

Introduction to Cloud Computing

LAB 06

Name: Hamad Naseem

ID: 2280143

BSSE 7-B

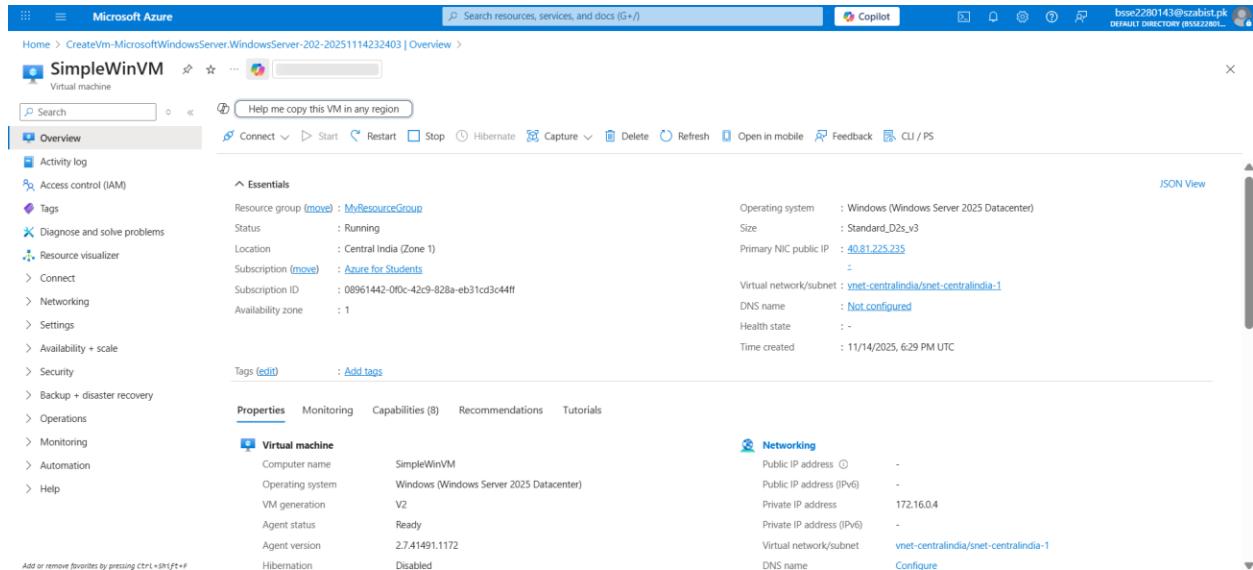
Task 1: Create a virtual machine

The screenshot shows the 'Networking' step of the Azure VM creation wizard. It includes fields for selecting a virtual network, subnet, and public IP address, along with options for NIC security groups. A warning message about exposing ports to the public internet is displayed. Navigation buttons at the bottom include '< Previous', 'Next : Management >', and 'Review + create'.

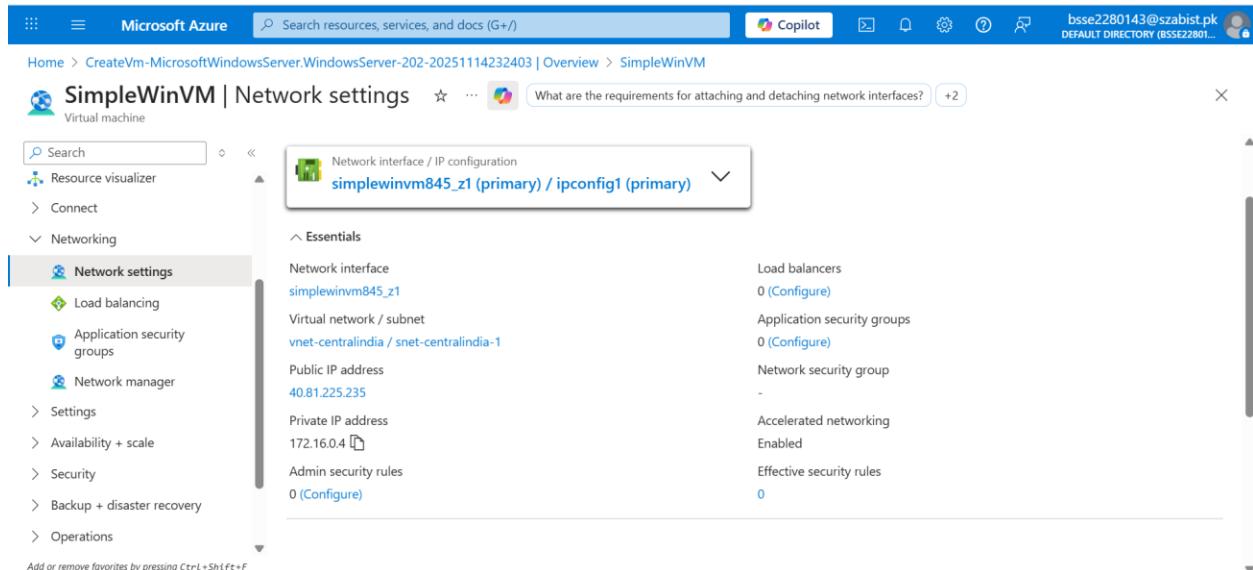
The screenshot shows the 'Monitoring' step of the Azure VM creation wizard. It includes sections for 'Alerts' (checkbox for enabling recommended alert rules), 'Diagnostics' (options for boot and OS guest diagnostics, with 'Disable' selected), and 'Health' (checkbox for enabling application health monitoring). Navigation buttons at the bottom include '< Previous', 'Next : Advanced >', and 'Review + create'.

Introduction to Cloud Computing

LAB 06



The screenshot shows the Microsoft Azure portal interface for a virtual machine named "SimpleWinVM". The main navigation bar at the top includes "Microsoft Azure", a search bar, and various icons for account management. Below the bar, the title "SimpleWinVM" and "Virtual machine" are displayed. A prominent "Help me copy this VM in any region" button is visible. The left sidebar contains a tree view with nodes like "Overview", "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Resource visualizer", "Connect", "Networking", "Settings", "Availability + scale", "Security", "Backup + disaster recovery", "Operations", "Monitoring", "Automation", and "Help". The "Overview" tab is selected. The main content area displays detailed information about the VM, including its resource group ("MyResourceGroup"), status ("Running"), location ("Central India (Zone 1)"), subscription ("Azure for Students"), and various configuration details like operating system ("Windows Server 2025 Datacenter"), size ("Standard_D2s_v3"), and network settings ("Virtual network/subnet: vnet-centralindia/snet-centralindia-1"). A "JSON View" link is also present. At the bottom of the main content area, there are tabs for "Properties", "Monitoring", "Capabilities (8)", "Recommendations", and "Tutorials".



The screenshot shows the Microsoft Azure portal interface specifically for the "Network settings" of the "SimpleWinVM" virtual machine. The title bar indicates the current page is "SimpleWinVM | Network settings". The left sidebar has a "Networking" section with a "Network settings" node selected. The main content area displays the "simplewinvm845_z1 (primary) / ipconfig1 (primary)" network interface configuration. It includes sections for "Essentials" (Network interface: simplewinvm845_z1, Virtual network / subnet: vnet-centralindia / snet-centralindia-1, Public IP address: 40.81.225.235, Private IP address: 172.16.0.4), "Load balancers" (0 (Configure)), "Application security groups" (0 (Configure)), "Network security group" (-), "Accelerated networking" (Enabled), and "Effective security rules" (0). A search bar and a help message ("What are the requirements for attaching and detaching network interfaces?") are also visible.

Introduction to Cloud Computing

LAB 06

The screenshot shows the Microsoft Azure portal interface for a virtual machine named "SimpleWinVM". The left sidebar navigation menu is visible, with "Application security groups" selected. The main content area displays a network interface configuration for "simplewinvm845_z1 (primary) / ipconfig1 (primary)". A large shield icon indicates "No application security groups to display". Below the icon, a descriptive text explains the purpose of application security groups. A prominent blue button at the bottom right says "Add application security groups".

Task 2: Create a network security group

The screenshot shows the Microsoft Azure portal interface for a Network Security Group named "myNSGSecure". The left sidebar navigation menu is visible, with "Overview" selected. The main content area displays the "Essentials" section, which includes resource group information ("MyResourceGroup"), location ("Central India"), subscription details ("Azure for Students"), and a list of inbound security rules. A table at the bottom lists these rules, including one for port 65000 allowing traffic from any source to any destination.

Introduction to Cloud Computing

LAB 06

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and various icons. The main content area is titled 'myNSGSecure | Network interfaces' under 'Network security group'. On the left, a sidebar lists options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings (Inbound security rules, Outbound security rules), Network interfaces, Subnets, and Properties. A message bubble at the top right says 'Saved network interface' with the note 'Successfully saved network security group for network interface 'simplewinvm845_z1''. The main pane displays a table of network interfaces:

Name	Public IP address	Private IP address	Virtual machine
simplewinvm845_z1	40.81.225.235	172.16.0.4	SimpleWinVM

Task 3: Configure an inbound security port rule to allow RDP

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and various icons. The main content area is titled 'SimpleWinVM | Connect' under 'Virtual machine'. On the left, a sidebar lists options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect (Connect, Bastion, Windows Admin Center), Networking, and Network settings. A modal window titled 'Remote Desktop Connection' is open, showing an error message: 'Remote Desktop can't connect to the remote computer for one of these reasons: 1) Remote access to the server is not enabled 2) The remote computer is turned off 3) The remote computer is not available on the network'. It also contains instructions: 'Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.' Below the modal, there are fields for 'VM port' (set to 3389), 'Connection prerequisites' (with 'Check inbound NSG rules' selected), and 'Connect using RDP file' (with a 'Download RDP file' button). A 'See details' link is also present.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and various icons. The main content area is titled 'SimpleWinVM | Network settings' under 'Virtual machine'. On the left, a sidebar lists options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, and Network settings. A message bubble at the top right says 'How can I make this VM secure?' and 'What are the requirements for attaching and detaching network interfaces? +1'. The main pane shows the 'Network security group myNSGSecure' attached to the network interface 'simplewinvm845_z1'. It impacts 0 subnets and 1 network interface. A table of inbound port rules is displayed:

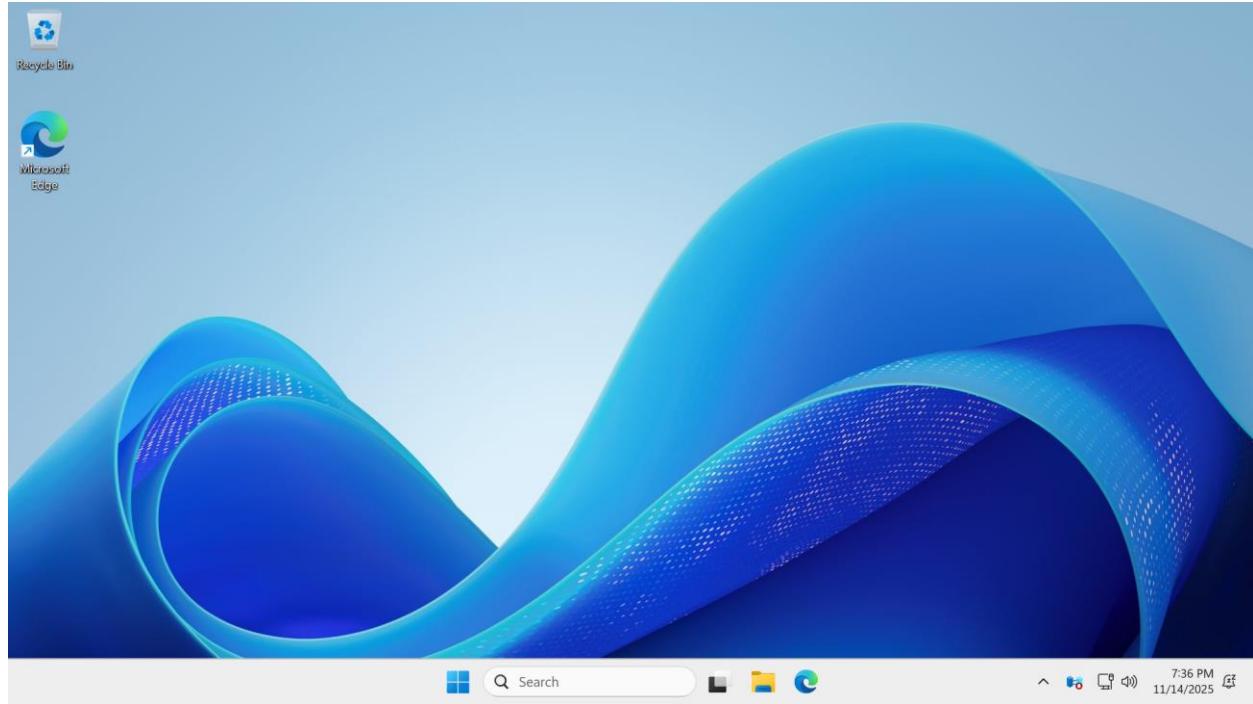
Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Introduction to Cloud Computing

LAB 06

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure', a search bar, and various icons. The main content area is titled 'SimpleWinVM | Network settings' under the 'Virtual machine' section. It displays a 'Network security group myNSGsecure (attached to network interface: simplewinvm043_21)' which impacts 0 subnets and 1 network interfaces. A 'Create port rule' button is visible. Below this, a table lists network security rules:

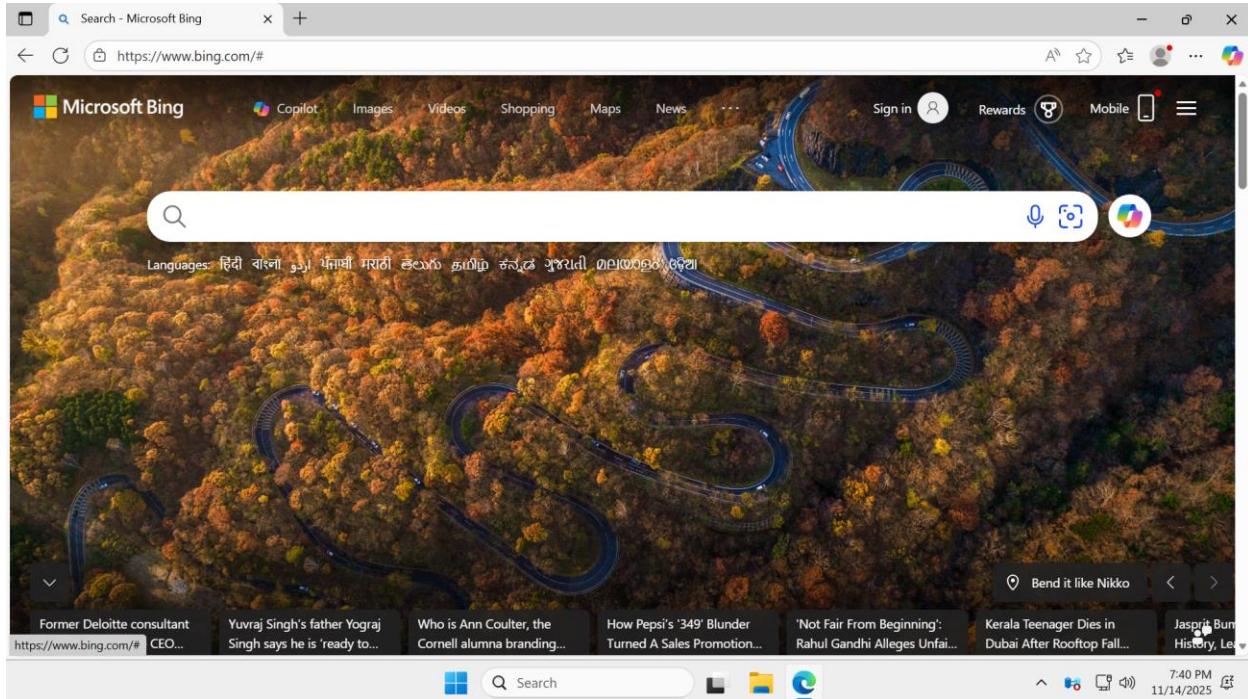
Priority ↑	Name	Port	Protocol	Source	Destination	Action
300	AllowRDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny



Introduction to Cloud Computing

LAB 06

Task 4: Configure an outbound security port rule to deny Internet access



A screenshot of the Microsoft Azure portal showing the network settings for a virtual machine named "SimpleWinVM". The left sidebar shows the navigation path: Home > Compute infrastructure > Virtual machines > SimpleWinVM. The main area displays the "Network settings" for the VM, which has an IP address of 172.16.0.4. It shows an "Admin security rules" section with 0 rules and a "Rules" section with 4 inbound port rules. On the right, a modal window titled "Add outbound security rule" is open, showing the configuration for a new rule. The "Action" is set to "Deny", the "Priority" is 4000, the "Name" is "DenyInternet", and the "Description" field is empty. There are "Add" and "Cancel" buttons at the bottom of the modal.

Introduction to Cloud Computing

LAB 06

