Bachelor's thesis

Information and Communications Technology

2019

Juuso Kössi

VIRTUALIZATION SOLUTIONS

Implementing virtual desktop infrastructure

TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information and Communications Technology

2019 | 31 pages

Juuso Kössi

VIRTUALIZATION SOLUTIONS

Implementing virtual desktop infrastructure

This thesis is about implementing a Windows server-based nonpersistent virtual desktop infrastructure (VDI). VDI is desktop virtualization solution that operates on a client-server basis. In VDI, the server is hosting virtual machines and the client machines connect to them with remote access tools. Nonpersistent means that virtual machines are not personal and many users can use the same virtual machine.

After disconnecting from the virtual machine, they are set back on a ready state or the next user. The implementation in this thesis is a demonstration that is created on two physical computers. There are notifications for parts which should be carried out differently in enterprise environments for the implementation to be used efficient and secure. The implementation includes a domain controller and a virtualization server. The virtualization server is hosting the virtual desktop infrastructure. The domain controller is the virtual server and the virtualization server is installed directly on the physical device. Both of the physical devices are using a Windows server operating system and hyper-V as hypervisor. The virtualization server does host virtual workstations.The virtual workstations were configured to be set back on a ready state for the next user, after the previous user ends its session. Because both of the physical devices are also hosting virtual machines, the virtual switches need to be implemented on them.

The domain controller hosts the domain, the Dynamic Host Configuration Protocol (DHCP) and the Domain Name System (DNS) services for the whole implementation. The virtualization server hosts the roles of the Hyper-V, the remote desktop connection broker, the remote desktop web access and the remote desktop virtualization host. The virtualization server will have a virtual machine collection accessible from the local area network. The domain controller controls which domain users can access the virtual machine collection. Connecting with virtual workstations is achieved by connecting with the remote desktop web access service. After logging in with domain credentials, the virtual machine collection will be available if the credentials have permission to use the VDI virtual machines.

KEYWORDS:

Server virtualization, desktop virtualization, hypervisor.

OPINNÄYTETYÖ AMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tieto- ja viestintätekniikka

2019 | 31 sivua

Juuso Kössi

VIRTUALISOINTIRATKAISUT

Virtuaalisen työasemaympäristön toteutus

Opinnäytetyössä luotiin Windows-palvelimelle virtuaalinen työasemaympäristö. Virtuaalisessa työasemaympäristössä virtuaalikoneet on keskitetty palvelimelle. Asiakaskoneella saa yhteyden virtuaaliseen työasemaan etätyöpöytäsovelluksella. Valitussa työasemaympäristö ratkaisussa käyttäjillä ei ollut omaa henkilökohtaista virtuaalista työasemaa. Sen sijaan käyttäjä sai virtuaalikonekokoelmasta yhden virtuaalisen työaseman käyttöönsä istunnon ajaksi.

Tässä opinnäytetyössä tehty demonstraatio virtuaalisesta työasemaympäristöstä toteutettiin kahdella fyysisellä tietokoneella. Joitakin asioita on syytä tehdä todelliseen käyttöön tulevassa toteutuksessa toisin, jotta toteutus olisi tietoturvallinen ja tehokas. Työn toteutusvaiheessa on tuotu esille asetukset ja ratkaisut, joita todelliseen toteutukseen tulisi tehdä. Toteutus sisälsi toimialuetta hallinnoivan palvelimen sekä virtualisointipalvelimen. Virtualisointipalvelin ylläpiti virtuaalisen työasemaympäristön palveluita sekä virtuaalisia työasemia. Virtuaaliset työasemat oli määritetty käyttäjän uloskirjauduttua palautumaan automaattisesti ennalta määritettyyn puhtaaseen tilaan seuraavaa käyttäjää varten. Toimialuetta hallinoiva palvelin oli toteutettu virtuaalikoneena ja virtualisointipalvelin oli asennettu suoraan toisen tietokoneen laitteistolle. Molemmat palvelimet käyttivät Windows-palvelinkäyttöjärjestelmää ja hyper-V-virtualisointialustaa. Koska molemmat fyysiset tietokoneet ylläpitivät virtuaalikoneita, oli niihin tehtävä virtuaalinen kytkin.

Toimialuetta hallinnoiva palvelin tarjosi koko kokoonpanolle toimialueen, Dynamic Host Configuration Protocol (DHCP) ja Domain Name System (DNS)-palvelut. Virtualisointipalvelin tarjosi toteutukselle seuraavat palvelut: Hyper-V, remote desktop connection broker, remote desktop web access server ja remote desktop virtualization host. Virtualisointipalvelimelle tehtiin virtuaalinen työasemakokoelma, jonka virtuaalikoneisiin pystyi lähiverkosta muodostamaan etätyöpöytäyhteyden. Etätyöpöytäyhteys muodostetaan ottamalla yhteys remote desktop web access palveluun Internet Explorer -verkkoselaimen kautta. Jos toimialueen käyttäjätunnuksella riittää oikeudet, pystyy se sisäänkirjauduttua ottamaan etätyöpöytäyhteyden virtuaaliseen työasemaan.

ASIASANAT:

Palvelinvirtualisointi, työasemavirtualisointi, virtualisointialusta.

CONTENTS

FIGURES

LIST OF ABBREVIATIONS

DHCP	The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on UDP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks. (https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)
DNS	The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. (https://en.wikipedia.org/wiki/Domain_Name_System)
IP	The Internet Protocol (IP) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. (https://en.wikipedia.org/wiki/Internet_Protocol)
OS	An operating system (OS) is system software that manages computer hardware and software resources and provides common services for computer programs. (https://en.wikipedia.org/wiki/Operating_system)
OU	In computing, an organizational unit (OU) provides a way of classifying objects located in directories, or names in a digital certificate hierarchy. (https://en.wikipedia.org/wiki/Organizational_unit_(computing))
RAM	Random-access memory (RAM) is a form of computer data storage that stores data and machine code currently being used. (https://en.wikipedia.org/wiki/Random-access_memory)
VDI	Virtual desktop infrastructure (VDI) is a virtualization technology that hosts a desktop operating system on a centralized server in a data center. (https://searchvirtualdesktop.techtarget.com/definition/virtual-desktop-infrastructure-VDI)
VM	Virtual Machine (VM) is a virtual computer.
VMM	Virtual Machine Monitor (VMM) is a older term for hypervisor.

1 INTRODUCTION

This thesis introduces type 1 and type 2 hypervisors, virtual machine concepts and the virtual desktop infrastructure. For the practical part of the thesis, a Windows-based virtual desktop infrastructure will be implemented and its phases will be documented in detail.

Virtualization is a technology which allows physical devices functionality to executed like software. Different virtualization solutions are used even in small modern networks and can improve local area network (LAN) performance. Network designers have to design virtualization solutions at the same time as physical network topology in order for the network to be uniform. The virtualization of physical devices such as computers transfers processing power needs from one device to another and sifts network traffic loads as well. Virtualization solutions can improve network performance as well as bring significant financial benefit. Every network is different and each solution needs to be considered individually for each network. Virtualization allows for centralized management, but also adds difficulty to secure network environment. The newest virtualization trend is cloud computing, which allows server and software virtualization. Understanding virtualization and possible solutions are essential for working with networks.

2 VIRTUAL MACHINE

A virtual machine is virtualized computing. Virtual machines need a physical device to run on and an additional software layer called a hypervisor. The hypervisor, sometimes also called a virtual machine monitor (VMM), works as an interface between the virtual machine and physical components. The task of the hypervisor is to control the access and usage of physical resources allocated for each virtual machine. Another task is to isolate virtual machines from each other. The hypervisor adds more flexible uses for the virtual machine compared a normal computer. Hypervisors are divided into two types depending on how they work. It is important to know the differences between them to choose the right one for specific needs [1].

2.1 Type 1 hypervisor

Matthew Portnoy has defined Type 1 hypervisor as follows: “A type 1 hypervisor runs directly on the server hardware without an operating system beneath it. Because there is no other intervening layer of software between the hypervisor and the physical hardware, this is also referred to as a bare-metal implementation. Without an intermediary, the Type 1 hypervisor can directly communicate with the hardware resources in the stack below it, making it much more efficient that the type 2 hypervisor.” [1, p.23]. Type 1 hypervisors are generally more secure because virtual machines are better isolated [1, p. 24]. Because of this property, the type 1 hypervisor suits well for server virtualization and other demanding scenarios. Figure 1 visualizes where a type 1 hypervisor is implemented.

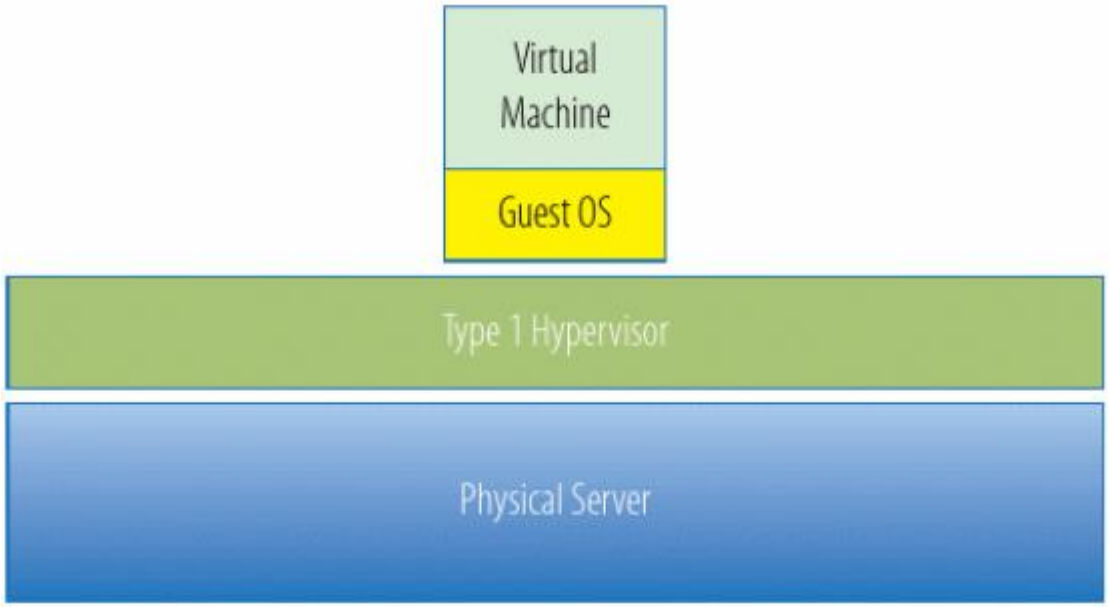

Figure 1. Type 1 hepervisor. [1]

2.2 Type 2 hypervisor

A type 2 hypervisor does run on top of the OS on a physical computer. This one additional layer, which a type 1 hypervisor does not have, makes virtual machines working on top of type 2 hypervisor slower. Every request and return message must be handled by the OS in between, which causes unnecessary delay for virtual machines. The OS in between adds security risks. For example, a maliciously infected virtual machine can affect the OS where the hypervisor is installed and so affect other virtual machines. A system failure of the OS or reboot also affects virtual machines [1, pp. 25-26]. The type 2 hypervisor does still have its advantages over type 1. It is generally easier to install and manage. The type 2 hypervisor is well-suited for learning and testing environments, where availability and performance are not so important. Type 2 hypervisors are good enough for single workstation virtualization even in more demanding scenarios. Figure 2 visualizes where a type 2 hypervisor is implemented.

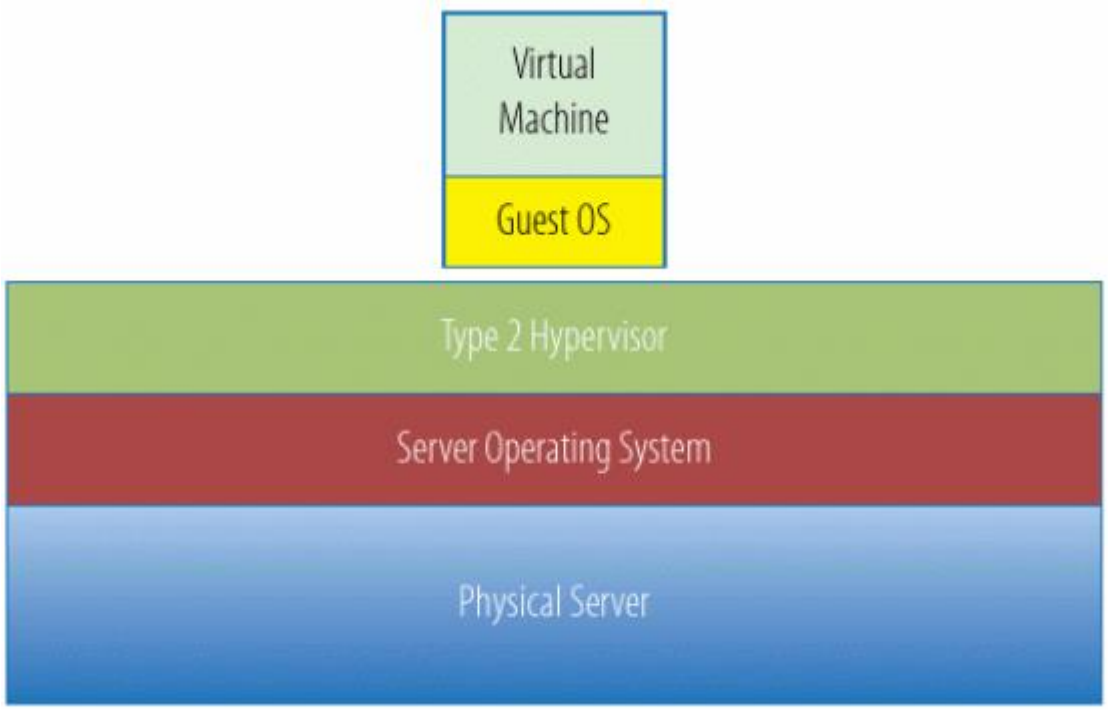

Figure 2. Type 2 hypervisor. [1]

2.3 Virtual machine security and redundancy

Virtual machines can be snapshotted for backups easily. These snapshots can be quickly transferred to another server and a virtual machine can be set up in a different physical location. Multiple servers can be chosen to host the same service there where redundancy is needed.

Backup devices can be preconfigured in a desktop virtualization scenario where cheap client devices are used only to achieve a remote desktop connection to the virtual machine locating on the server. Companies can have some of these cheap client devices ready to be switched instantly. Personalized physical workstation replacement and software installations can take much longer time.

From a security perspective, virtualization adds another layer of an attack surface and is always a challenge. The same methods can not be used to secure and monitor virtual and physical computers. There are malware and attacks that are dedicated to breaking into virtual machine systems. Some of the malware are able to detect if the host is virtual or physical and adapt to make them harder to be detected. Virtual machine security is a whole different field of network security that needs dedication and understanding to

master. In a virtual machine environment remote connection, virtual hard disks and configuration files need to be secured. Additional protocols, different firewall and monitoring solutions need to be deployed to secure virtualization environment. If these security features are poorly deployed, the virtual machine performance can drop dramatically. [2]

Considering the chance of physical device theft, having virtual workstations stored in a data center on the server is much more secure. Unauthorized persons should not be able to access a data center. With a carefully planned social engineering attack, somebody with malicious intentions can be into contact with the physical workstation much more easily and steal its data or the physical device.

2.4 Virtual switch

Because virtual machines have to share a physical network adapter, virtual switching is needed. Hypervisors have tools for creating the virtual switch for virtual machines to use. Virtual switching tools are slightly different between different hypervisors, but the basic functionality is the same. The internal virtual switch allows virtual machines to interconnect to the local host if it has an OS installed on and virtual machines on that one physical machine. No internet access can be gained for virtual machines in this manner. Alternatively, the virtual switch can be external and have access outside to one physical machine by sharing a physical network adapter with the virtual switch to use. The virtual switch connects multiple virtual machines together just like the physical switch connects physical machines. Similar to the physical switch having gateway link, an external virtual switch has a network adapter connected to it.

3 SERVER VIRTUALIZATION

Server virtualization is the oldest form of virtualization. In case of hardware failures and because of security reasons, it is common to install only one service on one server. Dedicated server hardware is powerful and this kind of service implementation occasionally leaves resources unused. With virtualization solutions, multiple virtual serves can run on one hardware without causing unnecessary security risks and service interfering. With proper solutions, moving and replacing virtual servers from broken server hardware with new ones is easy and fast.

3.1 Virtualization platforms for servers

High performance is demanded from servers. Because of that without an exception enterprise level virtual servers run on top of type 1 hypervisor. Peter Tsai has made statistics of the most used virtualization platforms illustrated in Figure 3.

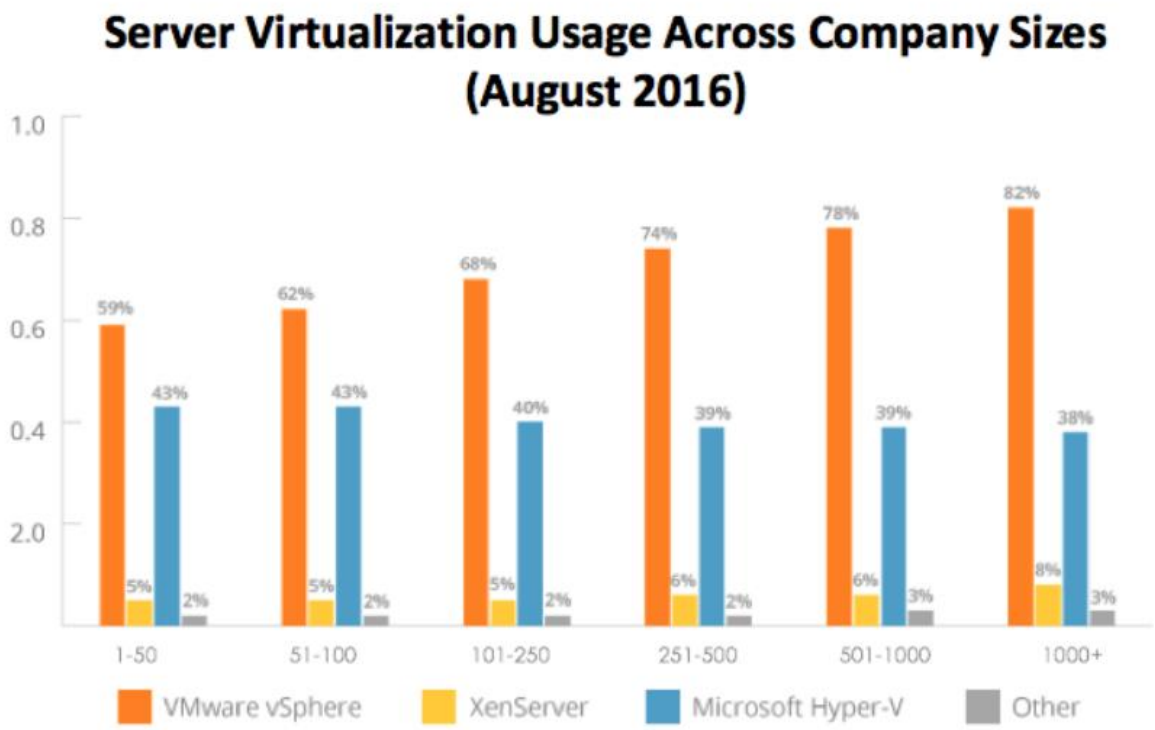

Figure 3. Server virtualization usage [3].

The above statistics are from 2016, but there have not been major changes to either of these hypervisors. That is why it can be assumed that the usage has stayed within 10% marginal from 2016 and VMware ESXi and Microsoft hyper-V are still most used virtualization platforms.

3.1.1 VMware ESXi

VMware was first to bring hypervisor commercially available. The VMware hypervisor is still most commonly used across the globe. VMware ESXi is a type 1 hypervisor that does not have other functions than work as hypervisor. The management of VMware ESXi is conducted by connecting to the management IP address with a web browser. After logging in, the management console shows where the installed virtual machines can be managed. VMware ESXi has a free version and paid licensed version with more advanced properties. For enterprise use, the purchased version has to be used because the free license does not have every needed feature to make implementation secure and fault tolerant. The purchased version has a vSphere client that allows for centralized management of ESXi hypervisors. The free version can be used to host a few virtual machines and is suitable, for example, for learning environments and labs.

3.1.2 Microsoft Hyper-V

Hyper-V is inbuilt software in Windows server operating systems as well as in Windows 10. The Hyper-V role needs to be activated before it can be used. Regardless of where the operating system (OS) Hyper-V is running, it is managed from an easy-to-use graphical user interface. This makes hyper-V very easy to manage and access. The Hyper-V is a type 1 hypervisor even it is managed like most of the type 2 hypervisors. The Windows server OS and hyper-V are commonly used when hosting services for Windows-based environments.

3.2 Server virtualization advantages

The server hardware is powerful and expensive. Because of that, resources should be used as efficiently as possible. Combining multiple servers that are run on low use into one physical machine can bring significant financial savings. Savings can come from

equipment investments and from use expenses. Every server uses electricity to run and needs external cooling as well. Besides the electricity usage, physical space consumption requires a larger data center, which can be very expensive. Virtualization decreases the amount of physical machines needed, which is a great saving in total.

Server virtualization provides flexibility for the server user. If a new service is needed and an existing physical server has unused resources, a new service can be deployed as a new virtual server. When companies grow, the traffic load for services will also increase. Virtual servers are easier to deploy elsewhere than physical servers. Load balancing can be conducted for virtual machines separately, which allows for prioritising the bandwidth needs of other services.

4 DESKTOP VIRTUALIZATION

Desktop virtualization can be implemented locally or with remote desktop solutions that run on the server. ”Remote desktop virtualization implementations operate in a client/server computing.” [4]. ” A common implementation of this approach involves hosting multiple desktop operating system instances on a server hardware platform running a hypervisor.” [4]. Solutions like that are called virtual desktop infrastructure (VDI) solutions.

4.1 Local desktop virtualization

Local desktop virtualization can be used to create a virtual computer inside physical desktop. Windows hyper-V or type 2 hypervisors or are usually used for local virtualization because they are easy to manage and free to install. VMware workstation player, VMware fusion, Oracle VirtualBox, Parallels Desktop for Mac are examples of commonly used type 2 hypervisors [5]. Local desktop virtualization can be useful if software need to be run are not compatible with the current OS. Most commonly this means software that is available for Machitos, Windows or Linux operating systems only. However especially in industrial use some old machines and software can be run only with very old OS that can be virtualized on new hardware.

4.2 Virtual desktop infrastructure

Margaret Rouse has made a great summary of Virtual desktop infrastructure (VDI) solutions: ”There are two main approaches to VDI: persistent and nonpersistent. Persistent VDI provides each user with his or her own desktop image, which can be customized and saved for future use, much like a traditional physical desktop. Nonpersistent VDI provides a pool of uniform desktops that users can access when needed. Nonpersistent desktops revert to their original state each time the user logs out.” [6]. In large enterprises where multiple users do the same work tasks and have the same software needs nonpersistent VDI is a better solution. It allows fast and easy upgrading of virtual machines for the group of users at once. OS images and virtual machines can be kept very light weigth for server hardware if user files are chosen not to be saved. In

this case users would have to have a network shared drive or cloud storage for personal files. Management of persistent VDI requires more time because OS Images can't be updated as easily if there are personal files saved on virtual machines.

4.3 Remote desktop virtualization advantages and disadvantages

Remote desktop virtualizations changes the physical placement of desktop from workstation to server. While a server is doing all processing it lovers the requirements of the client machine to having only enough power to run remote connect. This allows use of cheap end point client machines or even mobile devices. Even high performance client computers usually have much shorter life cycle than actual server hardware. Servers are expensive, but depending on how many workstations can be virtualized to a single server and cheap client machines that can bring significant financial benefit. Latency for other internal servers is also decreased when the virtual machine is already running inside the datacenter. As a down side, the server will be using more network resources in remote desktop deployment. Also, when client machines would use only locally installed software, now causes remote control traffic between server and client.

5 IMPLEMENTING VIRTUAL DESKTOP INFRASTRUCTURE

As hands-on part of the thesis, the author decided to demonstrate implementation of VDI in Windows server-based environment. The author chose to implement nonpersistent version and make configurations with the aim of keeping the solution as lightweight for hardware as possible. After the implementation has been completed, the VDI does provide one collection of virtual workstations for domain users to use.

5.1 Implemention topology

VDI demonstration that the author created had two Windows servers on it. Servers were serving the roles of domain controller and virtualization server. Virtualization server was hosting virtual machine collection and serving roles necessary for VDI to work. At first the author tried to implement these two servers as virtual machines on one physical computer hardware. Quickly the author noticed that hardware resources were insufficient and second physical computer had to be added. Physical computer A had a domain controller running as a virtual machine. Physical computer B had the virtualization services installed directly on its hardware. Since only two computers were used a switch was not needed and computers were directly connected with the Ethernet cable. Both physical machines had virtual machines running on them. This required implementing virtual switches on both of physical computers. The servers ran Windows server 2012 R2 OS. Virtual machines in VM collection had Windows 7 running on them. Hyper- V was used as a hypervisor. Figure 4 visualizes this setup.

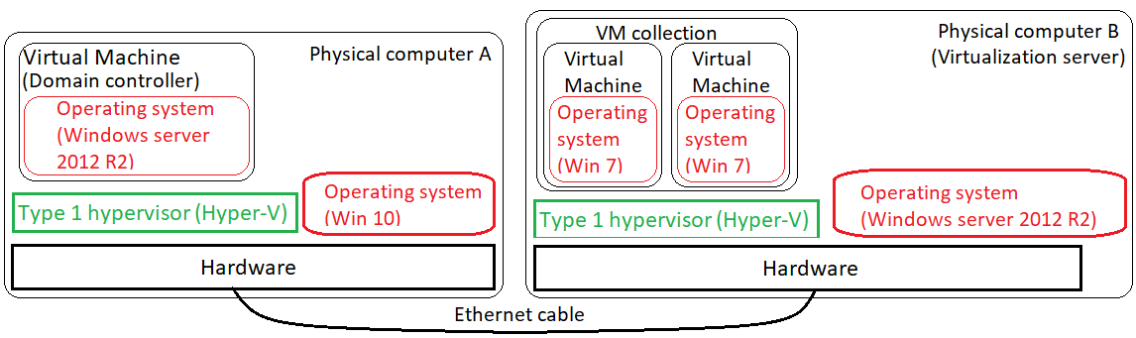

Figure 4. Implemention topology.

5.2 Setting up domain controller.

The domain controller is needed in a VDI environment to control who can access virtual machines in the collection. The domain controller does also manage virtual machine profiles. In this demonstration domain controller does serve also as a DNS server and DHCP server.

5.2.1 Installing hyper-V on windows 10

Physical computer A is running Windows 10. Hyper-V is built in windows 10 OS but not activated by default. Activation can be done from Control Panel\Programs\Programs and Features. There is turn Windows features on or off link. That link opens pop up window where hyper-V needs to be selected and activated.

5.2.2 Creating virtual machine

Once hyper-V is installed virtual machine needs to be deployed. Deployment is easy to do by clicking new virtual machine button and the following pop up windows instructions shown in Figure 5.

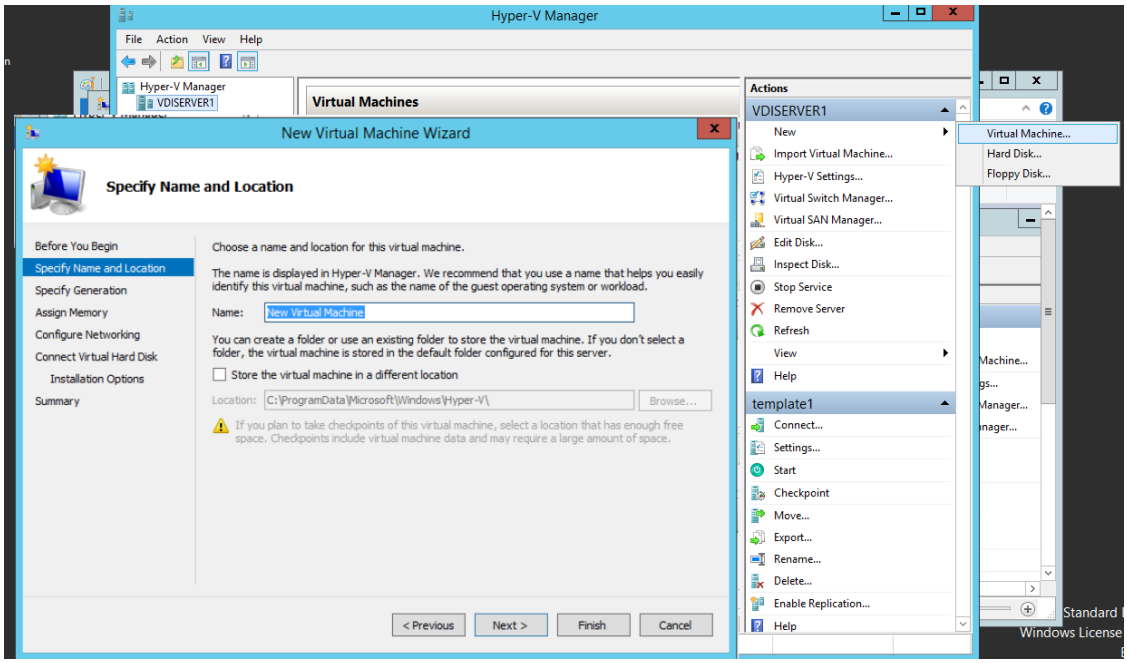

Figure 5. New VM.

During deployment, virtual machine useable RAM memory is limited and virtual hard disk created. It is possible to Insert operating system (OS) image file to the virtual machine or use the existing virtual hard drive. After the virtual machine is created it needs to be turned on. At this point, the OS starts installing if the OS image file has been inserted into a virtual machine. OS installation happens just like installing the OS in a physical device. Domain controller services are needed in the Windows VDI implementation so Windows server 2012 R2 OS image can be used.

5.2.3 Creating domain

After the OS is running it is wise to choose an address range for this domain to use and give a static IP address from range to this server. After the IP address is set, it is time to start adding services to the server. This server needs to be a domain controller. Server manager has easy to use add roles and features wizard. With that wizard active directory domain services role needs to be installed on the server. After the role is installed notification appears. Clicking that notification opens a new wizard. In that wizard there is an option to add this new server as domain controller into the existing domain or create a new one. In this case, the new domain needs to be created. The new domain is named in the first page. The next page has a domain name system (DNS) service auto selected to be installed. That service needs to be installed as well. In the third page, NETBIOS domain name is given. This name is shown as the domain name when logging in as a domain user and needs to be remembered. After that, all needed configurations are set. The server needs to be rebooted after that. When the server does power up the built in administrator account has been promoted to the domain administrator account. This Administrator account should not ever be used as main logon account for security reasons. The built in administrator account has highest possible rights of the domain. This makes it a security threat because the user name is always same and that account is the first one which hackers try to use for accessing the domain. For these reasons a new account should be created for that domain and given administrator rights for administrative use. After the new account is created the default administrator should be disabled from use. At this point, another new user should be added with only domain user rights. This account can be used for testing later on.

5.2.4 Implementing DHCP

Domain controller needs dynamic host configuration protocol (DHCP) service. The DHCP service needs to be installed with earlier used add roles and features wizard. DHCP is needed to manage IP addresses of the virtual machines that are going to be added to the domain. After installation, DHCP service is found under server manager tools. In this demonstration IPv4 protocol is used. The domain is found under DHCP services. After selecting the domain, under it opens options for IPv4 and IPv6. When IPv4 partition is opened it appears empty. The configuration has to be done by clicking add new scope. A new scope wizard appears to assist the creation of new scopes. The scope needs to be named at the beginning. After that scope starting and ending point needs to be selected. Selected IP address range creates an address space that needs to be used for domain devices. The wizard allows excluded range to be set as well. The excluded addresses can be used for switches and servers that need a static IP address. In this demonstration at least three excluded addresses are needed. Two of the addresses are used for the servers and one is used for the virtual switch. In a larger implementation, the minimum amount of excluded addresses needed would be higher depending on how many excluded addresses would be needed. While selecting an excluded address range, the server IP address needs to be included within the range. The wizard allows also sharing default gateway information. It is important to fill this address to network traffic to find out of the subnet. The next page of the wizard asks for the DNS address. In this demonstration, the domain controller will also host DNS. On the last page, the administrator has to choose whether the scope is activated or not. The scope needs to be activated. The following actions can be completed for the scope to be activated faster: Refresh DCHP for IPv4, restart DHCP from the server name on the left and finally refresh DHCP server. After that DHCP is running.

5.2.5 Implementing the virtual switch

The virtual switch needs to be implemented because virtual computer needs to be part of the network. Since this scenario has only one subnet, no switching is needed. This means that all addresses to the whole subnet can be given from the domain address pool created earlier. The virtual switch manager is found from under hyper-V manager.

Inside virtual switch manager there is a button which allows the creation of a new virtual switch shown in Figure 6.

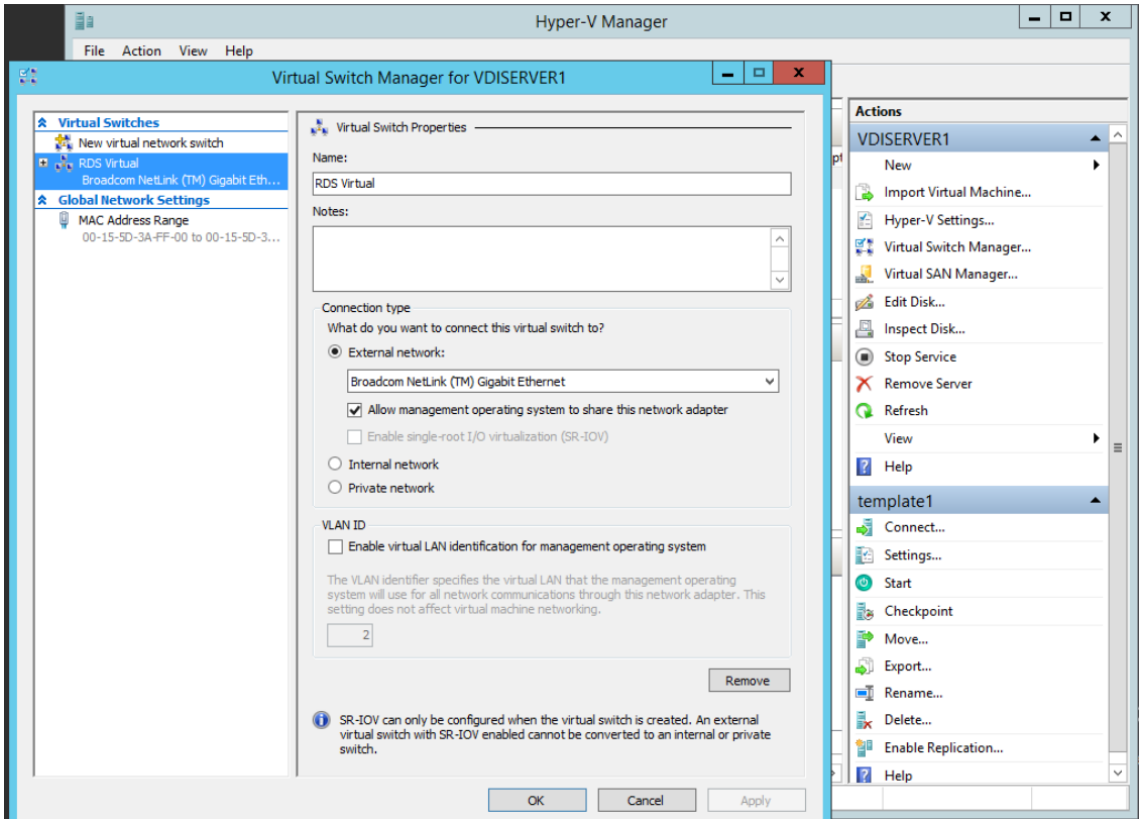

Figure 6. Virtual switch.

The external virtual switch is chosen because the virtual machine must connect to other machines outside of the physical computers. The external virtual switch needs to be connected to the physical Ethernet adapter. After the virtual switch is configured physical adapter hands off configured for the virtual switch. The virtual switch appears under network adapter settings. Now that virtual switch can be configured the same way as a physical network adapter. When the physical network adapter is shared with a virtual switch physical computer uses IP address from the virtual switch. The virtual switch is shown as the Hyper-V virtual Ethernet adapter. The virtual switch needs an IP address from the address space excluded addresses. After an address has been set the virtual domain controller server needs to be connected to the virtual switch. The connection is configured from inside hyper-V manager and virtual server adapter settings. When the virtual server is connected to the virtual switch, it is ready to connect other devices once the cable is connected and IP address is matching the same subnet on the other end.

5.3 Setting up virtualization server

VDI server will be installed directly on the hardware, when the installation is ready the IP address is set to match one of the DCHP pools excluded IP addresses. After the IP address is set the VDI server will be able to communicate with the domain controller and needs to be added to the domain. The configuration is set from Control Panel\System and security\System. Navigate under the system settings and change domain settings. The full domain name needs to be written down. Administration level domain user credentials are asked if the domain name match and internet connection does work between the domain controller and the new computer being added. After the credentials are verified the computer is added to the domain and needs to be restarted. After the computer powers up it can be accessed with the domain user accounts. In order to configure the server, administration level credentials need to be used. Hyper-V is the first role that needs to be added with the added roles wizard.

5.4 Creating preconfigured OS image with sysprep

VDI allows multiple virtual machines to be implemented across many servers during the implementation. For the implementation to be successful some system preparation (sysprep) need to be done for OS image. Sysprep is built in software in the Windows OS. In order to use sysprep, clean Windows OS must first be installed normally. The OS image is going to be used for VDI Hyper-V integration services need to be updated, if Integration services are not updated multi deployment will fail.

Integration services setup disk needs to be inserted into the virtual machine from the virtual machine action bar. After the setup disk is inserted it is found under the network as a drive. Clicking the drive gives notification that says integration services are running an older version. Installation dialog opens and allowing it makes the installation automatically.

The last required task is to sysprep the virtual machine. Sysprep does turn OS into the hardware independent state and cleans it up. All installed drivers and software are saved, but personal files and hardware information is deleted. This is very useful for implementing multiple machines at once. Only one OS image needs to be created which

can already include at least most of the needed programs. When this OS image is later applied to machine software within OS image are also deployed automatically.

Creating OS file that already contains drivers and other software can also be used for other purposes than virtual machines only. Big enterprises that deploy computers regularly use as pre-configured OS images as possible to ease workload and save time.

When all wanted installations are done to OS image sysprep needs to be run. By default sysprep software is found at C:\Windows\System32\Sysprep. Note that sysprep can not be found with the Windows search function to prevent accidental use. Running the software starts dialog box shown in Figure 7.

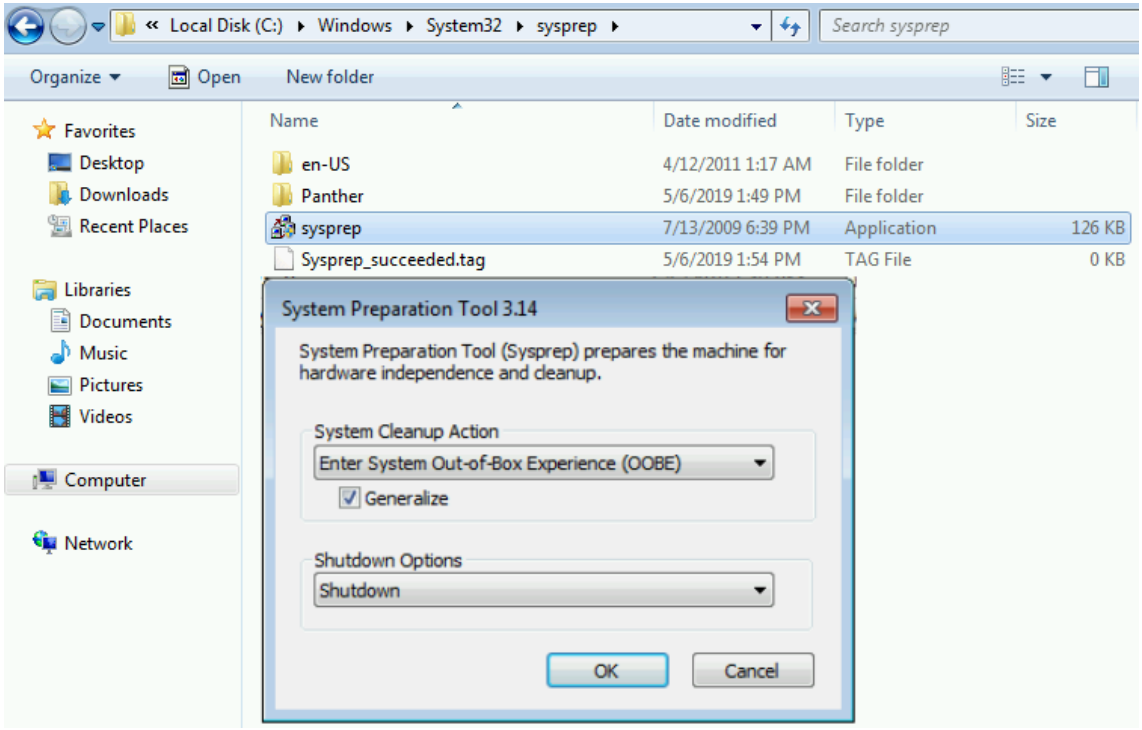

Figure 7. Sysprep.

The first drop down option is set correctly by default, but the generalize option needs to be chosen. Another option is the shutdown option that has 2 good options depending on how the prepared OS image will be used.

In case where the modified OS image needs to be captured, saved and used elsewhere the restart is chosen. After the virtual machine does power up system needs to be booted to network. That gives option to run OS setup or capture the image. In this state, the

Image is still clean of hardware information and needs to be captured and saved to the server.

Another option is not power up the virtual machine and keep it as a template for the VDI virtual machines. During the VDI implementation, the system prepared clean OS image can be used directly from the virtual machine.

The image should not be system prepared multiple times or it might cause errors starting to occur in OS operation. The easiest way to modify already used OS image is to snapshot it before the sysprep is run. This allows virtual machine roll back to the same state as OS image but before sysprep. Additional software and updates can be installed and snapshot can be taken again to capture state before the sysprep for the later updating.

5.5 Implementing VDI services

The VDI implementation creates a virtual machine collection that needs to be controlled by the domain controller. A new organizational unit (OU) must be created on the domain controller. This OU is created under the active directory domain users and computers. Correct folder location for this OU is right under the domain at the same level as users collection shown in Figure 8.

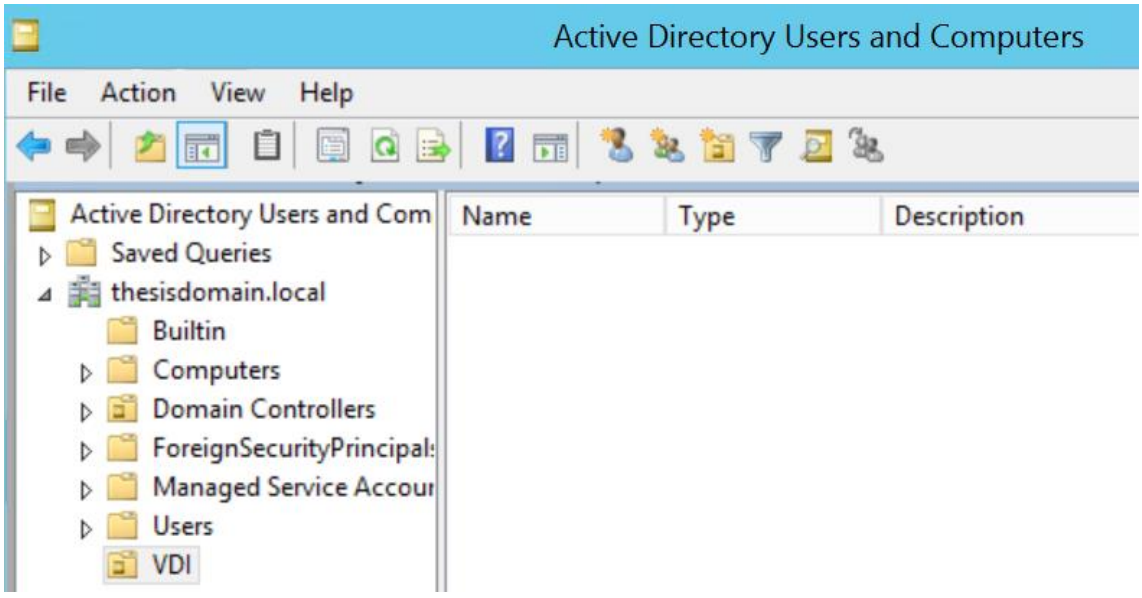

Figure 8. New OU.

5.5.1 Installing remote desktop services

The remote desktop services installation is found under the add roles and features wizard. Selecting that follows option to Standard deployment of services across multiple servers or quick start just for one. The standard deployment has more options and should be chosen. The next page of the wizard asks which type of the deployment this will be. Options are virtual machine-based desktop deployment or session-based desktop deployment. VDI is Virtual machine-based deployment. This option will install the roles of the remote desktop connection broker, remote desktop web access and of the remote desktop virtualization host. One or more of the servers can be chosen for each of those roles to run on. All services can also run on a single server, if no more is available.

5.5.2 Configuring remote desktop services

Remote desktop services need to be configured on the virtualization server from deployment properties under the deployment overview. The connection broker service needs to have permissions to the OU containing virtual machines. Permissions can be given under the active directory section. The domain name and OU under the domain need to be selected. OU has to be the same where the virtual machine profiles will be soon added, for this implementation to work.

5.5.3 creating virtual machine collection

The virtual machine collection needs to be created for VDI. The collection will hold copies of the same virtual machine and on connect, one will be given to the domain user to control. The new collection is created from Server Manager/Remote Desktop Services/Collections. On the right side of that page there is tasks button which has an option to create a new virtual machine collection shown in Figure 9.

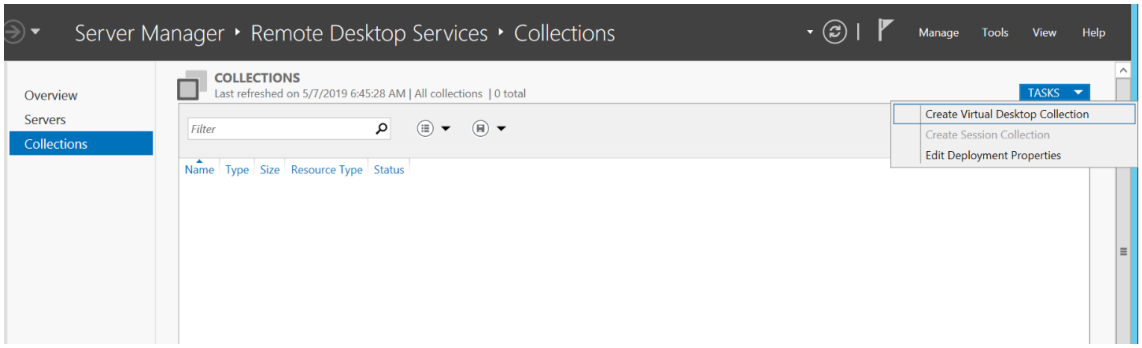

Figure 9. Create VM collection.

Assisting dialog helps creating a new collection. At first, new collection needs to be named. This name is the same that is shown to users when they log on the web access server. The next option allows the administrator to choose which type of virtual desktop collection this is. Options are pooled and personal. Personal virtual machines are in use of a single user only and the pooled option allows multiple users to use the same virtual machine during different times. With the pooled option, less machines can usually be deployed. The downside of this is that the machines can't be customized as well by users. For this VDI implementation, the pooled option is chosen. On the next page existing system prepared virtual machine or OS image file can be chosen as the template for new virtual machines. In this VDI implementation, the system prepared virtual machine can be used. On the next page Timezone and domain are selected for new virtual machines. On this page OU in the domain must also be selected as a place where virtual machine profiles will be created.

All settings are set for the virtual machines and one or more hyper-V servers must be chosen to host virtual machines. Multiple servers can be chosen and all of those servers would receive an equal number of virtual machines. In this demonstration and only one server running hyper-V, the virtualization server is chosen. At this point, permission is given to the domain user groups who are intended to use the virtual desktops. Numberof the virtual machines to be created to the collection is chosen at this point. For this implementation and to demonstrate the effect two virtual machines are enough. Desktops can be given names with an up running number suffix at the end. Location where the virtual machine disks are stored need to be configured next shown in Figure 10.

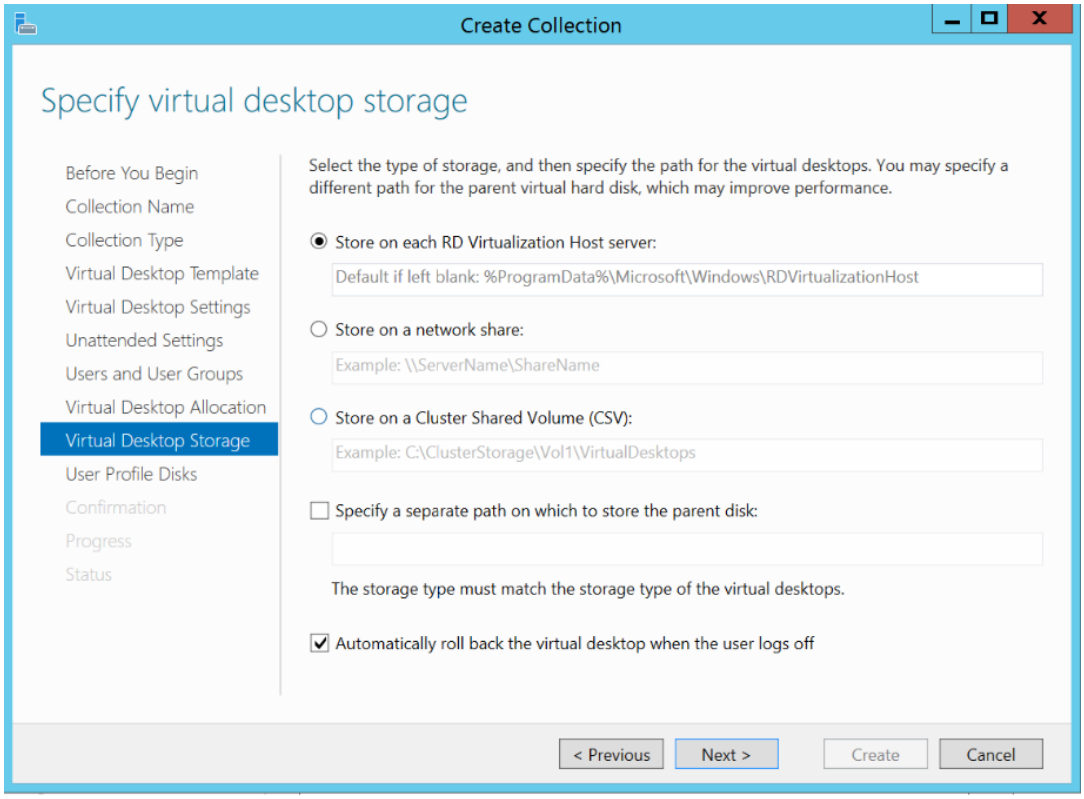

Figure 10. VM collection storage options.

The server itself can be used as a location for disks or then for example network share. The network share would be a smart choice for the real enterprise environment. On that same page there is also an option to roll back virtual machines to the clean state after user logs off. This helps to keep computers clean of junk files. This option is great to implement in example to school environments. This option suits well for the goal of this VDI. The next page allows the administrator to select if these virtual machines store user profiles or not. Choosing not to save the user profile saves significant amount of space on the virtual machines and allows them to be deployed with less memory. This suits a goal of this VDI implementation and is the chosen option. On the next step virtual machines are deployed.

5.6 Testing VDI solution

Virtual machines appear on the virtual machine manager if everything has been configured correctly. Notice that virtual machines have RDV rollback checkpoints. That

is a clean state of the OS where connection broker sets back virtual machines after the user disconnects. Virtual machines and the checkpoint are visible in Figure 11.

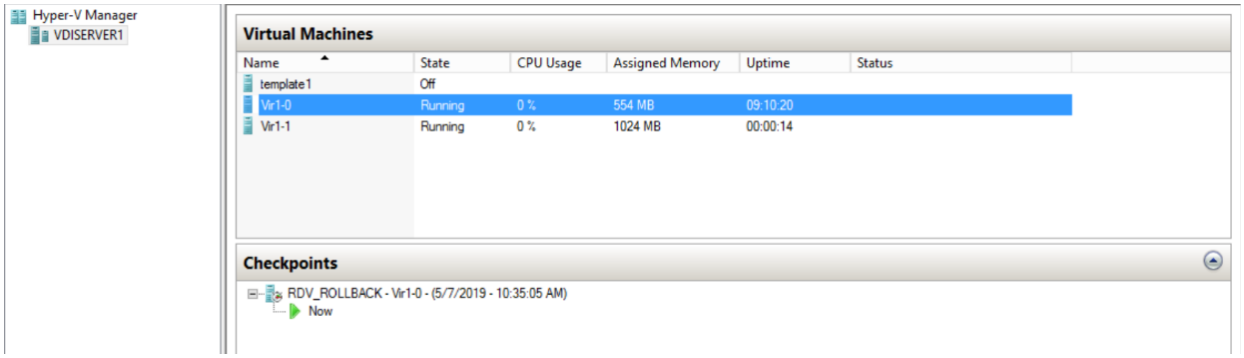

Figure 11. Virtual machines and rollback chekpoint.

Virtual machines should have gotten an IP address from the domain controllers DHCP. Figure 12 shows IP address leases for virtual machines.

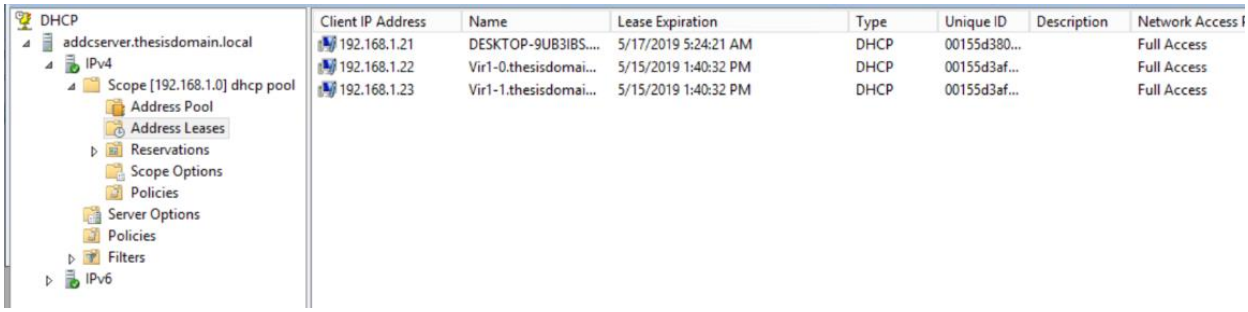

Figure 12. DHCP leases.

Virtual machines are also found under the OU at the domain controller if the implementation has been successful. Figure 13 shows created an OU holding the virtual machine profiles.

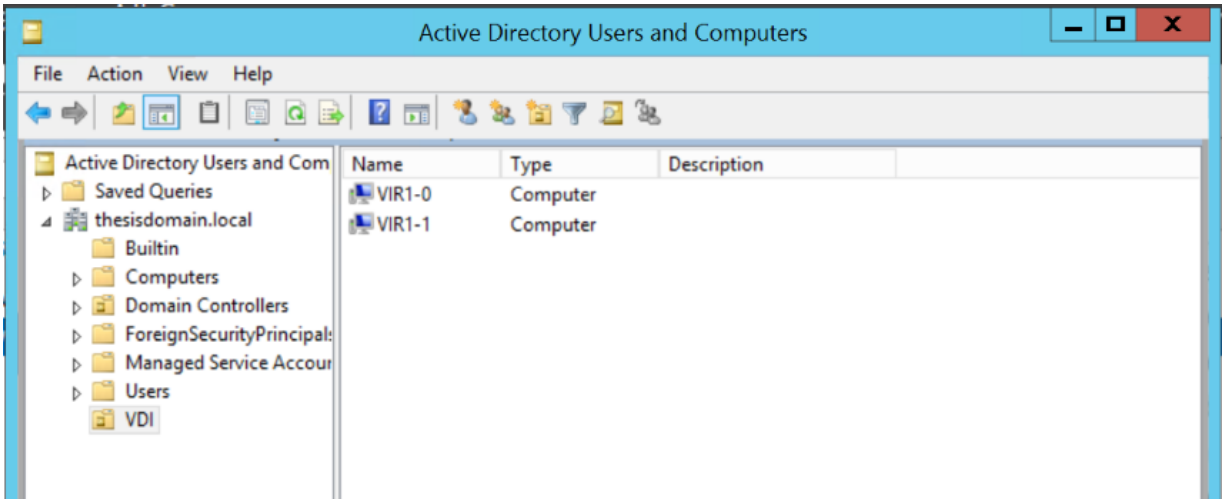

Figure 13. OU with virtual machine collection.

Virtual machines can be connected from the local area network. This is done by connecting the web access server https://server name/rdweb with the internet explorer. The login prompt asking for domain user credentials is shown in Figure 14.

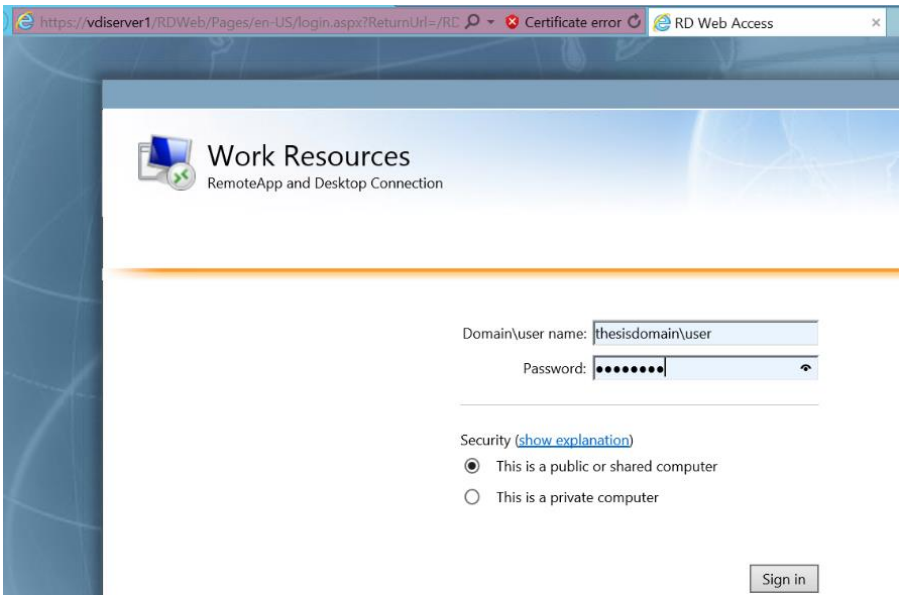

Figure 14. Remote desktop web access login.

After logging in the remote desktop collection is shown on the remote app and desktops page if the domain credentials have permission for it. Virtual desktops1 is the pool

created earlier containing two virtual machines. Figure 15 shows the VM collection and connect window.

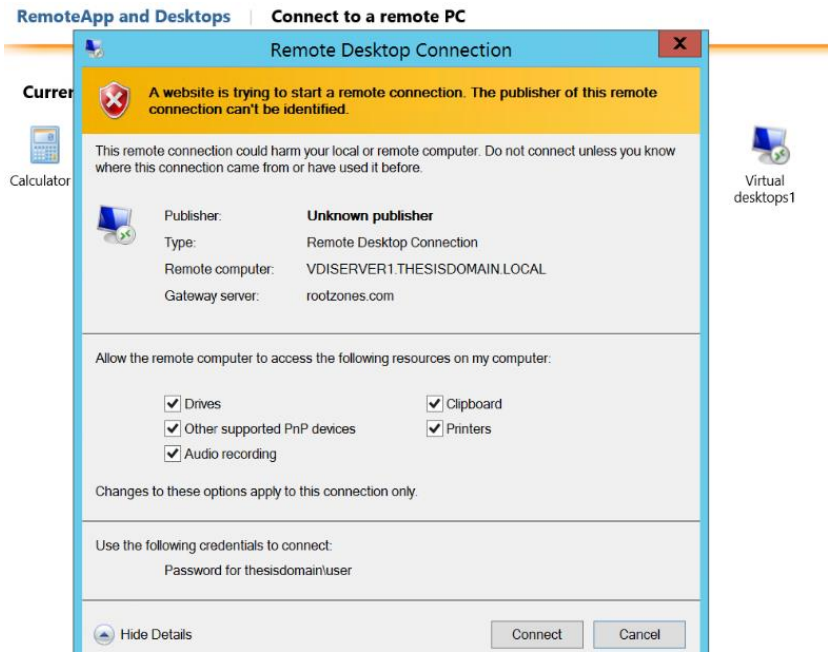

Figure 15. Virtual machine collection.

Figure 16 shows a remote desktop connection connecting to the virtual machine from the pool.

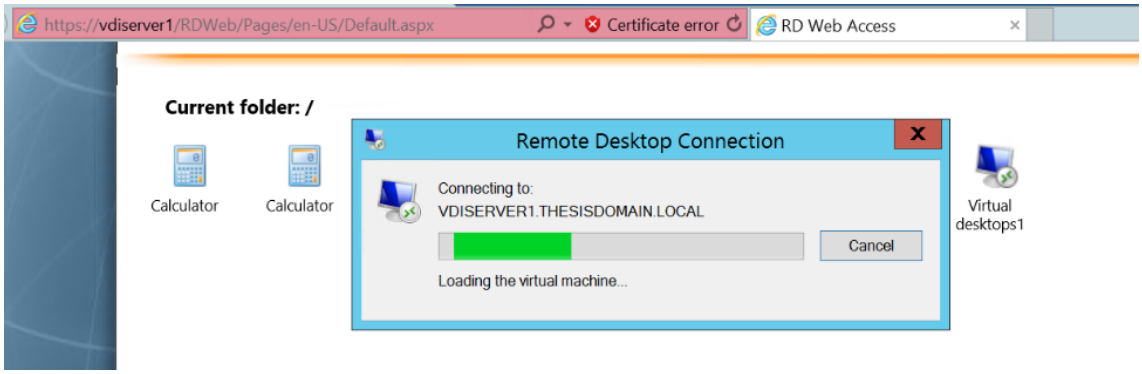

Figure 16. Remote desktop connection.

After the remote desktop connection is made, VM is in use for the user as long as it is connected. After the user does disconnect, the connection broker server does roll VM back to clean state for the next user to connect.

6 CONCLUSION

Different virtualization solutions are an essential part of modern networks. A VDI solution is a modern workstation virtualization technology used in enterprises. A VDI services suit the best enterprises which have several employees using the same sets of software. Secondly, a VDI suits very well for use in a shift work environment. The VDI solution implemented in Chapter 5 is functional but has only the basic structure of VDI. New virtual machine collections can be easily added to the existing implementation to serve new groups of users. However, in order to implement a VDI into an enterprise environment, it needs to be enhanced.

From a security perspective, all VDI-related services should be installed on different servers. Multiple hyper-V servers should be in use and virtual machines should be divided among them for redundancy. Virtual machine hard drives should be stored on a network share or dedicated storage server. Virtual machines need to be protected with firewalls and network traffic monitoring software. Additional software and hardware can be added to extend connection options beyond the LAN.

The creation and updating of existing virtual machine images should be well managed. To achieve that, image versions need to be documented and stored in a centralized manner.

REFERENCES

[1] Portnoy, M. Virtualization Essentials. 2nd ed. Indianapolis, Indiana: John Wiley & Sons, 2016. p. 334, ISBN 9781119267744 (e-book).

[2] Shackleford, D. Virtualization Security : Protecting Virtualized Environments. Indianapolis, Indiana: John Wiley & Sons, 2012. p. 334, ISBN 9781118333754 (e-book).

[3] Tsai, P. Server Virtualization and OS Trends. [Online]. 2016. [Accessed 15 May 2019]. Available from: https://community.spiceworks.com/networking/articles/2462-server-virtualization-and-os-trends

[4] Wikipedia, Desktop Virtualization [Online]. [Accessed 10 May 2019]. Available from: https://en.wikipedia.org/wiki/Desktop_virtualization

[5] Wikipedia, Hypervisor [Online]. [Accessed 8 May 2019]. Available from: https://en.wikipedia.org/wiki/Hypervisor

[6] Rouse, M. Virtual Desktop Infrastructure (VDI) [Online]. 2017. [Accessed 13 May 2019]. Available from: https://searchvirtualdesktop.techtarget.com/definition/virtual-desktop-infrastructure-VDI