization can be used in different or a combination of storage devices, storage virtualization can be broken up into two general classes: block virtualization and file virtualization. Figure 19 shows this relation.

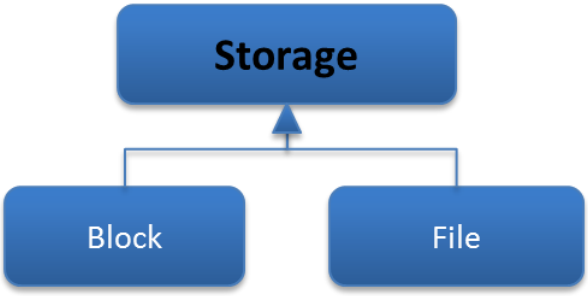

Figure 19 Storage virtualization classes

Network virtualization

In section 3.1.5 network virtualization was characterized by three types of technologies: Virtual LAN (VLAN), Virtual IP (VIP) and Virtual Private Network (VPN). This is depicted in figure 20.

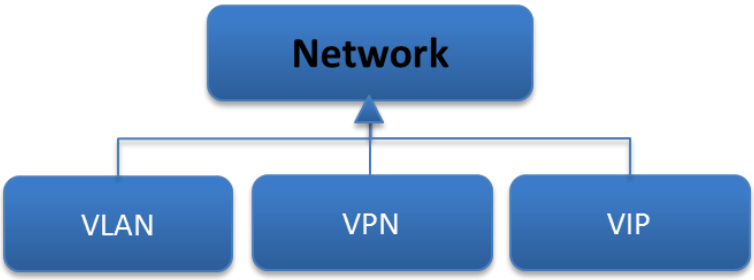

Figure 20 Network virtualization classes

Management

The class "management" consists of a set of technologies, which can be used for management purposes and are shown in figure 21. However, management technologies for virtualization are still young and immature technologies. In the near future more and management technologies with more features are expected. According to section 4.3 there are currently five types of management technologies for virtualization: performance, configuration, asset, capacity, and cost-control.

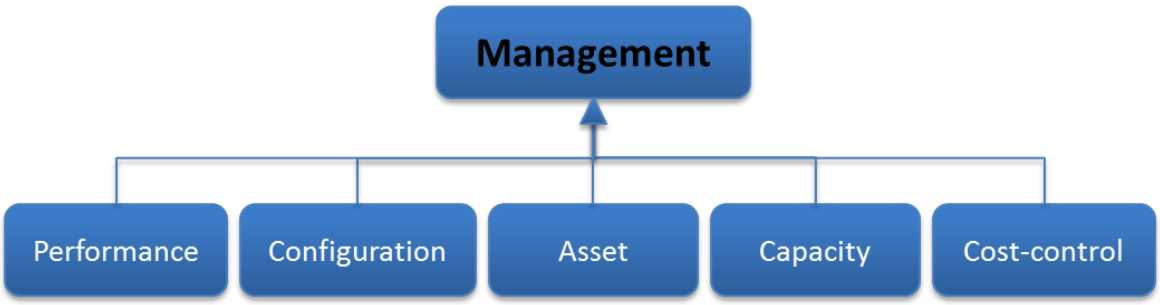

Figure 21 Management class

Security

Section 4.3, describes a security technologies that are developed specifically for virtualization. There are two types of security tools for virtualization: virtual security appliances and hypervisor appliance. This is shown in figure 22.

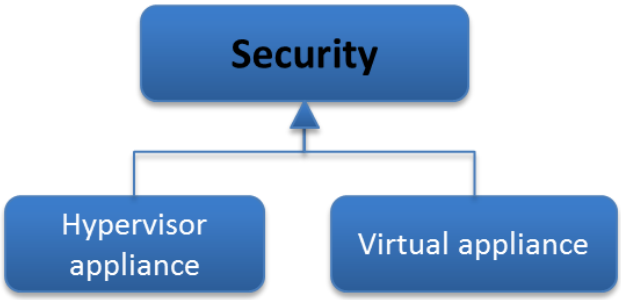

Figure 22 Security class

The taxonomy model that is constructed above, presents an overview of all the different types of virtualization technologies. The taxonomy model can be used for different purposes. First of all it can be used to show what kind of virtualization technologies exist. Secondly, the taxonomy model can be used

to point out trends and in which domains new types of technologies are expected. The taxonomy model can be the starting point in these discussions. In figure 23, the entire taxonomy model is depicted.

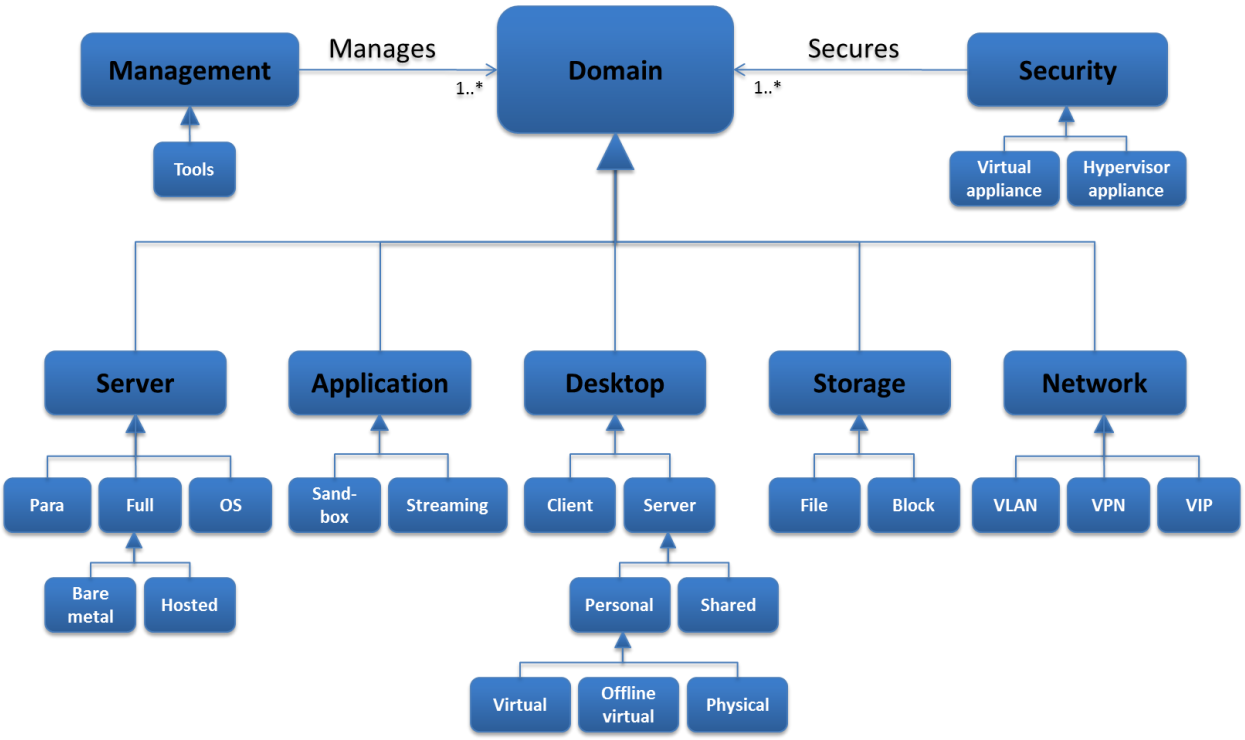

Figure 23 Taxonomy model in full detail

5.3 Summary and outlook

In chapter 5, the virtualization technologies of previous chapters were used to design a taxonomy model. The Unified Modeling Language (UML) was used to create the taxonomy model, because it is well-known standardized format and is able to visualize the technologies and their relations. During the analysis phase, it became apparent that there are several domains in which virtualization technologies can be categorized. Furthermore, current developments pointed out additional technology groups of virtualization technologies, which are management and security. Both additional technology groups are composed of technologies that affect or support each of the five domains. In UML, a class diagram is used to visualize the taxonomy model in which the five domains and the two additional technology groups are defined as classes.

However, the management and security classes encompass only a set of virtualization technologies and must not be confused with other aspects of management and security, such as the making of policies and their execution. The taxonomy model answers the third research question, which states:

- *How can the virtualization technologies be structured?*

In the next chapter, a case study is conducted to evaluate the research findings. In the evaluation, not only the taxonomy is discussed, but has also been used to explore and describe the virtualization trends.

The case study provides information about the virtualization trends and the reliability of the taxonomy model. The case study findings are used to answer the fourth and last research question.

6. Evaluation using case study method

In previous chapters, virtualization technologies have been analyzed and structured in a taxonomy model. In this chapter, a case study method is used to evaluate the taxonomy model to see whether the virtualization technologies are structured correctly, but also to explore what virtualization trends are. In section 6.1, the case study method is explained. Interviews have been conducted with virtualization experts from Atos Origin and various virtualization vendors to evaluate the taxonomy model and at the same time to identify the virtualization trends to look for possible business opportunities. This is discussed in section 6.2 and 6.3. In section 6.4, conclusions are drawn from the case study. In section 6.4.1, the remarks on the taxonomy model are discussed that have been made in the case study. Secondly, section 6.4.2 discusses the conclusions regarding the virtualization trends. Furthermore, the quality of the case study is discussed in section 6.5. Finally, a summary and an outlook on the remaining chapters are given in section 6.6.

6.1 Case Study

The case study method is used to evaluate if the taxonomy model is structured correctly, but also to identify virtualization trends. For the case study, interviews have been held with respondents who are familiar with virtualization technologies. The interviews have been used to see whether the classification of the taxonomy model is correct and also complete. At the same time, respondents have been asked their opinion regarding the trends and business side of virtualization. In the interviews different types of questions were asked. Questions were asked about the taxonomy and virtualization trends. Also, to get information about the business side of virtualization, questions have been asked about the business reasons/needs, challenges and personal views on virtualization technologies. These questions can offer more insight in possible business opportunities. They hold valuable information of which certain type of virtualization technologies might be upcoming and interesting from a business point of view. For example, information about the business reasons/needs, challenges can explain a certain need or challenge that an upcoming virtualization technology will address, which can make it an interesting business opportunity. The results are used to evaluate the taxonomy model and are also compared to see what the virtualization trends are.

For the case study, the data collection consisted of interviews with experts that have expertise in virtualization. Experts have been contacted from Atos Origin as well as from virtualization vendors. During the evaluation phase, the aim was to include a large variety of experts to gain as many different insights as possible. Otherwise, there is the potential pitfall of becoming overly dependent on information from a key respondent, whereas combining information from other respondents can bring different or additional insights. However, due to the limited time scope of this project and availability of experts we managed to conduct interviews with four experts from Atos Origin and four experts from virtualization vendors. The initial idea was to include more experts with expertise in different virtualization domains to gather enough information on virtualization trends and to explore each virtualization domain of the taxonomy model. However, time and availability of respondents was limited and the results provided mainly information about the main virtualization trends. A detailed study of the business opportunities of virtualization technologies was not possible within the timeframe of this research project.

The respondents from Atos Origin and various virtualization vendors were divided into two cases of which the results have been compared afterwards. The first case was held with experts from Atos Origin and is called the internal group. The second case with the virtualization vendors is called the external group. A distinction is made between the internal and external group, because of the difference in expertise. Virtualization vendors are expected to have detailed knowledge of their software products and the latest developments of virtualization technologies. Experts from Atos Origin are expected to have more knowledge of implementation of virtualization technologies. This diversity may give distinct results. Also, experts from virtualization vendors might be more marketing orientated and biased, because they are representing their company's products on the virtualization market.

6.2 Case 1: internal group

In the interviews with experts from Atos Origin questions were asked about the taxonomy model, virtualization trends, business reasons, challenges and views on virtualization. The four respondents that were interviewed had a different expertise. Respondent 1 is a principal solution architect, who has expertise in many different areas. He writes many papers on IT related matters, such as virtualization and cloud and is seen as a visionary in Atos Origin. Respondent 2 is a solution lead architect and is involved in many virtualization implementations. Respondent 3 is a product manager and has knowledge of all types of IT-related products including virtualization products. Respondent 4 is a portfolio manager and has expertise in computing, network and storage related technologies.

In table 3, overview is made of the main interview topics and their results by using short descriptions and key words. In appendix D, a detailed report can be found of the interviews with the four respondents.

Table 3 Interviews internal group

Respondent	1	2	3	4
Taxonomy opinions	Management in particular is a challenge and important	Management and security is not something new.	Management tools and security will receive much attention.	All areas of virtualization technologies are covered.
Virtualization trends	Utility computing, packaging of computing resources	High availability and disaster recovery products.	VDI , managements and security products	Cloud integration services and cloud security services
Business reasons	Cost saving, flexibility	Cost savings, flexibility	Cost saving, flexibility, responsiveness to react to business requirements	Cost reduction and creating independency
Main Challenges	Capacity management/ utilization risk	Configuration takes a lot of effort. Still limited flexibility.	Immatureness of virtualization.	Provisioning of bare essentials
Personal views	Virtualization will	In future there will	Virtualization will	Virtualization is not

	become pervasive.	be no good reason not to virtualize	play an integral role for cloud	going to stop and its beginning of a new direction.

Starting with the taxonomy model, there was a general opinion among the respondents that the taxonomy model covered the different types of virtualization technologies. Overall, the feedback led to some minor corrections in the taxonomy model. In the security class, virtual security appliances were missing and in the management class the asset tools were missing. However, respondent 3 mentioned that the relationships between the domains are not shown in the taxonomy model. For instance, it does not illustrate the dependency of desktop virtualization and server virtualization. For desktop virtualization, server virtualization is first needed. He recommended that a layered approach might be more suitable.

Continuing with the virtualization trends the answers between the respondents were slightly different. One of the main reasons that became very apparent in the interviews was the different area of expertise of each respondent. It was very clear in the interviews that each respondent had more knowledge about particular virtualization technologies. Respondents 1 and 4 both mentioned utility computing or cloud as the main trend. Their view is that virtualization technologies will facilitate the packaging of computing resources in what is called “cloud” that will enable the offering of IT services. The general idea is that organizations can purchase IT services and pay in the same manner as a metered service for the resources they use. Though this research is about virtualization technologies, cloud services are a development of which virtualization technologies are the building blocks that make it possible. However, respondents 3 had detailed knowledge in many virtualization domains and specifically point out, VDI, management tools and security tools as the main virtualization trends.

The business reasons for using virtualization technologies were very clear for each respondent, which was in particular cost saving. Cost saving is seen as the main reason why virtualization became popular. While not all of the virtualization technologies are certain to bring cost savings, server virtualization has been the most popular virtualization technology to cut cost in organizations. Next to cost savings, flexibility is the second reason as it allows organizations to react more quickly to business needs. An example that one of the respondents gave was when a company wants to deploy a new web service, virtualization allows for instant deployment of IT resources to host the web services, because new servers can be deployed in minutes.

When discussing the main challenges of virtualization the opinions of each respondent were varied. However, there was a general opinion that virtualization technologies still need to improve and implementation is often not so easy. As can be seen in table 1, there are management challenges, configuration challenges and immatureness of virtualization technologies. The respondents noted that virtualization technologies are still maturing and that virtualization vendors have given more attention to important areas such as management and security. In virtual environments, areas like management and security are not well covered as in traditional IT environments.

Lastly, the personal views of the respondents showed that they see virtualization technologies as something that is going to change the IT world and will not go away. While developments continue they expect that virtualization will manifest in many IT-related products.

6.3 Case 2: external group

Similar to case 1, in the interviews with experts from virtualization vendors, questions were asked about the taxonomy model, virtualization trends, business reasons, challenges and personal views on virtualization. The virtualization vendors that were interviewed are: VMware, Microsoft, Citrix and Quest Software. The first three are the three largest virtualization vendors [99]. While VMware is still the market leader in virtualization, Microsoft and Citrix are not far behind with their virtualization products.

Respondent 1 is a solutions architect and senior system engineer at VMware and has an advising role. He does many presentations and workshops for VMware. Respondent 2 is the principal product architect at Quest Software and has expertise in virtualization products. Respondent 3 is a business partner manager at Citrix and is the primary point of contact and intermediary regarding Citrix products. Respondent 4 is a product marketing manager from Microsoft and has detailed knowledge about virtualization products.

In table 4 the results of interviews are shown in keywords. In appendix D a detailed report can be found of the interviews with the four respondents.

Table 4 Interviews external group

Respondent	1. VMware	2. Quest	3. Citrix	4. Microsoft
Taxonomy opinions	Security is an integral part of all the other domains. Management tool is an option.	Management and security are very important	Management and security are an integral part and condition for successful virtualization	Correct, but I would add user profile virtualization as additional domain. Management is vital to success.
Virtualization trends	Desktop virtualization and Cloud	Desktop, application virtualization and management tooling	Desktop - new way of working	Desktop, Application and management tooling
Business reasons	Cost savings, flexibility	Cost savings, more flexibility (faster service delivery)	Cost saving, flexibility	Cost saving, flexibility
Main challenges	Cultural change, different mindset	Return of investment (ROI) of desktop virtualization.	Return of investment (ROI) on short term	Management is one of the greatest challenges
Personal views	Virtualization will become the standard and will not go away.	Desktop and app as a Service delivered in cloud	Virtualization tends to go to “consumerization”. Users determine what they want.	Further automation of IT infrastructure.

In the interviews, the taxonomy model was observed in a positive way, but some remarks were made that suggest a revision of the taxonomy model. All the respondents mentioned that management and security are very important technologies for successful implementation of virtualization. Especially management technologies are currently receiving much attention. However, a remark was made by

respondent 3 that user state or profile virtualization is an important development and is an additional virtualization domain. The same goes for presentation or access virtualization, which is also not present in the taxonomy model. Furthermore, the taxonomy model does not illustrate the relationships and dependencies between the domains.

When discussing the trends, the answers between all the respondents were quite similar. Desktop virtualization is one of the technologies that is expected to become important in the years to come and is already very popular. One of the main reasons of its popularity, that was addressed, is the possibility for organization to offer what is called “a new way of working”. Employees can access their desktop from anywhere, anyplace and anytime.

Also, among the respondents there was a clear and similar opinion about the main business reasons for using virtualization technologies. Respondents answered that the popularity of virtualization is mainly due to its cost saving aspects. Respondent 1 of VMware said that with the economic recession of the recent years their organization still made profits, as organizations seek ways to cut cost. The second business reason is flexibility, which enables IT to react much faster and easier to business needs/requirements.

The opinions of the respondents on the main challenges of virtualization were varied. Respondent 1 had a more broad vision about virtualization and explained the cultural change that virtualization brings. He explained that people are hesitant to share their IT resources with others. People do not see the benefits of sharing resources more effectively with others when they are not using it. According to him, there is a lack of understanding when people are not familiar with IT and are hesitant about sharing their (unused) resources. Respondent 2 mentioned in particular desktop virtualization and explained the challenges. Implementing desktop virtualization in large organizations requires enormous investments of which short term cost benefits are uncertain. Respondent 3 had a similar but general opinion that organizations are very careful about their investments and a return of investment (ROI) within a period of 3 to 4 years is not attractive. Respondent 4 explained that management is one the greatest challenges. Many organizations are not mature and ready enough to implement some of the virtualization technologies. The example he gave is desktop virtualization, which requires proper security, application and profile management for successful implementation.

The views of the respondents indicated that virtualization vendors see virtualization technologies as the future of IT and will not go away. The view of respondent 1 on virtualization is that virtualization brings a new way of working that will enable IT service providers to react and deliver much faster and easier to business needs. Respondent 2 is thinking about cloud services that are made possible by virtualization. According to respondent 3, an important development in virtualization is that technology is available which enable users to determine where they work and what applications they need. Respondent 4 thinks that further development of virtualization technologies will lead to more automation of IT, which means that technology will automate more IT-related tasks.

6.4 Conclusion of case studies

The case study method was used for two reasons. First of all, the main reason is the evaluation of the taxonomy model. Secondly, the case study is used to gain insight into the virtualization trends. Conclusions regarding the taxonomy model and virtualization are discussed consecutively in section 6.4.1 and 6.4.2.

6.4.1 Taxonomy model evaluation

The respondents of the two case studies provided a good evaluation of the taxonomy model. When comparing both results, there are many similarities. In both cases, the respondents were positive about the taxonomy model. However, important remarks were made that have to be taken into account. First of all, the relationships and dependencies between the virtualization domains are not illustrated very well in the taxonomy model. One of the respondents mentioned that a layered approach can show the dependencies between the virtualization domains and might be a better way to structure the virtualization domains.

Furthermore, an important virtualization domain called user state virtualization was not shown in the taxonomy model. The same goes for presentation or access virtualization. In chapter 4, user state and presentation/access virtualization were mentioned as an integral part of desktop virtualization. In a traditional desktop, the operating system, applications and user profile are welled together into one large entity called desktop. User profile virtualization makes it possible to separate the user profile layer as application virtualization does with the application layer. User state virtualization is not shown in the taxonomy model as well as presentation/access virtualization that provides the graphical interface of the desktop at the location of the user. Both are virtualization domains.

Lastly, management and security can also be seen as virtualization domains, because management and security technologies are developed that are specifically made for virtualization. The remarks of the respondents were taken into account and have led to a revision of the taxonomy model. The revised taxonomy model is shown and discussed in chapter 7.

6.4.2 Virtualization trends

The two cases provided many insights in the trends of virtualization. Results of both cases showed that the business reasons are first of all cost savings and secondly flexibility. The opinions of all respondents were exactly the same on this subject. Regarding trends and challenges there were some differences. While the virtualization vendors talked about desktop virtualization and management tools the answers from the Atos Origin experts were more varied. They talked more about cloud services and not virtualization technologies in specific. A plausible reason might be the background and expertise of the experts. In case 2, the respondents of the virtualization vendors had more knowledge about different types of virtualization technologies. However, one particular respondent from case 1, who is a product manager with detailed knowledge on different virtualization domains had a similar opinion.

The overall findings show that desktop and management technologies are becoming very popular and receive much attention by virtualization vendors. Reasons for its popularity are the need of organizations for seeking new flexible and easier methods of offering work places and the limited functionalities of traditional management tools for virtual environments. For successful management of virtualization environments new tools are needed that are virtualization aware and provide more functionality to manage virtual environments more effectively. Management issues have been addressed on configuration management and capacity management. By tackling these difficulties more cost savings are possible. Furthermore, security technologies for virtualization are receiving more attention by virtualization vendors. According to the case study, security is also very important for successful implementation of virtualization, but security tools that are fully aware of the virtualization

layer are lacking. Much development in security tools for virtualization is expected in the coming years.

Lastly, the views of all the respondents indicate that virtualization technologies are likely to go away, but will become an integral and vital part of IT infrastructures. In the years to come, virtualization technologies are expected to grow more towards the business side of an organization, because it allows IT to react much faster to business needs than traditional environments.

6.5 Quality of Case study

To establish the quality of any empirical social research, four tests have been used that are common to all social science methods [100]. The four tests are construct validity, internal validity, external validity and reliability. Yin [101] describes case study tactics for dealing with these four tests. For each test the tactics are explained which are used for this case study.

Construct validity

Construct validity is about identifying the correct operational measures for the concepts being studied [100]. For this research, the case study focused on trends in virtualization technologies. Construct validity in this case is about how much the findings reflect the virtualization trends in the real world. Yin [101] describes three tactics to increase construct validity when doing case studies. These are using multiple sources of evidence, establish a chain of evidence and have the case study report reviewed by key informants. For this research one of the three tactics can clearly be identified. First of all, multiple sources of evidence were used. Interviews were conducted with experts of different organizations. However, the goal was to contact a larger group of experts with expertise in all the different virtualization domains. More respondents are needed to research the business opportunities of virtualization technologies, but the two cases did provide information about the main virtualization trends.

Internal validity

Internal validity is for explanatory case studies that are seeking to establish a casual relationship, whereby certain conditions are believed to lead to other conditions [100]. Tactics are pattern matching, explanation building, addressing rival explanations and using logic models. The case studies of this research can be described as an exploratory study, because it seeks to identify trends and are not concerned with this kind of causal situation. Therefore internal validity is applicable for explanatory studies and not exploratory studies.

External validity

External validity deals with the generalization of the research findings beyond the immediate case study. The external validity test is concerned with extent to which the results of a case study can be held true for other case studies. The advised tactics are to avoid using single cases, because they offer a poor basis for generalization [100]. In this case study, two cases have been used of which the results were compared. The results were very similar and provided many views on the matter. The differences in answers between respondents are not contradictions of other results, but give additional insight in what is going on. The questions that were being asked were very open and one answer is not better than the other, but provided an additional view on the subject at hand. When more cases or respondents are added to the case study, it is expected that this will lead to more insights instead of contrasting results.

Reliability

Reliability is about demonstrating that if study is repeated the same results will follow. The emphasis is about doing the same case over again and not replicating the results of one case by doing another. The tactic for this test is to make as many steps operational as possible and to develop a case study database. In section 6.1, the research procedures of the case study have been described, which can be used to repeat the case study. Also, in appendix D the collected data is stored with detailed reports of the interviews that can be reviewed.

6.6 Summary and outlook

The case study provided a lot of information about the main virtualization trends, but also constructive remarks on the taxonomy model. The overall findings of the virtualization trends are that the desktop virtualization and management technologies are becoming very popular and receive much attention by virtualization vendors. Reasons are that organizations seek new flexible way of offering work places and traditional management tools are insufficient for virtual environments. For successful management of virtualization environments, tools are needed that are virtualization aware and provide more functionality to manage virtual environments effectively. Furthermore, management issues have been addressed and the main business reason for virtualization is in particular cost savings. By tackling the issues of virtualization more cost savings are possible. Furthermore, security is also seen as very important. Security tools for virtualization are expected to receive much attention in the coming years. In the case study the answer has been given of the fourth and last research question that states:

- What are the virtualization trends?

The case study provided much insight in the trends of virtualization technologies. However, regarding the business side of the technologies more research is needed to discuss the business aspects in more detail. The number of respondents was insufficient to explore all the virtualization domains for business opportunities.

In chapter 7, a new taxonomy model is presented that has taken into account the remarks of the experts of the case study. Chapter 8 reflects on the choices made throughout the course of this research project. In chapter 9, conclusions are given that answer the main research question. Also, recommendations have been made for Atos Origin in which possible business opportunities are discussed based on the research findings.

7. Revised taxonomy model of virtualization domains

In the previous chapter, the case study method was used to evaluate the taxonomy model. In the two cases that were presented, virtualization experts made some important remarks on the taxonomy model. The results of the case study indicated that the taxonomy model lacked to illustrate the relations and dependencies between the main virtualization domains. Also, not all virtualization domains were present in the taxonomy model. It was also suggested that with a layered model approach, the dependencies between the virtualization domains can be made visible.

Therefore, a revision of the taxonomy model is presented in this chapter that aims to structure the virtualization domains in a correct way. In figure 24, the revised taxonomy model is presented, which uses a layered approach to portray the relations between the virtualization domains instead of UML. The use of the modeling language UML for the taxonomy of chapter 5 did lead to an overview of the structure and hierarchy between the domains and the underlying type of technologies, but was limited due to the fact that it would make the taxonomy model overly complex when we tried to illustrate the relationships between the virtualization domains in a correct way. For this reason, a layered approach was chosen to structure the virtualization domains in a more suitable way. In section 7.1, each layer of the taxonomy model is discussed in turn, starting at the bottom. In section 7.2, conclusions have been drawn from the revised taxonomy model.

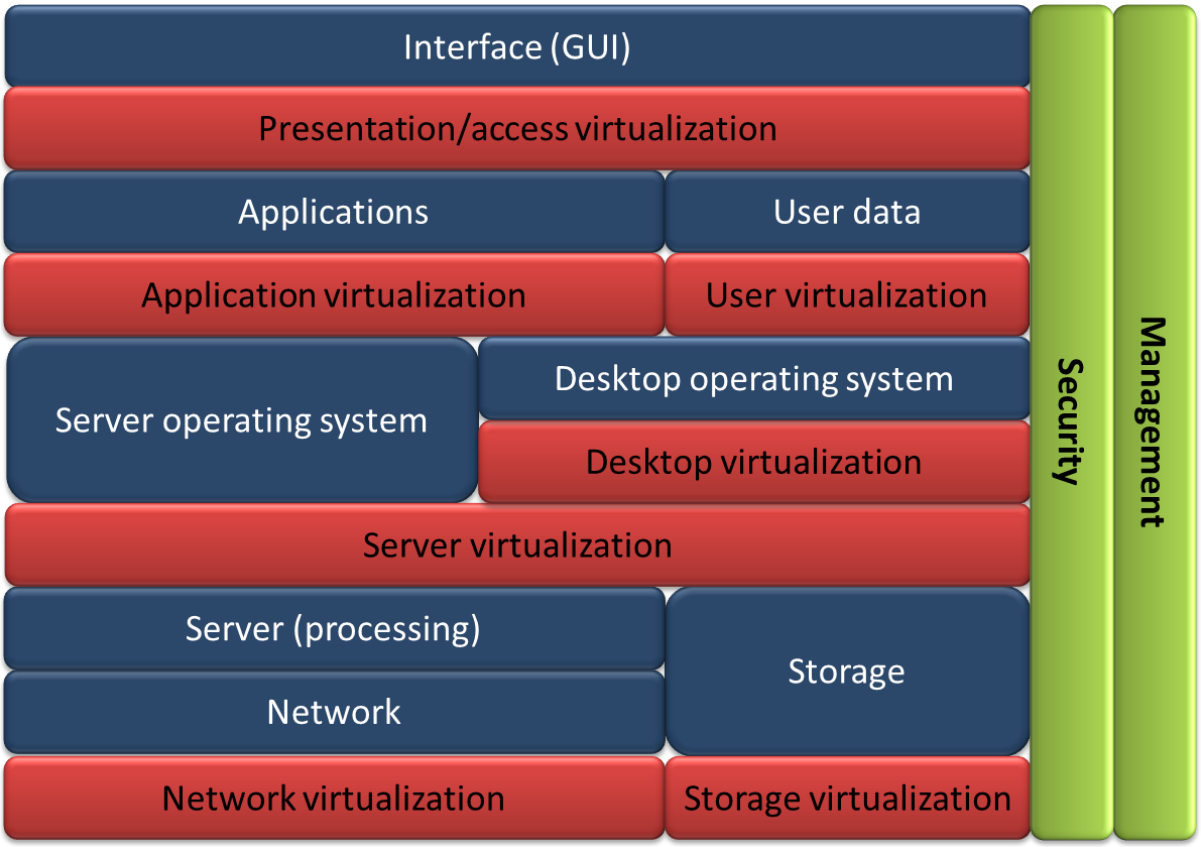

Figure 24 Revised taxonomy model

7.1 Layers of the taxonomy model

Figure 24 illustrates the architecture of a virtual server and consists of multiple hardware and software layers that operate together as a system. The following layers will be discussed consecutively: the blue layers, the red layers and green layers.

The blue layers

The blue layers indicate the hardware and software layers that are present in a typical server environment. On the bottom, the network layer is concerned with the network requests of the upper layers and facilitates the communication from server to server or storage device, which can be located on the same private network or on a public network, such as the Internet. It is responsible for controlling the network operations imposed by the server and operating system in the upper layers by delivering or transferring data from source to destination.

The storage layer is concerned with the storage and retrieval of data. The storage layer is put next to the server (processing) layer as well as the network layer, because storage can be a storage device attached to the server via a network (SAN and NAS) or local storage directly attached to the server. The server (processing) layer is concerned with carrying out the instructions of operating system layer above. The server consists of hardware components that process the instructions imposed by the upper layers, such as a Central Processing Unit (CPU), memory, or a Network Interface Card (NIC).

The server and desktop operating system layer act as intermediaries with applications and computer hardware. It is a software platform that manages the applications of the upper layer and handles the request of the computer programs or applications. Furthermore, it regulates the ways applications communicate with computer hardware and the way users interact with the other layers in the model. However, in a traditional server environment without virtualization, a server operates one type of operating system (OS) or instance at a time. With virtualization, which will be explained in the red layers below, multiple instances or operating systems with their own applications can operate at the same time. Each instance is called a virtual machine, which was explained in chapter 3. This way, it is also possible to host multiple virtual machines with pre-configured desktops, next to other virtual machines that host a web server or database. These virtual machines are called virtual desktops. Therefore, in a virtual environment multiple (desktop or server) operating systems can exist next to each another. In figure 24, a distinction is made between two types of operating systems: server and desktop. The difference is that a desktop operating system is a special instance or virtual machine in which desktop virtualization is used to create virtual machines with the purpose of hosting desktops.

The application layer is concerned with requests and tasks imposed by the interface layer above. The applications in the layer are designed to perform an activity or set of tasks that can be performed when a request or action is made in the interface layer above.

The user data layer is concerned with the actions and changes made in the application layer. In a desktop environment, users can performs tasks such as installing new applications, making or editing of documents, changing settings to their preference, etc. These tasks produce new personal data, which are called user data.

The interface layer is the point of interaction between a user and the lower layers. The Graphical User Interface (GUI) allows people to interact with computer programs in the layers below by offering graphical icons and elements which can be controlled.

The red layers

The red layers in the taxonomy illustrate the levels and layers in which the main virtualization domains relate to each other. On the bottom, network virtualization and storage virtualization can be applied in the network layer and the storage layer. For network and storage virtualization technologies it is not a prerequisite to have server virtualization or other types of virtualization technologies.

Server virtualization takes place above the server (processing) and storage layer and beneath the operating system layer. This layer is also called the virtualization layer, which enables the creation of multiple isolated instances called virtual machines. Each virtual machine is equipped with their own OS and application(s), which means that multiple operating systems can operate at the same time. Server virtualization comes also equipped with network and storage virtualization technologies. Furthermore, with server virtualization it is also possible to create virtual desktops, which is another term for a virtual machine intended for desktop purposes. In the same manner as virtual machines, multiple virtual desktops can be placed on a server, which means that multiple desktop operating systems can be placed on top of the server virtualization layer.

Desktop virtualization is placed directly on top of the server virtualization layer. A virtual desktop is a virtual machine. Depending on the type of desktop virtualization technology, virtual desktops can be made for each user or a (shared) virtual desktop for a group of users.

Application virtualization takes place above the operating system layer and allows for the decoupling of the applications layer from the operating system layer. This way, applications can be isolated from the OS and can be executed without installation on the OS. Application virtualization technologies have been used without other virtualization domains, such as server virtualization and desktop virtualization. However, full application virtualization requires presence of a virtualization layer or server virtualization. Full application virtualization means using the full palette of application virtualization technologies, where applications are streamed or executed from a central location. This way, applications can be updated or changed from one point in a central location.

User virtualization, also known as user state or profile virtualization creates an abstraction layer between user data by separating user data, such as profile settings, user application data and storage data from OS and application. The user data is now stored separately from the application or OS and not interwoven.

Presentation or also called access virtualization creates an abstraction layer between user interface and the other layers below, which allows to user to access and control the other layers remotely. There are many different protocols for access virtualization. Some protocols allow different type of devices or handhelds to be used to remotely access their desktops, applications, etc. The General User Interface (GUI) is streamed towards the device. User virtualization and presentation or access virtualization are both virtualization domains that in particular are used in combination with desktop virtualization.

The green layers

The green layers show the relation between the management and security domain with the other main virtualization domains. Both management and security tools are also seen as types of virtualization technologies, because with virtualization new security and management issues have been addressed. This has led to the development of new management and security tools for virtual environments.

Management and security tools have a relation with each of the other layers and have a supporting function. For each particular layer, management and security tools can be used to provide management or security measures.

7.2 Conclusions

Comparing the revised taxonomy model with the previous taxonomy model presented in chapter 5, the layered approach is able to structure the virtualization domains in a more correct way, because it illustrates their relations as well as their dependencies. Also, the revised taxonomy model demonstrates a virtual server architecture in which all virtualization domains have been structured. While the previous taxonomy model did not structure the virtualization domains in similar manner, it does provide a detailed overview of the different types of virtualization technologies that exist in the virtualization domains. However, the revised taxonomy model was able to structure the virtualization domains in a more suitable way and at the same time has taken the expert remarks of the case study into account. Therefore, the revised taxonomy model is the definitive taxonomy model of this research project.

8. Reflection

Throughout the course of the research project choices were made, which are explained in this chapter. At the beginning of the research project, the main goal was to understand the concept 'virtualization' and explore the virtualization technologies and virtualization services. At this point, we aimed to obtain as much information about virtualization as possible. A first search through literature showed that there were many virtualization vendors, virtualization technologies, virtualization services and a lot of papers describing virtualization products of virtualization vendors. In the different papers, it became apparent that the amount of virtualization products was enormously and it was too extensive to research all virtualization products and services. Also, each virtualization vendor used different terms for similar types of products and similar types of services that are in fact different underneath. Therefore, a demarcation was made to explore the general types of virtualization technologies that cover all the types of virtualization products.

Furthermore, due to the huge load of information on virtualization it was difficult to decide what to explain in the report and in how much detail. That is why some of the chapters were put in the appendix. Also, we hope that the research report is accessible and understandable for researchers who are not familiar with virtualization.

After the design of the taxonomy model the initial idea was to explore the virtualization trends and look for business opportunities. During this phase of the research, the aim was to contact a wide variety of experts with expertise in different types of virtualization technologies. This way, detailed information can be gathered of each specific virtualization domain that might help explore the business side of these virtualization technologies. The case study research was somehow limited, because it was difficult to arrange a meeting with a large group of experts in the available amount of time of this research project. However, a small group of experts was contacted of which the case study results did provide information about the main virtualization trends and some possible business opportunities. The information extracted from the interviews gave some insight in business opportunities, but further research is needed to explore the business aspects of the virtualization technologies in more detail.

During the virtualization events we encountered many virtualization companies with a certain specialization. For example, in the storage domain there were many small companies that offered distinct storage virtualization technologies. Hence, further research might be able to gather detailed information about each specific virtualization domain. Furthermore, criteria need to be defined on which a business opportunity is based. The main focus of this research has been the structuring of virtualization technology domains and identifying virtualization trends, which give a general direction for business opportunities. However, additional research about the business side of virtualization technologies is needed to address the business opportunities in detail.

9. Conclusions & Recommendations

The main research question of this master's thesis was:

Which trends in virtualization technologies can be identified and how can they be structured?

The research was conducted in phases. For the different phases the main research question was divided into four research questions. The second part of the research question was answered by designing a taxonomy model that was able to structure the virtualization technologies. For the first part of the research question, a case study was held to gain insight in the virtualization trends that provided a general direction of possible business opportunities.

In section 9.1, conclusions are given that answer the main research question. Section 9.2 contains the recommendations for Atos Origin that are based on the findings of the research project.

9.1 Conclusions

During the research project, it became apparent that there are many different types of virtualization technologies, which can be categorized into several virtualization domains. These virtualization domains have been structured in a taxonomy model, which is depicted in figure 25.

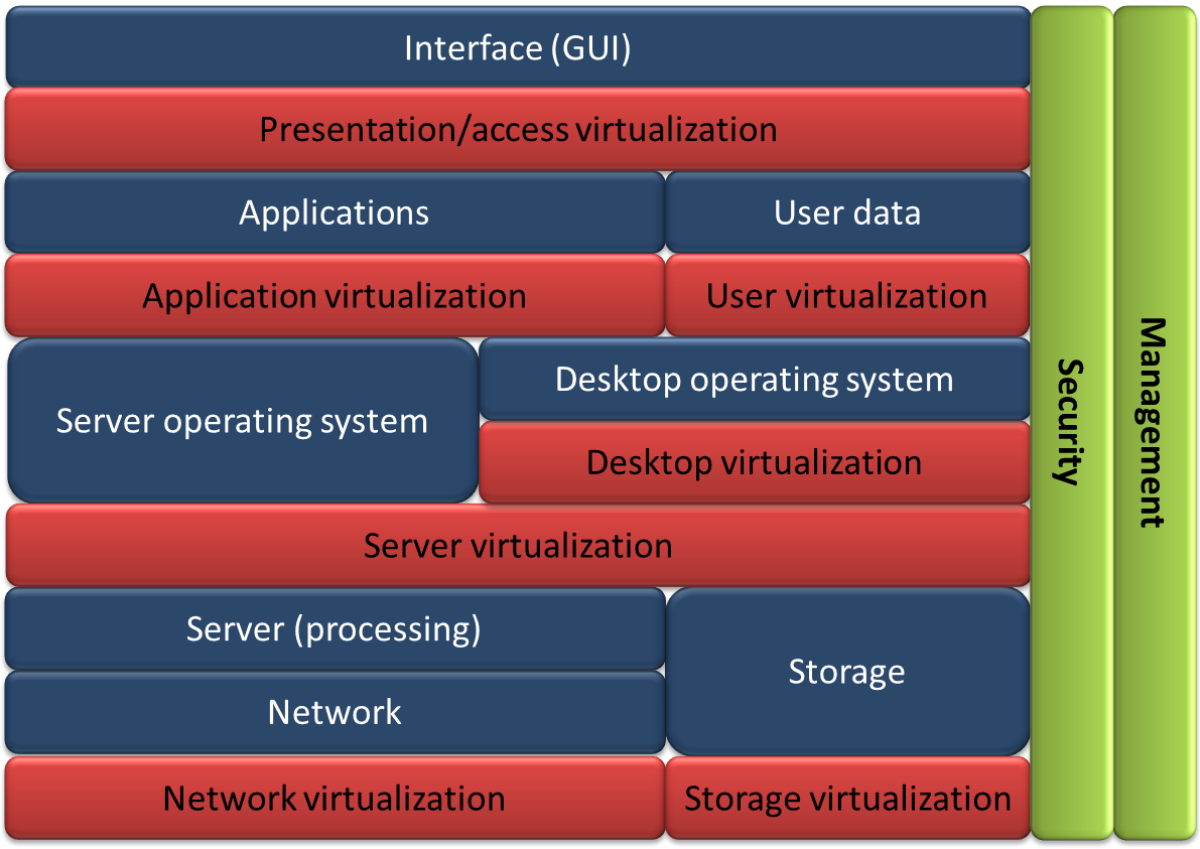

Figure 25 Taxonomy model

Figure 25 illustrates the architecture of a virtual server and consists of multiple hardware and software layers that operate together as a system. The blue layers are the hardware and software, which can be found in a typical server environment. The main virtualization domains are indicated as red layers and the other two virtualization domains as green layers. In the green layers, management and security are virtualization domains that have a supporting function towards all the other layers, because management and security technologies can be used to provide management or security measures for each particular layer. Management and security are indicated as separate virtualization domains, because new management and security tools have been developed for virtualization in particular.

The taxonomy model presents a structured overview of the virtualization domains and their relations and dependencies. It represents a typical server architecture that is composed of server (processing) hardware, storage, network, one or more operating systems and software applications. Starting from the bottom, the taxonomy shows the different hardware and software layers as well as the function and position of the virtualization domains.

Furthermore, a case study was conducted to evaluate the taxonomy model and to obtain information about the virtualization trends. Interviews were conducted with experts from Atos Origin as well as experts from several virtualization vendors. From these interviews it was possible to gain insight in the main trends of virtualization. The main virtualization trends are in the desktop domain, management domain and security domain.

Desktop virtualization

Desktop virtualization is a virtualization domain in which many developments have been made. The case study showed that desktop virtualization is an emerging virtualization technology that is becoming very popular. One of the main reasons for its popularity is that it allows organizations to facilitate new and flexible ways of working. With desktop virtualization, organizations can offer their employees access to their workplace desktop from anywhere, anyplace and anytime. It enables employees to work on their preferable location. Workplaces for employees can be instantly deployed and managed from a central location.

Management tools

While there are many management tools for traditional IT environments, management tools for virtual environments are often insufficient. Research has shown that virtualization is accompanied with many challenges, in particular regarding management. Virtual environments require management similar to traditional environments, but without the appropriate tools this is very difficult. The case study indicated that management tools are very important for the successful implementation of virtualization and vendors are currently focused to address the limited functionalities of traditional management tools. At the moment, more and more management tools are being developed that provide more functionality. The management tools are expected to tackle many challenges of virtualization, such as capacity and configuration management.

Security tools

New technologies bring new security risks, which is also the case with virtualization. While more IT infrastructures are being virtualized, security for virtualization has become more critical to address. Research indicated that there are many security risks and issues with virtualization technologies that

pose a significant challenge for virtualization and security vendors. One of the main issues with virtualization is the lack of security technologies to be (fully) aware of virtual environments. Virtual security appliances have been developed, but still pose security risks, because they are placed inside virtual machines above the virtualization layer. Progress in this area has been lacking over the years. However, attention for security technologies has increased by virtualization vendors and development has started on security appliances that are placed inside the virtualization layer or hypervisor. This way, the security appliance is fully aware of the virtualization layer. New security tools based on this hypervisor approach are expected to appear in near future.

The initial idea was to explore possible business opportunities for every main type of technology. However, the case study of the research project was limited, because this research did not cover the business aspects of the virtualization technologies in detail. The case study did provide information about the main trends of which some general directions for business opportunities could be extracted. Nonetheless, more research is needed to explore each domain in detail for business opportunities by extending the case study with experts from more virtualization vendors.

9.2 Recommendations for Atos Origin

The following recommendations have been made for Atos Origin in particular. These recommendations are based on the findings of this research project.

- **Desktop virtualization is expected to continue and increase its growth significantly in the years to come. However, combining desktop virtualization with application virtualization and user state virtualization hold interesting business opportunities. Application virtualization is currently offered as a separate service. Combining this service with desktop virtualization and user state virtualization allows for a better desktop service offering. This combination is also called the three layered approach and is different from standard VDI solutions.**
  An interesting development in desktop virtualization is user (state/profile) virtualization. In combination with application virtualization, it allows for the separation of the desktop environment into three layers. OS, application and user profile layer. This separation makes it possible to manage each layer independently without impacting the other layer. This layered approach enables administrators to build and test various layers without affecting the other layers. It reduces complexity and manageability of delivering virtual desktops. Application virtualization is currently offered as a separate service. Application virtualization, desktop virtualization in combination with user virtualization can be offered as one desktop virtualization service.

- **Interesting developments are happening for virtualization security technologies. Keep an eye out for new virtual security appliances, as it can help providing better security solutions to the customer.**
  Traditional security tools are often not suitable, because they are not designed with the awareness of the virtualization layer. While more and more physical servers are being virtualized, security issues associated with virtualization have become more critical to address.

Research indicated that virtualization creates new security challenges, because virtual machines are mobile, which make IT infrastructures more dynamic. As mentioned in the conclusions, security appliances are being developed that are placed in the virtualization layer. This is the first kind of security appliances that are specifically designed for the virtualization layer and might be an interesting development for Atos Origin, because it can help providing better security solutions for virtual environments.

- **New management tools, specially designed for virtualization, tackle a lot of management issues and hold interesting business opportunities. These management tools can offer clients better control of their virtual IT environment and can be provided via a new virtualization management service.**
  Virtual IT environments require the similar management as traditional IT environments with the exception that traditional management tools offer limited functionality for virtualization environments. Currently, virtualization vendors are addressing this issue and are developing management tools with better functionality that provides users more insight and control of their virtual IT environment. While management tools for virtualization are still immature there are some interesting technologies that hold business opportunities. The case study indicated that management is very important for successful implementation of virtualization. Virtualization vendors are currently focused to address the management issues, such as configuration management, capacity management and asset management. Management tools can be used to give the customers additional functionalities that enable them to manage their resources more effectively, which can lead to additional cost savings. Cost savings are often the main business reasons for using virtualization. However, management tools do not only help customers to increase their cost savings, but also reduce complexity in controlling virtual environments. In figure 26, different types of management tools are depicted that can be used to provide a new virtualization management service that would offer clients better control of their virtual IT environment. The management tools are described below.

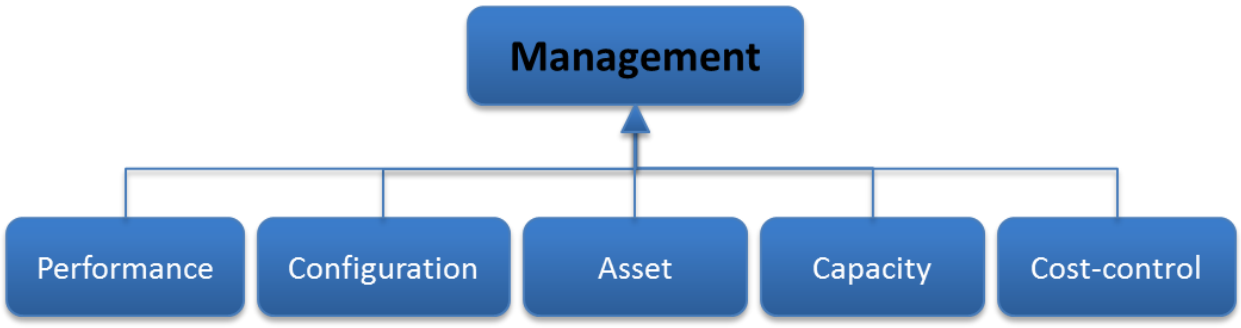

Figure 26 Management tools

The management tools that are depicted in figure 26 are five types of management tools, which software vendors began developing for virtualization. In the near future more types of management tools for virtualization might appear. Below each type of management tool is explained.

- Application performance monitoring tools can graphically map the virtual environment and are equipped with an automated discovery feature for servers in both virtual and physical infrastructures. The performance management tool enables an organization to monitor and analyze the performance of the virtual infrastructure. It measures the latency experienced between application and end-users and can identify application performance bottlenecks. Furthermore, applications can be tested how they would perform in a virtualized environment, which can eliminate uncertainty about making critical business applications virtual.

- Configuration management tools can be used to track configuration of virtual machines, analyze their configuration and check whether they comply with the standards determined by the organization. Customers have the ability to pro-actively to see how changes will impact the virtual environment in what way. For instance if an organization want update or add a new SAN storage, this management tool can show which virtual machines it will impact.

- Asset management tools that can be used to analyze and track what assets an organization has in their IT environment. An asset can be hardware components, but also software, such as applications and virtual machines.

- The capacity management tools can be used to provide the customer an automated approach to estimate the capacity that is needed, unused and forecast timing of shortfalls. Also impacts can model to analyze the effect of capacity changes.

- Cost control management tools can be used to provide the customer the ability to manage their costs in an automated way. Cost control tools offer insight in resource utilization of users and budget requirement for different departments of an organization and help determine where most of the costs are being made. It allows for customers to optimize the budgets of an organization.

Literature

[1] IDC. (2006). DOI=http://www.networkworld.com/news/2006/102506-idc-virtualization.html

[2] Bittman, T.J. (2009). *Virtual Machines and Market Share Through 2012*. Gartner. Publication date: 7 October 2009

[3] Searchdatacenter.com. *Definition of infrastructure*. DOI=http://searchdatacenter.techtarget.com/sDefinition/0,,sid80_gci212346,00.html

[4] Dynamic quest. DOI=http://www.dynamicquest.com/virtualization.php

[5] Bhatia, S.; Motiwala, M.; Muhlbauer, W.; Valancius, V.; Bavier, A.; Feamster, N; Peterson, L.; Rexford, J. (2008). *Hosting virtual networks on commodity hardware*. Georgia Tech Computer Science Technical Report GT-CS-07-10.

[6] Cherkasova, L; Gardner, R. (2005). *Measuring cpu overhead for i/o processing in the xen virtual machine monitor*. Proceedings of the USENIX Annual Technical Conference (ATEC). Berkeley, CA, USA, pp. 24-24.

[7] Soltesz, S.; Potzl, H.; Fiuczynski, M.; Bavier, A.; Peterson, L. (2007). *Container-based operating system virtualization: A scalable, high-performance alternative to hypervisors*. Proceedings of the ACM SIGOPS European Conference on Computer Systems, pp. 275-287

[8] Keller, E.; Green, E. (2008). *Virtualizing the data plane through source code merging*. SIGCOMM Conference and the Co-located Workshops - PRESTO'08: Proceedings of the ACM Workshop on Programmable Routers for Extensible Services of Tomorrow, pp. 9-14. ISBN: 978-160558181-1

[9] Egi, N.; Greenhalgh, A.; Handley, M.; Hoerdt, M.; Mathy, L.; Schooley, T. (2007). *Evaluating xen for router virtualization*. Proceedings - International Conference on Computer Communications and Networks, ICCCN, art. no. 4317993, pp. 1256-1261. ISBN: 978-142441251-8

[10] Adams, K.; Agesen, O. (2006). *A comparison of software and hardware techniques for x86 virtualization*. ACM SIGPLAN Notices, 41 (11), pp. 2-13. DOI=http://delivery.acm.org/10.1145/1170000/1168860/p2adams.pdf?key1=1168860&key2=2402819611&coll= portal&dl=ACM&CFID=57809500 &CFTOKEN=27978298

[11] Atos Origin. *Adaptive virtualization services*. DOI=http://www.nl.atosorigin.com/NR/rdonlyres/3D2BFCC0-6DBF-4BBD-AC46A8BA380AB407/0/AdaptiveVirtualizationServices_lowres.pdf

[12] Mens, T.; Van Gorp, P. (2006). *A Taxonomy of Model Transformation*. Elsevier. Electronic Notes in Theoretical Computer Science 152. pp. 125-142

[13] March, S. T., and Smith, G. (1995). *Design and Natural Science Research on Information Technology*. Decision Support Systems (15:4). December 1995, pp. 251-266.

[14] Baskerville, R; Pries-Heje, J; Venable, J. (2009). *Soft Design Science Methodology*. Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology. Article No. 9. ISBN:978-1-60558-408-9

[15] Hevner, A.R.; Ram, S.; March, S.T.; Park, J. (2004). *DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH* . MIS Quarterly Vol. 28 No. 1. March 2004. pp. 75-105

[16] Singh, A. (2004). *An introduction to virtualization*. DOI=http://www.kernelthread.com/publicationsvirtualization.

[17] Kiyanclar, N. (2005). *A survey of virtualization techniques focusing on secure on-demand cluster computing*. ArXiv Computer Science e-prints. November 2005. Provided by the SAO/NASA Astrophysics Data System.

[18] Ray, E.; Schultz E. (2009). *Virtualization security*. ACM International Conference Proceeding Series, art. no. 42

[19] Bolton, D. *Definition of virtualization*. DOI=http://cplus.about.com/od/glossar1/g/virtualization.htm

[20] EDACafe. (2009). *Roundtable: Virtualization & Simulation*. DOI=http://www10.edacafe.com/nbc/articles/view_weekly.php?articleid=748878&page_no=1

[21] Armstrong, B. (2004). *Virtualization versus Emulation*. Virtualization Program Manager. DOI=http://blogs.msdn.com/virtual_pc_guy/archive/2004/10/18/243821.aspx

[22] NetIQ. (2010). *Virtualizing Your Mission-Critical Applications: Seven Things You Must Know*. DOI=http://www.bdstrategy.com.au/virtualization/38-virtualization/342-virtualizing-your-mission-critical-applications-seven-things-you-must-know

[23] Sun Microsystems. (2009). *Data Center Optimization: Three Key Strategies*. Whitepaper. CIO Custom Solutions Group. DOI=http://whitepapers.techrepublic.com.com/abstract.aspx?docid=1621377

[24] Unisys. (2008). *The Virtualization Landscape to 2010*. White paper. DOI=http://whitepapers.zdnet.com/abstract.aspx?docid=1115307

[25] van Heerdern, H. (2009). *Virtualization – proper planning key for flawless execution*. Starship systems. DOI=http://www.eepublishers.co.za/view.php?sid=19016

[26] Murphy, *A. Virtualization defined – eight different ways*. White paper. DOI=http://www.f5.com/pdf/white-papers/virtualization-defined-wp.pdf

[27] Gammage, B.; Dawson, P.; Phelps, J.R.; Colville, R.J.; Scott, D.; Margevicius, M.A.; Basso, M.; Haight, C.; Williams, D.; Butler, A.; Cosgrove, T.; Fabbi, M.; Hewitt, J.; Kleynhans, S.; MacDonald, N.; Russell, D.; Govekar, M.; Kumar, R.; Buchanan, S.; Passmore, R.E.; Runyon, B.; Bittman, T.J.; Mishra, N.; Da Rold, C.; Ridder, F. (2009). *Hype Cycle for Virtualization*. Gartner, 21 July 2009

[28] Schumate, S. (2004*). Implications of Virtualization*. Technical Report 2004. DOI=www.dell.com/downloads/ global/power/ps4q04-20040152-Shumate.pdf

[29] Popek, G.J; Goldberg, R. P. (1974). Formal Requirements for Virtualizable Third Generation Architectures". Communications of the ACM 17 (7): 412 –421. DOI=http://doi.acm.org/10.1145/361011.361073.

[30] Smith, J.E. ; Nair, R. (2005). *Architectures of Virtual Machines*. IEEE Computer Society Press. May 2005. Volume 38(5), pp. 32-38

[31] Fisher, T. *Driver definition*. DOI= http://pcsupport.about.com/od/termsag/g/term_driver.htm

[32] Reuben, J.S. (2007). A Survey on Virtual Machine Security. Helsinki University of Technology

[33] VMware Icons and Images. (2009). DOI=www.vmguru.nl/.../ppt_library_vmware_iconsdiagrams_q109_final.ppt

[34] Madden, B. (2010). *Type 1 and Type 2 Client Hypervisors*. DOI=http://blog.sharevm.com/2010/03/09/type-1-and-type-2-client-hypervisors/

[35] Rizo, J. *A Listing of Virtualization and Remote Control Solutions: Running Windows or Linux Software on a Macintosh and Running Mac OS on other Platforms*. DOI=http://www.macwindows.com/emulator.html

[36] Goldberg, R. P. (1973). *Architectural Principles for Virtual Computer Systems*. Harvard University. pp. 22–26. DOI=http://www.dtic.mil/cgi-bin/GetTRDoc?AD=AD772809&Location=U2&doc=GetTRDoc.pdf.

[37] Cotton, P. (2008). *Sun xVM Hypervisor Overview*. DOI=http://www.sun.com/bigadmin/sundocs/articles/xvmhvsrovw.jsp

[38] Cochrane, N. (2010). *Stacking up the hypervisors*. CRNtech. DOI=http://www.crn.com.au/Feature/173728,stacking-up-the-hypervisors.aspx

[39] VMware. *DRS and DPM*. DOI=http://www.vmware.com/products/drs/

[40] VMware. *High availability*. DOI=http://www.vmware.com/products/high-availability/

[41] Man, A. (2007). *The pros and cons of virtualization*. BTQ, DOI=http://www.devx.com/vmspecialreport/Article/30383

[42] dos Santos Ramos, J.C.C.(2009). *Security Challenges with Virtualization*. Thesis, December 2009, DOI=http://docs.di.fc.ul.pt/jspui/bitstream/10455/3282/1/Thesis-JRamos-FCUL.pdf

[43] LANDesk Whitepaper. (2007). *LANDesk® Application Virtualization*. DOI=http://www.landesk.com/WorkArea/downloadasset.aspx?id=2393

[44] Spruijt, R. (2010). *Desktop virtualization and the power of App-V and Windows 7*. DOI=http://www.brianmadden.com/blogs/rubenspruijt/archive/2010/02/22/desktop-virtualization-and-the-power-of-windows-7.aspx

[45] Ruest, D.; Ruest, N. (2008). *Presentation virtualization: Centralized app management in Windows Server 2008*.
DOI=http://searchvirtualdesktop.techtarget.com/tip/0,289483,sid194_gci1305049,00.html

[46] Microsoft. (2008). *Desktop virtualization Strategy*.
DOI=http://download.microsoft.com/download/6/F/8/6F8EF4EA-26BD-48EA-BF45BFF00A3B5990/Microsoft%20Client%20Virtualization% 20Strategy%20White%20Paper_final.pdf

[47] Techtarget. *What is storage virtualization?*
DOI=http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci991633,00.html

[48] Morgen, B. (2006). *Virtualization*. Research Paper.
DOI=http://www.windowsecurity.com/whitepapers/Virtualization.html

[49] Ramos, S.J.C.C. (2009). *Security Challenges with Virtualization*. Thesis, December 2009,
DOI=http://docs.di.fc.ul.pt/jspui/bitstream/10455/3282/1/Thesis-JRamos-FCUL.pdf

[50] Chowdhury, M. K.; Boutaba, R. (2009). *A survey of network virtualization*. Elsevier. Computer Network 54(2010) 862-876

[51] Cisco. *What is a network switch vs. a router?*
DOI=http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/connect_employees_and_offices/what_is_a_network_switch/index.html

[52] Hucaby, D.; McQuerry, S. (2002). *VLANs and Trunking*. Cisco Press.
DOI=http://www.ciscopress.com/articles/article.asp?p=29803&seqNum=6

[53] Atos Origin. *Adaptive Virtualization Services*.
DOI=http://www.nl.atosorigin.com/nlnl/services/diensten/infrastructure_professional_services/adaptive_virtualization_services/default.htm

[54] Atos Origin. *Disaster Recovery Virtualization*.
DOI=http://www.nl.atosorigin.com/NR/rdonlyres/7389A0A5-27A0-4AEF-BB4A4E8DF925A2BC/0/AVS_DisasterRecoveryVirtualization_lowres.pdf

[55] Yadav, S. *Centralized Desktop & Presentation Virtualization*.
DOI=http://www.siliconindia.com/guestcontributor/guestarticle/185/Centralized_Desktop__Presentation_Virtualization_Sudarshan_Yadav_.html

[56] VMware. *Disaster Recovery*.
DOI=http://www.vmware.com/solutions/continuity/disasterrecovery.html

[57] Hasan,R. (2005). *History of linux*. DOI=https://netfiles.uiuc.edu/rhasan/linux/

[58] Hanavan, P. (2009). *Virtualization for the Mid-Sized Business*. ITWorld.
DOI=http://www.itworld.com/small-business/66659/virtualization-mid-sized-business

[59] Barrett, A. (2006). *VMware users worry about virtual machine sprawl*. Executive Editor, Storage Media Group. 14 Aug 2006. DOI=http://searchservervirtualization.techtarget.com/news/article/0,289142,sid94_gci1209313,00.html

[60] Silberschatz,A.; Galvin, P.B.; Gagne, G. (2001). *Operating System Concepts*. John Wiley & Sons, Inc., New York, NY, USA, 2001. ISBN 0471417432.

[61] Muehlberger, B. (2005). *Top 5 benefits of server virtualization*. ITWorld. DOI=http://www.itworld.com/nls_windowsserver050411

[62] Techtarget. *Challenges of server virtualization*. DOI=http://searchservervirtualization.techtarget.com/topics/0,295493,sid94_tax313949,00.html

[63] Jennings, C. (2009). *VMware: five biggest challenges of server virtualization*. DOI=http://www.computerweekly.com/Articles/2009/10/16/238145/vmware-five-biggest-challenges-of-server-virtualisation.htm

[64] Philip Winslow, P.; Semple, R.; Maynard, J.; Simson, D.; McGrath, B. (2007). *Desktop Virtualization Comes Of Age*. Credit Suisse. 26 November 2007

[65] LANDesk Whitepaper. (2007). *LANDesk® Application Virtualization*. DOI=http://www.landesk.com/WorkArea/downloadasset.aspx?id=2393

[66] Torode, C. (2007). *Application virtualization myths debunked*. Techtarget. DOI=http://searchwinit.techtarget.com/news/article/0,289142,sid1_gci1273299_mem1,00.html

[67] Buchanan, S. (2009). *Do New Virtualization and Streaming Use Cases Bend or Break Software Licensing Rules?* Gartner. Publication Date: 23 April 2009

[68] VMware presentation. (2010). *Desktops as a Managed Service*. VMware Virtualization Forum 2010 Nijkerk.

[69] Sun Microsystems. (2009). *Data Center Optimization: Three Key Strategies*. Sun Microsystems. DOI=http://whitepapers.techrepublic.com.com/abstract.aspx?docid=1621377

[70] Ritter, T. (2009). *Desktop virtualization network challenges: A primer*. Techtarget. DOI=http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1370184,00.html

[71] Lackorzynski, A.; Döbel, B.; Böttcher, A.; Härtig,H.; Roitzsch, M. (2008). *L4 - virtualization and beyond*. Korean Information Science Society Review.

[72] Suzuki, Y.; Moriyama, M. (2006). *What Issues Does Storage Virtualization Solve? The Benefits of Hitachi's Virtualization Solutions.* IDC Whitepaper

[73] VIFX. *Virtualization and Storage risks*. DOI=http://www.vifxasia.com/risks/

[74] NetworkworldAsia. (2010). *Business benefits of network virtualization*. 3Com. Feb 18, 2010. DOI=http://www.networksasia.net/content/business-benefits-network-virtualization

[75] Davis, D. (2009). *Server Virtualization, Network Virtualization & Storage Virtualization Explained*. Petri IT Knowledge Base, DOI=http://www.petri.co.il/server-virtualization-network-virtualization-storage-virtualization.htm

[76] DiNicolo, D. (2006). *VLAN Benefits*. CCNA Study Guide Chapter 03 DOI=http://www.2000trainers.com/cisco-ccna-03/ccna-vlan-benefits/

[77] Chowdhury, M. K.; Boutaba, R. (2009). *A survey of network virtualization*. Elsevier. Computer Network 54(2010) 862-876

[78] Kent, S.; Seo, K. (2005). *Security Architecture for the Internet Protocol*. RFC 4301 (December 2005).

[79] Milanova, A.; Fahmy, S.; Musser, D.; Yener, B. (2006). *A secure programming paradigm for network virtualization (invited paper).* Proceedings of the Third International Conference on Broadband Communications, Networks, and Systems. (BROADNETS'2006).

[80] VMware. (2009). *History of virtualization*. DOI=http://www.vmware.com/virtualization/history.html

[81] Bittman, T.J. (2008). *Server virtualization trends in 2008: Everything changes*. Gartner. 11 March 2008

[82] van Enter, W. (2010). *Transform your business with VMware*. Presentation: VMware Forum 2010 Nijkerk. VMware

[83] Humpreys, J. (2006). *System virtualization: Sun Microsystems Enables Choice, Flexibility and Management*. IDC. Whitepaper

[84] Bittman, T.J. (2009). *Virtual Machines and Market Share Through 2012*. Gartner. 7 October 2009.

[85] Tan, S. (2010). *Forecast: Understanding the Opportunities in Virtualization Consulting and Implementation Services*. Gartner. Publication Date: 11 March 2010, ID Number: G00174840

[86] Symonds, M. (2010*). Cloud and its effects on business*. Atos Origin. Whitepaper. 29 January 2010

[87] Hinchcliffe, D. (2008). *Comparing Amazon's and Google's Platform-as-a-Service (PaaS) Offerings.* ZDNet. 11 April 2008. DOI=http://www.zdnet.com/blog/hinchcliffe/comparing-amazons-and-googles-platform-as-a-service-paas-offerings/166

[88] VMware Virtualisatie Forum. (2010). *Agenda*. DOI=http://www.vmwareforum.com/vforum/nijkerk/agenda.php

[89] Noordam, A.; van Loenen, R. (2010). *Securing the virtual World*. Presentation VMware Forum 2010. Trend Micro

[90] Groenhuis, R.; Smith, J. (2010). *Transform the Management of Your Virtualized Datacenter*. Presentation VMware Forum 2010 Nijkerk. VMware

[91] VMware Virtualisatie Forum. (2010). *Event information*. DOI=http://p2v.nl/events/vmwarevirtualisatie-forum

[92] MacDonald, N. (2010). *Addressing the most common security risks in data center virtualization projects*. Gartner. 25 Januari 2010

[93] Simic, B. (2008). *Virtual Vigilance: Managing Applications Performance in Virtual Environments*. Aberdeen Group.

[94] Jump, A.; Gammage, B. (2009). *Emerging Technology Analysis: Hosted Virtual Desktops*. Gartner. 17 Februari 2009

[95] Lammers, J.W. (2010). *Building an Internal Cloud that is ready for the external Cloud*. Presentation VMware Forum 2010. VMware

[96] Haight, C. (2007). *Survey identifies server virtualization needs and trends*. Gartner. 29 August 2007.

[97] Booch, G.; Rumbaugh, J.; Jacobson , I. (1998).*Unified Modeling Language User Guide, The*. Addison Wesley. First Edition October 20, 1998.

[98] UML tutorial. DOI=http://www.sparxsystems.com/resources/uml2_tutorial/

[99] Bednarz, A. (2010). VMware vs. Microsoft vs. Citrix. Network World. June 07, 2010. DOI=http://www.networkworld.com/news/2010/060710-tech-argument-citrix-vmware-microsoft.html

[100] Kidder, L.; Judd, C.M. (1986). *Research methods in social relations* (5th ed.). New York: Holt, Rinehart & Winston.

[101] Yin, R.K. (2009). *Case Study Research Design and Methods*. Fourth Edition. Applied social research methods series volume 5.

[102] Goldberg, R.P. (1974). *Survey of virtual machine research*. Computer, pages 34–45, 1974.

[103] Strachey, C. (1959). Time sharing in large fast computers. In International Conference on Information Processing, pages 336–341. UNESCO, June 1959.

[104] Brodkin, J. (2009). *With long history of virtualization behind it, IBM looks to the future*. Network World. April 30, 2009.

[105] Creasy, R.J. (1981). *The origin of the VM/370 time-sharing system*. IBM Journal of Research & Development. Vol. 25 No. 5, September 1981, pp. 483-490

[106] VMware. (2009). *History of virtualization*. DOI=http://www.vmware.com/virtualization/history.html

[107] Bittman, T.J. (2009). *Virtual Machines and Market Share Through 2012*. Gartner. Publication date: 7 October 2009

Appendix A: History of virtualization

The future of technology always has its roots in the past and the beginning of virtualization goes back much further in time than many would expect. Already in 1974, Robert P. Goldberg said: “virtual machines have arrived". Although this is, in fact, our current reality, it seems to have been the reality of the last 40 years with the slow adoption of virtual machines [102]. Virtualization then known as timesharing, was first developed in 1960 by IBM [103]. At that time the goal was to evaluate the then emerging time sharing system concepts. One of the problems presented at the time was the high cost of the machines, which were inefficiently used by people. Therefore, a time-sharing system should make an operating system more interactive to let multiple users come into the system simultaneously. However, the programming of the operating system became extremely complex using conventional methods consisting of punches and batch jobs. IBM's engineering team in Cambridge, Massachusetts, came up with a novel approach that gave each user a virtual machine (VM), with an operating system that doesn't have to be complex because it only has to support one user. Virtual machines where identical “copies” of the underlying hardware. A component called the virtual machine monitor (VMM) ran directly on “real” hardware. Multiple virtual machines could then be created via the VMM, and each instance could run its own operating system [104]. A virtual machine monitor (VMM) is also called hypervisor.

In 1964, IBM Cambridge Scientific Center begins development of CP-40, an operating system for the System/360 mainframe to create virtual machines within the mainframe. This operating system was the first step to create virtual machines on these mainframes. It could support up to fourteen simultaneous virtual machines. CP-40 was the IBM’s first hypervisor, which gave each mainframe user what was called a conversational monitor system (CSM), essentially a single-user operating system. CMS stands initially for Cambridge Monitor System, then it was designed as Console Monitor System, but at the end it was renamed to Conversational Monitor System. The CSM was a lightweight single-user operating system supporting time-sharing capabilities. CP-40 allowed multiple operating systems to run simultaneously and is noted as the first hypervisor with full virtualization. Before that period, virtualization of hardware only went as far as allowing multiple user applications to be run and not implement a complete simulation of the underlying hardware [105]. The CP-40 was soon replaced by the CP-67 in 1965. The CP-67 had a new component called the "Blaauw Box" designed by Gerrit Blaauw one of the principal designers of the IBM System/360. This component was the first practical implementation of paged virtual memory. CP-67 had the functionality of memory sharing across virtual machines while providing each user with his own virtual memory space. This new hypervisor was considered as the first fully virtualized virtual machine operating system and because of this, it is referred in many documentation as the beginning of virtualization. The benefits of virtualization were impressive. Virtualization made it possible to provide test platforms for software testing and development so that now all of that activity could be done so much more efficiently. Furthermore, it enabled an interactive environment, where a test application could be run and when the application failed the virtual memory showed exactly what was happening. This made debugging and testing more effective [104]. The hypervisors that IBM made were not originally planned as a product. Virtualization

was an internal research project and the hypervisor stayed as an internal project inside IBM. The hypervisor did become commercially available product in 1972.

In the 1970s Intel developed the first microprocessor, which in 1978 was named the “x86 processor”. This introduction of the microprocessor led to the development of personal computers (PCs). Throughout the late 1970s and into the 1980s, computers were developed for household use, offering personal productivity, programming and games. The development of the personal computer (PC) pushed mainframes and subsequently virtualization to the background. Personal computers made it possible to have more processing power available to individual users without the use of mainframes. At this point the technology was only being used in labs. While there was a clear need for virtualization on the mainframe in the 1960s, according to VMware, the idea of building hypervisors for new platforms was abandoned during the 1980s and 1990s when client-server applications and inexpensive x86 servers and desktops led to distributed computing. In 1980s and early 1990s, x86 computers lacked the horsepower to run multiple operating systems, but were so inexpensive that organizations would deploy dedicated hardware for each application. Also, the broad adoption of Windows and the emergence of Linux as server operating systems in the 1990s established x86 servers as the industry standard. And as the chip performance increased so dramatically, organizations that typically run one application per server to avoid the risk of vulnerabilities when running multiple applications on one server, now experience underutilization of their servers [106].

This underutilization, due to the increased chip performance, is one of the main reasons VMware invented virtualization for the x86 platform. This was a challenging task, since x86 computers were not build with virtualization in mind. These x86 computers were originally designed to run only a single operating system and a single application. However, in 1999 VMware managed to overcome this challenge and released the first virtualization software for x86 computers, making it possible to run multiple operating systems and multiple applications on the same computer at the same time, increasing the utilization and flexibility of hardware. VMware developed the first hypervisor for the x86 architecture in the 1990s, which caused the rebirth of virtualization on x86 architectures. Today, x86 computers are faced with the same problems of inflexibility and underutilization that mainframes faced in the 1960s. Virtualization can address this underutilization and other issues. This is why in the past years there is a significant increase in interest for virtualization. While VMware is still the market leader, more vendors entered the virtualization marked and started to develop virtualization software [107].

Appendix B: Terminology

Batch processing/Batch Jobs: Batch processing is execution of a series of programs ("jobs") on a computer without manual intervention. Batch jobs are set up so they can be run to completion without manual intervention, so all input data is preselected through scripts or command-line parameters. This is in contrast to "online" or interactive programs which prompt the user for such input. A program takes a set of data files as input, process the data, and produces a set of output data files. This operating environment is termed as "batch processing" because the input data are collected into batches on files and are processed in batches by the program.

Bare metal hypervisor: Virtualization platform that runs directly on the hardware and does not require a separate host operating system. Examples are Hyper-V, ESX Server, and Citrix XenServer.

Computer architecture: In information technology, especially computers and more recently networks, architecture is a term applied to both the process and the outcome of thinking out and specifying the overall structure, logical components, and the logical interrelationships of a computer, its operating system, a network, or other conception. An architecture can be a reference model, such as the Open Systems Interconnection (OSI) reference model, intended as a model for specific product architectures or it can be a specific product architecture, such as that for an Intel Pentium microprocessor or for IBM's OS/390 operating system.

Denial of service (DoS) attack: A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

Fully virtual: A virtual machine that completely emulates all hardware devices.

Guest Operating System: The operating system that is installed and runs inside of a virtual machine environment that would otherwise operate directly on a separate physical machine.

Hardware-level Virtualization: In this approach, the virtualization layer sits on top of the hardware exporting the virtual machine abstraction. And since the virtual machine looks like the hardware, all of the software written for it can operate successfully in the virtual machine.

Host operating system: hypervisors are called host operating systems. The virtual machines that run on top of the hypervisor are called guest operating systems.

Host: A host machine is a term that is used for the physical machine/server on which the virtualization software is installed. It contains the physical resources such as the processors, memory, hard disks, network adapters and other resources that the virtual machine utilizes. It is also called a physical server.

Hosted Virtualization: in this virtualization approach, partitioning and virtualization services run on top of a standard operating system on the host machine. With this method, the virtualization software relies on the host operating system to provide the services needed to talk directly to the underlying hardware.

Hypervisor: A hypervisor is a thin layer of software that provides access to hardware resources and provides virtual partitioning capabilities, and it runs directly on the hardware or on the 'bare-metal' of the machine, but underneath higher-level virtualization services. The hypervisor is directly responsible for hosting and managing virtual machines running on the host, although overall benefits can vary widely from one vendor's hypervisor to another. As is mentioned above, the term hypervisor is often used to describe a Virtual Machine Monitor (VMM). In literature, these to terms are seen as the same.

Operating-System Virtualization: Here, the virtualization layer sits between the operating system and the applications that install and run on the operating system. The virtual instances are written for the particular operating system being virtualized.

Network interface card (NIC) is a hardware device that handles an interface to a computer network and allows a network-capable device to access that network.

Para virtualization: A virtualization approach that exports a modified hardware abstraction which requires the guest operating system to be modified and ported before it can be allowed to run in the virtualized environment as a virtual machine. Therefore, its use requires an open source operating system whose source is publicly available and open to modification such as Linux.

Pay per use. Capabilities are charged using a metered, fee-for-service, or advertising based billing model to promote optimization of resource use. Examples are measuring the storage, bandwidth, and computing resources consumed and charging for the number of active user accounts per month. Clouds within an organization accrue cost between business units and may or may not use actual currency.

Physical server (host): The term physical server refers to the hardware that does the actual computing processing imposed by the software, such as operating system and applications. A virtual server cannot operate without a physical server, also called the host. The virtual machines/servers that are placed on the physical server/host are called guests.

Private cloud. The cloud infrastructure is owned or leased by a single organization and is operated solely for that organization.

Public cloud. The cloud infrastructure is owned by an organization selling cloud services to the general public or to a large industry group.

Sandboxing: Virtual machines are useful to provide secure, isolated environments (sandboxes) for running foreign or less-trusted applications. Virtualization technology can, thus, help build secure computing platforms.

Snapshot: An image of the state of a virtual machine at a specific point in time that includes all the data plus the configuration information for the VM, to allows the return to that state in the future after changes have been made.

Virtual Machine (virtual server, workload): the virtual machine (VM) is the virtualized representation of a physical machine that operates and is maintained by the virtualization software. A virtual machine is typically comprised of either a single file or a group of files that can be read and executed by the virtualization platform. Each virtual machine is a self-contained operating environment that behaves as if it is a separate computer. A virtual machine emulates a complete hardware system, including but not limited to a processor, memory, network adapter, removable drives and peripheral devices. Multiple virtual machines configured with different guest operating systems are capable of operating on the same host machine simultaneously.

Virtualization Software: Virtualization software is a generic term denoting a software technology that provides a layer of abstraction in order to create logical environments for operating systems or application instances to execute in isolation from one another.

Virtual Disk: The term refers to the virtual machine's physical representation on the disk and is composed of a single file or a group of files that are located on the host machine's hard drive or on a remote storage location. It appears to the virtual machine as if it were a physical hard disk. Virtual disks offer a number of benefits over their physical counterparts such as portability and ease of backup.

Virtual Machine Monitor: virtual machine monitor (VMM) is the software that runs in a layer between a hypervisor or host operating system and one or more virtual machines that gives the virtual machine abstraction to the guest operating systems. The VMM virtualizes certain hardware resources such as the CPU, memory and physical disk, and it creates emulated devices for virtual machines running on the host machine. The VMM can export a virtual machine abstraction that is identical to a physical machine so that the standard operating system can run just as if it were on physical hardware. Often the term VMM and hypervisor are both used together and seen as the same.

Workload: In computing, the workload is the amount of processing that the computer has been given to do at a given time. The workload consists of some amount of application programming running in the computer and usually some number of users connected to and interacting with the computer's applications. A defined workload can be specified as a benchmark when evaluating a computer system in terms of performance (how easily the computer handles the workload), which in turn is generally divided into response time (the time between a user request and a response to the request from the system) and throughput (how much work is accomplished over a period of time). However the use of the word "workload" is also used in the virtualization world to refer to virtual machines. Running of virtual machines on a physical server are referred as workloads.

Appendix C: Benefits and challenges of virtualization

This supplement reading of this appendix is meant to hand additional insights on the benefits and challenges of virtualization technologies. In this appendix, an overview is made of the benefits and challenges of virtualization technologies of each virtualization domain. This overview holds information about the reasons why organizations might be interested in a particular virtualization technology and what challenges are to be expected. Also, some of the challenges are the foundation for the development of new technologies that must tackle these challenges. An example of this can be found in chapter 4. However, a demarcation is made in this chapter to list only the benefits and challenges of each virtualization domain. The reason for this is that a description of all the benefits and challenges of every specific technology requires information about all the specific virtualization technologies and products of software vendors. This is a very extensive list and requires additional research. The benefits and challenges are described that reoccur in different literature sources [56-79]. Below the benefits will be discussed for each virtualization domain that was previously explained in chapter 3. The virtualization domains are server virtualization, application virtualization, desktop virtualization, storage virtualization and network virtualization. Beginning with server virtualization in section C.1, first the main benefits are discussed and afterwards the main challenges.

C.1. Server virtualization

C.1.1. Benefits

Consolidation: increasing utilization

Looking at the history of operating systems, Microsoft and Linux started its popularity in the 90s and were accepted by data centers as a good operating system [47, 57]. However, the problem with operating systems is that when an application crashes it also can lead to a crash of the operating system. For this reason, administrators started to apply the philosophy of single-purpose servers, running a single application per server. This would prevent the failure of one application, causing the operating system to fail, to disrupt any other application running on another server. For each new business application, it was also necessary to use another server. Also, for security reasons there was a general notion that the attack surface will be smaller when fewer applications are installed on a server. This led to the situation of server sprawl where multiple, under-utilized servers take up more space and consume more resources than can be justified by their workload [59]. This underutilization can be tackled with server virtualization where a stack of multiple physical servers is virtualized into multiple virtual machines on one physical server, also called server consolidation. This is illustrated in figure 26 below.

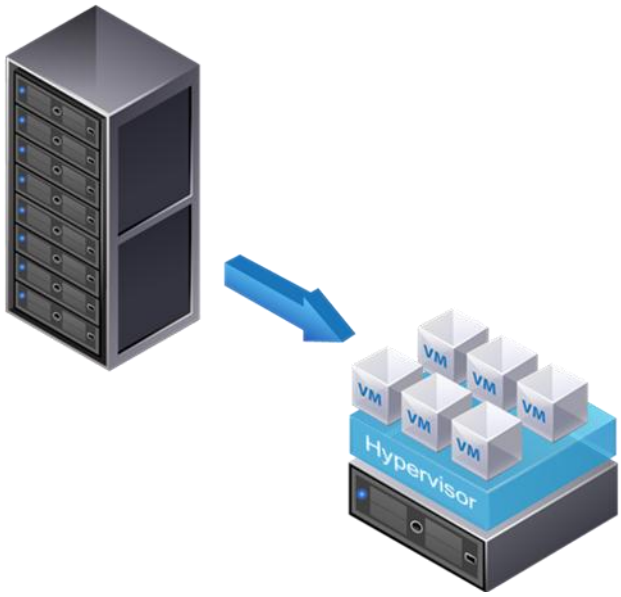

Figure 27 Server consolidation

Sever consolidation is often used for servers that use a small amount of their capacity. This way, a large number of servers can be virtualized into one physical server. This way significant cost savings can be made, by reducing the number of physical servers. By having these virtual machines running at the same time, the server uses resources more efficiently and therefore less physical hardware is required to accomplish its goal. Furthermore, servers which require a relative larger amount of resources or support critical business applications are seen as less suitable for virtualization. Depending on the number of VMs and type of applications on the VM a hypervisor generates more overhead. Critical business applications that are used on a daily basis may use a significant amount of resources of a physical server. When the resource requirements reach close to maximum resource capability of a server there can be a possible performance decrease with server virtualization. However, this is only the case with servers that reach maximum capacity. Therefore, it is important that the resources for these critical business applications are available and committed. Server virtualization brings many additional benefits, which will be explained in the section “reliability” below. While server virtualization is mainly seen as an attractive technology for underutilized servers, because of cost savings, additional benefits makes it also attractive for more heavy utilized servers [58]. The potential of virtualization goes beyond consolidating servers and potential cost savings on hardware.

Reliability

As server virtualization liberates software from hardware, servers running in virtual machines are hardware independent. This means that they are highly portable compared to physical machines. They can be easily backed up and cloned. By having each application within its own "virtual server" you can prevent one application from impacting another application when upgrades or changes are made. Also, resources can be aligned with business goals, meaning the highest value applications gain priority over less value applications. Dedicated resources can further be provided to important business units. Furthermore, it is possible to develop a standard virtual server build that can be easily duplicated which

will speed up server deployment and recovery from failure. This also means that maintenance of a server can be done with zero-downtime as the virtual machines can be duplicated and moved from server to server. Hardware utilization can be optimized automatically, by scanning the utilization of the servers continuously to respond to changing conditions, such as server failure. High availability is essential for corporate environment where availability of their services is crucial to the success of their business. One of the advantages of using virtual machines is that it can be restored very easily, if updated backups have been made, then the IT manager can simply restore that file on another machine. If any problem happens to one of the servers, there would be another server that could temporary support the VMs that where running on that server. This example shows also another benefit of virtual machines, which is disaster recovery (DR). Some companies have their disaster recovery center in another geographic location and applying a hot standby allows them to easily replicate the VM to their DR center and when needed, be able to quickly make the services available. Another advantage of virtualization on disaster recovery is when facing an exploit that can compromise a server, is the ability to use a VM non-infected copy of the affected VM, patch them and turn into production, leaving the infected system for analysis and evaluation [49].

Data center Space & Energy

Without virtualization, companies have realized that most of their systems were running at ratios of 10 percent or less of utilization, yet these systems continue to require space, power and cooling system as any other machine [58]. With server virtualization the space utilization in the data center can be significantly increased through consolidation. Furthermore, in a situation where there is server sprawl the number of physical server can be reduced significantly. Reducing the number of servers, additional benefits can be gained by generating less heat from servers resulting in a reduction of cooling requirements. Also, energy cost saving can further be decreased by lowering the number of power supplies. However, not only consolidation can result in energy savings. Virtual machines can be allocated to physical servers, to increase utilization. When a physical server is not fully utilized, a virtual machine from another physical server which has very low utilization can automatically transfer its virtual machine(s) to the server with higher utilization. After this, with live migration the server will be idle and can be ordered to shut down, resulting in more efficient use of resources and power savings.

Testing environment

Virtual machines offer a perfect environment for development and research. According to Silberschatz et al. [60], changing an operating system is a difficult task because they are complex programs and since they execute in kernel mode, the impact of changing a pointer can destroy the entire file system. Therefore, it is necessary to test all changes to the operating system. With server virtualization, the system programmer can have their own virtual machine and system development or test can be done on those virtual machines instead of on a physical machine. This reduces the system development time and cost, increasing the productivity. It is also useful for testing software solutions. Using virtualization, a company can try some solutions without the necessity of using many real servers. The same way it is useful for software developers to simulate the production environment using virtual machines, and that way, debugging their applications. In addition to testing new solutions, virtual machines are useful to test new patches before applying them into production systems. Virtual Machines are also very useful

for forensic team research purposes. It is possible to clone a potentially compromised host into a VM and do further investigation without the need of the physical machine. The investigation team can also take advantage of snapshots to return to a previous state. The same can be said for malware investigation team. It can be very useful to use a VM since it guarantees isolation and to have the ability to use the snapshot function. However, malware does not always have the same behavior inside a VM as on a normal computer.

C.1.2 Challenges

Management

As the number of physical servers can significantly be reduced through consolidation it tends to ease the burden for system administrators to manage servers. While this might be true, server virtualization introduces a new issue called virtual machine sprawl. In contrast to deploying new physical machines, which can take days to weeks, server virtualization enables the deployment of virtual machines within a couple of minutes [35]. Because creating new virtualized servers is so quick and easy, many organizations have a problem with "VM Sprawl" [59]. With VM Sprawl, the number of virtual machines running in a virtualized infrastructure increases over time, simply because of the ease of creating new VMs, not because those VMs are absolutely necessary for their business operations. In testing environments, virtual servers are used to test new applications. Because it is easy to deploy a virtual server, the pitfall is to keep deploying virtual servers for testing. To prevent VM sprawl, an organization needs to carefully analyze the need for all new VMs and ensure that their existence is justified. Also, depending on the license models of the vendors, VM sprawl is likely to increase the cost of the virtual infrastructure. Furthermore, server virtualization creates a concentrated point of failure. Running multiple virtual servers on a physical server causes more servers to fail at the same time in case of a hardware failure. Nevertheless, the plus side is that the virtual servers can be rebooted on another physical server in a relatively short amount of time.

Software & Hardware License

While more vendors have entered the market, competition between the vendors will tend to lead to cheaper virtualization software packages and hardware [62]. Some hypervisors packages have already become without license cost, but require the purchase of additional tooling. Therefore, software packages still need to be purchased and configured. In order to use the software packages licenses need to be bought.. Also, while the software packages continue to support more applications, not all types of applications are currently supported for virtualization. Organizations need to carefully decide which applications are suitable candidates and which applications need to be tested.

Training

On the virtualization market there are many different software technologies and tools. Understanding the different technologies and tools is prerequisite for IT staff in organizations. The approaches of the software vendors for implementing server virtualization can be very different and may require knowledge in overlapping specialization areas. In large enterprises, IT staff is often specialized in key functional areas such as servers, storage and networking [63]. Because all of these areas overlap each other in the virtual infrastructure, it is crucial to clearly delineate roles and decide on who is responsible

for what. It may also be necessary to train and prepare personnel across the IT department to work in a virtual environment. In order to solve problems in a virtual infrastructure IT staff needs to have expertise in different areas.

C.2 Application virtualization

C.2.1 Benefits of application virtualization

Just as server virtualization abstracts a computer's operating system from its hardware, application virtualization abstracts a program's executables, configuration files and dependencies from the operating system. Each virtualized application runs within its own environment, which includes registry entries, libraries, supporting executables and anything else that is needed for the application to run. Because the application does not use resources outside its environment, it allows application to run on other operating systems than it was designed for. Also, because application virtualization isolates applications from one another, the operating system conflicts between applications are reduced. Security increases as the application can be accessed remotely and does not have to be physically installed on the operating system. Incompatible applications and even multiple versions of the same application can run side by side at the same time [64]. Application virtualization lets the registry and the file system of the operating system untouched. Hence, it can protect the operating system and other applications from poorly written or buggy code. Also, applications that depend on additional software such as drivers or libraries can be easily installed, which makes deploying upgrades and patches easier. Instead of running an installer on each computer, or trusting users to do it, IT staff can replace the old application with the new version, which is directly available to be distributed to users. This allows applications to be copied to portable media and then imported to client computers without need of installing them. When an updated application is not functioning properly, fallback to a previous version is easy. Multiple versions of the same application can run simultaneously, which also removes the need of a testing environment. Therefore, deployment of applications can be done much easier, since applications can be centrally managed. Organizations have to ability to control access, track usage, quickly test, deploy, update and remove virtual applications. Application virtualization can make application provisioning easier, through the possibility of on-demand application streaming. Application streaming is a technology that streams portions of the virtualized application to the user’s computer. A virtualized application image is stored on a server where the user computer connects to. Instead of the entire file being transferred, only portions of the application are streamed, speeding up the time it takes to launch the program. The image is also cached locally, so portions of the application that have already been used do not have to be send again. Application virtualization enables administrators to maintain a secure, clean and stable user desktop [65]. Also, application virtualization can store application usage history, which can be used to analyze license cost of software, depending on the type of license fee. However, this is also one of the challenges with application virtualization which is described below in section 4.2.2.

C.2.2 Challenges of application virtualization

Software compatibility

While application virtualization sounds very promising, not all software can be virtualized [66]. Some types of software such as anti-virus applications and other monitoring tools require heavy integration with the OS which can be very difficult. However, as developments continue more applications are expected to be made compatible.

Software license distribution

Application virtualization can be a huge challenge for organizations in terms of software licensing. Currently, many organizations are disappointed by licensing cost implications, because the ways in which they want to use software are not always envisioned in the application license agreements [67]. Current licensing models of software vendors allow software to be installed on a limited number of devices or users. With application virtualization, applications become more mobile and can be run on any configured device attached to the network. Depending on the way the applications are distributed, software license can be an issue. In certain scenarios it is impossible to show on which devices an application is installed. However, virtualization makes it possible to central manage all applications and incorporate an distribution policy, which can decide if an user has access to an application and can show the number of users that have accessed the application. Often used license models of “Per user” and “Per device” licensing can be very expensive for organizations and research literature shows that organizations want a more flexible license relationship between users and devices [67]. Before implementing application virtualization, it is important to understand the type of software license of the applications and hardware licenses. Application virtualization makes it possible to get a better insight in the software licenses due to central management. However, application virtualization can turn out to be very expensive with the wrong type software and hardware license.

C.3 Desktop virtualization

C.3.1 Benefits of desktop virtualization

Management and security with desktop virtualization

One of the most significant benefits of desktop virtualization is that it gives IT administrators an easy and centralized way to manage desktops. Desktop virtualization brings easy and fast provisioning of virtual desktops, work place environments for employees and can include security features. For example, virtual desktops can be “locked-down” to prevent unauthorized data or applications being run on the desktop [68]. Also, the most common used desktop virtualization technology, called VDI, brings more security as data is protected in a central location. Like application virtualization, virtual desktops can easily be updated centrally. The desktops can be accessed from a wide range of devices and places. Hence, desktop virtualization brings flexibility, accessibility, security and freedom [69]. Freedom means that every user can have their own virtual desktop, which can be accessed from any place. Furthermore, desktop virtualization has the benefits of server virtualization, where resources are handled in an efficient manner and failures can be recovered more easily.

C.3.2 Challenges of desktop virtualization

End-user experience

Running virtual desktops from a central and remote location requires the streaming of application data towards the users location. Users may experiences slow performance of applications [70]. Currently, the playback of media application, such as video, can have significant delays when there is not enough bandwidth is available. Furthermore, multimedia applications, which require graphic processing power, are often not supported. Furthermore, users need to have continuous connection to the internet to access their desktop. As their desktop is managed remotely on a central location, it can be restricted to install applications that are not suitable for desktop virtualization or illegal. This could be considered a loss of user autonomy and privacy.

Software license and cost

As explained in section C.2.2, desktop virtualization has the same software license problems as application virtualization. It is important for organization to know that they have the correct licenses for their virtual desktops. Furthermore the implementation of a Virtual Desktop Infrastructure (VDI) requires a significant investment and does not reduce desktop costs, including hardware, software, storage, and network. Therefore, if an organization only motive is to increase cost savings, desktop virtualization might not be suitable.

C.4 Storage virtualization

C.4.1 Benefits

Manageability, Scalability, Availability and Security

With storage virtualization all available storage capacity is pooled. Therefore, system administrators no longer have to search for disks that have free space to allocate to a particular host or server. A new logical disk can be simply allocated from the available pool, or an existing disk can be expanded. Storage can be assigned where it is needed at that point in time, reducing the need to guess how much a given host will need in the future. Manageability increases as storage can be centrally managed. This makes it easier to manage tasks such as backup, archiving or recovery, by disguising the actual complexity of the Storage Area Network (SAN) [71]. Furthermore, due to the new provision capabilities scalability is increased, because it is easier to respond to additional capacity needs [72]. It enables a fast response to rapid changes in demand. Also, when there is a failure on one of the storage systems or maintenance is required, other storage systems in the resource pool remain available, which reduces downtime and increases availability.

C.4.2 Challenges

Management

Meta-data management information is one of the most valuable assets of storage virtualization [73]. The meta-data contains the logical data of the actual location of the data on the storage systems. While storage is seen as a single logical unit, the data is stored on various storage systems. If the meta-data is lost, so is the link to the (actual) location of the data. Without the mapping information, it would be virtually impossible to reconstruct the logical drives. Furthermore, while storage virtualization allows the possibility to manage storage systems centrally, management of storage can become complex. While a virtual storage infrastructure benefits from a single logical disk, the storage systems must still be

managed. Problem determination and fault isolation can also become complex, due to the abstraction layer of virtualization. Management tools can help locate problems of storage systems in the network.

C.5 Network virtualization

Network virtualization is an example of a technology that improves the overall network framework while maintaining traditional network cabling and physical connection methods [74]. Network virtualization is still early ages and currently there are many network virtualization projects going on [74, 75]. The network virtualization projects use different approaches and network architectures that have their own benefits and challenges.

C.5.1 Benefits of Network virtualization

While network virtualization is still in its early stages there are a number of benefits that network virtualization offers. With network virtualization, network applications are moved into the network devices, which provide additional capabilities and benefits, such as improved network speed, reliability, flexibility, scalability, and security. Also, network virtualization requires the need of fewer network hardware. Considering the number of cables, network cards, routers and other network equipment used in a data center, hardware can be significantly reduced. Network management can be a tedious and time-consuming business for an administrator. With network virtualization, files, images, programs, and folders are centrally managed from a single physical site. Storage media such as hard drives and tape drives can be easily added or reassigned. Storage space can be shared or reallocated among the servers. Network virtualization intends to improve productivity, efficiency of the administrator by performing many of these tasks automatically, thereby disguising the true complexity of the network. Furthermore, security can be increased in a virtual network. Each user can be assigned their own virtual network, where traffic between virtual networks remains separate and distinct from other users in the network [76]. Virtual networks are also very scalable as they can span an entire organization and even beyond. They are very flexible as users can be grouped logically. If users need to access or change to another virtual network location, instead of moving their computer, they can easily be assigned to a different virtual network [76].

C.5.2 Challenges of network virtualization

Security and privacy

While network virtualization isolates virtual networks, it also isolates faults and attack impacts in a network. However, it does not necessary overcome existing threats, intrusions and attacks to physical and virtual networks [77]. To some extent, network virtualization brings a new array of security vulnerabilities. For instance, a denial-of-service (DoS) attack against the physical network in a virtualized environment will also affect all the virtual networks running on that network. In literature various security vulnerabilities and safety measures such as encryption can be found to increase security and privacy [78, 79].

Appendix D Case study interviews

In the two sections below, a detailed report of the expert interviews is given. First, the internal group is described and secondly the external participants. The external participants are from virtualization vendors VMware, Citrix, Quest and Microsoft. In table 5, the names of the participants are described.

Table 5 Interviews

Interviewee	1	2	3	4
Internal Group	Mick Symonds	Jacco van Hoorn	Gerard Scheuierman	Joris Haverkort
External Group	Michel Roth *(Quest Software)*	Jan Willem Lammers *(VMware)*	Robert-Jan Ponsen *(Citrix)*	Robert Bakker *(Microsoft)*

1. Interviews internal group

Respondent 1: Mick Symonds

1. What is your function at Atos Origin?
   Principal Solutions Architect. Also GMO Cloud Program

2. a) What is the view of Atos Origin on virtualization?
   There is no one single view: separate views per operation and product segment. Some see opportunity to earn money from projects. Others see benefits from operating a virtualized environment.

   b) What is the strategy of Atos Origin with regard to virtualization?
   Ditto. Make money out of it.

3. Looking at the current portfolio of Atos Origin, which products or services are popular?
   You can better ask other people inside Atos Origin.

4. Which products or services do you expect to become important in the years to come?
   Utility Computing in its broadest sense, which embeds virtualization within it. With Cloud Value Components on top from which utility computing is the underlying infrastructure.

5. Customers can have different business needs for virtualization. What are the most important business reasons of customers for virtualization?
   1. *Cost saving*
   2. *Flexibility due to abstraction layer.*

   Number 1 is always cost saving. In negotiations whatever they talk about, quality of service in the end it is always primary cost saving. The other far more important thing, which I think they only appreciate over years is what I summarize as flexibility. Having that abstraction

layer where you host a virtual machine and it does not matter what the box is underneath. We always forget how it was when a box would arrive and someone would have to install a particular operating system that has to be installed on that box. It was configured for that box. You don't have that these days you can just run image and it just runs. If they want a different color shape or size that have a problem. That is where virtualization comes in as long as we can physically fit it on the box we don't care if they want it to have four processors or whose version of an operating system.

6. What do you think is the greatest challenge of virtualization today?
   One of the greatest challenges of today is capacity management and utilization risk. There is the risk that either we have a room full of machines and nobody is using them or that we have a few machines and suddenly someone wants another machine and we don't got them. And either of those is a risk as in the first case it is costing us a lot of money to have a machine that is doing nothing and in the second case they go somewhere else as someone else has got them.

7. What is your personal view/opinion on virtualization for the future?
   That it will become pervasive. Everything will be virtualized in some shape or form. Like virtual desktops now that gives the ability for people to work from anywhere they want. It used to be that, before you're day that people really had to go to the office and work. If somebody called you 3 am in the morning to fix something, you had to go on your bike or car and drive to the office and fix it. But you have now PCs, virtual private networks, wireless, decent email programs you name it. All sorts of things none of which make an enormous difference on their own, but adding them together it makes a hell of a difference. And that's the effect, and I think that is where virtualization is not just one of those, but it sort of embeds all these other things. It means that you are no longer expecting, but you will build something for a specific physical environment, to deliver a particular functionality and it will get what it needs from the outside world which will be virtualized. You will need a network connection but you won't know are care what sort of network connection it is cause it will be a VPN or something. So you will just access a resource and the technology will make sure that it looks like as do it sat next to your machine and is responding to you. You will have no idea if it is from the other side of the world. That is the real advantage and the abstraction that everything works as if in a perfect world.

In my research, I am currently working on a taxonomy model showing the various types of virtualization technologies. These various types are divided into different domains: Server, Application, Desktop, Storage, Network, Security and Management. In the taxonomy, I introduce Security and Management as additional domains. The reason for this is that in my analysis on the current virtualization developments, I encountered a particular attention towards management and security of virtual environments. Bridging the gap from virtualization to cloud I think that security and management are playing a vital role.

8. What is your opinion on these 2 matters?

My opinion about these two matters is that we have to work out what we mean by "Cloud Security" and we have a team of people who are trying to understand what we mean by cloud security and what we can do about it. It is in particular the technologies, but what also our actions what we do when we have

for instance access to certain data and publish it. The biggest issue to management is understanding the service management architecture, how it fits together.

9. Do you think the model classifies the virtualization technologies in a correct way?
I prefer reference models (shapes) and the dependency of things.

Respondent 2: Jacco van Hoorn

1. What is your function at Atos Origin?
   Solution/Lead Architect of department AVS

2. a) What is the view of Atos Origin on virtualization?
   There is no exact answer to what view Atos Origin has and it depends from what level or department you look. For Atos Origin as a company the interest in virtualization is mainly a source of work and income.

   b) What is the strategy of Atos Origin with regard to virtualization?
   To position itself as an ideal medium to save on exploitation costs of IT environments and present itself as the ideal partner to realize this.

3. Looking at the current portfolio of Atos Origin, which products or services are popular?
   From view of AVS department and fellow departments server virtualization using VMware ESX/vSPhere (hypervisor) is most popular.

4. Which products or services do you expect to become important in the years to come?
   I expect that there will be an increase in the need for High Availability and Disaster recovery products in combination with virtualization. Meaning Fault Tolerance and Site Recovery Manager (SRM) if VMware. The reason for this is that availability of IT environments are becoming more important and the products mentioned above make it for more companies financially feasible.

5. Customers can have different business needs for virtualization. What are the most important business reasons of customers for virtualization?
   The idea of saving cost and green "IT". However, this a no guarantee with virtualization).

6. What do you think is the greatest challenge of virtualization today?
   I think at this moment backup, storage virtualization and the cost of shared storage. A challenge with storage virtualization is the limited flexibility of storage in virtual environments. There is a lot of effort needed to configure storage for virtual environments. Not all products work not as well or easy as you think should be. Site Recovery Manager (SRM) from VMware for instance requires a lot of effort to configure it properly.

7. What is your personal view/opinion on virtualization for the future?
   That very soon there will be no good reason to think of for Wintel (Windows and Intel) stems to run physically and tat also in the Unix world there will be more and more adoption of virtualization. I think there will come an increasing shift in bringing traditional Unix environments to virtual Windows systems. Besides this, you see that there is once more a

movement of insourcing IT environments at non-IT companies (returning outsourced IT environments). On enterprise level virtualization together with cloud computing will ensure that this movement will be kept in check.

In my research, I am currently working on a taxonomy model showing the various types of virtualization technologies. These various types are divided into different domains: Server, Application, Desktop, Storage, Network, Security and Management. In the taxonomy, I introduce Security and Management as additional domains. The reason for this is that in my analysis on the current virtualization developments, I encountered a particular attention towards management and security of virtual environments. Bridging the gap from virtualization to cloud I think that security and management are playing a vital role.

8. What is your opinion on these 2 matters?
That management and securing of shared (=Cloud) environments is not something new. Regarding the technology, it is not so exciting. It is mainly the scale that has to be changed and the exciting part lies in bringing or adding more structure. The only way to keep hold of management and security in shared environments is structure.

9. Do you think the model classifies the virtualization technologies in a correct way?
Do client and server not have to be reversed? VM sprawl and inactive VMs are no security risk, but ordinary operational risks

---

Respondent 3: Joris Haverkort

1. What is your function at Atos Origin?
   Product manager

2. a) What is the view of Atos Origin on virtualization?
   Offering a way to create more flexibility, where virtualization is used to achieve this.

   b) What is the strategy of Atos Origin with regard to virtualization?
   There is no single view or strategy that Atos Origin has that covers all aspects or services that Atos Origin offers. There is a lot of attention on cloud computing with regard to virtualization, but I cannot really say that this can be seen as a strategy of Atos Origin. I think the strategy of Atos Origin is to try to virtualize IT infrastructures as much as possible to prepare the way for cloud.

3. Looking at the current portfolio of Atos Origin, which virtualization products or services are popular?
   VDI is the most upcoming virtualization service that is becoming increasingly popular. Furthermore server virtualization is something more standard now, which is the starting point of virtualization. Currently there is also much attention of management products for virtualization, such as monitoring tooling.

4. Which products or services do you expect to become important in the years to come?
   Apart from cloud services, as this is very broad subject, I think virtualization management and everything around this will become extremely important. These are the "on top" services on

server desktop etc. that will become important. What normally is done in the physical world will shift to the virtual world. Good monitoring solution, good capacity management, asset management, software alliance administration. A lot of things that of the physical world are currently possible on the virtual world, but a lot more is possible on the virtual world. What you see is a lot of focus on specializing products. Server, desktop and application are becoming more of standard products that come with virtualization. In the coming years I think a lot of focus will be on management and security of virtualization. Also I think that in the next years platforms will become more and more multi-vendor, which means that the kind of vendor software that runs under need it will not become so important.

5. Customers can have different business needs for virtualization. What are the most important business reasons of customers for using virtualization?
   In general the reason is always cost savings, something that with VDI is not so certain. Next to cost savings is bringing extreme flexibility with virtualization. Also often virtualization goes well together with the objectives of need of the organization.
   In summery reasons are flexibility, continuity, scalability, agility and especially the responsiveness to react to business requirements. If an organization wants to put a new web service with a new product online, a new server can be deployment with a mouse click. This capacity on-demand creates many new possibilities. Shorter time to market. Networking, security and virtualization management will play an important role in the coming years.

6. What do you think is the greatest challenge of virtualization today?
   I think the immatureness of virtualization. Not on all aspects but in general. Everything what we did the physical way we now need to do in the virtual way. Here you see that there is not enough attention for areas like security. Through experience people learn, but there are many areas that are not covered yet. For instance asset management or business process monitoring. Many things around virtualization such as "on top" services around the main services is currently the challenge with virtualization. More and better products are entering the market, but still, this is the challenge at the moment.

7. What is your personal view/opinion on virtualization for the future?
   In the coming years there will be great attention on cloud computing. The role virtualization will play an integral and underlying role in this. It will be the supporting technology that makes cloud possible. On hypervisor levels the type of software from whatsoever vendor will not be important, but most importantly will be the agreements and making of standards in which different platform can communicate and operate together.

In my research, I am currently working on a taxonomy model showing the various types of virtualization technologies. These various types are divided into different domains: Server, Application, Desktop, Storage, Network, Security and Management. In the taxonomy, I introduce Security and Management as additional domains. The reason for this is that in my analysis on the current virtualization developments, I encountered a particular attention towards management and security of virtual environments. Bridging the gap from virtualization to cloud I think that security and management are playing a vital role.

8. What is your opinion on these 2 matters?
Management tooling, security are important aspects that will receive much attention in the coming years. This "on top" tooling (management, virus protection) offers many possibilities for new service delivery.

9. Do you think the model classifies the virtualization technologies in a correct way?
I think the domains cover all aspects and areas of virtualization technologies. These domains cover everything that makes a cloud. It provides a very clear overview.

Respondent 4: Sander Lahpor

1. What is your function at Atos Origin?
   Portfolio manager for AIS. AIS does network, storage and compute. Network consists of KA LAN, DC LAN and WAN, fiber and MPLS. Storage consist of SAN, FSOD, Tier4 etc.

2. a) What is the view of Atos Origin on virtualization?
   Virtualization is something is a" must do" because of speed, scalability and standardization. Speed refers to the responsiveness of putting thing faster on the market.

   b) What is the strategy of Atos Origin with regard to virtualization?
   Regarding implementation. Start with one hypervisor, analyze hypervisor 2 en 3. Choose storage and networking that is appropriate with the hypervisor with eye for the "installed base".

3. Looking at the current portfolio of Atos Origin, which products or services are popular?
   What is popular is Cloud, which is actually utility computing. What is now very popular is shared cloud services and dedicated or private cloud. Here, a shared Cloud service is on one hypervisor or host, multiple virtual machines from different customers in our own data center and dedicated means that one machine or multiple are only used for one particular customer. This cloud refers to utility hardware. Utility hardware: Storage + compute +network. From my function I only look at this part of cloud.
   Also, Tier 4 storage is starting to become very popular. This type of storage is storage as you want it. Doesn't matter which type of network the storage attached on it can find itself or each other. Actually making a pool of storage systems.

4. Which products or services do you expect to become important in the years to come?
   Cloud integration services and cloud security services. What you see is people want to move from A to B, that is where integration services come in. Further, how to go safely from A to B is where security services come in. This type of services will come.

5. Customers can have different business needs for virtualization. What are the most important business reasons of customers for virtualization?
   This is actually creating independency. Independency means doesn't matter what hypervisor or software or hardware it works. Reduction of costs: TCO, CAPEX (what is on balance) -> OPEX(what you spend every month). And I also think time to market: how fast can you make something ready for the world. Software for instance is easier to offer on a virtual platform. This means flexibility.

6. What do you think is the greatest challenge of virtualization today?
   Reducing of blablalbla. There is lot of blablabla nowadays. Provisioning of bare essentials: connectivity automation, storage automation, security automation. Everyone says it's offering amazing things, but what you eventually want is a system, that gets it storage from somewhere. Currently, this is not so easy.

7. What is your personal view/opinion on virtualization for the future?
   Virtualization is not going to stop it is the beginning of a new direction. Virtualization will become important and manifest itself in consumer products: laptops, PDA, Smartphone and maybe in television products. Inside Atos Origin a step forward.

In my research, I am currently working on a taxonomy model showing the various types of virtualization technologies. These various types are divided into different domains: Server, Application, Desktop, Storage, Network, Security and Management. In the taxonomy, I introduce Security and Management as additional domains. The reason for this is that in my analysis on the current virtualization developments, I encountered a particular attention towards management and security of virtual environments. Bridging the gap from virtualization to cloud I think that security and management are playing a vital role.

8. What is your opinion on these 2 matters?
   I think that is a correct statement, in particular security. Security is something that lives on basis of legislation, company policies and direction for "correct procedures". A reliable way of working.

9. Do you think the model classifies the virtualization technologies in a correct way?
   Yes, at the moment yes. World will melt together toward 1 or 2 conglomerates.

2. Interviews external Group

VMware

Respondent 1: Jan Willem Lammers

1. What is your function?
   Solutions architect.

2. What is the main objective of your company with regard to virtualization?
   Making it possible for people to deliver IT as a Service. Looking for ways to create cost savings. This is one of the reasons why VMware still made profit during economic recession. Companies searched for ways to cut cost, virtualization was one of them.

3. Which products and/or services does your company offer regarding virtualization?
   We deliver many virtualization products. Looking at the taxonomy, we deliver products in every domain.

4. a) Looking at the current portfolio of your company, which products/services are popular?
   vSphere is the most popular product. It is our hypervisor or platform where all virtualization domains are available.

   b) Which virtualization products/services do you expect to become important in the years to come?
   Desktop virtualization will become important. Not because of the cost saving aspect, since large upfront cost are required, but offering the possibility to work at any place any time. Also automation, management tooling, will become important.

5. a) Organizations have various business reasons for virtualization. Which do you think are the most important business reasons of customers for virtualization?
   First of all cost saving, OPEX saving on operational cost. When people realize that they can get virtual servers faster for cheaper than physical servers for which they have to wait longer and cost more the step towards virtualization is easy. Besides cost saving important reasons are flexibility.

   b) Virtualization is current associated with a lot of challenges in differing areas. There are for instance organizational, technical and business challenges. How does your company coop with or tackle these challenges?
   VMware is constantly looking for new challenges to solve and asking customers in what way they can help them to make their company better. And there are currently so many possibilities with virtualization such as cloud, which offer VMware new challenges meaning more work.

   c) To what extents do these challenges influence the developments of new products and/or services?
   The product and services in some way originate from these challenges.

   d) What do you think is currently the biggest challenges of virtualization?

What is current still see is a lot of lack of understanding of people that are not familiar with IT. People still want to own their IT and not share their IT resources with others. People are still hesitant of sharing their resources. They don't perceive this as an advantage of using your resources more efficiently. When you don't need them others can use your resources. Eventually with Cloud it will be possible to get additional resources from somewhere else. There is the natural tendency of people wanting to posses something only for themselves. I think it is the cultural challenge about sharing with others.

6. a) What are the trends on virtualization at the moment?
   Desktop virtualizatie and Cloud.

   b) Which type of service do you think will play an important role in the coming years?
   Cloud, the ability to buy IT capacity in a flexible way. Where it does not matter if it is in a cloud or where the IT resources are.

   c) Which (new) type of products will play important role in this?
   VMware vCloud Service Director. A website where customers can buy virtual applications and immediately can see metadata where the SLA are described, how much it will cost (chargeback) per month etc. When the customer agrees the service will be automatically roll out and in production. Once it is operational the customer will be able to run it inside their cloud. Management tools play an important role here (inventory, chargeback).

7. What is your personal view/opinion on virtualization for the future?
   My view is that virtualization will become the standard it is not a hype. It is not a technology trend as it will not go away. It is a new way of working and building block for the datacenter. IT and business will grow more together and depending of what the business needs the IT service provider can react and deliver. The investments models will change as IT will play a more supporting role of a company's policy because of the flexibility where IT in the past played a more hampering role. It can react much faster and easier to business needs/requirements.

In my research, I am currently working on a taxonomy model showing the various types of virtualization technologies. These various types are divided into different domains: Server, Application, Desktop, Storage, Network, Security and Management. In the taxonomy, I introduce Security and Management as additional domains. The reason for this is that in my analysis on the current virtualization developments, I encountered a particular attention towards management and security of virtual environments. Bridging the gap from virtualization to cloud I think that security and management are playing a vital role.

8. What is your opinion on these 2 matters?
   Security is something needs to be inherent, not something that you can buy as an extra option. Our hypervisor is built in a way that is secure and meet certain security requirements, which are shown by the certification of our hypervisor.

   The challenge with cloud is not so much the underlying infrastructure or technologies in it by about creating open standards that make the movement of virtual machines across clouds

possible. Currently there are two standards OVF,where response time, security level or defined and vCloud API which enables the connection between datacenters.

Management tools will always be an option for organizations, because it might not be necessary needed for every organization. If an organization has a process that works for them and does not require too much work they don't have to automate that process.

Security is an integrated thing and management tools will always be on option.

9. Do you think the model classifies the virtualization technologies in a correct way?
Yes, it covers all aspects.

Quest Software

Respondent 2: Michel Roth

1. What is your function?
Principal Product Architect at Quest Software, Desktop Virtualization Group

2. What is the main objective of your company with regard to virtualization?
Helping customers realizing a successful application and desktop delivery project by delivering a project that helps to achieve this goal.

3. Which products and/or services does your company offer regarding virtualization?
Quest vWorkspace a desktop virtualization solution.

4. a) Looking at the current portfolio of your company, which products/services are popular?
Quest Software delivers 250+ products. From virtualization point of view Quest vWorkspace is the most popular product.

   b) Which virtualization products/services do you expect to become important in the years to come?
Desktop virtualization, Desktop as a Service, Software as a Service delivered via the Cloud.

5. a) Organizations have various business reasons for virtualization. Which do you think are the most important business reasons of customers for virtualization?
In particular cost savings. Lower maintenance costs, more flexibility and faster service delivery to customers (users).

   b) Virtualization is current associated with a lot of challenges in differing areas. There are for instance organizational, technical and business challenges. How does your company coop with or tackle these challenges?
We develop a product that must make it as convenient as possible to implement desktop virtualization. There is nothing we can do more.

   c) To what extents do these challenges influence the developments of new products and/or services?
We make an inventory of the challenges and develop our product in such away that the challenges are taken care of.

d) What do you think is currently the biggest challenges of virtualization?
Return of investment of desktop virtualization. It requires large upfront investments and benefits in terms of cost saving on short term are uncertain.

6. a) What are the trends on virtualization at the moment?
Desktop virtualization (VDI) and application virtualization.

b) Which type of service do you think will play an important role in the coming years?
Desktop as a Service, Application as a Service. Both delivered by Cloud.

c) Which (new) type of products will play important role in this?
Cloud-aware Application and desktop delivery products.

7. What is your personal view/opinion on virtualization for the future?
Desktop as a Service and Application as a Service that are offered in the Cloud.

In my research, I am currently working on a taxonomy model showing the various types of virtualization technologies. These various types are divided into different domains: Server, Application, Desktop, Storage, Network, Security and Management. In the taxonomy, I introduce Security and Management as additional domains. The reason for this is that in my analysis on the current virtualization developments, I encountered a particular attention towards management and security of virtual environments. Bridging the gap from virtualization to cloud I think that security and management are playing a vital role.

8. What is your opinion on these 2 matters?
There are both very important.

9. Do you think the model classifies the virtualization technologies in a correct way?
Yes.

Citrix

Respondent 3: Robbert Jan Ponsen

1. What is your function?
Business partner manager. I am responsible for all the system integrators in the Netherlands. Also, for Atos Origin I am the primary point of contact or intermediary regarding Citrix products.

2. What is the main objective of your company with regard to virtualization?
Customer satisfaction is our main objective. We think and do only from the perspective of the customer.

3. Which products and/or services does your company offer regarding virtualization?
We offer products in every domain described in your model. I do not have the technical knowledge to tell you about all the different virtualization technologies we have, but looking at the model most of it is covered. Currently our product XenDesktop has all kinds of virtualization technologies. Only for additional management tooling customers have to

acquire additional software package.

4. a) Looking at the current portfolio of your company, which products/services are most popular?
   XenApp or application virtualization is very popular. However desktop virtualization is currently very hot. Not only VDI but all kinds of desktop virtualization technologies. Hosted and local solutions. There is still lots of business in XenApp, but tends to go more towards XenDesktop.

   b) Which virtualization products/services do you expect to become important in the years to come?
   Desktop virtualization not only VDI. Not only VDI which requires an Internet connection. But also offline desktop solutions and client based solutions where employees can bring their own laptop and still run business applications of the organization.

5. a) Organizations have various business reasons for virtualization. Which do you think are the most important business reasons of customers for using virtualization?
   Green IT, cost savings, due to longer usage of your current hardware. Security of sensitive data that organizations want to protect. With desktop virtualization organization can introduce a "poison pill" in which unauthorized usage or expired accounts will automatically remove sensitive data.

   b) Virtualization is current associated with a lot of challenges in differing areas. There are for instance organizational, technical and business challenges. How does your company coop with or tackle these challenges?
   We have lots of contact with the market and have a proof of concept for the customer where they can see how the product works. We assist customers where we receive issues about why it does not work, or why does it not work this way etc. We have a direct line towards development, which will deal with the issues.

   c) To what extents do these challenges influence the developments of new products and/or services?
   In future releases a lot of field experience is put in, which influenced the development.

   d) What do you think is currently the biggest challenges of virtualization?
   I think that one of the biggest challenges is the cost come before the benefits. Currently companies want to invest only if they can have a return on investment (ROI) within one calendar year. The economic crisis has caused for companies to be very careful with their investment. A time period of 3 to 4 years of ROI is often not so attractive within companies at this moment.

   Also one of the challenges is the immatureness of organization or managers where they expect their employees to be present at the companies' location. In the new way of working managers need to be willing to manage on output. It this is the case it is possible to work anywhere anytime and anyplace. Not many organizations are mature enough to let their employees work in their own time
6. a) What are the trends on virtualization at the moment?
   Bring your own computer is currently a trend. New employee wants to choose their own

device to work with. It is a new way of working for the new generation workers, which accustomed to a more flexible way of working.

b) Which type of service do you think will play an important role in the coming years?
System integrators will become very important. They are independent parties, that can take on a lot of work for the customer and offer a choice of products. Customers have become more demanding and selling only one type of product is not enough. Therefore system integrators that also can manage the IT infrastructure of a customer will become important in the enterprise market.

c) Which (new) type of products will play important role in this?
XenDesktop and ThinClient. All kinds of virtualization technologies in one box.

7. What is your personal view/opinion on virtualization for the future?
I think virtualization tends to go to "consumerization". I see "consumerization" as an important development in virtualization. What it means is that I am the End-user and I pay, so I decide. I have this device and I want this kind of software (office) on it and that software I don't want on it. The user determines where, when and how he/she works and what application he/she needs or IT environment it wants. The technologies are currently available to do this.

In my research, I am currently working on a taxonomy model showing the various types of virtualization technologies. These various types are divided into different domains: Server, Application, Desktop, Storage, Network, Security and Management. In the taxonomy, I introduce Security and Management as additional domains. The reason for this is that in my analysis on the current virtualization developments, I encountered a particular attention towards management and security of virtual environments. Bridging the gap from virtualization to cloud I think that security and management are playing a vital role.

8. What is your opinion on these 2 matters?
Management and security are an integral part and condition for successful virtualization. Good management tooling is important to manage your resources, enable hosting of desktops, proper deployment of servers.

9. Do you think the model classifies the virtualization technologies in a correct way?
Yes, if you define the relations in that way where management and security or integrated in other virtualization technologies this is correct.

Microsoft

Respondent 4: Robert Bakker

1. What is your function?
   Product marketing manager

2. What is the main objective of your company with regard to virtualization?
   Helping customers finding suitable solutions.

3. Which products and/or services does your company offer regarding virtualization?
   Desktop, application, server, management. The whole package.

4. a) Looking at the current portfolio of your company, which products/services are popular?
   Currently, application virtualization is very popular. Also desktop virtualization in increasing. Management tooling is an area where a lot of profit is made.

   b) Which virtualization products/services do you expect to become important in the years to come?
   Public and private cloud. Also desktop virtualization is hot.

5. a) Organizations have various business reasons for virtualization. Which do you think are the most important business reasons of customers for virtualization?
   Cost saving -> flexibility -> business continuity

   b) Virtualization is current associated with a lot of challenges in differing areas. There are for instance organizational, technical and business challenges. How does your company coop with or tackle these challenges?
   …
   c) To what extents do these challenges influence the developments of new products and/or services?
   ….
   d) What do you think is currently the biggest challenges of virtualization?
   Management is one of the greatest challenges. Currently, there is a lot of talk about VDI. However many companies are not mature enough to implement VDI yet. First they have to have proper security management, provisioning of applications, identity management (user profiling).

6. a) What are the trends on virtualization at the moment?
   VDI, AppV and management tooling.

   b) Which type of service do you think will play an important role in the coming *years?*

Management will play an important role the coming years. Also private and public clouds will receive much attention

c) Which (new) type of products will play important role in this?
Cloud products. Customers don't have to have in-house IT infrastructure.

7. What is your personal view/opinion on virtualization for the future?
In the coming years there will be further automation of IT infrastructure. Desktop virtualization will be popular.

In my research, I am currently working on a taxonomy model showing the various types of virtualization technologies. These various types are divided into different domains: Server, Application, Desktop, Storage, Network, Security and Management. In the taxonomy, I introduce Security and Management as additional domains. The reason for this is that in my analysis on the current virtualization developments, I encountered a particular attention towards management and security of virtual environments. Bridging the gap from virtualization to cloud I think that security and management are playing a vital role.

8. What is your opinion on these 2 matters?
I think they are correct, management plays a vital role in successfully implement virtualization technologies.

9. Do you think the model classifies the virtualization technologies in a correct way?
Yes, but I would add user state virtualization. This is the virtualization of user data, which I see as an additional domain.