# Part 1 – Following through the process of creating a VM in Azure

1. Below screenshot tells that the VM has been configured with the required network settings and deployed successfully. Graphical user interface, text, application

   Description automatically generated
2. After deploying, we created an SSH and connected to the Linux VM with SSH. Below screenshot shows the execution of few Linux commands after connecting with SSH.

A screenshot of a computer

Description automatically generated

1. After this, we installed Apache web server on the VM and executed the *systemctl* command to view the status of HTTP server.

A screenshot of a computer

Description automatically generated

1. Below screenshot shows that the network setting rule has been updated to add the inbound port rule.

Graphical user interface, text, application, email

Description automatically generated

1. The IP address of the VM is pinged to view the default Apache server webpage.

Graphical user interface, text, application, email

Description automatically generated

# Part 2

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

The SSH helps us sign-in to the VM securely while on an unsecure connection. With the SSH key pair, we can sign-in without a password.

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

The public key is placed on your Linux VM or any other service that you wish to use with public-key cryptography, whereas the private key is what you present to verify your identity to your Linux VM when you make an SSH connection.

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

Secure Shell (SSH) is an encrypted connection protocol that allows secure sign-ins over

unsecured connections. SSH allows you to connect to a terminal shell from a remote

location using a network connection.

1. 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.

Yes, it affects the other instances too. If no security group is applied, then all traffic is allowed by Azure. If the VM has a public IP, this could be a serious risk, particularly if the OS doesn't provide a built-in firewall. The rules are evaluated in priority order, starting with the lowest priority rule. Deny rules always stop the evaluation. If a network interface rule blocks an outbound request, any rules applied to the subnet will not be checked. For traffic to be allowed through the security group, it must pass through all applied groups.

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

Last rule is a default rule added to every security group for both inbound and outbound traffic with a priority of 65500. That means to have traffic pass through the security group, you must have an allow rule, or the final default rule will block it.

a) Neither outbound nor inbound requests are allowed – Deny All rule

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

c) There are no restrictions: all outbound and inbound requests are allowed. – Allow rule

1. 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?

a) Username and password – SSH Connection

b) Private key – SSH keys

c) Private key with passphrase – to access the VM