

1

by Josh Naylor

Submission date: 09-Jan-2023 04:36PM (UTC+0000)

Submission ID: 194196008

File name: 32136_Josh_Naylor_1_460444_718183860.docx (21.91K)

Word count: 2272

Character count: 9444

Cloud computing Final

Josh Naylor

Table of Contents

WHAT ARE VIRTUAL HARD DRIVES?	1
HOW ARE VMS CREATED AND MANAGED?	2
VNETS	3
NETWORK SECURITY	4
REFERENCE:	5

What are virtual hard drives?

The definition of a virtual hard drive is that “a disk image format for storing the entire contents of a hard drive”. [1]. The hard drive is often called a VHD as short as you don’t want to write out full. It can also be called a VM or a virtual machine as this will make an existing hard drive and it will have all the data and all the different elements that will make the system work. The data can be used anywhere as you can move the data from a USB to any device in the world can hold data as this is how data can be moved that easy in these days. You can then have the data anywhere in the world and use it to your advantage. The physical hard drive and a virtual one is very similar as it mostly has the same software on it like the hard drive sector and a file system that will organize the file so they won’t get mess up on the server and the user can find them easy. “Just like a VHD a hard drive can create disk sectors, files and folders also run an OS and execute user applications.” [2]. The difference between the two is that the VHD is most always used on a VMware workstation so it has been designed to be used on a VM or it can be used on a Hyper-V VM as it must be used on a virtual machine infrastructure. The benefit of a VHD is that you can always add on the storage when you need it as you won’t have to move the data from one hard drive to another like in your computer at home but you would just add the data on top of it as it is not physical but it is stored on a physical hard drive but it is normally offsite and you would deal with the hard drive side of it. The VHD is managed by either the OS or the virtualization manager. There are 3 different types of VHD, and they are “formats are fixed, dynamic and differencing virtual.” [3]. The first one is the fixed this will give you a fixed amount of space on the VHD and then it can get full but then the benefits of it is that it has fast

processing speeds, and you can get constant fragmentation. The second one is the dynamic VHD, and this is good as you start with a minimum amount, and you can work your way up to a bigger size if you want to. It also has the added benefit of having a sped-up storage allocation. The last one is the differencing VHD, and this will make a copy of the existing disk. As you have two different disk you can have one and not change anything about the other one.

How are VMs created and managed?

A virtual machine is a space where you can use it to have as a personal computer that can be run a normal computer but then you can have another computer in it which would be a VM and that could be a higher spec system to run a business you might have so it would be easier to run as you can separate them. There is lot of companies that can be used to host a VM the two of the biggest ones are amazon web services or Microsoft Azure. You can also set the VM up a few ways as you can set it up using just a normal GUI which would have lot of different approaches you can have to set up your VM as you can just click on the option and then it will be on your VM when you open it or you can choose the option where you can use Bash code to set up the VM as this is the way where you can set it up with code and you can put anything you really want on the VM so it's up to you and not down to lots of options you choose from the page. When you make a VM you will have to have lots of different option for the VM the first thing is if you are paying for the subscription to the platform am doing it on Azure. You will first have to name it make sure you name it something that you can look back to and you know what is on it as you could have a lot of different VM open. After that you will need to select the region, this is important as you will need to know what region you are in as it will not work if you are not in the region, you are in so you can search it up where the closest data centre is for you. You will then need to choose the image and the size of the VM as the size of the VM is important as well as you will need to choose a size fir for you. If you are using a really big size and you don't need it, you will get charged a lot of the size of the VM but if you choose a size that is too small then you may have to get a new VM as often they won't let you change your size when you make your VM and you have already used it. You can then be very specific on what you want as the disks, networking, management, advanced and a few more. All of them do different things so it important to look at each one.

vNets

A virtual networking or a vNet is where all the everything will come together like the servers, VMs, all the devices and the data centres so everything is put together like a jigsaw. "This allows the reach of the network to be expanded as far as it needs to for peak efficiency, in addition to numerous other benefits." [6]. when you connect a WAN and a LAN to together it can become something stronger as you have the two working together and they can go for a longer range as they can go for over a half a mile. The reason VNET work so well because it uses modern technology as some of the technology in the network is a vSwitch software and this is a very smart piece of technology as it will virtualization software on a host server. This will allow you set up and configure a VNET to your preferences. Next is the virtual network adapter and this will make a gateway between the networks you might have. This is the important one as this is the physical network and you are "Required as a host for the virtual network infrastructure." [6]. This means that you must have the physical network to have the virtual one, so it is very important to have the physical one. next will be the VM and the devices as this is what will connect to your network and what will allow your whole network to come online as if you have the network and not the devices then you just have a network so it will be kind of pointless. It will also allow you to have a lot more functionality as you can do a lot more with the devices that are connected to the network than just the network. the next part of the VNET is the servers and this will be the basically the brain of the system as mostly everything will all go back to the server, and this is what you will have to keep safe from the attacks and the virus you might get on the network, or you could be in trouble. The next part is the firewall of the whole network as it is a wireless network it can be harder to secure the network as you have multiple attacks coming from around the world not like a physical one where you must be in the actual server to do the attack so you will need much stronger security with the network. you can use the firewall to stop threats and you can also monitor the whole network to see if there are any threats that will try and get into the system so you will never have to see a threat again. There are 3 different types of virtual networks the first is the VPN which stand for Virtual private network the next is the VLAN and that stand for Virtual Local area network the last one is the VXLAN and this stand for Virtual Extensible

local area network. the first is the VPN and that has become very popular in as it can help you mask your IP address and users have become more concerned about there privacy. You can allow login from anywhere in the world as you could be traveling and access it while traveling as this could be a benefit from someone that travels a lot. “VPNs provided a small-scope, fully virtual network that uses the internet to allow for people to connect.” [7]. The next one is the VLAN which will use partitions to then group devices on that network into different domains with the resources. You get a lot of different monitoring tools as well as management as this can be useful for many things as it can stop attacks. This tool is mostly commonly used on larger networks as they are more vulnerable you will need to monitor individually devices on the network, so it is easier. The last one is the VXLAN and that will create virtual switches to the endpoints for each tunnel. The VNET also uses a physical base case which can route data between the two different endpoints. The main benefits of the vNet are cost Savings as it is all in the cloud you can save a lot of money as some company is providing the cosy of the physical. You can also have a better security as you are making better as you are using domain segments and tunnelling encryption. You can also have better productivity as the network will be better configured as this can be better for the work of everyone.

Network security

The network security is very important as you need to have it on every network in the world. The security will help you protect yourself from breaches, threats, and intrusions as you won't want them on your network. There are different terms that will “describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility, and overall threat protection.” [4]. There is lots of different ways you can protect your network as you could use AV software and that will stop most of the virus that will try and get on to your network or you could use a firewall as this will stop the attacks by shielding it from the attacks. You could go with the VPN encryption as this will show the attacker a different IP address of the computer so the hacker can't get to the IP. You always need it the security as you need to protect your client's information as if you lose the information then your company would be in very big trouble as the information is personal and you need to keep it private. When designing the network security solution if it is designed well then you won't have much overhead but if you were you make it cheap from the beginning then you will have to pay for what you haven't spent in the past. You could also use access control as you can get this will allow certain people into your devices and this will stop users that have not been able to get access to the device so they can't get it and attack it. Most people in the workplaces use email as it is very versatile as you can send documents and messages at the same time, but it can be a very dangerous place as anyone can send an email to anyone in the workplace and it could have a virus on it that is why you would need email security as you don't want any virus on your computer. If you have a lot of employees, then they could make a mistake and

delete information that they should have done or if a hacker gets in and deletes data then you will need Data loss prevention this will be very handy when you need it, but you will not always need it. "Cybersecurity methodology that combines technology and best practices to prevent the exposure of sensitive information outside of an organization" [5]. If you want a place that you can just do anything that you want without any actions that might hurt the network, then you could use a sandbox as this will allow you to practise running code that you wouldn't want to do on the real network as it could hurt it and you would want to that. The sandbox will also open the files you want to and then look for virus on it so you can be sure to run it on the network without any actions.

Reference:

[1] [2] [3]

<https://www.techtarget.com/searchvirtualdesktop/definition/virtual-hard-disk-VHD>

[4][5]

<https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/>

[6] [7]

<https://www.bmc.com/blogs/virtual-network/>

FINAL GRADE

40

/100

GENERAL COMMENTS

Instructor

VM Resources (40):30

VM Images (35):10

Config Exercise (20): 0

Demo (5): 0

Feedback:

=====

Interesting discussion of VHDs and the management of VMS. Your answer could have provided more diagrams and I was anticipating a number of simple command line examples to demonstrate the concepts.

Also I was expecting some discussion/demo of VM images. But I will award you some additional marks for the security discussion.

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5
