

Creation and Deployment of Virtual Machine on Cloud

Mr. Ashwin Shinde*, Ms. Ketki Khante**, Mr. Dinesh Banabakode***,
Ms. Amruta Chopde****, Ms. Sheetal Parate*****

*(Department of Computer Science, DBACER, RTMN University, Nagpur.

** (Department of Computer Science, SBJITMR, RTMN University, Nagpur.

*** (Department of Information Technology, SBJITMR, RTMN University, Nagpur.

**** (Department of Information Technology, SBJITMR, RTMN University, Nagpur.

***** (Department of Information Technology, SBJITMR, RTMN University, Nagpur.

ABSTRACT

The desire to run multiple operating systems was the initial motive for virtual machines, so as to allow time-sharing among several single-tasking operating systems. In some respects, a system virtual machine can be considered a generalization of the concept of virtual memory that historically preceded it. Multiple OS environments can exist simultaneously on the same machine, isolated from each other. Virtual machine can offer an instruction set architecture that differs from real computers. In this paper we are presenting an innovative method of creating a virtual machine on Microsoft Azure Portal and its deployment to cater the needs of Easy maintenance, application provisioning, availability and convenient recovery.

Keywords – Azure, Deployment, Ubuntu, Virtual Machine.

I. INTRODUCTION

Virtual Machine is a completely separate individual operating system installation on your usual operating system. It is implemented by software emulation and hardware virtualization.

Virtual machine is a software implementation of a physical machine - computer - that works and executes analogically to it. Virtual machines are divided in two categories based on their use and correspondence to real machine: system virtual machines and process virtual machines. First category provides a complete system platform that executes complete operating system; second one will run a single program.

Frequently multiple virtual machines with their own OS's are used in server consolidation, where different services are run in separate virtual environments, but on the same physical machine.

Virtualization - A technology that has an enormous effect in today's IT world. It is a technique that divides a physical computer into several partly or completely isolated machines commonly known as virtual machines (VM) or guest machines. Multiple of these virtual machines can run on a host computer, each possessing its own operating system and applications. This gives an illusion to the processes on these virtual machines as if they are running on a physical computer, but in reality they are sharing the physical hardware of the

host machine. The software that allows multiple operating systems to use the hardware of the physical machine is called a hypervisor or a control program. Hypervisors sit between the operating system of the host machine and the virtual environment. There are various virtualization technologies available in the market, having their own merits and demerits.

In non-virtual environment, the applications running on the machine can see each other, and in some cases can even communicate with each other, whereas in virtual environment [1] the programs running in one guest machine are isolated from the programs running in another guest machine, in other words guest machines "provide what appear to be independent coexisting computers" [1] to their running programs. The degree of isolation should be strong enough that the vulnerabilities in one virtual machine should not affect either the virtual machines or the underlying host machine.

The computer that is being virtualized is of no difference from the computer that is not virtualized. The virtualized environment is vulnerable to all the traditional attacks and exploits that are common to the normal environment. The case is even worse in the virtualized environment, where there are several virtual computers running. The security expectations are higher in here because "there are more systems to protect" [2], more possible points of entry, more

On the settings pane, select **Yes** under **Use managed disks**, keep the defaults for the rest of the settings, and click **OK**. On the summary page, click **Ok** to start the virtual machine deployment.

II. CONNECT TO VM

After the deployment has completed, create an SSH connection with the virtual machine. Click the virtual machine. The VM can be found on the home screen of the Azure portal, or by selecting **Virtual Machines** from the left-hand menu.

Click the **connect** button. The connect button displays an SSH connection string that can be used to connect to the virtual machine.

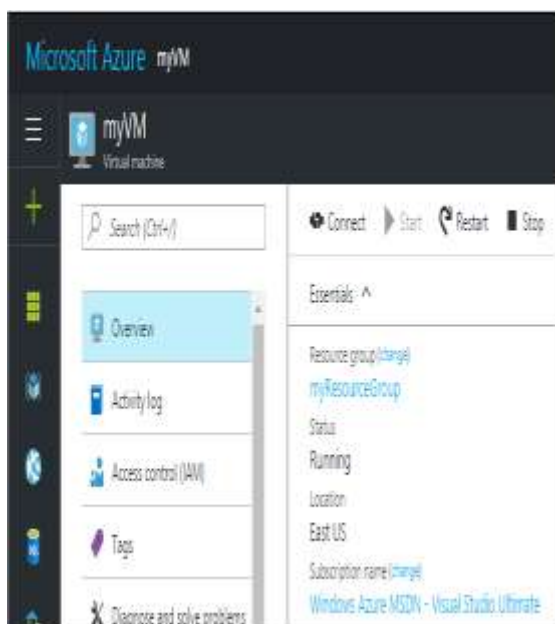


Fig. 3 My VM Section

Run the following command to create an SSH session. Replace the connection string with the one you copied from the Azure portal on Putty software. Open Putty as shown below.

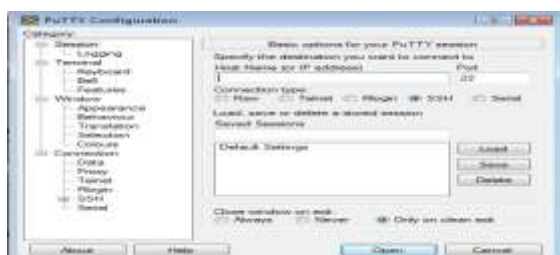


Fig. 4 Putty Terminal

Copy the IP address of your Virtual Machine created on Azure in the host Name field of Putty as shown below.

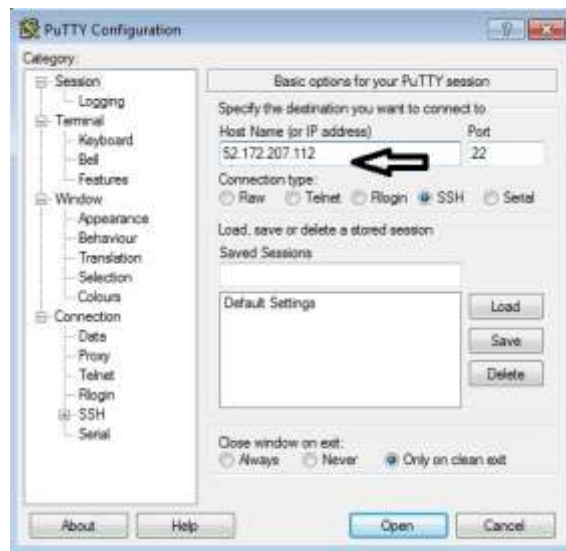


Fig. 4 Putty Configuration

Check the connection type as SSH and then click on ok button. After doing this a putty terminal will be opened. In this Terminal we need to login the username provided during creation of Virtual Machine as shown below.

Login as: azureuser 1

Next it will ask password for azureuser 1, so enter the password as shown below.

azureuser1@52.172.207.112's password: password

After entering password you will get connected to your ubuntu server machine with a message saying Welcome to Ubuntu 16.04.2LTS as shown below.



Fig. 5. MyVM at CMD

III. DELETING VIRTUAL MACHINE

When no longer needed, delete the resource group, virtual machine, and all related resources. To do so, select the resource group from the virtual machine blade and click Delete.

IV. CONCLUSION

A conclusion section must be included and should indicate clearly the advantages, limitations, and possible applications of the paper. Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

REFERENCES

- [1] J. Kirch, Virtual Machine Security Guidelines The center for Internet Security, September 2007.http://www.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf.
- [2] K.J. Higgins. Vm's create potential risks. Technival report, darkREADING, 2007.
http://www.darkreading.com/document.asp?doc_id-117908.
- [3] R. Naraine. Vm rootkits: Yhe next big threat eWeek, March 2006.
<http://www.eweek.com/article2/0,1759,1936666,00.asp>

Mr. Ashwin Shinde " Creation and Deployment of Virtual Machine on Cloud" International Journal of Engineering Research and Applications (IJERA) , vol. 7, no. 12, 2017, pp. 01-04.