

# AZURE Project

## Task 1

Create 3 users in Entra Id.

The screenshot shows the Microsoft Azure Default Directory Overview page. The left sidebar contains navigation links for Overview, Preview features, Diagnose and solve problems, Manage, External identities, Roles and administrators, Delegated admin partners, Enterprise applications, Devices, App registrations, Identity Governance, Application proxy, Custom security attributes, Licenses, Cross-tenant synchronization, Microsoft Entra Connect, Custom domain names, Mobility (MDM and WiP), Password reset, and User settings. The main content area has tabs for User, Group, and Enterprise application. The User tab is selected, showing options to Create new user, Invite external user, and Setup guides. Below these are sections for Basic information (Name: Default Directory, Tenant ID: 65b8B26-4204-458d-b23d-2e004e1bfaa2, Primary domain: itsraj562koutlook.onmicrosoft.com, License: Microsoft Entra ID Free) and Alerts (warning about migrating to converged authentication methods). A My feed section includes cards for Try Microsoft Entra admin center, Raj\_119153 profile, and Secure Score for identity (42.11%).

Three separate 'Create new user' dialog boxes are shown side-by-side. Each box has tabs for Basics, Properties, Assignments, and Review + create. The Basics tab for each user is selected. The user details are as follows:

User	User principal name	Display name	Password	Account enabled
user1	user1	user1	*****	<input checked="" type="checkbox"/>
user2	user2	user2	*****	<input checked="" type="checkbox"/>
user3	user3	user3	*****	<input checked="" type="checkbox"/>

The screenshot shows the Microsoft Entra ID Users page. The left sidebar includes links for All users, Audit logs, Sign-in logs, Diagnose and solve problems, Deleted users, Password reset, User settings, Bulk operation results, and New support request. The main area displays a table of users:

Display name	User principal name	User type	On-premises sync	Identities	Company name
Raj_119153	itsraj562k_outlook.com#E...	Member	No	MicrosoftAccount	
user1	user1@itsraj562koutlook....	Member	No	itsraj562koutlook.onmicrosoft.com	
user2	user2@itsraj562koutlook....	Member	No	itsraj562koutlook.onmicrosoft.com	
user3	user3@itsraj562koutlook....	Member	No	itsraj562koutlook.onmicrosoft.com	

## Task 2

- ➔ Assigning contributor access to user1 and user2 in RG1 Resources Group level.
- ➔ Assigning contributor access to user3 in RG2 Resources Group. Why because, User3 should not have access to VM of user1 and user2.

The screenshot shows the Azure Resource Groups - RG1 Access control (IAM) page. The left sidebar lists 'RG1' and 'RG2'. The main area displays 'Number of role assignments for this subscription' at 4, with 3 privileged assignments. A table lists three users: Raj\_119153 (Owner, Subscription), user1 (Contributor, This resource), and user2 (Contributor, This resource). The 'Role assignments' tab is selected.

Name	Type	Role	Scope	Condition
Raj_119153 itsraj562k.outlook.com#EX...	User	Owner	Subscription (Inherited)	None
user1 user1@itsraj562koutlook.o...	User	Contributor	This resource	None
user2 user2@itsraj562koutlook.o...	User	Contributor	This resource	None

The screenshot shows the Azure Resource Groups - RG2 Access control (IAM) page. The left sidebar lists 'RG1' and 'RG2'. The main area displays 'Number of role assignments for this subscription' at 4, with 2 privileged assignments. A table lists two users: Raj\_119153 (Owner, Subscription) and user3 (Contributor, This resource). The 'Role assignments' tab is selected.

Name	Type	Role	Scope	Condition
Raj_119153 itsraj562k.outlook.com#EX...	User	Owner	Subscription (Inherited)	None
user3 user3@itsraj562koutlook.o...	User	Contributor	This resource	None

## Task 3

user1 → Create virtual Machine1

user2 → Create virtual Machine2

user3 → Create Storage Account

➔ User1, user2 virtual machine.

The screenshot shows the Microsoft Azure portal interface for managing virtual machines. The top navigation bar includes 'Microsoft Azure' and 'Upgrade' buttons, a search bar, and a Copilot icon. The main area displays a table of virtual machines with columns: Name, Subscription, Resource group, Location, Status, Operating system, Size, Public IP address, and Disks. Two entries are listed: 'vm1' and 'vm2'. Both are in the 'Free Trial' subscription, 'RG1' resource group, located in 'East US', and are currently 'Creating'. The status bar at the bottom indicates 'Showing 1 to 2 of 2 records'.

➔ User3 storage account.

The screenshot shows the Microsoft Azure portal interface for managing a storage account named 'storageaccountuser3'. The left sidebar lists various storage services like Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Partner solutions, Data storage (Containers, File shares, Queues, Tables), Security + networking (Networking, Front Door and CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud), Data management, Settings, and Monitoring. The main pane displays the 'Essentials' tab with details such as Resource group (RG2), Location (eastus), Subscription (Free Trial), Disk state (Available), and Tag (edit). It also shows tabs for Properties, Monitoring, Capabilities (7), Recommendations (0), Tutorials, and Tools + SDKs. The 'Properties' tab is selected, showing sections for Blob service, File service, and Queue service, along with security and networking configurations. A yellow bar at the bottom indicates a successful update.

## Task 4

In vm1 add extra 50GB DataDisk.

The screenshot shows the Microsoft Azure portal interface for managing disks of the virtual machine 'vm1'. The left sidebar shows 'Disks' is selected under the 'Settings' category. The main pane displays the 'OS disk' section with a table for 'vm1\_0Disk\_1\_4949084fc684912ae6aec84ec9cfe'. It also shows the 'Data disks' section with a table for 'Extra\_50GB\_disk' (LUN 0, Size 50 GB, Premium SSD LRS storage type). A message box at the top right says 'Updated virtual machine' and 'Successfully updated virtual machine \'vm1\'.' A yellow bar at the bottom indicates a successful update.

→ 50GB DataDisk has been created.

## Task 5

Create fileshare in user3 account and mount it in the vm2 machine.

→ Fileshare1 created in user3 account.

Microsoft Azure

Home > Storage accounts > storageaccountuser3 | File shares > New file share >

**fileshare1** SMB File share

Search ...

Connect Upload Refresh Add directory Delete share Change tier Edit quota Give feedback

Enable Backup for file share "fileshare1" to protect your data. [Learn more](#)

**Overview**

Diagnose and solve problems

Access Control (IAM)

Browse

Operations

Storage account: storageaccountuser3

Resource group (move): RG2

Location: East US

Subscription (move): Free Trial

Subscription ID: c6e04692-5d5d-4f6f-9217-7f030e763051

**Properties** Capabilities (2) Tutorials

**Size**

- Maximum storage (GiB): 102400
- Used storage capacity (GiB): 0
- Access tier: Transaction optimized

**Performance**

- IOPS: 20000
- Throughput (MiB/sec): Varies by region. [Learn more](#)

**Backup**

**Feature status**

- Soft delete
- Large file shares

**Identity-based access**

- Directory service
- Domain

**SMB protocol settings**

- Security profile

**Connect**

Drive letter: Z

Authentication method:

- Active Directory or Microsoft Entra
- Storage account key

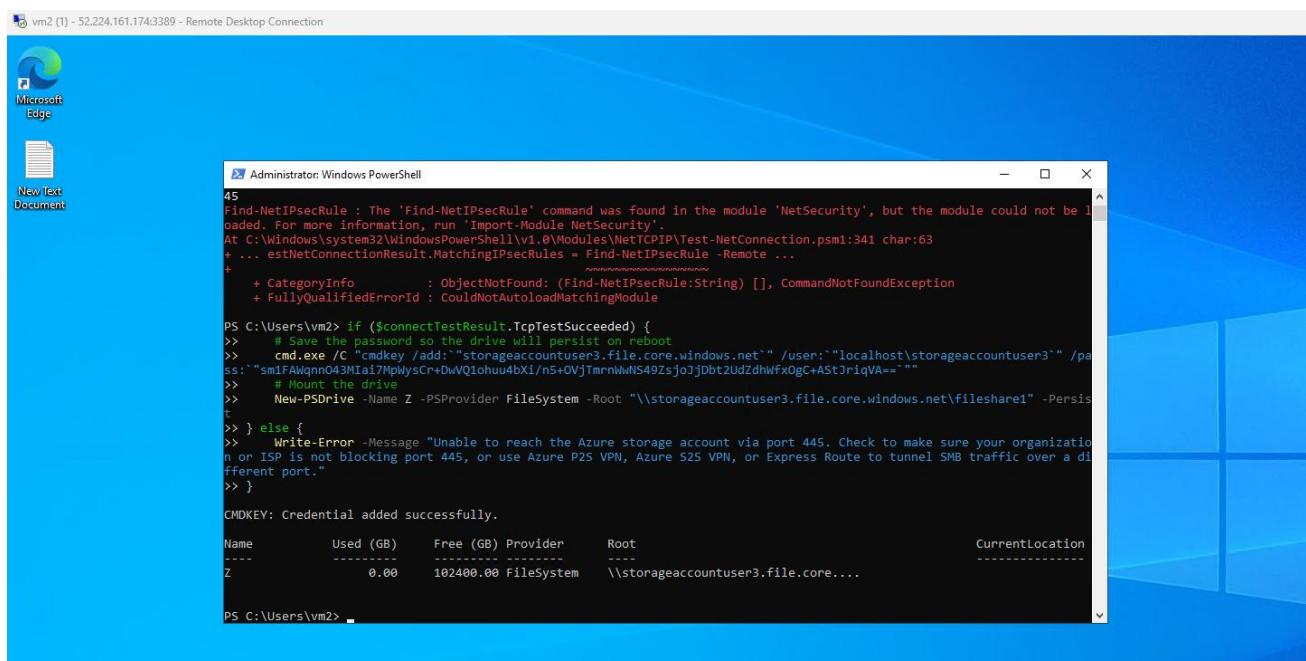
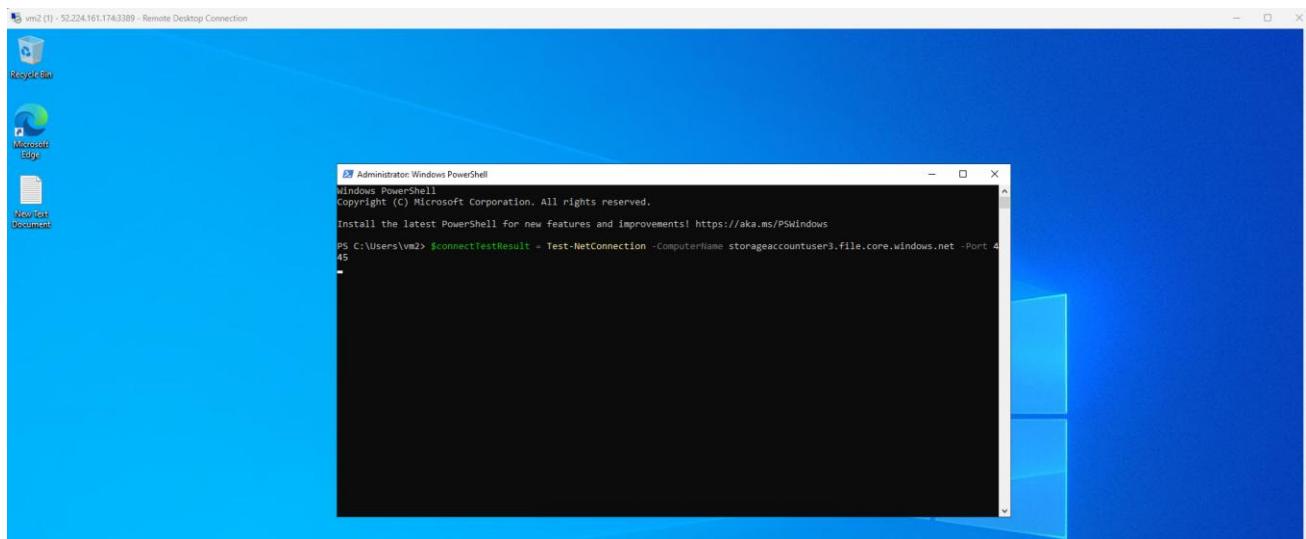
Connecting to a share using the storage account key is only appropriate for admin access. Mounting the Azure file share with the Active Directory or Microsoft Entra identity of the user is preferred. [Learn more](#)

**Hide Script**

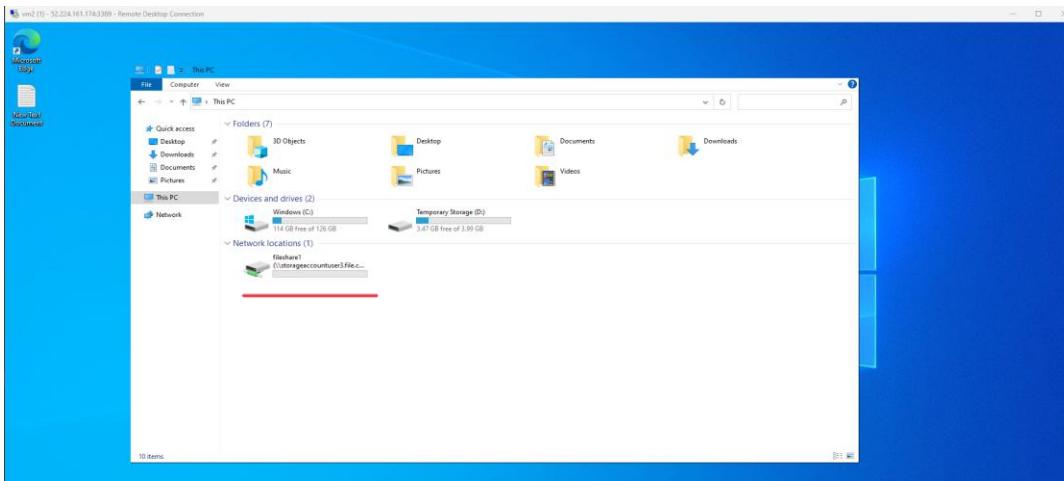
```
$connectTestResult = Test-NetConnection -ComputerName storageaccountuser3.file.core.windows.net -Port 445
if ($connectTestResult.TcpTestSucceeded) {
    # Save the password so the drive will persist on reboot
    cmdkey /add:"storageaccountuser3.file.core.windows.net" /user:"localhost\storageaccountuser3"
    /pass:"sm1fAkqmn043M1a17MpWysCr+0wV10chu4AbX/n5+OVjTmrnWl5492sjo3jb2l2dWfx0gC+ASTJriqVA="
    # Mount the drive
    New-PSDrive -Name Z -PSPrinter FileSystem -Root "\storageaccountuser3.file.core.windows.net\fileshare1" -Persist
} else {
    Write-Error -Message "Unable to reach the Azure storage account via port 445. Check to make sure your organization or ISP is not blocking port 445, or use Azure P2S VPN, Azure S2S VPN, or Express Route to tunnel SMB traffic over a different port."
}
```

This script will check to see if this storage account is accessible via TCP port 445.

→ Copying the script from fileshare1 and paste it in the vm2 PowerShell.



➔ Successfully mounted Fileshare1 in the vm2.



➔ If I create Sample File in the vm2 it will be reflected in fileshare1 which is in user3 storage account.

A screenshot showing two windows. On the left, a 'File Explorer' window on 'vm2' shows a new file named 'Sample File' has been created in the 'fileshare1' folder. On the right, a Microsoft Azure browser-based interface shows the 'fileshare1' blade in the 'Storage accounts' section. It displays a list of files, including 'Sample File.txt' and 'Sample File'. The 'Authentication method' is set to 'Access key'.

➔ If I upload BitLocker key in the fileshare1 which it will reflect in vm2 fileshare1.

A screenshot showing two windows. On the left, a 'File Explorer' window on 'vm2' shows a new file named 'BitLocker Recovery Key F44AC645-ED...' has been uploaded to the 'fileshare1' folder. On the right, a Microsoft Azure browser-based interface shows the 'Upload files' blade in the 'fileshare1' blade. It shows a success message 'Successfully uploaded file(s)' and a list of uploaded files, including 'BitLocker Recovery Key F44AC645-ED...'. Below it, a file explorer window on 'vm2' shows the same file 'BitLocker Recovery Key F44AC645-ED...' in the 'fileshare1' folder.

## Task 6

### Sending vm1 and vm2 logs to log analysis workspace using DCR.

→ Log Analysis Workspace was created.

The screenshot shows the Microsoft Azure Log Analytics workspace overview for 'vm1and2'. Key details include:

- Resource group: rg1
- Status: Active
- Location: East US
- Subscription: Free Trial
- Operational issues: 0

Links provided:

- Get Started with Log Analytics
- Connect a data source
- Configure monitoring solutions
- Monitor workspace health
- Useful links: Documentation site, Community

→ In DCR adding vm1 and vm2 resources, including the destination, which is LAW.

The screenshot shows the 'Create Data Collection Rule' page in Microsoft Azure. The 'Resources' tab is selected, showing two virtual machines, 'vm1' and 'vm2', both selected. The 'Scope' section shows they are under resource group RG1. The 'Select a scope' dialog is open, listing the same resources. At the bottom, there are 'Apply' and 'Cancel' buttons.

The screenshot shows the 'Data collection rules' page in Microsoft Azure, showing the 'dcrvm1and2' rule. The 'Data sources' section is selected, displaying 'Data source', 'Performance Counters', and 'Windows Event Logs' under 'Destination(s)'. The 'Azure Monitor Logs' option is selected.

→ Agent was created in both vm1 and vm2.

Microsoft Azure | Upgrade

Home > Virtual machines > vm1

**Virtual machines**

Default Directory (itsraj562k@outlook.onmicrosoft.com)

+ Create | Switch to classic | ...

Filter for any field... Name ↑

- vm1
- vm2

... Overview Activity log Access control (IAM) Tags Diagnose and solve problems Connect Networking Network settings Load balancing Application security groups Network manager Settings Disks Extensions + applications Operating system Configuration

**vm1 | Extensions + applications**

Virtual machine

Search | What extensions can help me keep my virtual machine secure? | What is the difference between VM applications and extensions? | What are the types of VM extensions available?

Extensions VM Applications

+ Add | Refresh | Update | Enable automatic upgrade | Disable automatic upgrade | Feedback

Search to filter items...

Showing all 1 items

Name	Type	Version	Latest Version	Status	Automatic upgrade
AzureMonitorWindows...	Microsoft.Azure.Monitor...	1.30.0.0	1.30.0.0	Transitioning	Disabled

→ When I type “perf” and “Event”, It shows all the results of vm1 and vm2.

Microsoft Azure | Upgrade

Home > Log Analytics workspaces > vm1andvm2

**Log Analytics workspace**

Default Directory (itsraj562k@outlook.onmicrosoft.com)

+ Create | Open recycle bin | ...

Filter for any field... Name ↑

- vm1andvm2

... Overview Activity log Access control (IAM) Tags Diagnose and solve problems Logs Settings Tables Agents Usage and estimated costs Data export Network isolation Linked storage accounts Properties Locks Classic Monitoring Automation Help

**vm1andvm2 | Logs**

Log Analytics workspace

Search | New Query 1 | New Query 2 | ... | + | Save | Share | ... | Queries hub

New Query 1 | Run | Time range : Last 24 hours | Limit : 1000 | KQL mode

1 Perf

Results Chart

TimeGenerated [UTC]	Computer	ObjectName	CounterName	InstanceName	CounterValue	CounterPath
> 12/21/2024, 1:28:58.480 PM	vm2	LogicalDisk	Disk Transfers/sec	_Total	6.549505	\Vm\LogicalDisk_Total\Disk Transfers/sec
> 12/21/2024, 1:28:58.480 PM	vm2	Process	Thread Count	_Total	596	\Vm\Process_Total\Thread Count
> 12/21/2024, 1:28:58.480 PM	vm2	LogicalDisk	Disk Reads/sec	_Total	2.116507	\Vm\LogicalDisk_Total\Disk Reads/sec
> 12/21/2024, 1:28:58.480 PM	vm2	Processor Information	% Processor Time	_Total	0.399647	\Vm\Processor information>Total % Processor Time
> 12/21/2024, 1:28:58.480 PM	vm2	System	System Up Time		1945.887372	\Vm\System\System Up Time
> 12/21/2024, 1:28:58.480 PM	vm2	LogicalDisk	Avg. Disk sec/Read	_Total	0.000401	\Vm\LogicalDisk_Total\Avg. Disk sec/Read
> 12/21/2024, 1:28:58.480 PM	vm2	Processor Information	% Privileged Time	_Total	0.136238	\Vm\Processor information>Total % Privileged Time
> 12/21/2024, 1:28:58.480 PM	vm2	Memory	Cache Bytes		16326656	\Vm\Memory\Cache Bytes
> 12/21/2024, 1:28:58.480 PM	vm2	System	Context Switches/sec		139.439453	\Vm\System\Context Switches/sec
> 12/21/2024, 1:28:58.480 PM	vm2	LogicalDisk	Avg. Disk Read Queue Length	_Total	0.000849	\Vm\LogicalDisk_Total\Avg. Disk Read Queue Length
> 12/21/2024, 1:28:58.480 PM	vm2	Process	Handle Count	_Total	18726	\Vm\Process_Total\Handle Count
> 12/21/2024, 1:28:58.480 PM	vm2	Processor Information	% User Time	_Total	0.234354	\Vm\Processor information>Total % User Time

2s 748ms | Display time (UTC+00:00) | Query details | 1 - 12 of 156

Microsoft Azure | Upgrade

Home > Log Analytics workspaces > vm1andvm2

**Log Analytics workspace**

Default Directory (itsraj562k@outlook.onmicrosoft.com)

+ Create | Open recycle bin | ...

Filter for any field... Name ↑

- vm1andvm2

... Overview Activity log Access control (IAM) Tags Diagnose and solve problems Logs Settings Tables Agents Usage and estimated costs Data export Network isolation Linked storage accounts Properties Locks Classic Monitoring Automation Help

**vm1andvm2 | Logs**

Log Analytics workspace

Search | New Query 1 | New Query 2 | ... | + | Save | Share | ... | Queries hub

New Query 1 | Run | Time range : Last 24 hours | Limit : 1000 | KQL mode

1 Event

Results Chart

TimeGenerated [UTC]	Source	EventLog	Computer	EventLevel	EventID
> 12/21/2024, 1:28:08.514 PM	Service Control Manager	System	vm2	4	inform
> 12/21/2024, 1:28:08.414 PM	Service Control Manager	System	vm2	4	inform
> 12/21/2024, 1:28:07.033 PM	Service Control Manager	System	vm1	4	inform
> 12/21/2024, 1:28:06.955 PM	Service Control Manager	System	vm1	4	inform
> 12/21/2024, 1:27:58.357 PM	Microsoft-Windows-CAP2	Application	vm2	4	inform
> 12/21/2024, 1:27:58.357 PM	Microsoft-Windows-CAP2	Application	vm2	4	inform
> 12/21/2024, 1:27:58.340 PM	Microsoft-Windows-CAP2	Application	vm2	4	inform
> 12/21/2024, 1:27:26.198 PM	Microsoft-Windows-Security-Audit	Security	vm2	0	inform
> 12/21/2024, 1:27:26.193 PM	Microsoft-Windows-Security-Audit	Security	vm2	0	inform
> 12/21/2024, 1:27:24.804 PM	Microsoft-Windows-Security-Audit	Security	vm1	0	inform
> 12/21/2024, 1:27:24.796 PM	Microsoft-Windows-Security-Audit	Security	vm1	0	inform
> 12/21/2024, 1:27:04.050 PM	Microsoft-Windows-Resource-Usage	System	vm1	3	warn

2s 489ms | Display time (UTC+00:00) | Query details | 1 - 12 of 164

## Task 7

### Converting VM1 OS Disk & Data Disk Encryption from PMK to CMK Using Azure Key Vault.

The screenshot shows the Azure portal interface for managing virtual machines. On the left, the navigation pane is open with 'vm1' selected. Under 'Disks', the 'OS disk' and 'Data disks' sections are visible. In the 'OS disk' section, the 'Encryption' column shows 'SSE with PMK'. In the 'Data disks' section, the 'Encryption' column also shows 'SSE with PMK'. To the right, a 'Create a key vault and key' dialog box is open, detailing the creation of a key vault named 'vm1keyvalut' in the 'Free Trial' subscription and 'RG1' resource group. The 'Encryption type' is set to 'Encryption at-rest with a customer-managed key'. The 'Key Vault' dropdown is set to 'Select a key vault'. The 'Key' dropdown is set to 'Select a key'. The 'Version' dropdown is set to 'Select a key version'. The 'Key details' section shows a key named 'vm1key' with an RSA key type and a size of 2048. The 'Recovery options' section includes settings for soft-delete, days to retain deleted vaults (90), and purge protection. The 'Key vault details' section shows the key vault name and tier (Standard). At the bottom of the dialog, there are 'Save' and 'Cancel' buttons.

**NOTE:** Changes to encryption settings can only be made when the Data Disk is unattached.

The screenshot shows the Azure portal interface for managing virtual machines. The navigation pane is open with 'vm1' selected. Under 'Disks', the 'OS disk' and 'Data disks' sections are visible. In the 'OS disk' section, the 'Encryption' column now shows 'SSE with CMK'. In the 'Data disks' section, the 'Encryption' column also shows 'SSE with CMK'. A success message in the top right corner states 'Updated virtual machine' and 'Successfully updated virtual machine \'vm1\'.' The status bar at the bottom right shows the user's email 'user1@itsra562koutlook.onmicrosoft.com' and the default directory 'ITSRA562...'.

→ Changed Data Disk encryption from PMK to CMK.

→ Changing OS Disk Encryption to CMK is possible after Stopping the Instance.

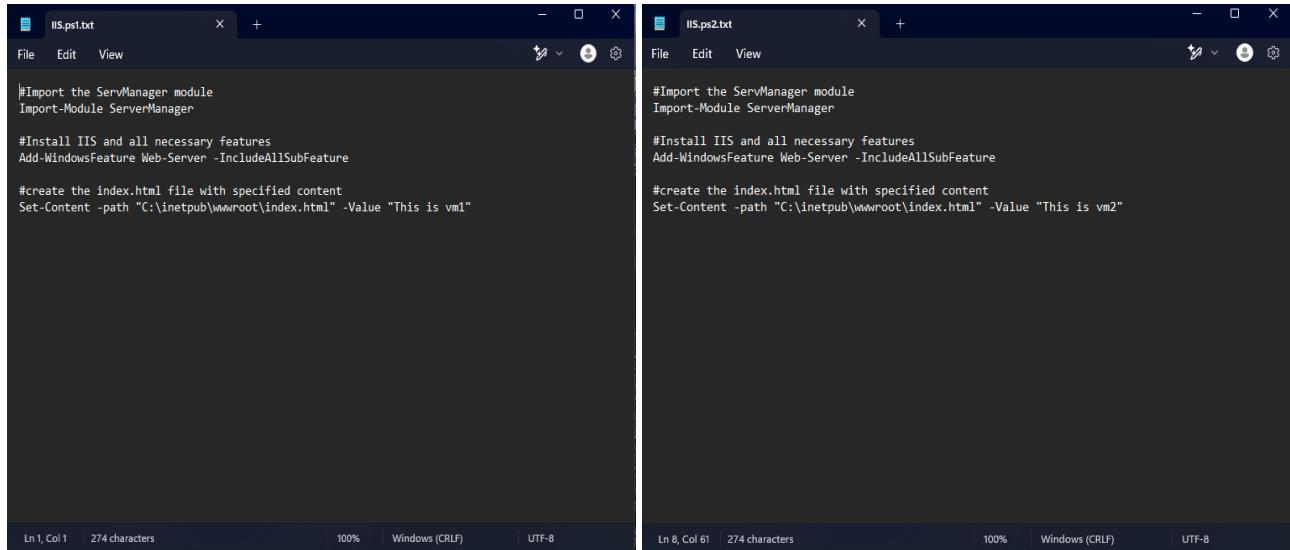
→ Changed OS Disk encryption from PMK to CMK.

➔ Now both OS Disk and Data Disk encryption was changed to CMK.

## Task 8

### Automating IIS Installation on VM1 and VM2.

→ I have 2 PowerShell script for Automating IIS.



The image shows two separate code editors side-by-side. Both editors have dark themes and are displaying PowerShell scripts. The left editor is titled 'IIS.ps1.txt' and the right one is titled 'IIS.ps2.txt'. Both scripts are identical, containing the following code:

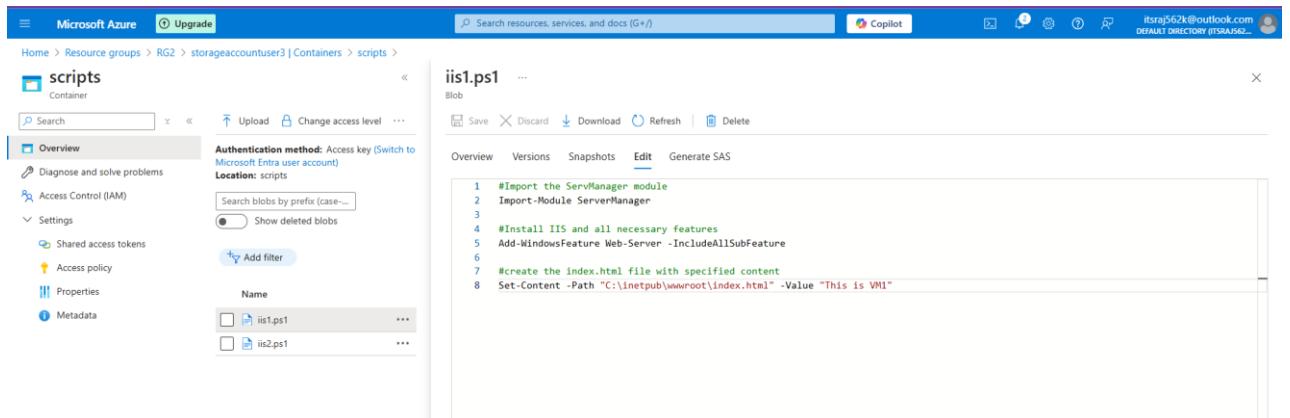
```
#Import the ServManager module
Import-Module ServerManager

#Install IIS and all necessary features
Add-WindowsFeature Web-Server -IncludeAllSubFeature

#create the index.html file with specified content
Set-Content -path "C:\inetpub\wwwroot\index.html" -Value "This is vm1"
```

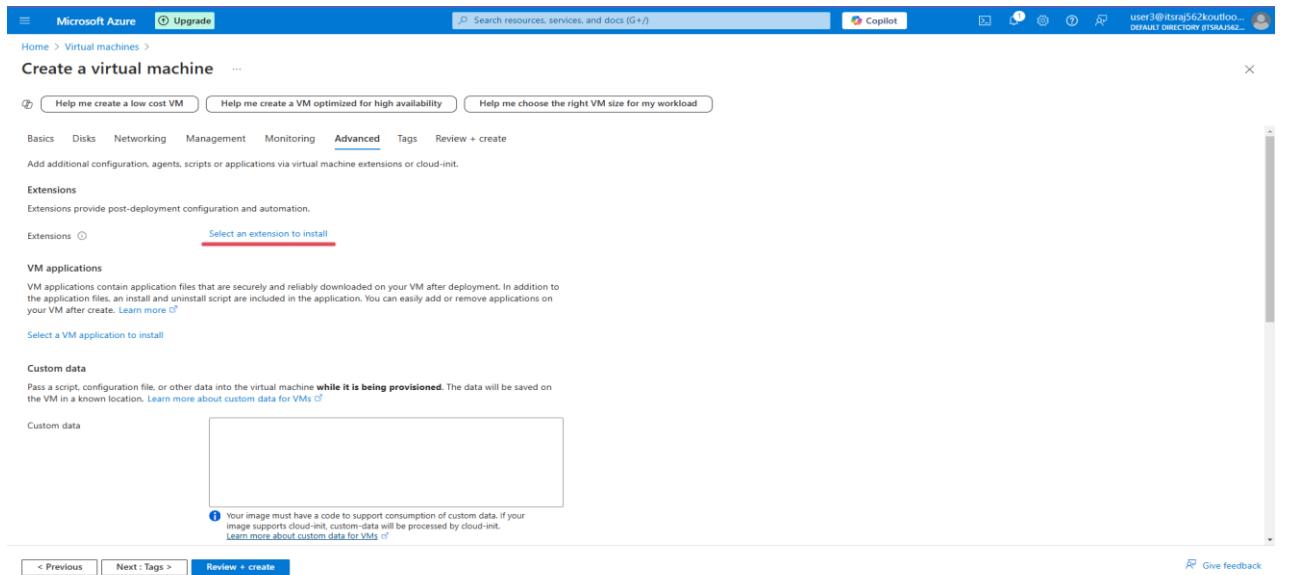
Both scripts are 274 characters long and are saved in Windows (CRLF) encoding with UTF-8 encoding.

→ Uploaded script into the storage account.



The screenshot shows the Microsoft Azure Storage Explorer interface. A container named 'scripts' is selected under the 'RG2' resource group. Inside the 'scripts' container, there are two blobs: 'is1.ps1' and 'is2.ps1'. The 'is1.ps1' blob is currently selected and its content is displayed in the main pane. The content is identical to the scripts shown in the previous image.

→ Creating vm1 and adding the extension.



The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The 'Advanced' tab is selected. In the 'Extensions' section, there is a red box around the 'Select an extension to install' link. Below it, the 'VM applications' section is visible, showing a note about application files being downloaded post-deployment. The 'Custom data' section at the bottom contains a large empty text area with a note about custom data requirements. At the bottom of the page, there are navigation buttons: '< Previous', 'Next : Tags >', and 'Review + create'.

Custom script extension

Custom script extension

Microsoft Corp.

Custom script handler extension for windows

Script file (Required)

Arguments (Optional)

→ PowerShell Script was added.

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

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions Extensions provide post-deployment configuration and automation.

Extensions  Microsoft Corp. Select an extension to install

VM applications VM applications contain application files that are securely and reliably downloaded on your VM after deployment. In addition to the application files, an install and uninstall script are included in the application. You can easily add or remove applications on your VM after create. [Learn more](#)

→ Created 2vm's with custom script.

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disk
vm1	Free Trial	RG2	East US	Running	Windows	Standard_B1s	-	1
vm2	Free Trial	RG2	East US	Running	Windows	Standard_B1s	-	1

→vm1

vm1 (5) - 135.237.59.165:3389 - Remote Desktop Connection

index.html

This is VM1

→vm2

vm2 (3) - 172.171.58.247:3389 - Remote Desktop Connection

index.html

This is VM2

## Task 9

### Adding Load Balancer to the vm's.

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Create load balancer ...

Home > Load balancing | Load Balancer > Create load balancer ...

Frontend IP configuration Backend pools Inbound rules Outbound rules Tags Review + create

A frontend IP configuration is an IP address used for inbound and/or outbound communication as defined within load balancing, inbound NAT, and outbound rules.

+ Add a frontend IP configuration

Name \*: frontedip

IP version: IPv4

IP type: IP address

Public IP address \*: Shared

Gateway Load balancer: None

Review + create < Previous Next : Backend pools > Download a template for automation Give feedback Save Cancel Give feedback

→ Added Backend Pool.

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Load balancing | Load Balancer > Create load balancer ...

Add backend pool ...

Name \*: backenpool

Virtual network: vm1-vnet (RG2)

Backend Pool Configuration: NIC

IP configurations

IP configurations associated to virtual machines and virtual machine scale sets must be in same location as the load balancer and be in the same virtual network.

+ Add | Remove

Resource Name	Resource group	Type	IP configuration	IP Address	Availability set
vm1	RG2	Virtual machine	ipconfig1	10.0.0.4	-
vm2	RG2	Virtual machine	ipconfig1	10.0.0.5	-

Save Cancel Give feedback

→ Added Inbound Rules.

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Create load balancer ...

Basics Frontend IP configuration Backend pools Inbound rules Outbound rules Tags Review + create

Load balancing rule

A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a group of backend pool instances. The load balancing rule uses a health probe to determine which backend instances are eligible to receive traffic.

+ Add a load balancing rule

Name ↑↓	Frontend IP configuration ↑↓	Backend pool ↑↓	Health probe ↑↓	Frontend Port ↑↓	Backend port ↑↓
lrule	frontedip	backenpool	lbhealth	80	80

Save

→ Removing Public IP from vm1 and vm2.

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar includes 'Microsoft Azure', 'Upgrade', 'Copilot', and user information ('itsraj562k@outlook.com', 'DEFAULT DIRECTORY ITSHAURAKH'). The main navigation bar shows 'Home > Network interfaces > vm1205'. The left-hand sidebar under 'Network interfaces' has sections like 'Create', 'Manage view', 'Search', 'Overview', 'Access control (IAM)', 'Tags', 'Settings', 'IP configurations' (which is selected), 'DNS servers', 'Network security group', 'Properties', 'Locks', 'Monitoring', 'Insights', 'Alerts', 'Metrics', 'Diagnostic settings', 'Automation', 'CLI / PS', 'Tasks', 'Export template', 'Help', 'Effective security rules', and 'Effective routes'. The 'IP configurations' section shows two entries: 'vm1205' and 'vm2381'. The right-hand pane is titled 'Edit IP configuration' for 'vm1205'. It contains tabs for 'IP Settings' (selected), 'Private IP address settings', and 'Public IP address settings'. In the 'IP Settings' tab, 'Enable IP forwarding' is checked, 'Virtual network' is set to 'vm1-vnet', 'Gateway load balancer' is 'None', and 'Subnet' is 'default (10.0.0.0/24) 249 free IP addresses'. In the 'Private IP address settings' tab, 'Allocation' is set to 'Dynamic'. In the 'Public IP address settings' tab, there is a note about unchecking 'Associate Public IP address' and a checkbox for 'Associate public IP address' which is unchecked. Buttons at the bottom include 'Save' and 'Cancel'.

→ Finally Load Balancer was created.

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation bar includes 'Microsoft Azure', 'Upgrade', 'Copilot', and user information ('itsraj562k@outlook.com', 'DEFAULT DIRECTORY ITSHAURAKH'). The main navigation bar shows 'Home > loadbalancer'. The left-hand sidebar under 'loadbalancer' has sections like 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Settings' (selected), 'Frontend IP configuration' (which is selected), 'Backend pools', 'Health probes', 'Load balancing rules', 'Inbound NAT rules', 'Outbound rules', 'Properties', 'Locks', 'Monitoring', 'Insights', 'Diagnostic settings', 'Logs', 'Alerts', 'Metrics', and 'Automation'. The right-hand pane is titled 'loadbalancer | Frontend IP configuration'. It shows a table with one item: 'frontedip' with IP address '135.234.210.188 (lbip)' and 'Rules count' 1. A yellow bar at the bottom of the page indicates a warning or note.

## Task 10

Subtask: 1 → Creating 2 subnet inside a Virtual Network (vnet) and establish RDP connection.

→ Creating 2 subnets.

The screenshot shows the 'Create virtual network' wizard in Microsoft Azure. The 'IP addresses' tab is selected. An IPv4 address space '10.0.0.0/16' is defined, covering the range 10.0.0.0 - 10.0.255.255, which includes 65,536 addresses. Two subnets are created: 'subnet1' with the range 10.0.0.0 - 10.0.0.255 and 'subnet2' with the range 10.0.1.0 - 10.0.1.255. Both subnets have a size of /24 (256 addresses). The 'Add IPv4 address space' button is visible at the bottom left.

The screenshot shows the 'vnet1 | Subnets' overview page in Microsoft Azure. The left sidebar shows navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Address space, Connected devices, and Subnets. The Subnets section is selected. It lists two subnets: 'subnet1' (10.0.0.0/24) and 'subnet2' (10.0.1.0/24), both with 251 available IPs.

→ Vm1 in subnet1 with public IP.

The screenshot shows the 'Create a virtual machine' wizard in Microsoft Azure. The 'Networking' tab is selected. The configuration includes: Virtual network: 'vnet1'; Subnet: 'subnet1 (10.0.0.0/24)'; Public IP: '(new) vm1-ip'; NIC network security group: 'Basic'; and Select inbound ports: 'RDP (3389)'. A warning message states: 'This will allow all IP addresses to access your virtual machine. This is only recommended for development or test environments. Use the Advanced mode in the Networking tab to create rules to limit inbound traffic to known IP addresses.' The 'Review + create' button is at the bottom.

→ Vm2 in subnet2 without public IP.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal. The 'Networking' tab is selected. The 'Virtual network' dropdown is set to 'vnet1'. The 'Subnet' dropdown is set to 'subnet2 (10.0.1.0/24)'. The 'Public IP' dropdown is set to 'None'. The 'NIC network security group' section has 'Basic' selected. Under 'Public inbound ports', 'Allow selected ports' is selected, and 'RDP (3389)' is listed. A warning message at the bottom states: 'This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.' At the bottom, there are 'Next: Management >' and 'Review + create' buttons.

→ RDP connection was established b/w two 2 vm's in the separate subnet.

The screenshot shows the Microsoft Azure 'Virtual machines' dashboard. On the left, a list of VMs shows 'vm1' and 'vm2'. In the center, a window titled 'vm1 - 172.191.227.137:3389 - Remote Desktop Connection' is displayed, showing the Windows desktop of 'vm2'. On the right, the 'vm2' details pane is open, showing the following information:

rating system	: Windows (Windows Server 2022 Datacenter Azure Edition)
nic IP address	: Standard B2s (2 vcpus, 4 GiB memory)
virtual network/subnet	: vnet1/subnet2
i name	: -
lth state	: -
created	: 12/22/2024, 10:06 AM UTC
Networking	
Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.0.1.4
Private IP address (IPv6)	-
Virtual network/subnet	vnet1/subnet2
DNS name	-
Size	
Size	Standard B2s
vCPUs	2
DATA	4 GiB

## Subtask: 2 → Block RDP connection between Subnets, Allow Inside Each Subnet.

### → Subnet1 NSG rules.

vm1 | Network settings

Network security group vm1-nsg (attached to networkInterface: vm1220)

Inbound port rules (6)

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
310	AllowMyIpAddressCustom8080Inbound	8080	TCP	Any	49.37.213.57	Allow
320	AllowMyIpAddressRDPInbound	3389	TCP	Any	49.37.213.57	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound port rules (4)

Priority	Name	Port	Protocol	Source	Destination	Action
300	DenyAnyRDPOutbound	3389	TCP	Any	Any	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

### → Subnet2 NSG rules.

vm2 | Network settings

Network security group vm2-nsg (attached to networkInterface: vm212)

Inbound port rules (5)

Priority	Name	Port	Protocol	Source	Destination	Action
300	RDP	3389	TCP	Any	Any	Allow
320	RDPinbound	3389	TCP	49.37.213.57	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound port rules (4)

Priority	Name	Port	Protocol	Source	Destination	Action
300	DenyAnyRDPOutbound	3389	TCP	Any	49.37.213.57	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

→ If I connect vm2 in the subnet2 using subnet1 vm by RDP, it should not connect.

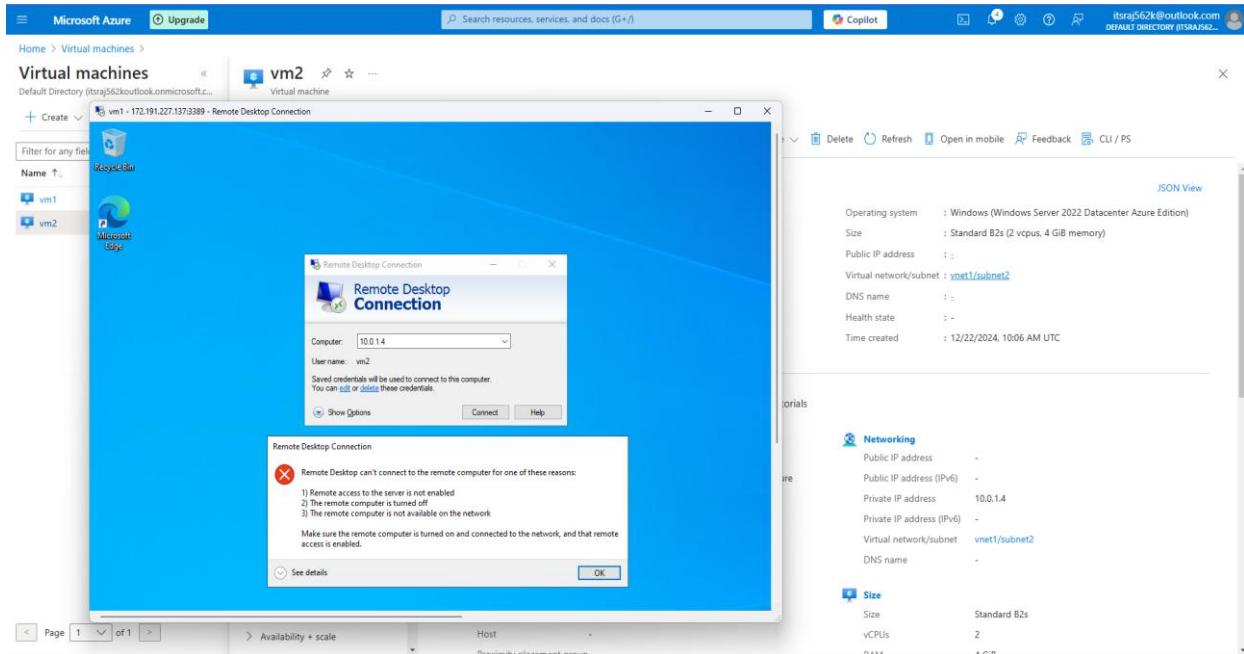


Figure 1 RDP connection was not established

→ If I removed the NSG rules it should work.

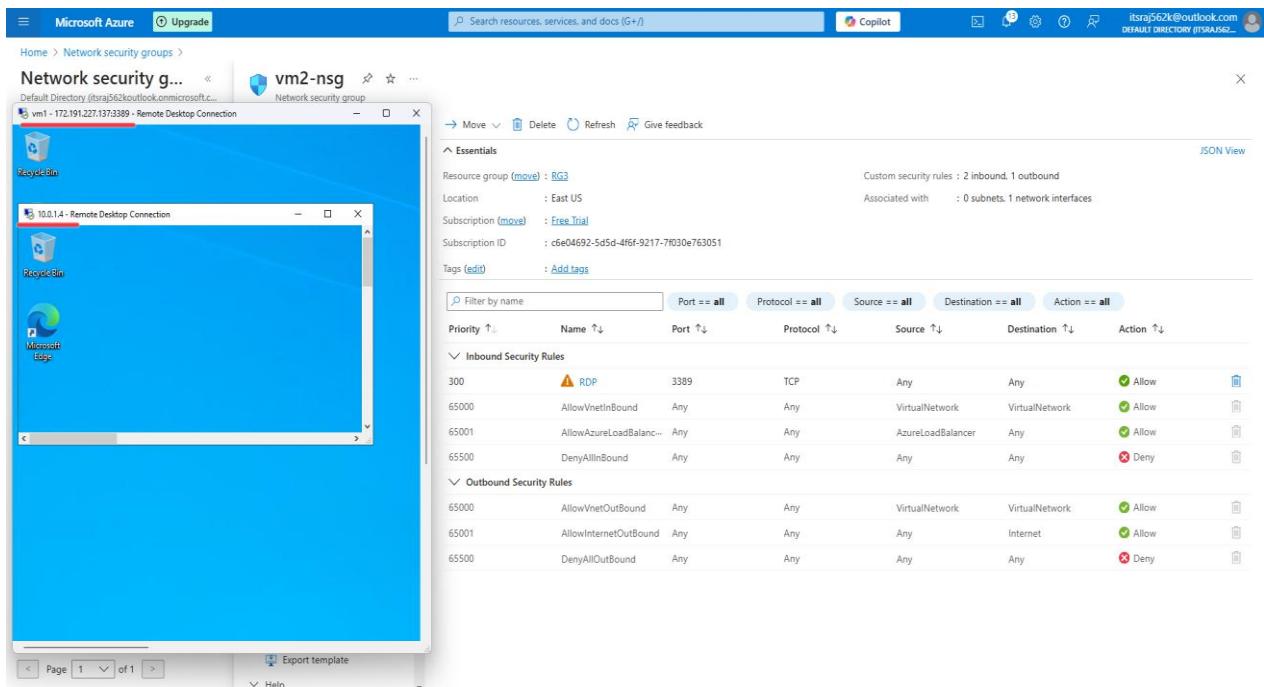


Figure 2 RDP connection was established sucessfully

## Subtask: 3 → Peering connection.

→ Creating another vnet with different IP range.

**NOTE:** If 2 vnet has same IP range peering will not establish.

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. On the left, the 'Create virtual network' blade is open, showing the 'IP addresses' tab selected. It displays the configuration of a new address space (192.168.0.0/24) with a subnet named 'default' (192.168.0.0 - 192.168.0.255). On the right, a modal window titled 'Edit subnet' is open, allowing for further subnet configuration. The 'IPv4' section is set up with an address range of 192.168.0.0/24, a starting address of 192.168.0.0, and a size of /24 (256 addresses). The 'Private subnet' section is also visible, though it is not enabled. At the bottom, there are 'Save' and 'Cancel' buttons.

→ Creating vm2 in the above subnet without public IP.

The screenshot shows the Microsoft Azure portal interface for creating a new virtual machine. The 'Create a virtual machine' blade is open, with the 'Networking' tab selected. In the 'Network interface' section, the 'Virtual network' is set to '(new) vnet4', the 'Subnet' is set to '(new) subnet1 (191.168.0.0/16)', and the 'Public IP' dropdown is set to 'None'. A warning message at the bottom states: '⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.' Below this, the 'Review + create' button is visible.

The screenshot shows the Microsoft Azure portal interface for managing virtual machines. The 'Virtual machines' blade is open, displaying a list of two VMs: 'vm1' and 'vm2'. Both VMs are listed under the 'Subscription equals all' filter. The table columns include Name, Subscription, Resource group, Location, Status, Operating system, Size, Public IP address, and Disks. For 'vm1', the Public IP address is 172.191.227.137 and the Disks count is 1. For 'vm2', the Public IP address is '-' and the Disks count is 1. The 'Maintenance' column shows three dots for both VMs.

Figure 3 Vm2 in diff region without public IP

## → Creating peering connection between 2 different vnet's.

The screenshot shows the Azure portal interface for creating a peering connection. It is divided into three main sections:

- Remote virtual network summary:** Shows the peering link name as "vm1tovm2", deployment model as "Resource manager", and subscription as "Free Trial".
- Remote virtual network peering settings:** Includes checkboxes for "Allow 'vnet1' to access 'vnet4'" (checked), "Allow 'vnet1' to receive forwarded traffic from 'vnet4'" (checked), and "Allow gateway or route server in 'vnet1' to forward traffic to 'vnet4'" (unchecked).
- Local virtual network summary:** Shows the peering link name as "vm2tovm1".
- Local virtual network peering settings:** Includes checkboxes for "Allow 'vnet1' to access 'vnet4'" (checked), "Allow 'vnet1' to receive forwarded traffic from 'vnet4'" (checked), and "Allow gateway or route server in 'vnet1' to forward traffic to 'vnet4'" (unchecked). There is also a checkbox for "Enable 'vnet1' to use 'vnet4's remote gateway or route server" (unchecked).

At the bottom, there are "Add" and "Cancel" buttons.

This screenshot shows the "Peering" section for "vnet1". It lists one peering connection named "vm2tovm1" which is "Fully Synchronized" and "Connected" to "vnet4". The "Peering sync status" is "Enabled".

This screenshot shows the "Peering" section for "vnet4". It lists one peering connection named "vm1tovm2" which is "Fully Synchronized" and "Connected" to "vnet1". The "Peering sync status" is "Enabled".

→ In Vm1, RDP connection was established to vm2 in another region vnet without public IP.

This screenshot shows the Azure portal interface for managing virtual machines. On the left, the "Virtual machines" blade shows two VMs: "vm1" and "vm2". The "vm2" card is selected, showing its details on the right. The details include:

- Operating system:** Windows (Windows Server 2019 Datacenter)
- Size:** Standard B2s (2 vcpus, 4 GiB memory)
- Public IP address:** -
- Virtual network/subnet:** vnet3/subnet1
- DNS name:** -
- Health state:** -
- Time created:** 12/22/2024, 11:41 AM UTC

The "Networking" section shows:

- Public IP address:** -
- Private IP address (IPv6):** -
- Private IP address (IPv4):** 192.168.0.4
- Virtual network/subnet:** vnet3/subnet1
- DNS name:** -

The "Size" section shows:

- Size:** Standard B2s
- vCPUs:** 2
- RAM:** 4 GiB

A "Remote Desktop Connection" window is open, showing the Windows desktop of "vm2". The desktop includes icons for "Recycle Bin" and "Microsoft Edge".