

INTRODUCTION TO CLOUD COMPUTING

Lab Task 02 (Create A Virtual Network)

Name: Ariha Zainab

ID: 2280138

Section: SE 7-B

Task 1: Create a virtual network

The screenshot shows the Microsoft Azure portal interface for creating a new virtual network. The top navigation bar includes 'Microsoft Azure', a search bar, 'Copilot', and user information. The main title is 'Create virtual network'. Below it, a green banner indicates 'Validation passed'. The 'Review + create' tab is selected. The 'Basics' section contains the following details:

Subscription	Azure for Students
Resource Group	RG_LAB2
Name	vnet1
Region	East Asia

The 'Security' section shows:

Azure Bastion	Disabled
Azure Firewall	Disabled

At the bottom, there are 'Previous', 'Next', and 'Create' buttons, along with a link to 'Download a template for automation'.

The screenshot shows the Microsoft Azure portal interface for the 'vnet1' virtual network. The top navigation bar includes 'Microsoft Azure', a search bar, 'Copilot', and user information. The main title is 'vnet1' under 'Virtual network'. The left sidebar shows 'Overview' and other options like 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Resource visualizer', 'Settings', 'Monitoring', 'Automation', and 'Help'. The main content area displays the 'Essentials' section with the following details:

Resource group (move)	: RG_LAB2
Location (move)	: East Asia
Subscription (move)	: Azure for Students
Subscription ID	: 57a8b5a5-89cd-44d7-aaaf-c65ebdf15a43
Address space	: 10.0.0.0/16
Subnets	: 1 subnet
DNS servers	: Azure provided DNS service
BGP community string	: Configure
Virtual network ID	: bd0df19a-d8be-4629-8a75-44dee3e47c35

Below this, there are tabs for 'Topology', 'Properties', 'Capabilities (5)', 'Recommendations', and 'Tutorials'. The 'Capabilities' section highlights three features: 'DDoS protection', 'Azure Firewall', and 'Peerings'.

INTRODUCTION TO CLOUD COMPUTING

Lab Task 02 (Create A Virtual Network)

Task 2: Create two virtual machines

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar and a navigation bar with icons for Copilot, Home, and Overview. On the right, it shows the user's email (bsse2280138@szabist.pk) and a 'DEFAULT DIRECTORY (BSSE22801...)' button.

The main content area displays the 'ArihaVM1' virtual machine details. The left sidebar has a 'Overview' tab selected, along with other options like Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Connect, Networking, Settings, Availability + scale, and Security. A search bar is at the top of the sidebar.

The main panel shows the 'Essentials' section with the following details:

Setting	Value
Resource group (move)	RG_LAB2
Status	Running
Location	East Asia (Zone 1)
Subscription (move)	Azure for Students
Subscription ID	57a8b5a5-89cd-44d7-aaaf-c65ebdf15a43
Availability zone	1
Operating system	Windows (Windows Server 2025 Datacenter)
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Primary NIC public IP	20.2.81.108
Virtual network/subnet	vnet1/snet-eastasia-1
DNS name	Not configured
Health state	-

At the bottom of the main panel, there's a note: 'Add or remove favorites by pressing Ctrl+Shift+F'.

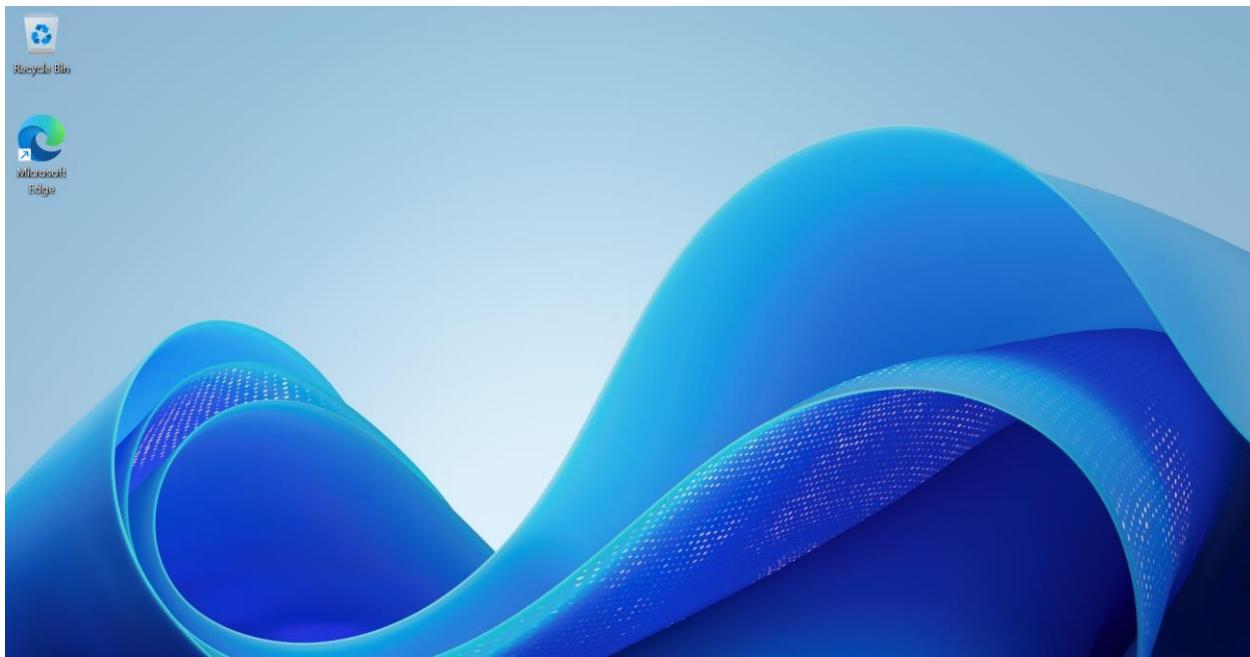
This screenshot is identical to the one above, showing the 'ArihaVM2' virtual machine details in the Microsoft Azure portal. The sidebar, main panel content, and overall layout are the same, displaying the 'Essentials' section with identical configuration values for both VMs.

INTRODUCTION TO CLOUD COMPUTING

Lab Task 02 (Create A Virtual Network)

Task 3: Test the connection

VM1:



Windows Security

←

☰

Home

Virus & threat protection

Firewall & network protection

App & browser control

Device security

Protection history

Restore settings

Privacy Statement

Domain network

Firewall is on.

Private network

Firewall is off.

Turn on

Public network (active)

Firewall is off.

Turn on

Allow an app through firewall

Network and Internet troubleshooter

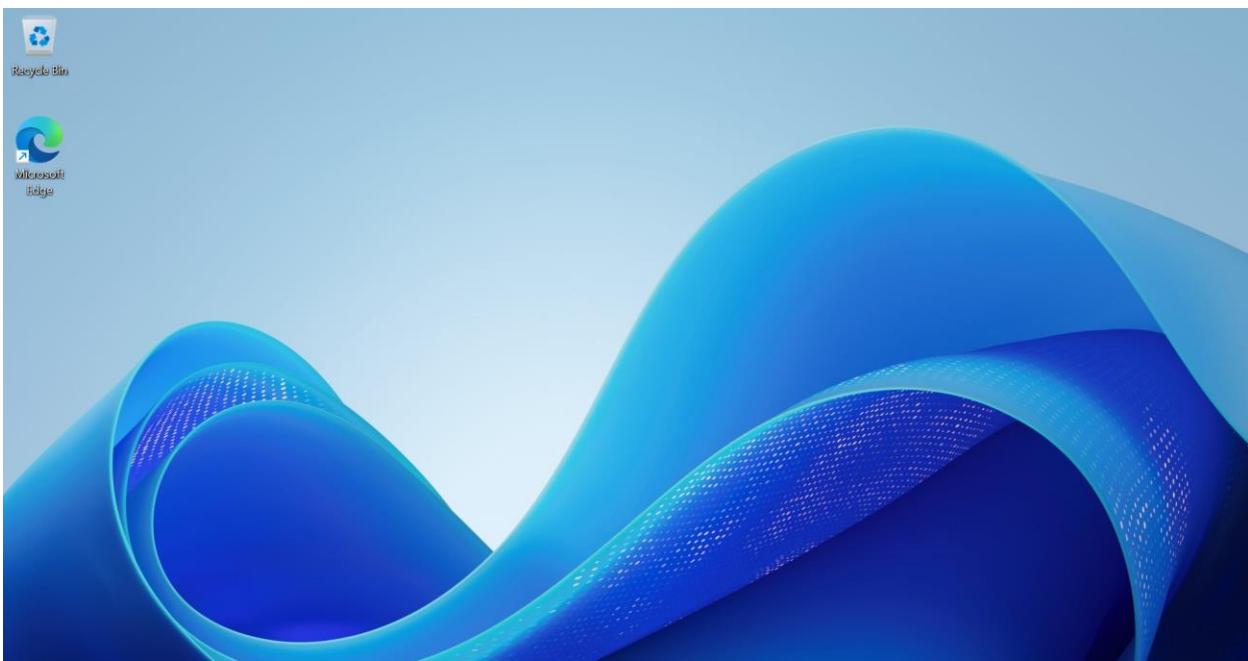
Settings

A screenshot of the Windows Firewall & network protection settings window. The 'Firewall & network protection' section is selected. It shows three network profiles: 'Domain network' (firewall on), 'Private network' (firewall off), and 'Public network (active)' (firewall off). Buttons for 'Turn on' or 'Turn off' are available for each profile. At the bottom, there are links for 'Allow an app through firewall' and 'Network and Internet troubleshooter'. The left sidebar lists other security features like Virus & threat protection and Device security.

INTRODUCTION TO CLOUD COMPUTING

Lab Task 02 (Create A Virtual Network)

VM2:



Windows Security

Firewall & network protection

App & browser control

Device security

Protection history

Settings

Restore settings

Domain network

Private network

Public network (active)

Turn on

View and change privacy settings for your Windows Server 2025 Datacenter device.

Privacy settings

Privacy dashboard

Privacy Statement

Microsoft Defender Firewall is using settings that may make your device unsafe.

Restoring default settings will remove all Windows Defender Firewall settings that you have configured for all network locations. This might cause some apps to stop working.

Firewall is on.

Firewall is off.

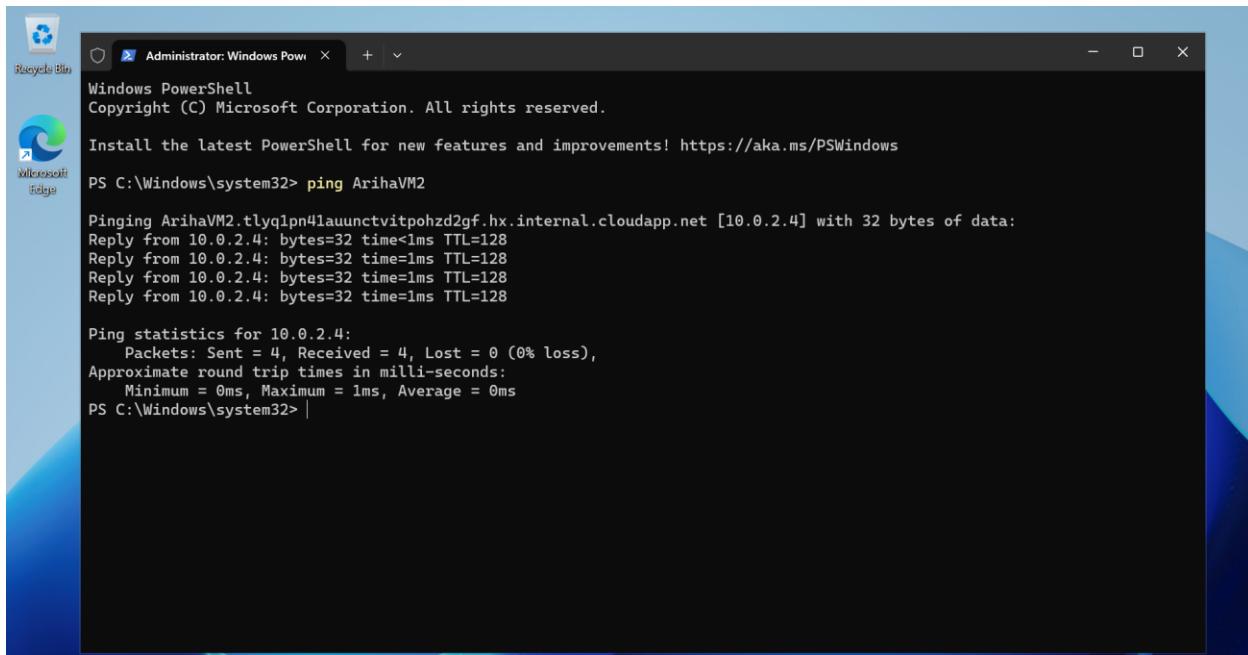
Firewall is off.

The screenshot shows the Windows Security interface, specifically the 'Firewall & network protection' section. It displays three network profiles: 'Domain network' (firewall on), 'Private network' (firewall off), and 'Public network (active)' (firewall off). A warning message at the top left states that Microsoft Defender Firewall is using settings that may make the device unsafe, and restoring default settings will remove all configurations. The 'Domain network' section shows the firewall is on. The 'Private network' section shows the firewall is off with a 'Turn on' button. The 'Public network' section also shows the firewall is off. On the right side, there is a sidebar with privacy-related links: 'View and change privacy settings for your Windows Server 2025 Datacenter device.', 'Privacy settings', 'Privacy dashboard', and 'Privacy Statement'.

INTRODUCTION TO CLOUD COMPUTING

Lab Task 02 (Create A Virtual Network)

PING FROM VM1 TO VM2:



A screenshot of a Windows PowerShell window titled "Administrator: Windows Powe". The window shows the output of a "ping" command. The command "ping ArihaVM2" was run from the path "PS C:\Windows\system32>". The output shows four successful replies from the target IP "10.0.2.4" with TTL=128, and the ping statistics indicate 0% loss.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> ping ArihaVM2

Pinging ArihaVM2.tlyq1pn4lauunctvitpohzd2gf.hx.internal.cloudapp.net [10.0.2.4] with 32 bytes of data:
Reply from 10.0.2.4: bytes=32 time<1ms TTL=128
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128
Reply from 10.0.2.4: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.2.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
PS C:\Windows\system32> |
```