IST 615 – Cloud Management

School of Information Studies, Syracuse University
Fall 2024

Lab - 1

Name of the Author: **Karan Shah**

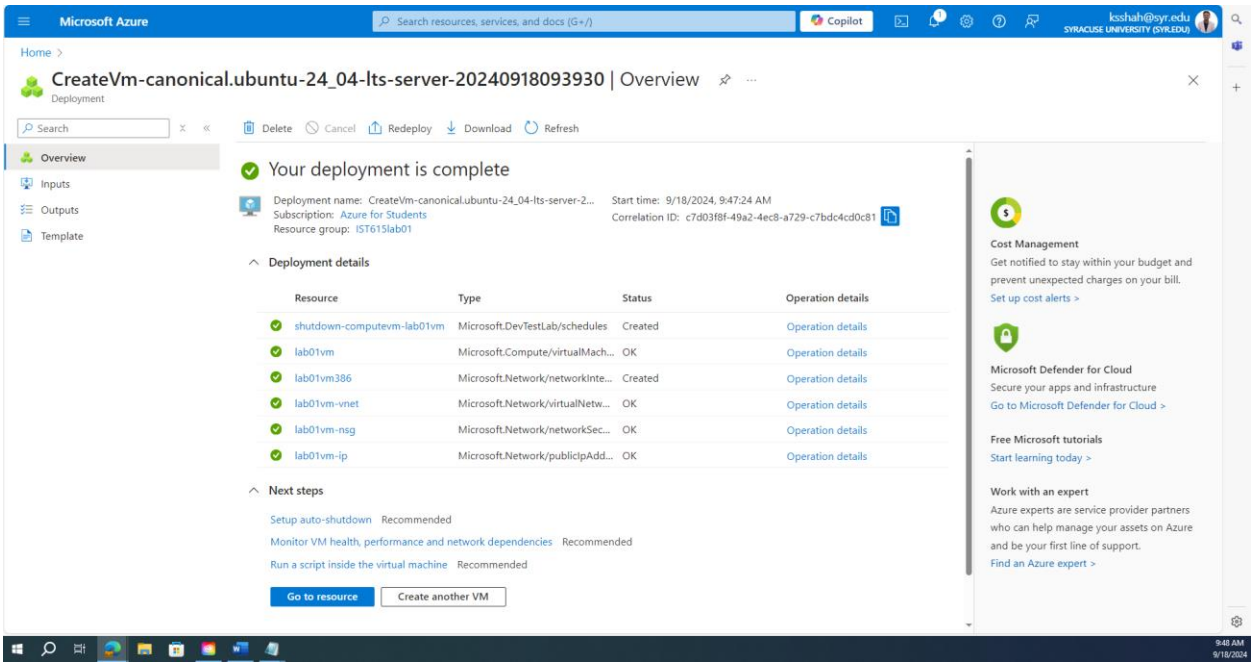
Lab Due: 9/20/2024

Assignment Submitted: 9/18/2024

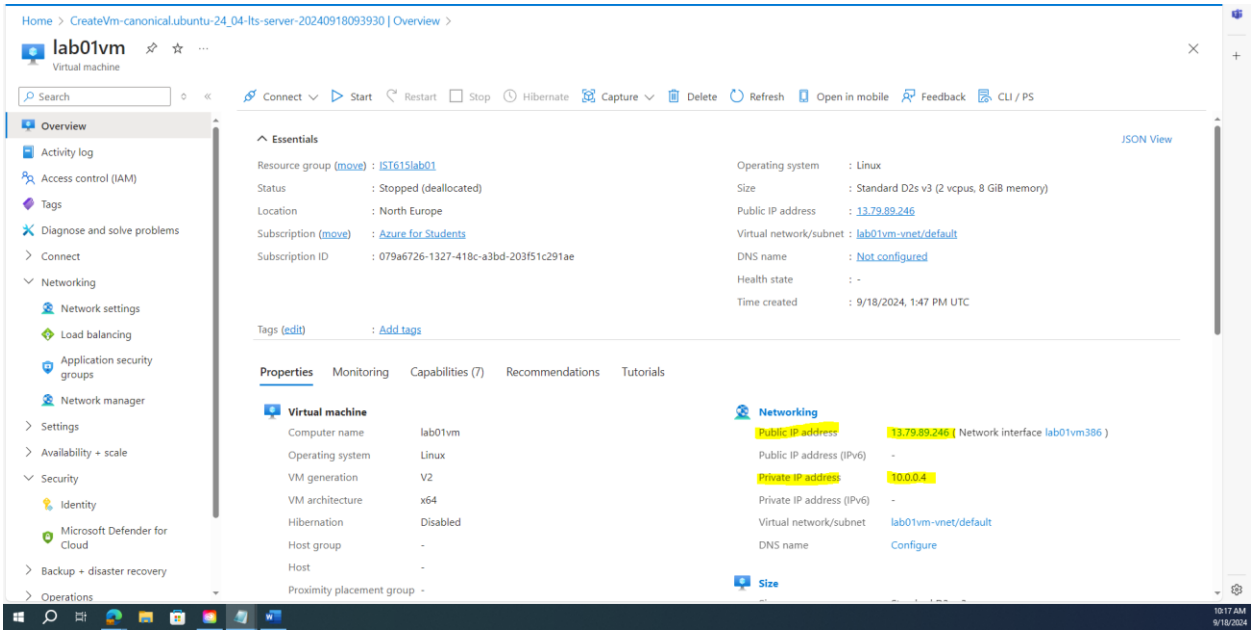
(The document has **4 pages** with the cover page)

Part 1 (50 points):

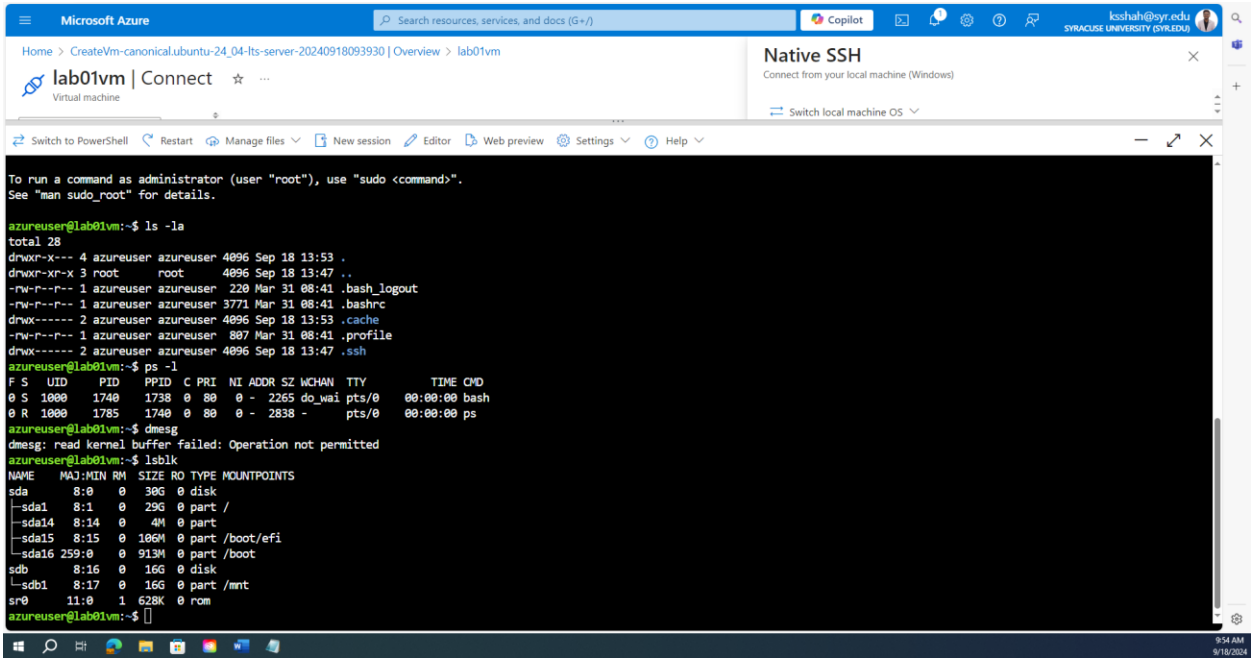
Include all the screenshots required throughout the lab guide. Provide a small description of what is being shown in each screenshot



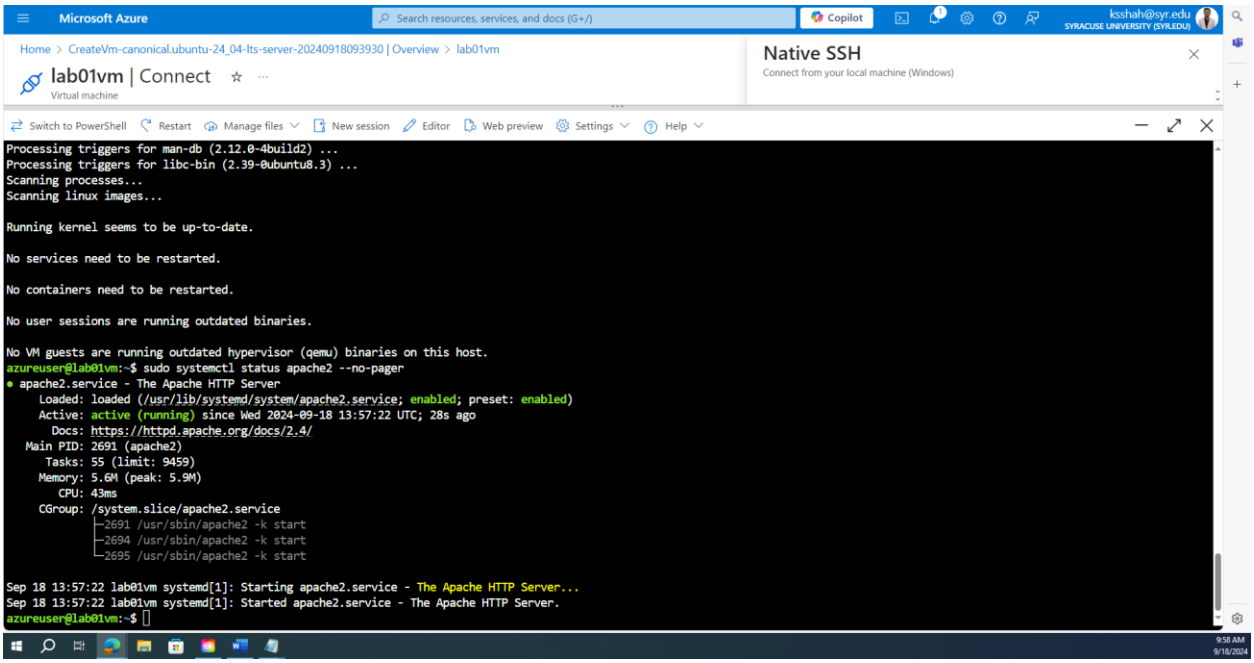
SCS01(a)- The above screenshot shows VM has finished creating



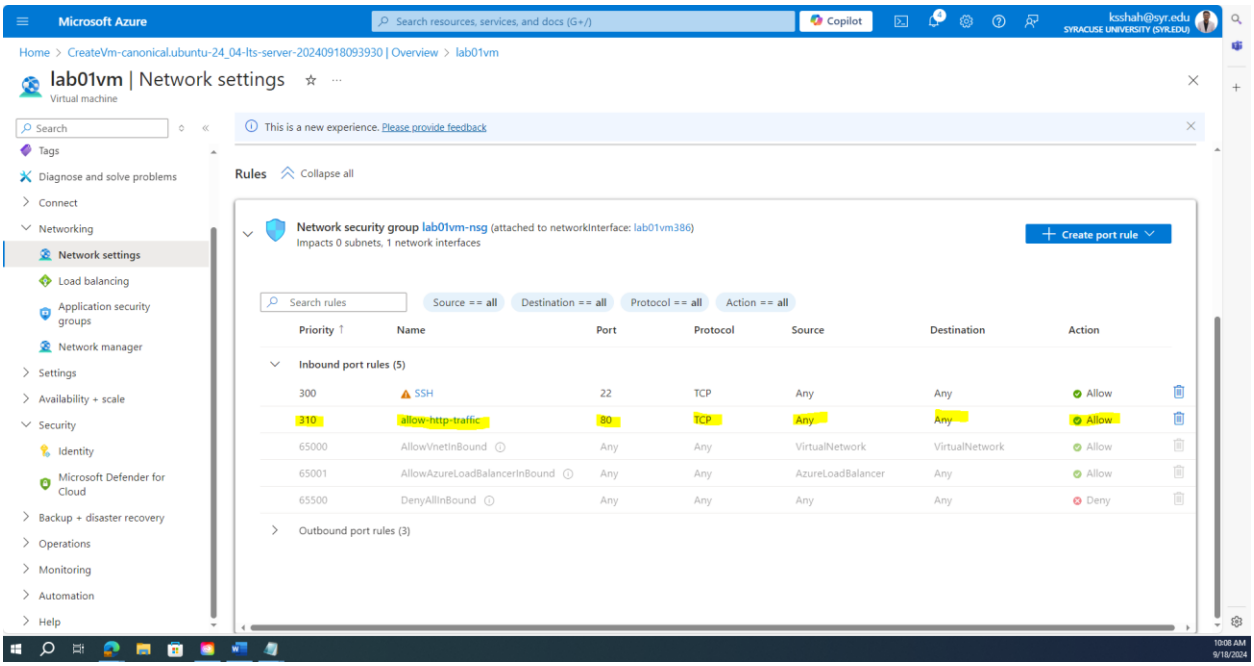
SCS01(b)- The above screenshot shows VM has public and private IP Address



SCS02 - The above screenshot shows that I have connected to the VM.



SCS03 - The above screenshot shows the output of the systemctl command and that I have an active HTTP server.



SCS04 - The above screenshot shows that I have added the new inbound port rule to the VM.

SCS05 - The above screenshot shows that the Apache server default web page loads and IP address of my VM/website is highlighted in yellow

Part 2 (50 points):

1. What is a key pair and what is it used for?

A key pair consists of two parts: a public key and a private key. It is used for secure authentication, allowing you to sign in to Linux-based Azure virtual machines (VMs) without a password.

- **The public key** is placed on the Linux VM or other services that use public-key cryptography and can be shared with anyone.
- **The private key** is used to verify your identity when making an SSH connection to the VM. This key should be kept confidential, like a password.

Using an SSH key pair is a more secure approach if you only access the VM from a few computers. The same key pair can also be used to access multiple Azure VMs and services.

2. Who stores the public portion of the key pair? Who stores the private portion of the key pair?

The **public portion** of the key pair is stored on the Linux VM or any other service you want to access securely. It can be shared with anyone who needs to authenticate with the server.

The **private portion** of the key pair is stored by the user on their personal device or computer. The user must keep the private key confidential, as it is used to verify their identity when making an SSH connection to the VM.

3. What is SSH? What is it used for?

Secure Shell (SSH) is an encrypted connection protocol used to allow secure sign-ins over unsecured connections. It enables you to connect to a terminal shell on a remote system using a network connection, providing secure remote access to that system.

SSH is primarily **used for** secure communication and management of remote servers or devices, ensuring that the data exchanged during the connection is protected from unauthorized access

4. When you make a change to a network security group rule, does the change affect only the instance you're currently working on or other instances, too? Explain.

A modification to a network security group (NSG) rule can impact more than just the instance you're working on at the time. NSGs can be linked to a subnet on the virtual network (which affects all instances inside that subnet) or a network interface (which affects individual instances).

Any changes you make to a rule on an NSG connected to a subnet will affect every instance inside that subnet. The modification will only impact the particular instance linked to that network interface if the NSG is tied to a particular network interface. As a result, the extent of the modification is determined by the NSG's association inside your network.

5. What is the effect of the default network security settings for a new virtual machine?

b) Outbound requests are allowed. Inbound traffic is only allowed from within the virtual network.

6. Suppose you have several Linux virtual machines hosted in Azure. You will administer these VMs remotely over SSH from three dedicated machines in your corporate headquarters. Which of the following authentication methods would typically be considered best-practice for this situation?

c) Private key with passphrase