

Ameer Umar Khan - 2280137
Introduction to Cloud Computing - Assignment 1
Lab 06

Task 1:

The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The top navigation bar includes the Azure logo, search bar, Copilot button, and user account information (ameerumar320@gmail.com). The main content area is titled 'Create a virtual machine' under 'Compute infrastructure | Virtual machines'. Step 1, 'Basics', is currently selected. The configuration details are as follows:

Setting	Value
Subscription	Azure for Students
Resource group	(new) task_6
Virtual machine name	SimpleWinVM
Region	Central India
Availability options	No infrastructure redundancy required
Zone options	Self-selected zone
Security type	Trusted launch virtual machines
Enable secure boot	Yes
Enable vTPM	Yes
Integrity monitoring	No
Image	Windows Server 2025 Datacenter: Azure Edition - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Enable Hibernation	No
Username	azureuser
Already have a Windows license?	No

At the bottom of the screen, there are navigation buttons: '< Previous', 'Next >', and a prominent blue 'Create' button.

The screenshot shows the continuation of the 'Create a virtual machine' wizard, specifically step 2: 'Networking'. The configuration details are as follows:

Setting	Value
Virtual network	(new) SimpleWinVM-vnet
Subnet	(new) default (10.1.0.0/24)
Public IP	(new) SimpleWinVM-ip
NIC network security group	None
Accelerated networking	On
Place this virtual machine behind an existing load balancing solution?	No
Delete public IP and NIC when VM is deleted	Disabled

At the bottom of the screen, there are navigation buttons: '< Previous', 'Next >', and a prominent blue 'Create' button.

portal.azure.com/#create/Microsoft.VirtualMachine-ARM

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

ameerumar320@gmail...
DEFAULT DIRECTORY (AMEEURU...)

Sign out

Create a virtual machine

Validation passed

Help me create a low cost VM | Help me choose the right VM size for my workload | Help me create a VM optimized for high availability

patch orchestration options | Azure-orchestrated patching (preview): patches will be installed by Azure
Reboot setting | Reboot if required

Monitoring

Alerts	Off
Boot diagnostics	Off
Enable OS guest diagnostics	Off
Enable application health monitoring	Off

Advanced

Extensions	None
VM applications	None
Cloud init	No
User data	No
Disk controller type	SCSI
Proximity placement group	None
Capacity reservation group	None

< Previous | Next > | Create | Download a template for automation | Give feedback

No security groups to display

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

ameerumar320@gmail...
DEFAULT DIRECTORY (AMEEURU...)

SimpleWinVM | Application security groups

+ Add application security groups | Remove | Refresh | Give feedback

inbound

Networking

Network settings

Load balancing

Application security groups

Network manager

simplewinvm24 (primary) / ipconfig1 (primary)

No application security groups to display

You can use application security groups to configure network security as natural extension of an application's structure, by arbitrarily grouping VMs and defining network security policies based on those groups. You can reuse your security policy and scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, so you can focus on your business logic.

Add application security groups | Learn more

Task 2:

The screenshot shows the Microsoft Azure portal interface for creating a Network Security Group (NSG). The top navigation bar includes links for Home, Network security group, and Create network security group. The main content area displays the 'Create network security group' wizard, currently on the 'Review + create' step. A green banner at the top indicates 'Validation passed'. The 'Basics' section shows the following configuration:

- Subscription: Azure for Students
- Resource group: task_6
- Region: Central India
- Name: myNSGSecure

The 'Tags' section shows 'None'.

At the bottom of the wizard, there are buttons for 'Create', '< Previous', 'Next >', and 'Download a template for automation'.

On the right side of the screen, a 'Sign in with a different account' button is visible. The bottom of the screen shows the Azure search bar and other navigation links.

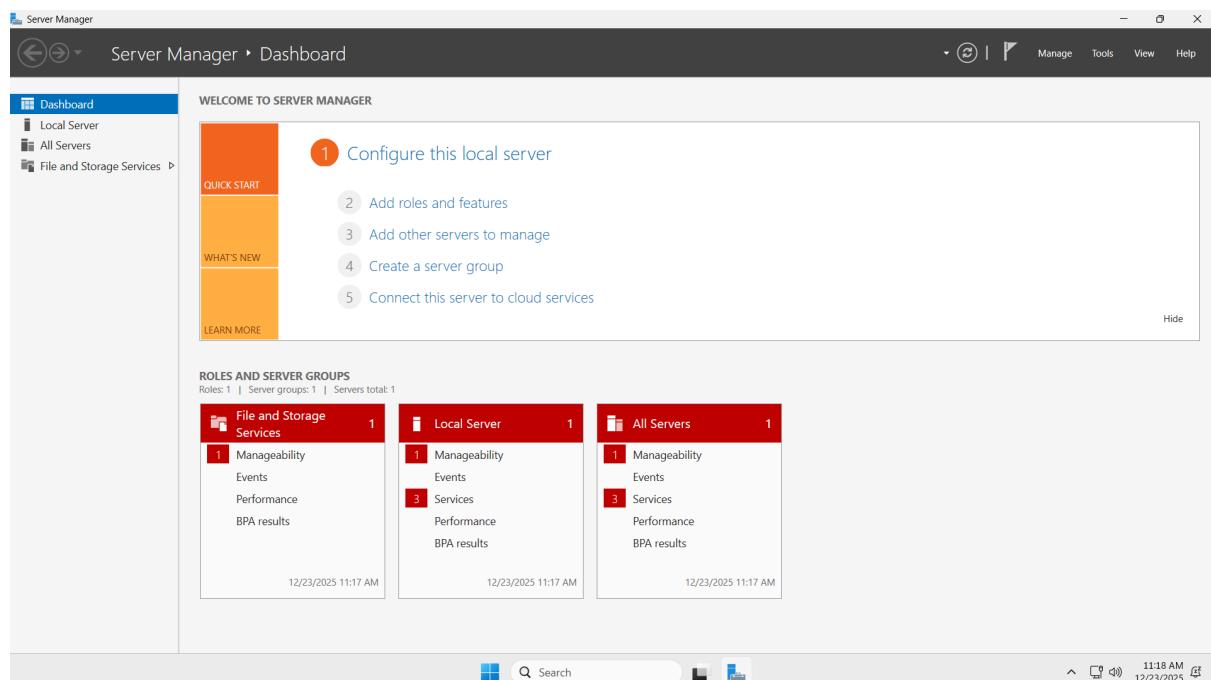
In the center, a modal dialog titled 'Associate network interface' is open. It asks for a 'Network interface association' and lists 'simplewinvm24' as an option. The 'OK' button is visible at the bottom of the dialog.

Task 3:

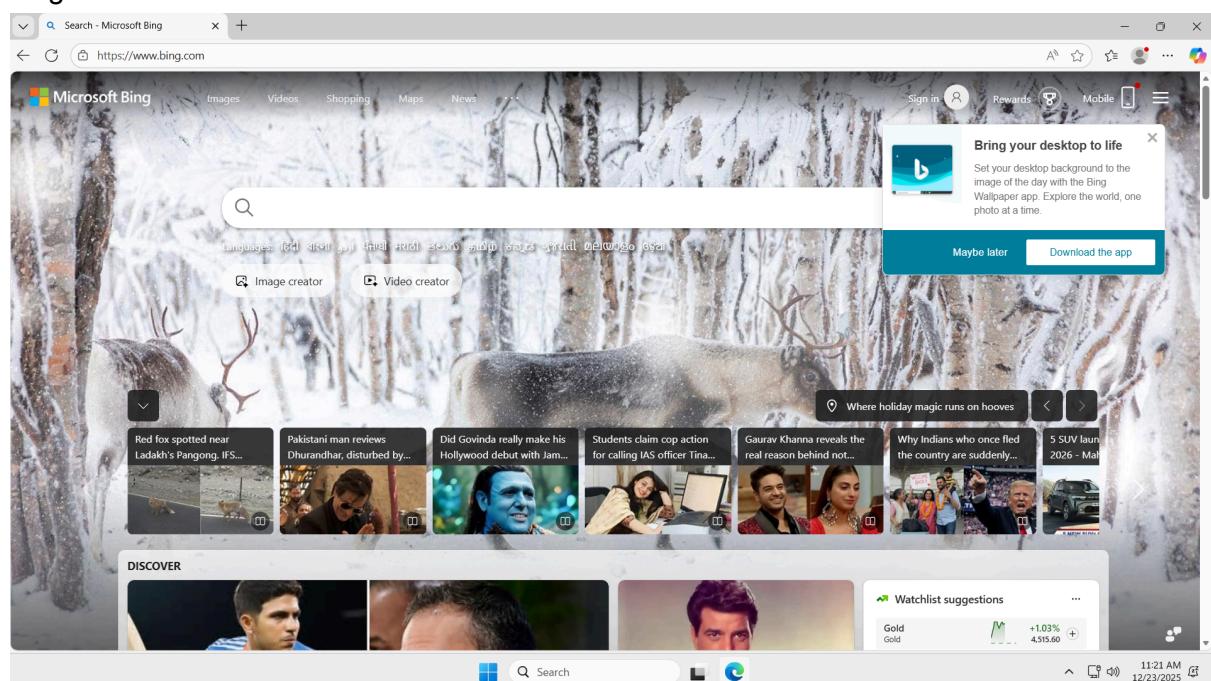
The screenshot shows the Microsoft Azure portal interface. The left sidebar is titled 'Compute infrastructure | Virtual machines' and lists various options like Overview, All resources, Infrastructure, and Virtual machines. Under 'Virtual machines', there is a single item named 'SimpleWinVM'. The main content area is titled 'SimpleWinVM | Connect' and shows a 'Remote Desktop Connection' dialog box with the 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'. Below this, it says 'Make sure the remote computer is turned on and connected to the network, and that remote access is enabled.' To the right of the dialog, there are sections for 'Windows' (Local IP: 119.73.97.169, Public IP: 4.213.96.169, port 3389), 'More ways to connect (4)', and a 'Sign in with a different account' button.

Inbound rule added:

This screenshot shows the same Azure portal interface as the previous one, but with a different focus. The left sidebar shows the 'Virtual machines' section with 'SimpleWinVM' selected. The main content area is titled 'SimpleWinVM | Network settings' and shows the 'Rules' tab. A new rule is being configured with the name 'AllowRDP'. The configuration includes: Source: Any, Source port ranges: *, Destination: Any, Service: RDP, Destination port ranges: 3389, Protocol: TCP, and Action: Save. The 'Save' button is highlighted in blue.



Task 4: Bing is accessible



Adding outbound rule

The screenshot shows two windows side-by-side. On the left is the Microsoft Azure portal's 'Virtual machines' blade for a 'SimpleWinVM'. It lists one VM named 'SimpleWinVM'. A message at the top says, 'You are viewing a new version of Browse experience. Click here to access the old experience.' On the right is a 'Network settings' blade for the same VM, specifically the 'Inbound' security rules section. A new rule is being added with the following details:

- Service:** myVSSecure
- Public IP address:** 4.213.96.169
- Private IP address:** 10.1.0.4
- Destination port ranges:** *
- Protocol:** TCP (selected)
- Action:** Deny (selected)
- Priority:** 4000
- Name:** DenyInternet

At the bottom of the blade are 'Add' and 'Cancel' buttons. Below the Azure window is a Microsoft Edge browser window showing a connection error for 'www.microsoft.com'. The error message is: 'Hmmm... can't reach this page' and 'www.microsoft.com took too long to respond'. It suggests trying to check the connection or proxy/firewall. The error code shown is 'ERR_CONNECTION_TIMED_OUT'. There is a 'Refresh' button at the bottom of the browser window.