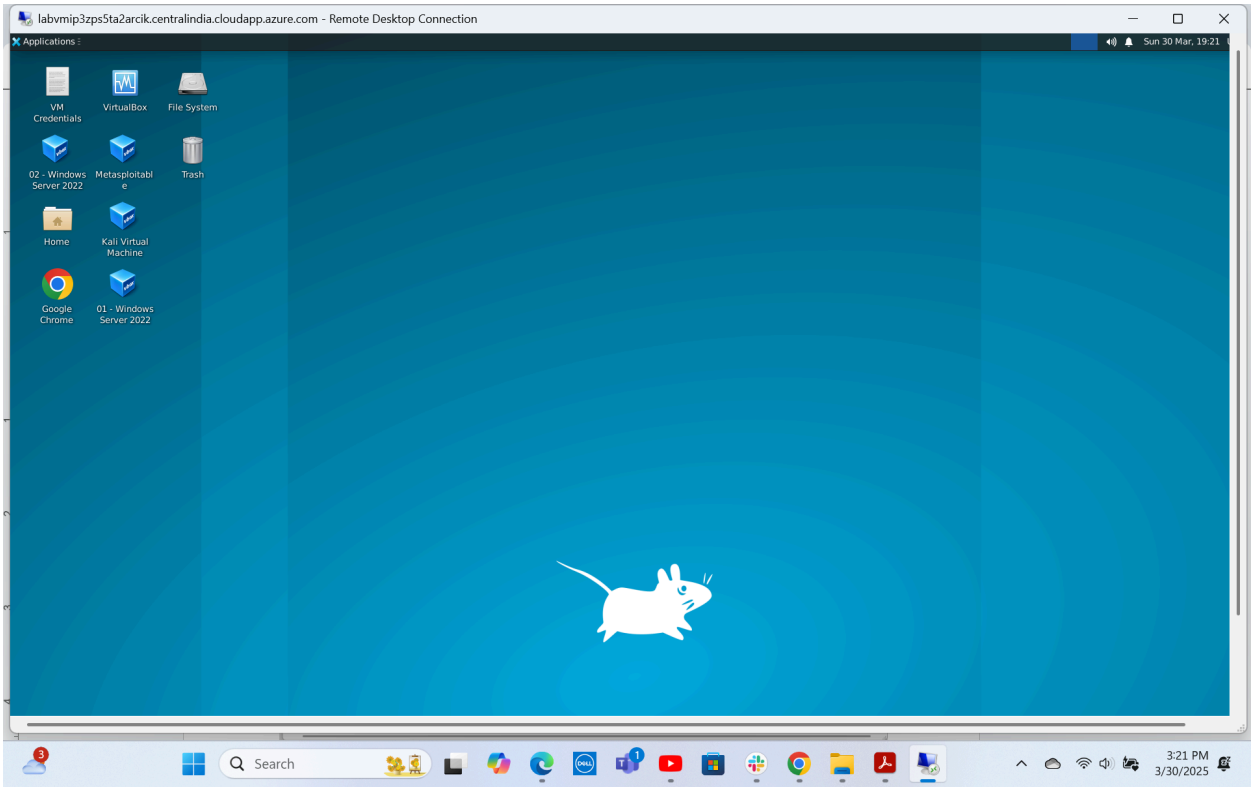
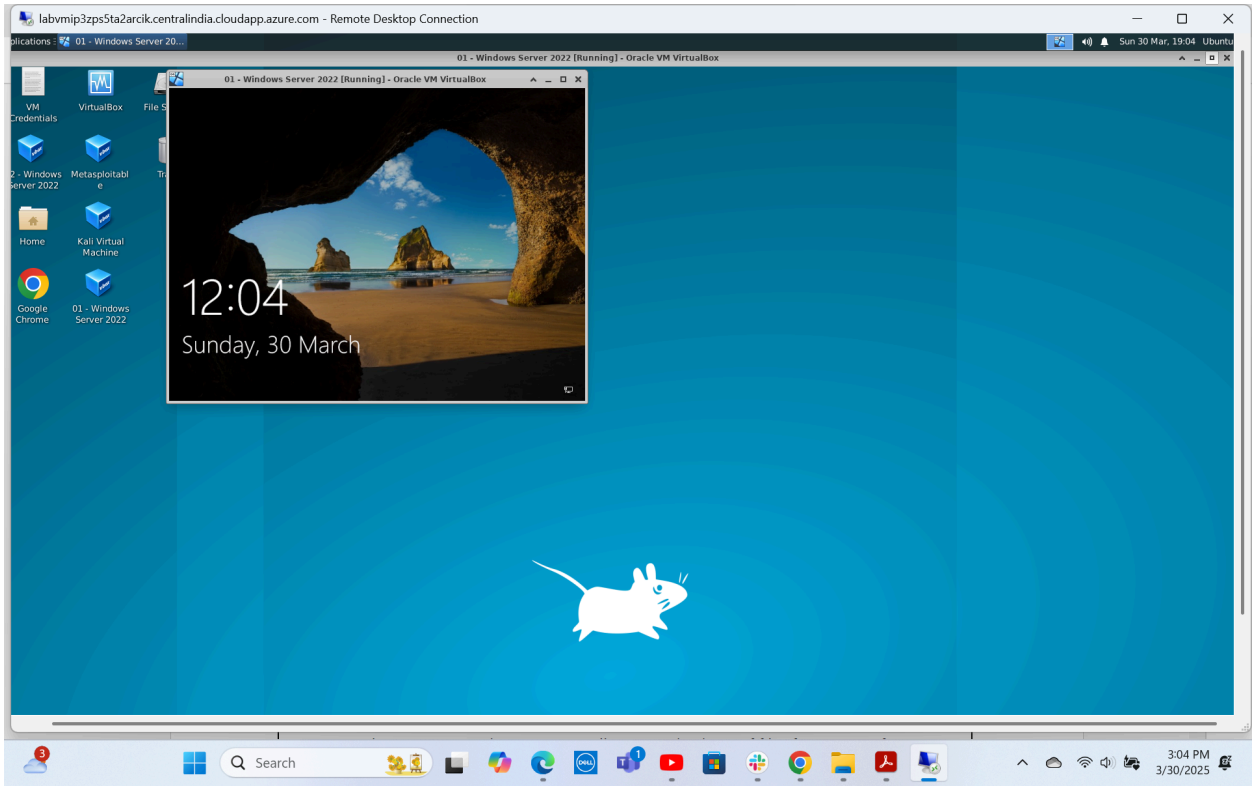
Project Topic: Automating Common IT Tasks By Janefrances Nwachukwu
Output Screenshots

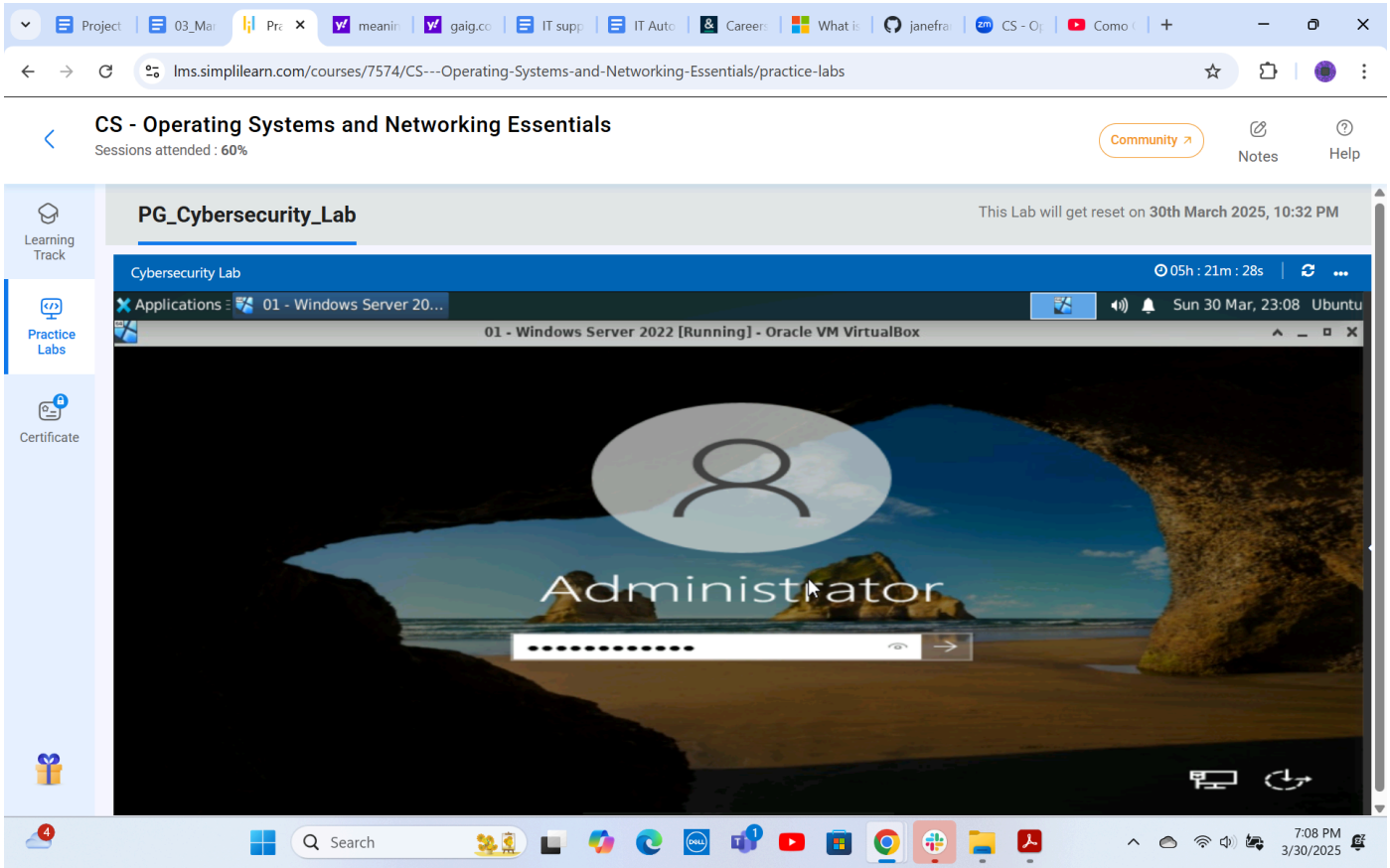
Step 1: Evaluated strategies for automating system monitoring
1.1 Opening Windows Server 22



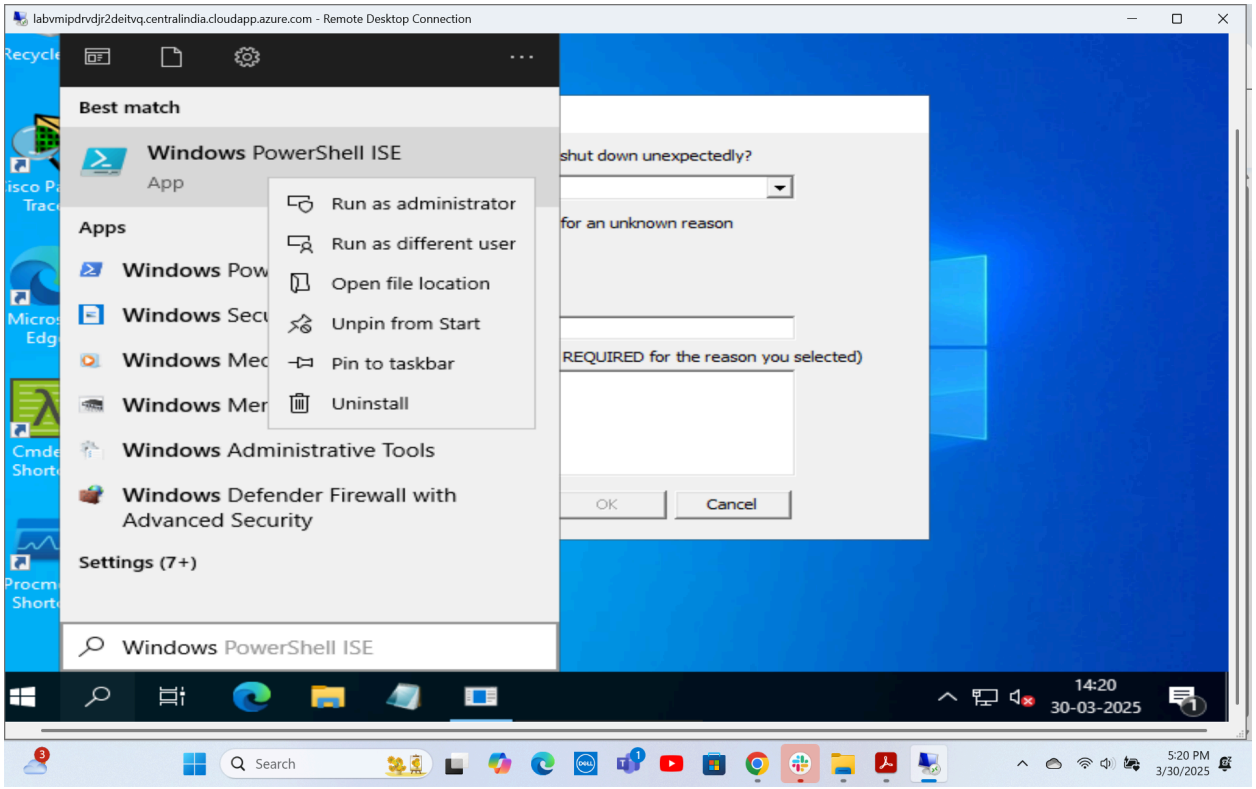
1.2



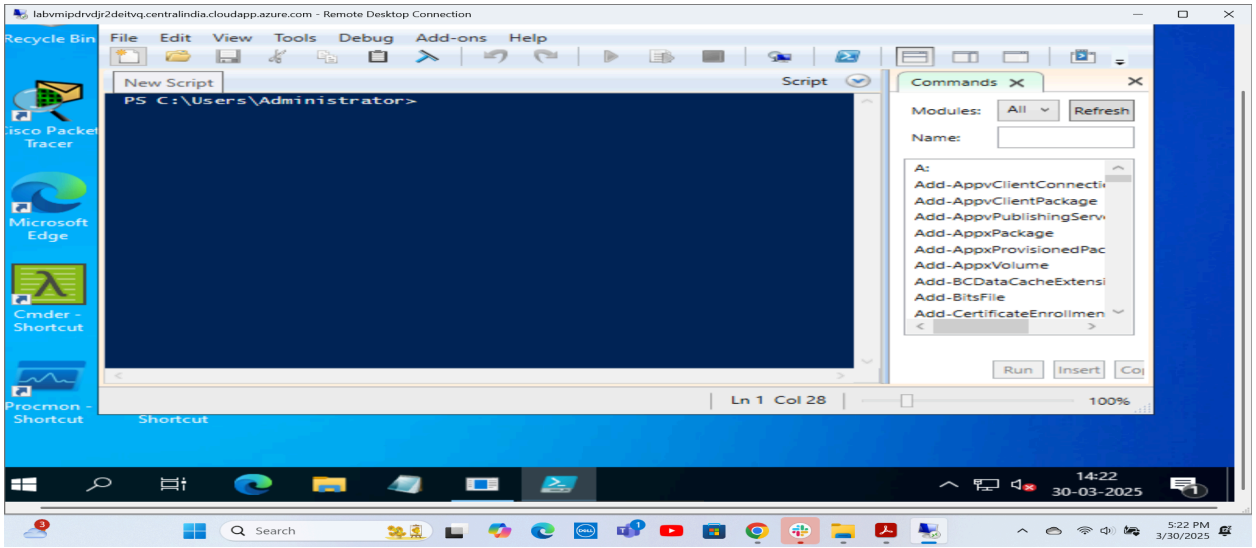
1.3 Logged in as an Administrator



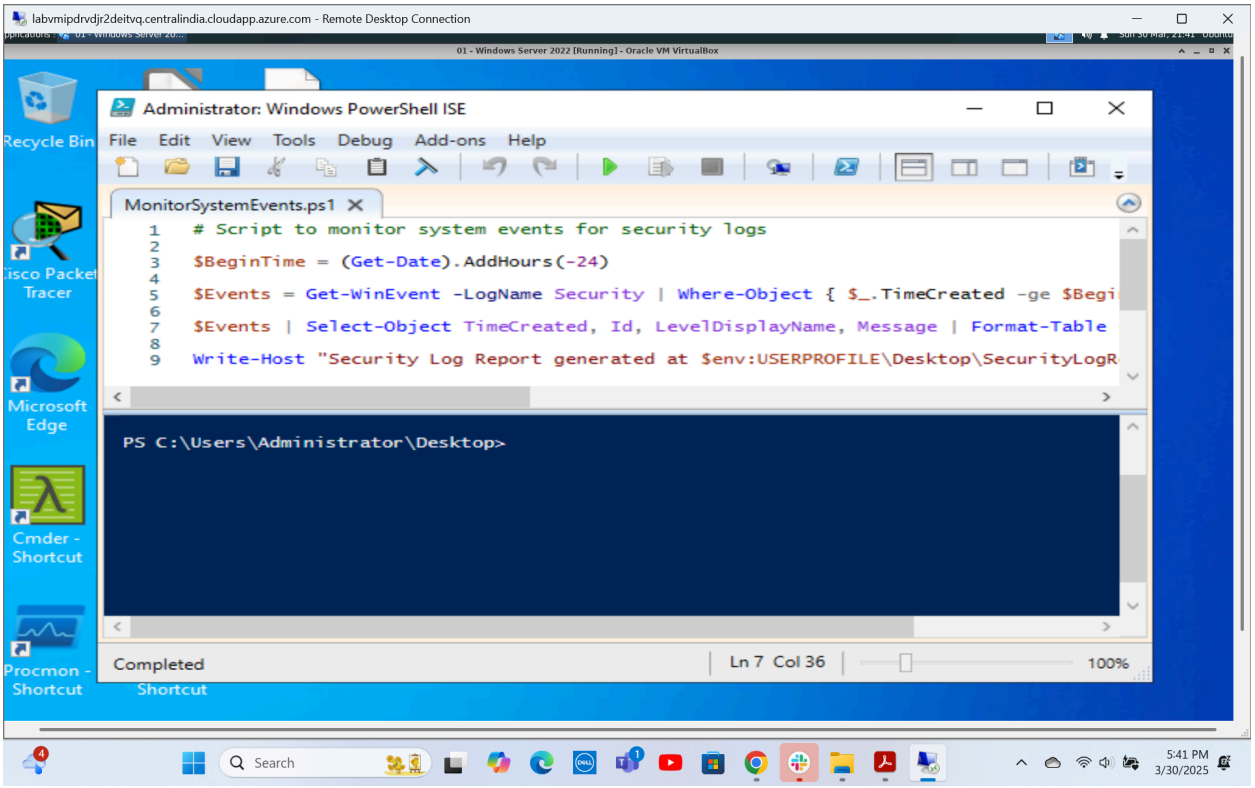
1.4 Running PowerShell as an Administrator

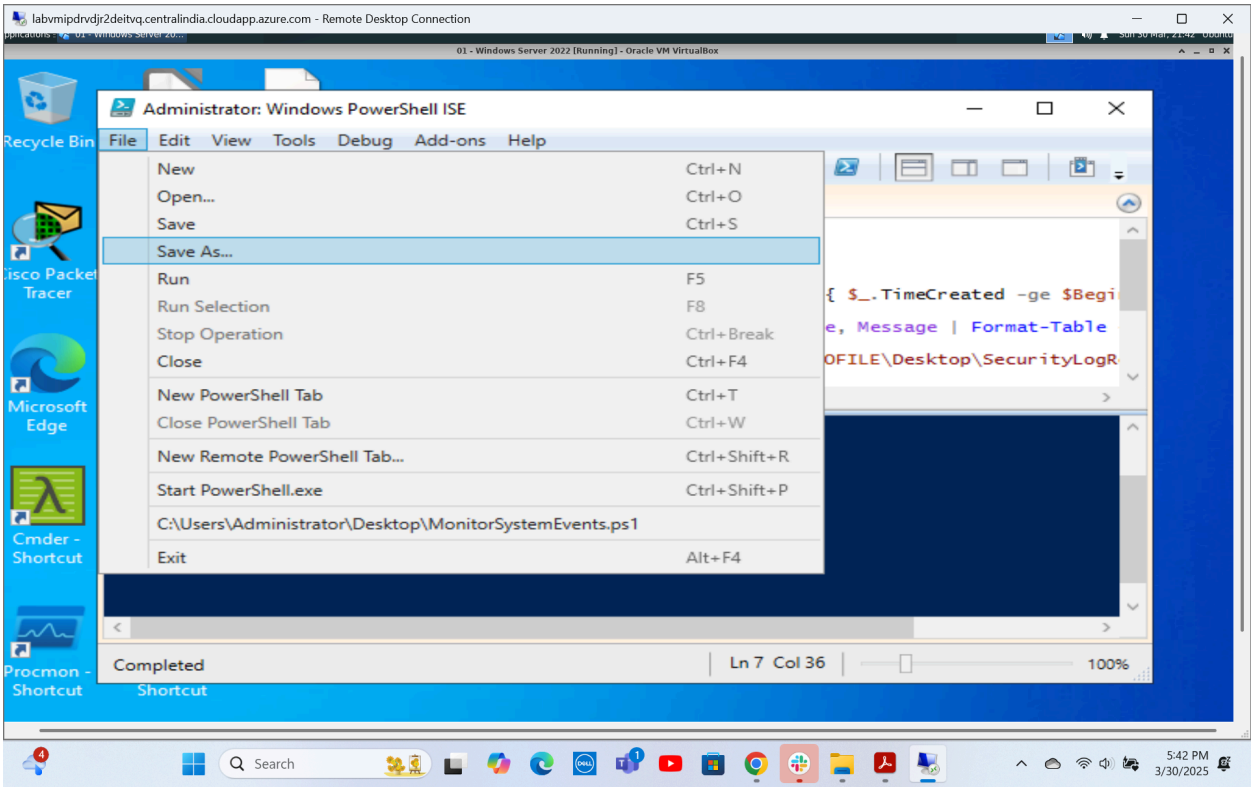


1.5 Opened a new script

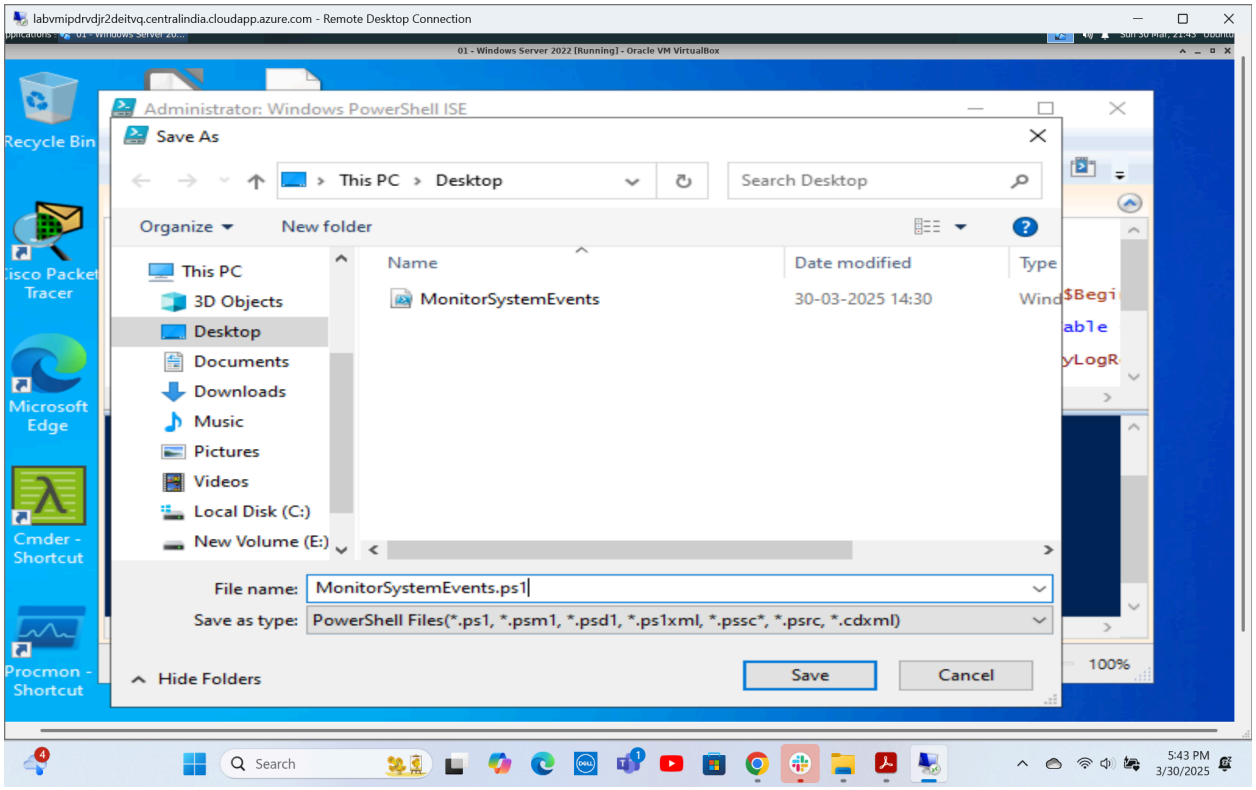


1.6 Created a new script

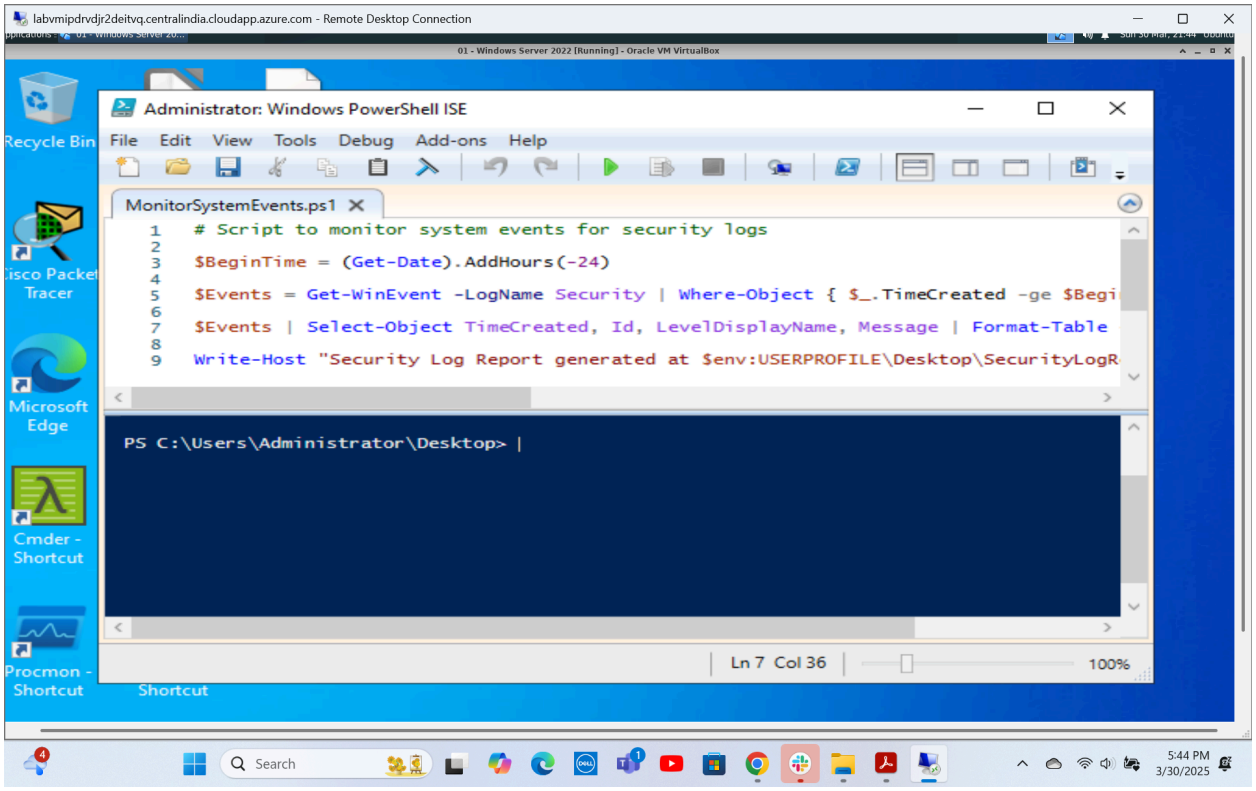

labvmipdrvdjr2deitvq.centralindia.cloudapp.azure.com - Remote Desktop Connection
01 - Windows Server 2022 [Running] - Oracle VM VirtualBox
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
MonitorSystemEvents.ps1
1 # Script to monitor system events for security logs
2
3 $BeginTime = (Get-Date).AddHours(-24)
4
5 $Events = Get-WinEvent -LogName Security | Where-Object { $_.TimeCreated -ge $Begi
6
7 $Events | Select-Object TimeCreated, Id, LevelDisplayName, Message | Format-Table
8
9 Write-Host "Security Log Report generated at $env:USERPROFILE\Desktop\SecurityLogR
PS C:\Users\Administrator\Desktop>
Completed
Ln 7 Col 36
100%
Recycle Bin
Cisco Packet Tracer
Microsoft Edge
Cmder - Shortcut
Procmon - Shortcut
Search
5:41 PM
3/30/2025


labvmipdrvdjr2deitvq.centralindia.cloudapp.azure.com - Remote Desktop Connection
01 - Windows Server 2022 [Running] - Oracle VM VirtualBox
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Run F5
Run Selection F8
Stop Operation Ctrl+Break
Close Ctrl+F4
New PowerShell Tab Ctrl+T
Close PowerShell Tab Ctrl+W
New Remote PowerShell Tab... Ctrl+Shift+R
Start PowerShell.exe Ctrl+Shift+P
C:\Users\Administrator\Desktop\MonitorSystemEvents.ps1
Exit Alt+F4
{ $_.TimeCreated -ge $Begi
e, Message | Format-Table
OFILE\Desktop\SecurityLogR
Completed
Ln 7 Col 36
100%
Recycle Bin
Cisco Packet Tracer
Microsoft Edge
Cmder - Shortcut
Procmon - Shortcut
Search
5:42 PM
3/30/2025

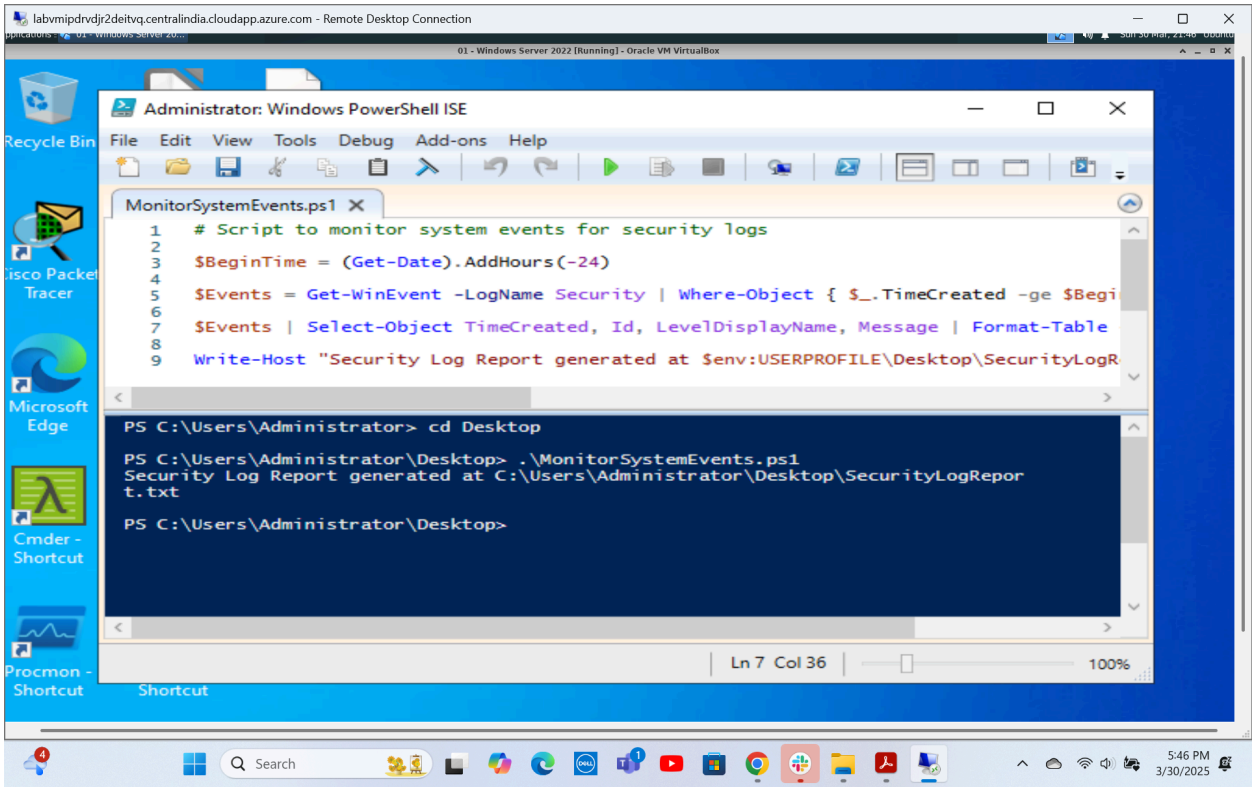
1.7 Saved Script on Desktop as **MonitorSystemEvents.ps1**



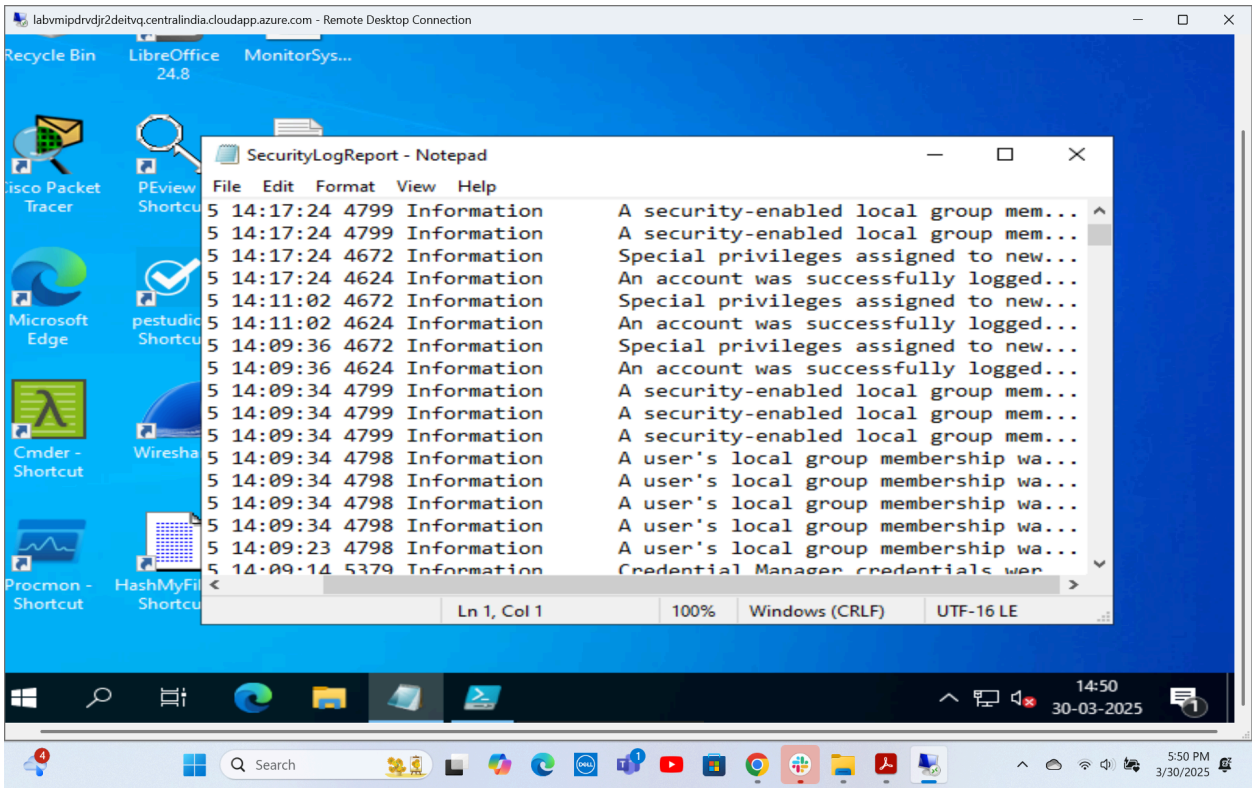
1.8 Navigated to the script's location by running the following command **cd Desktop**



1.9 Executed the script by running the following command **.\MonitorSystemEvents.ps1**

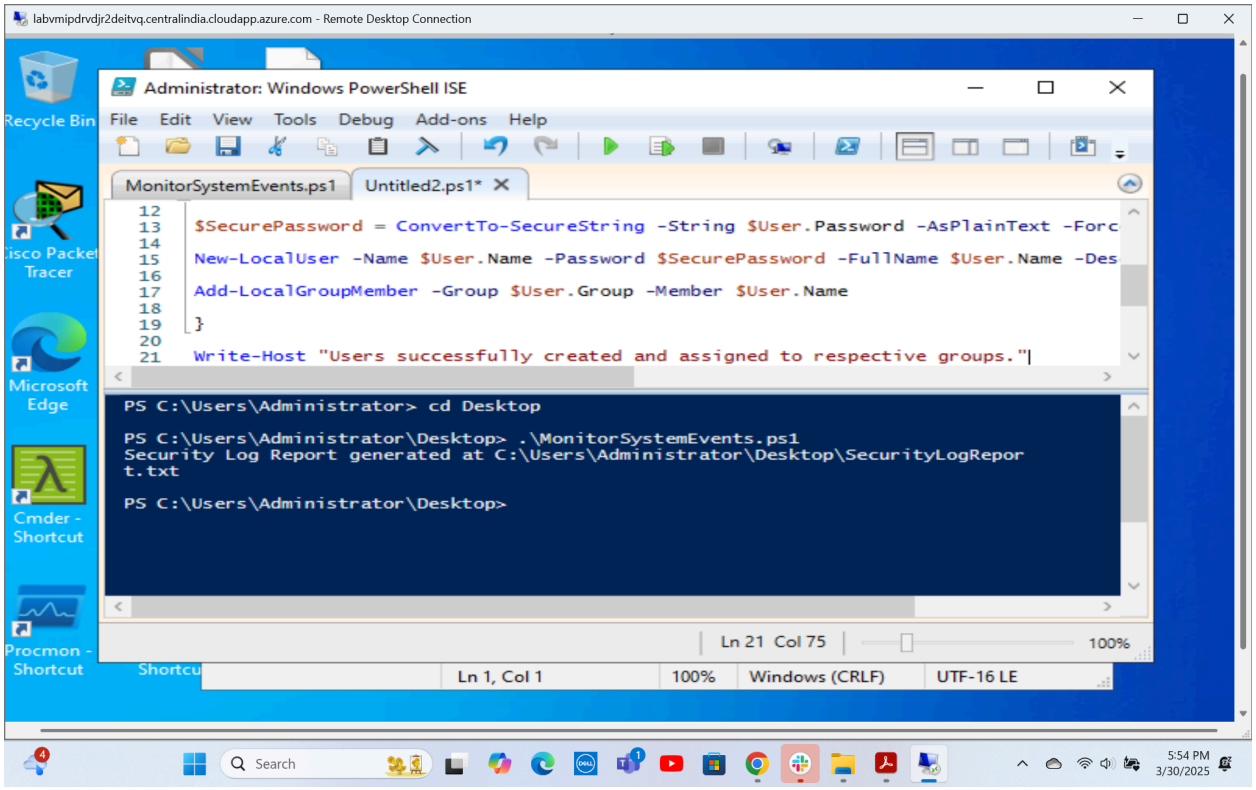


1.10 Browsed for a file named **SecurityLogReport.txt** containing the filtered security events

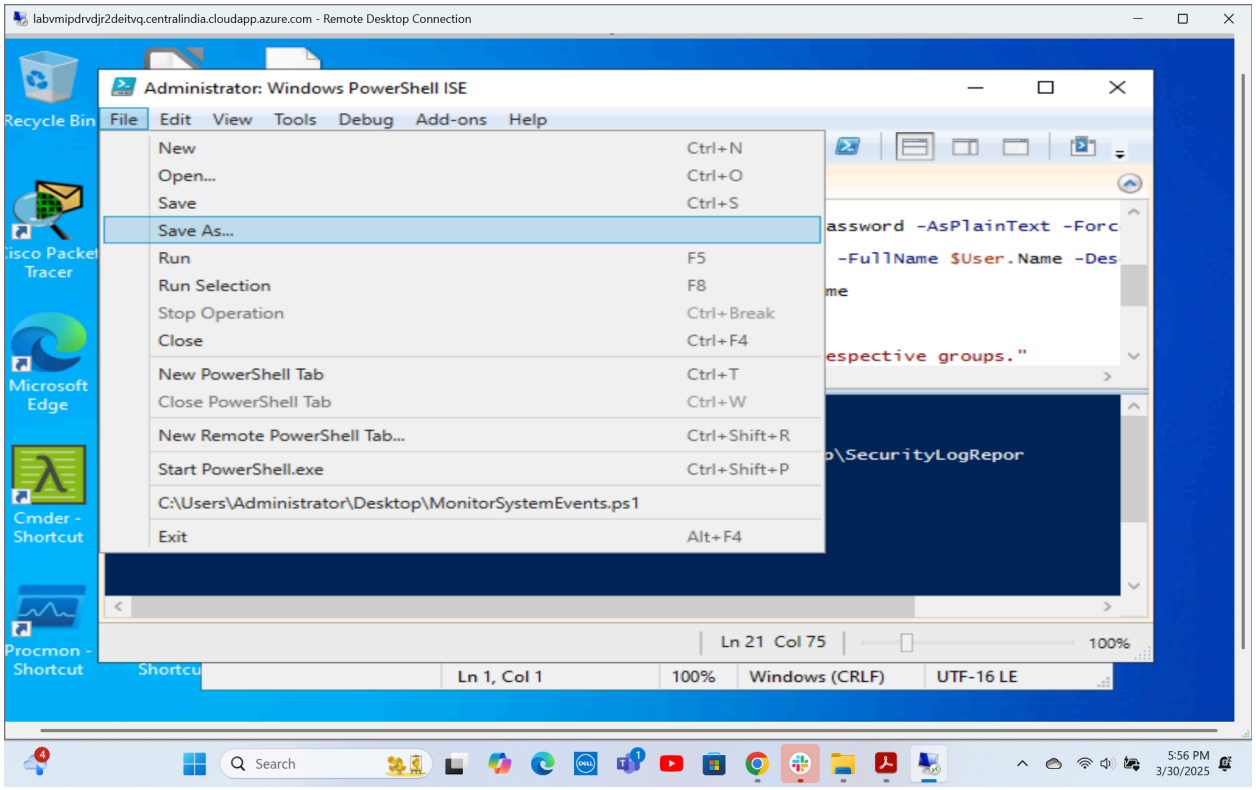


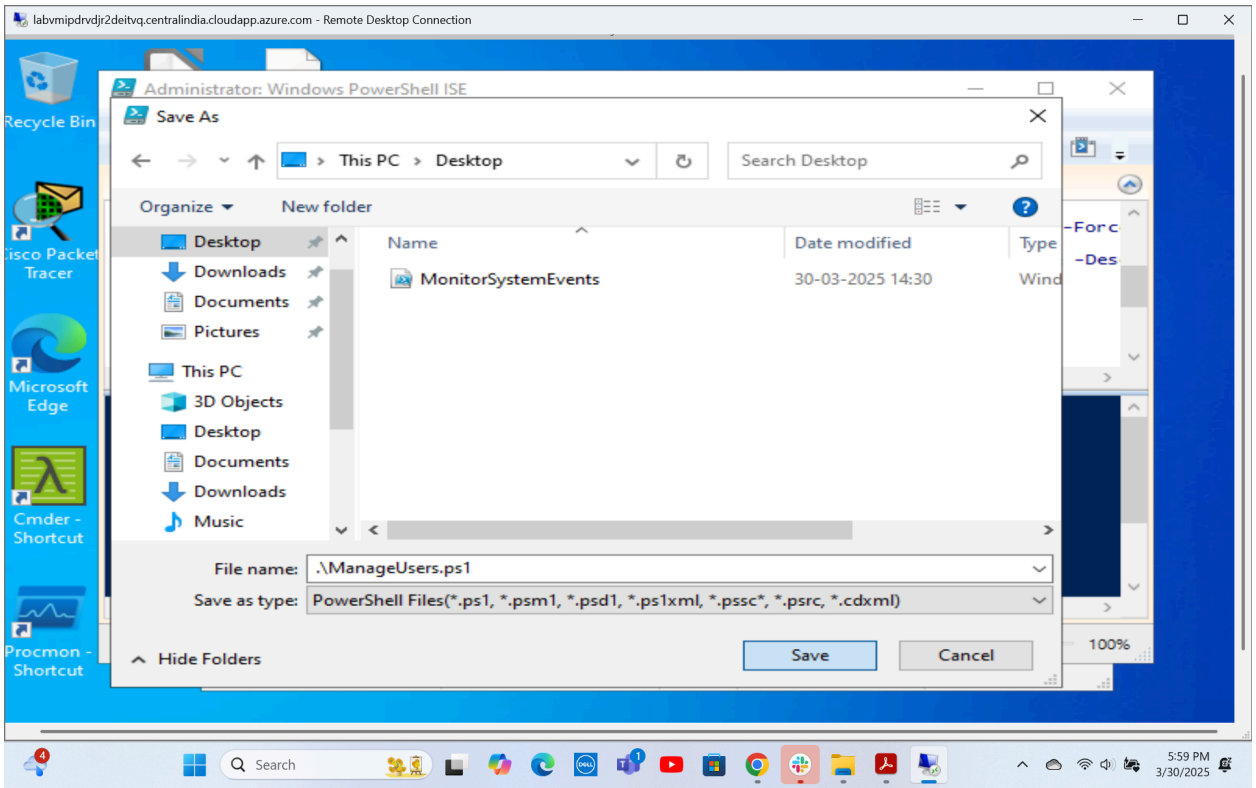
Step 2: Analyzed methods to optimize user management

2.1 Repeated step 1.5 to open a new script and added multiple users, set their passwords, and assigned them to groups

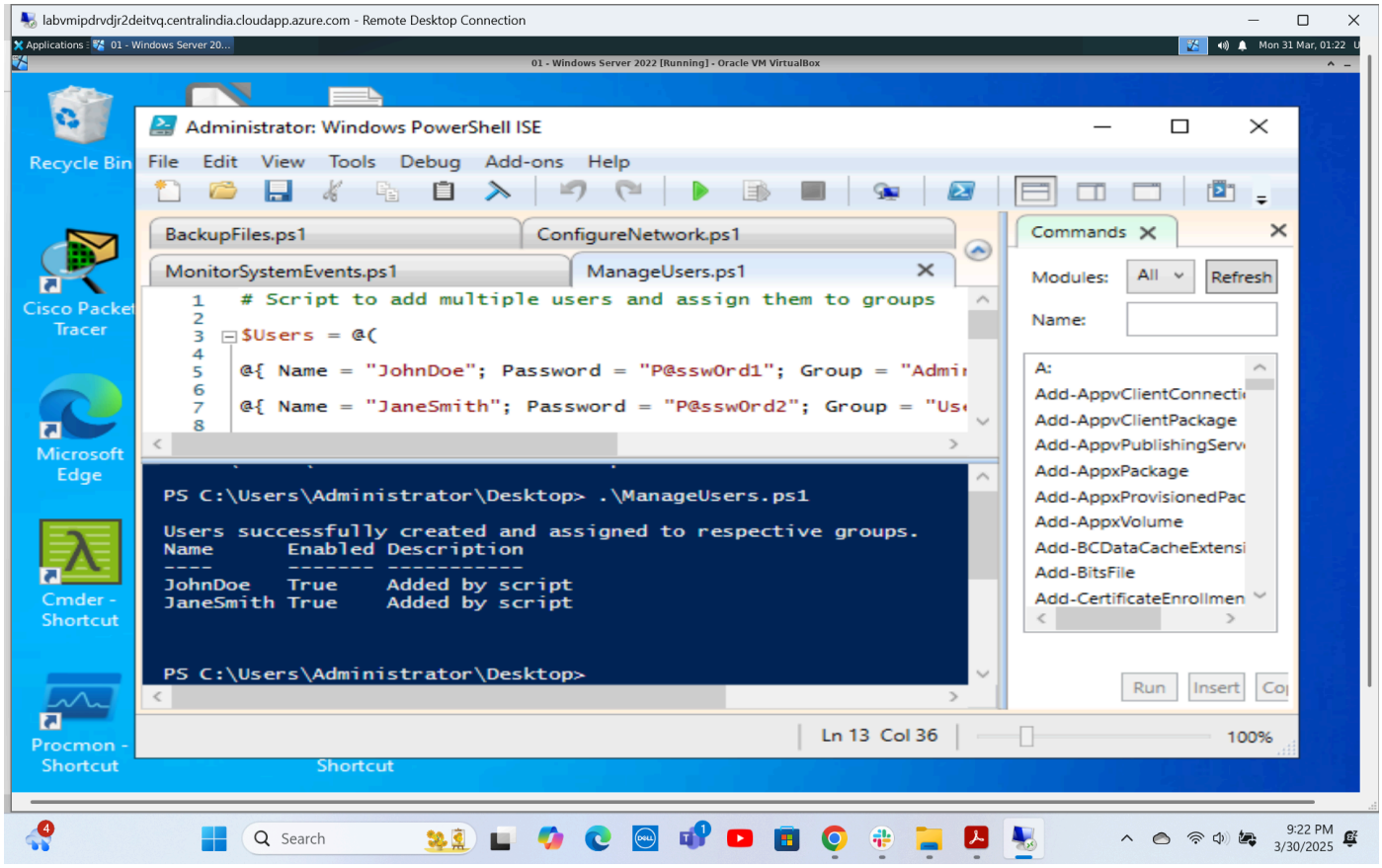


2.2 Saved the script on the Desktop as **ManageUsers.ps1**



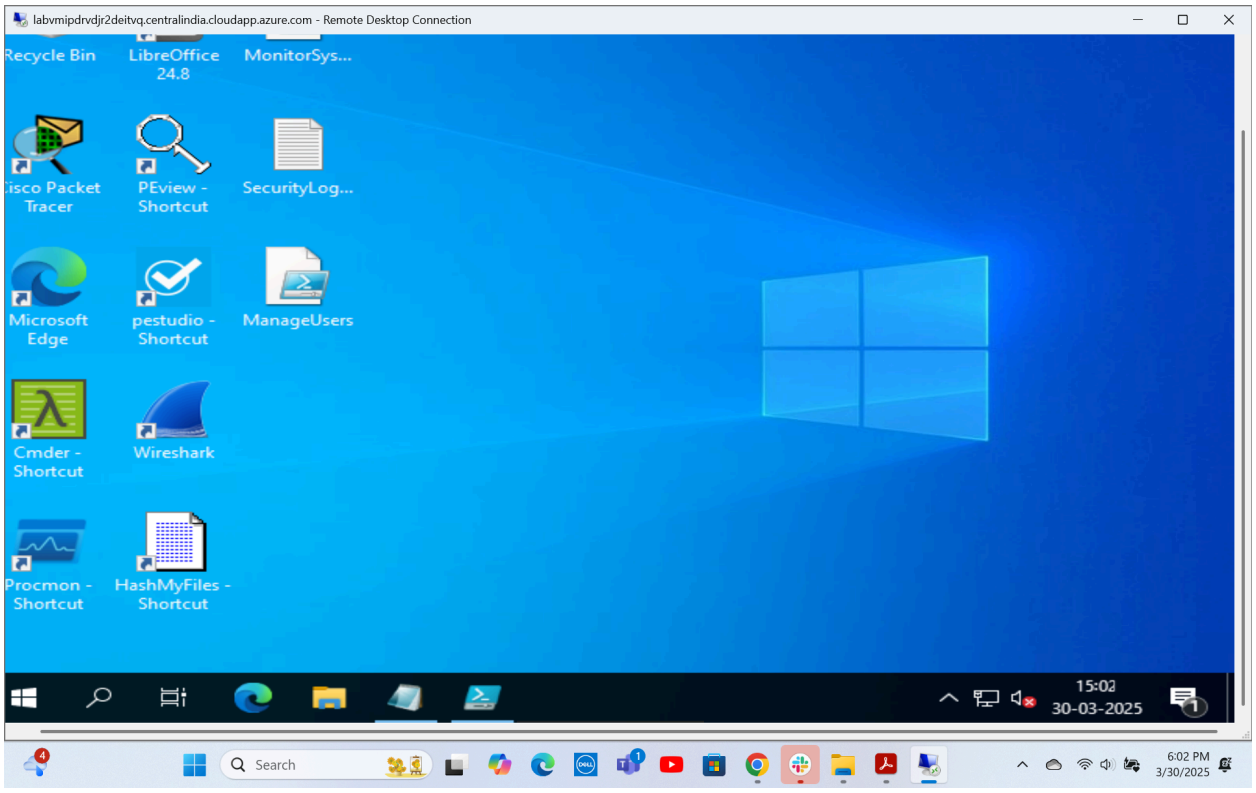


2.3 Executed the script by running the program using .\ManageUsers.ps1

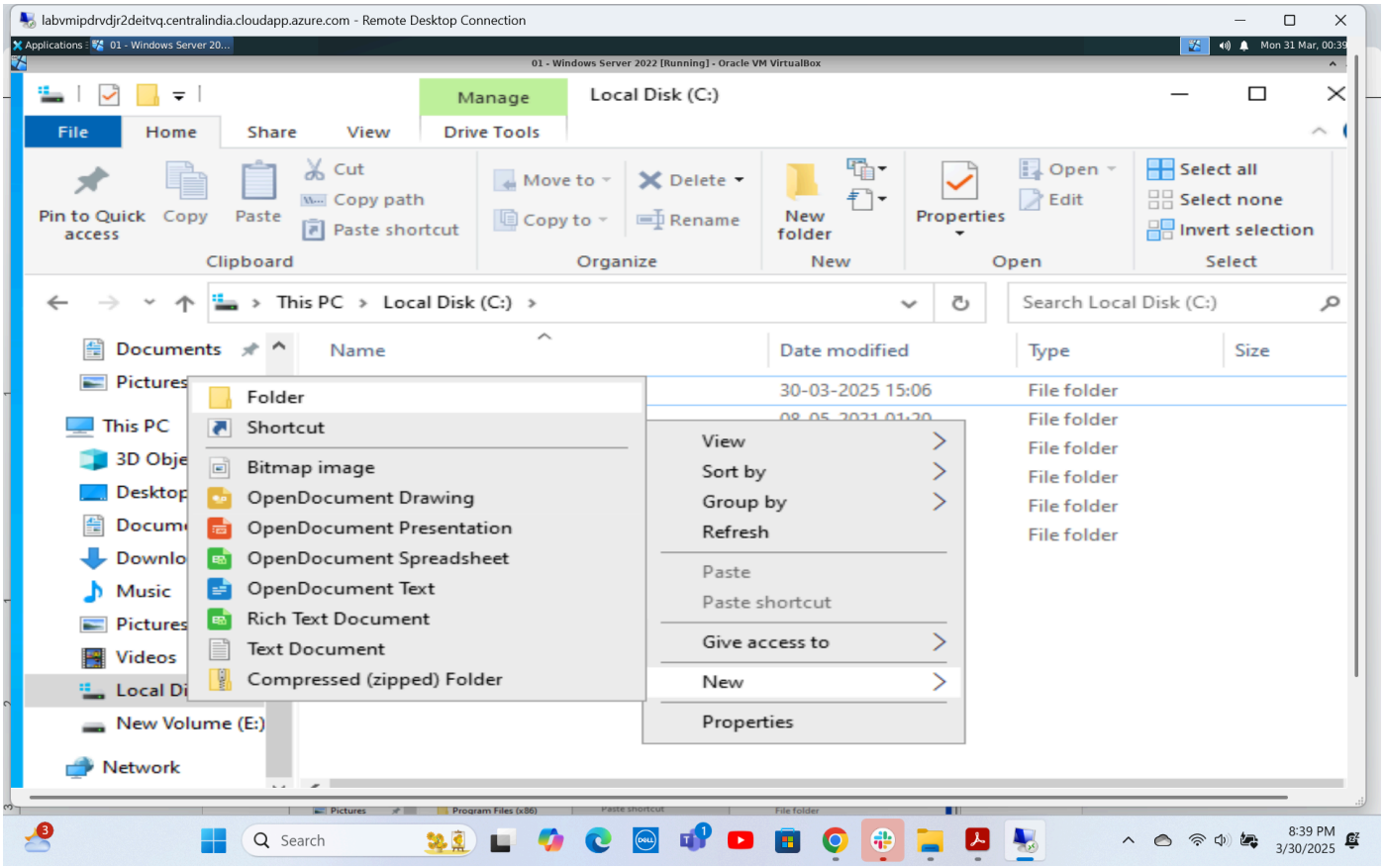


Step 3: Create a streamlined process for file management

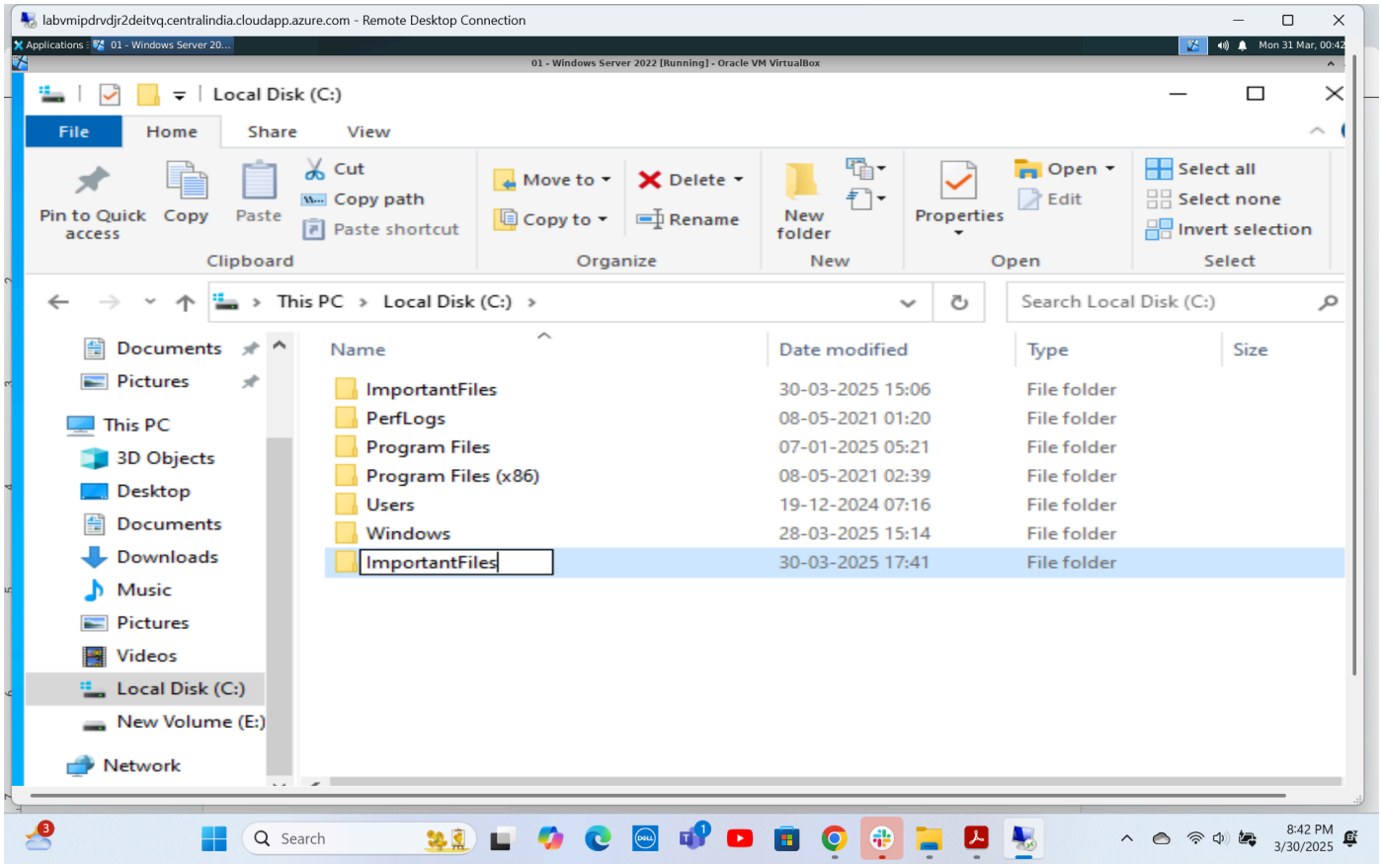
3.1 Click on File Explorer in the menu tab to create a dummy data folder



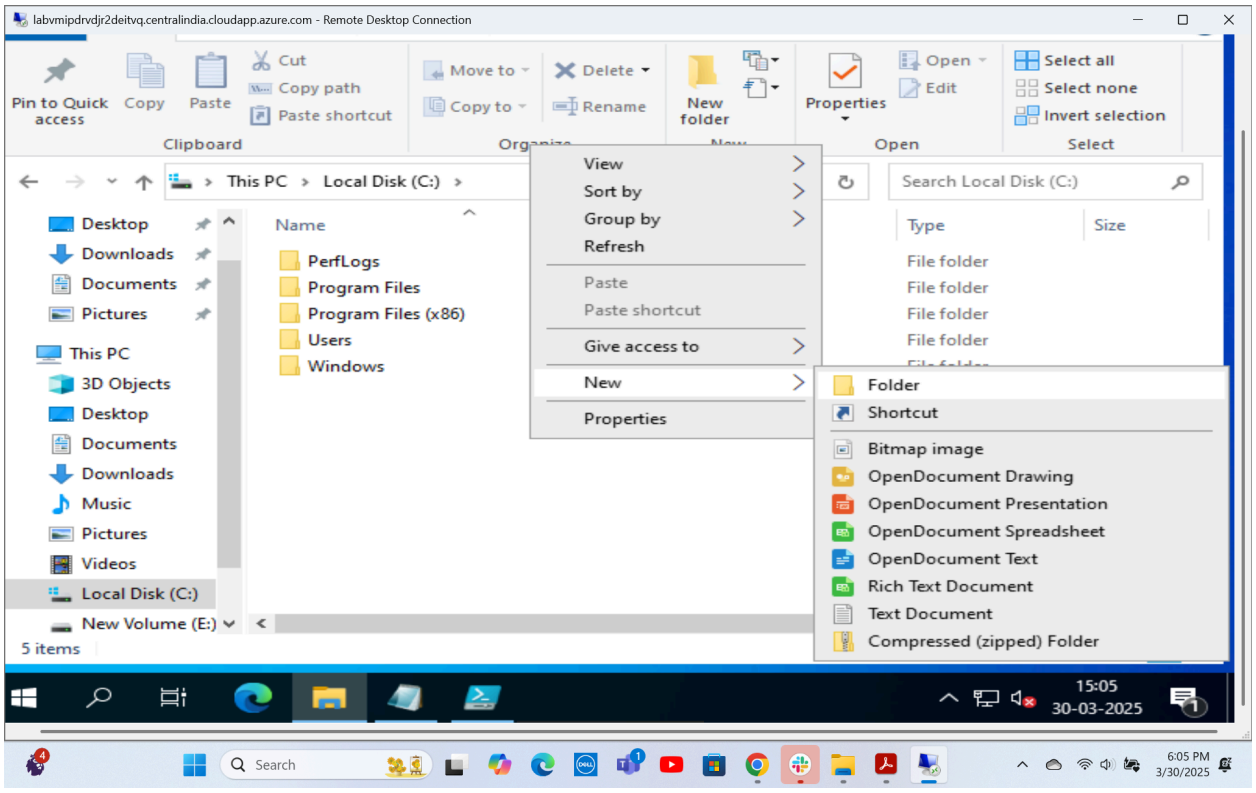
3.2 Navigated to **This PC**, opened **C Drive** and created a new folder

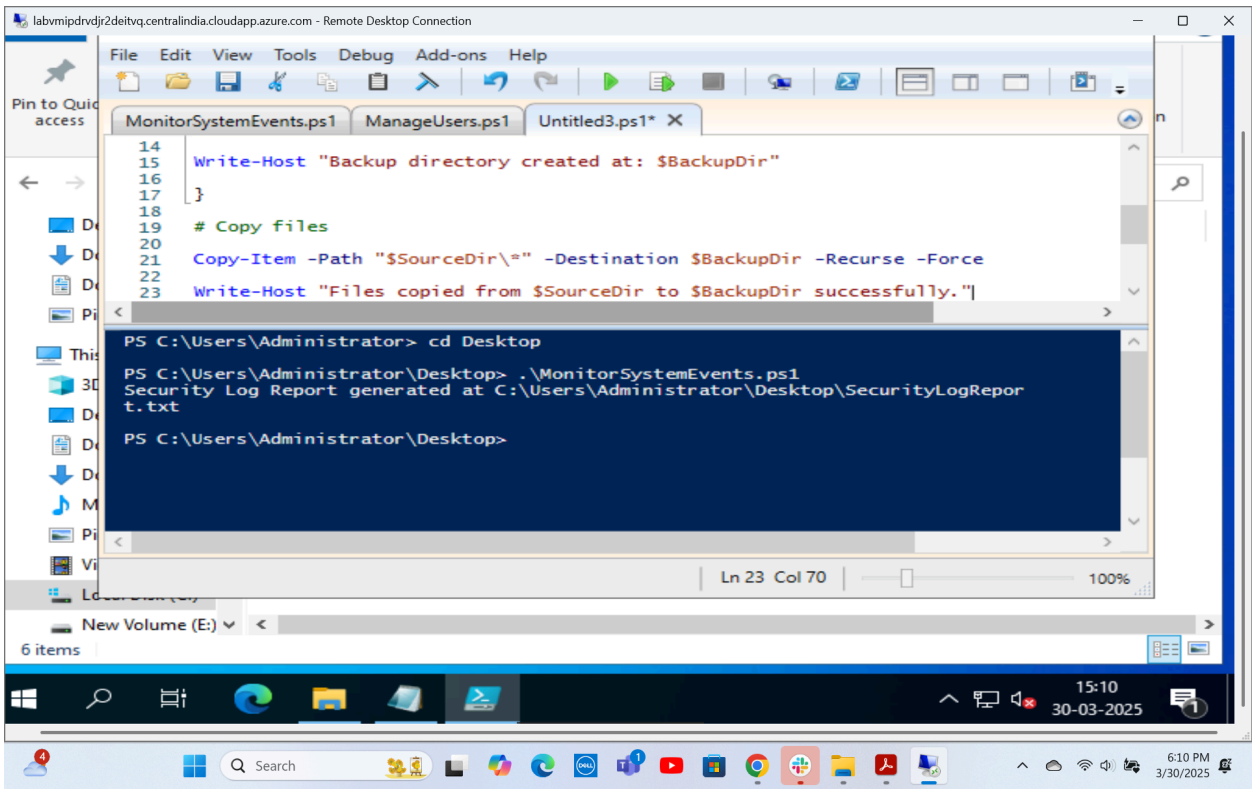


3.3 Named the folder as **ImportantFiles** and saved it

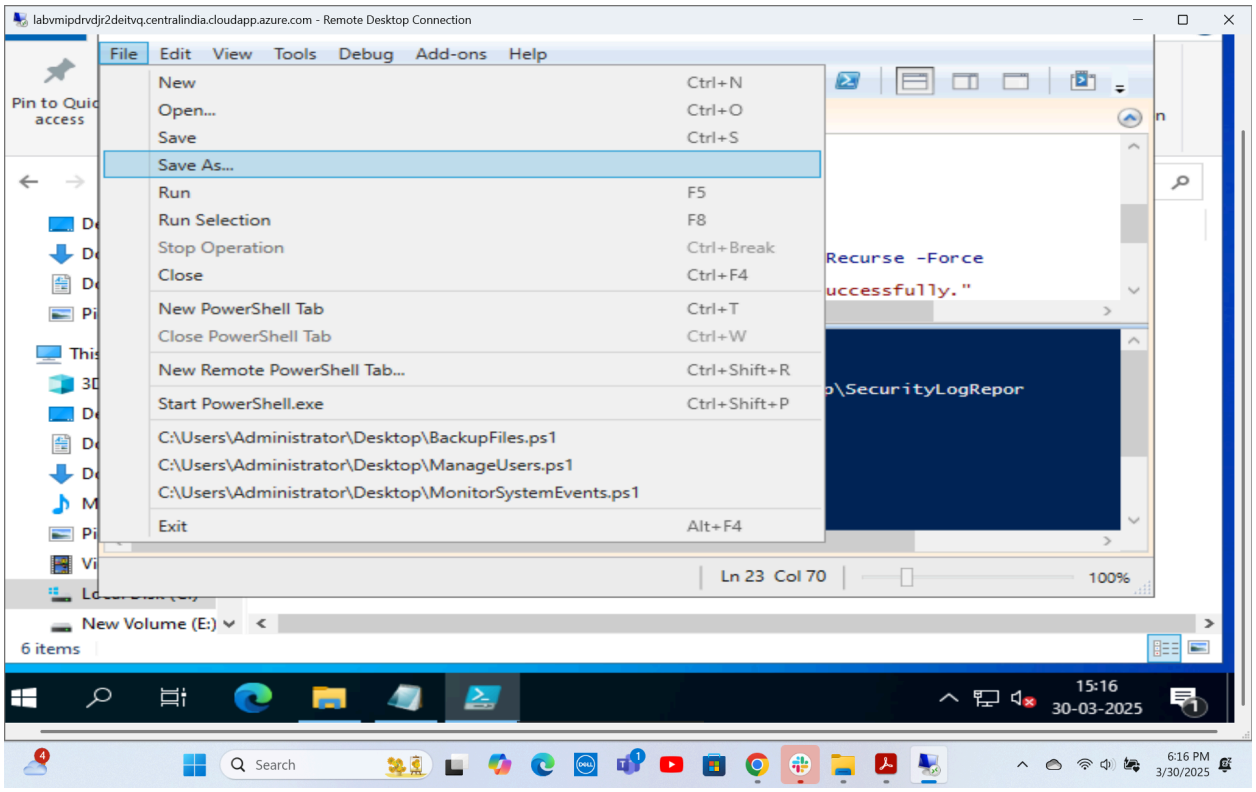


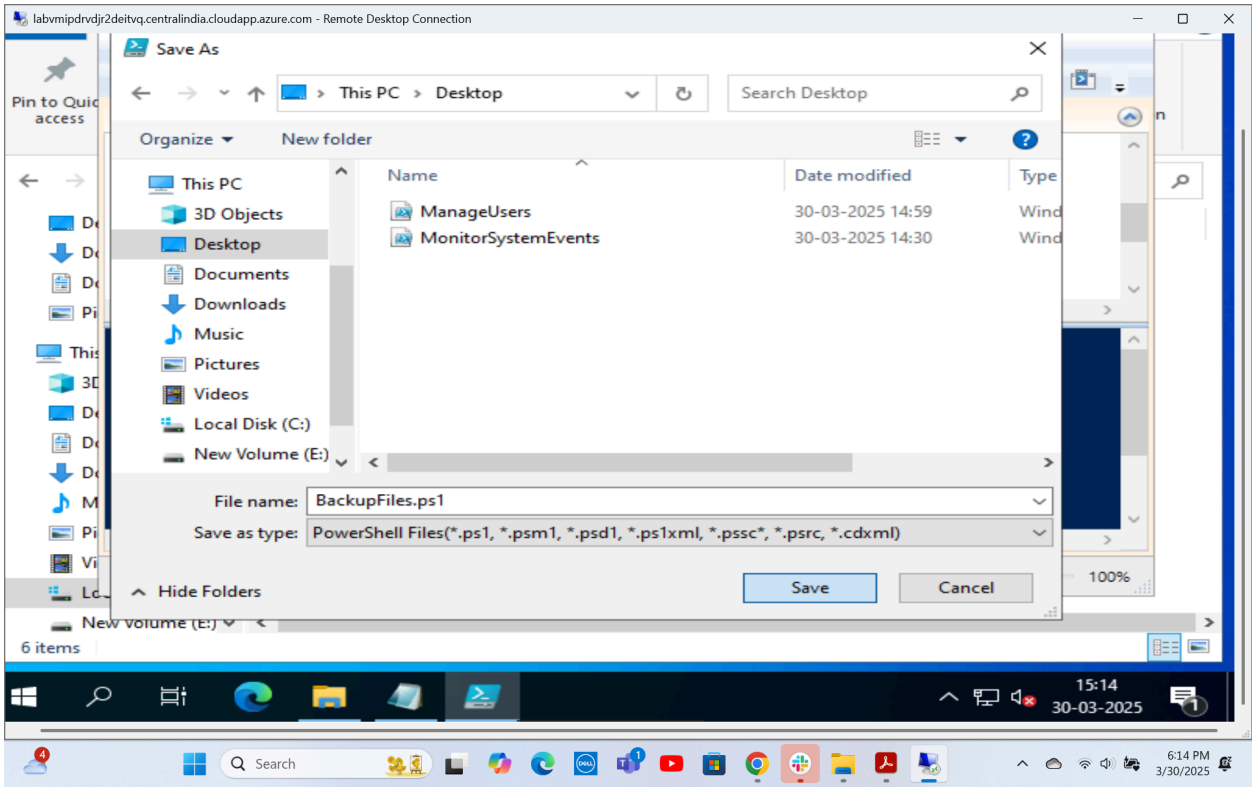
3.4 Navigated back to PowerShell and **repeated step 1.5.** Typed the script to implement file backup in the **E Drive:**



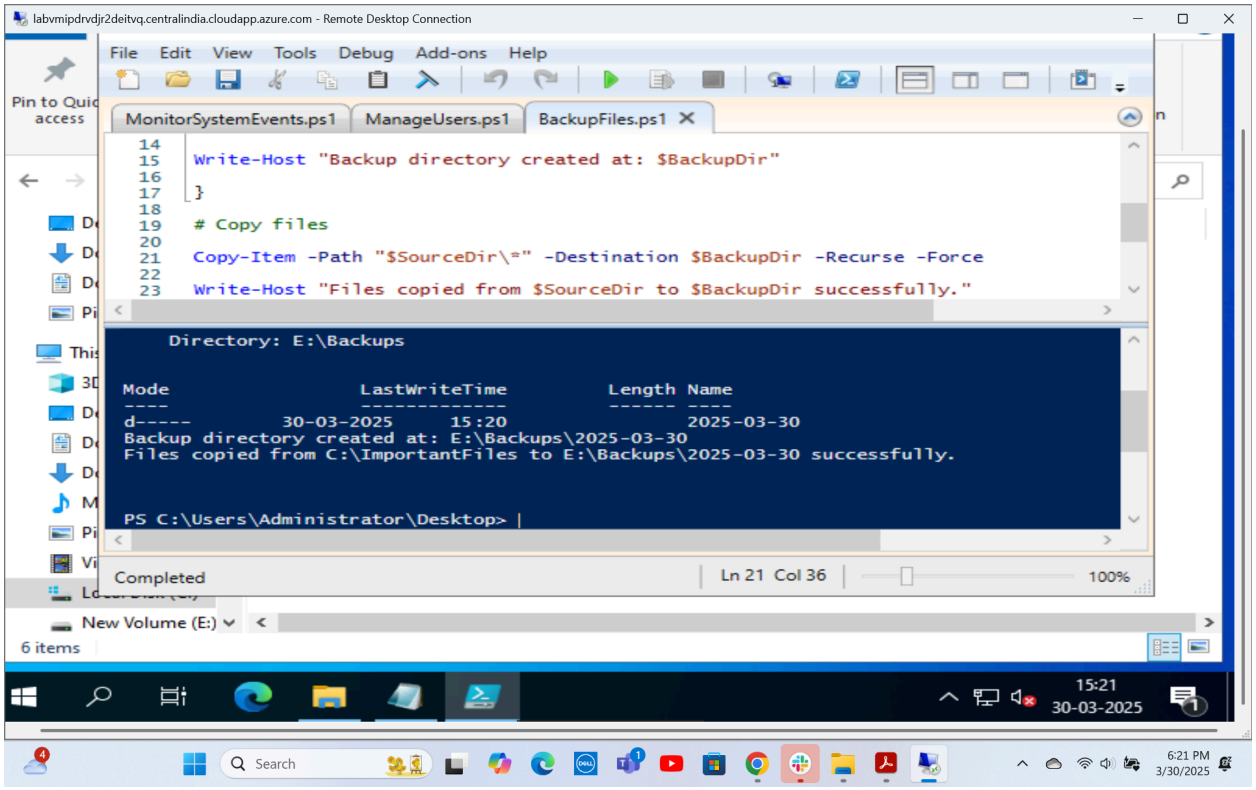


3.5 Repeated step 2.3 and saved the file with the name **BackupFiles.ps1** on the **desktop**



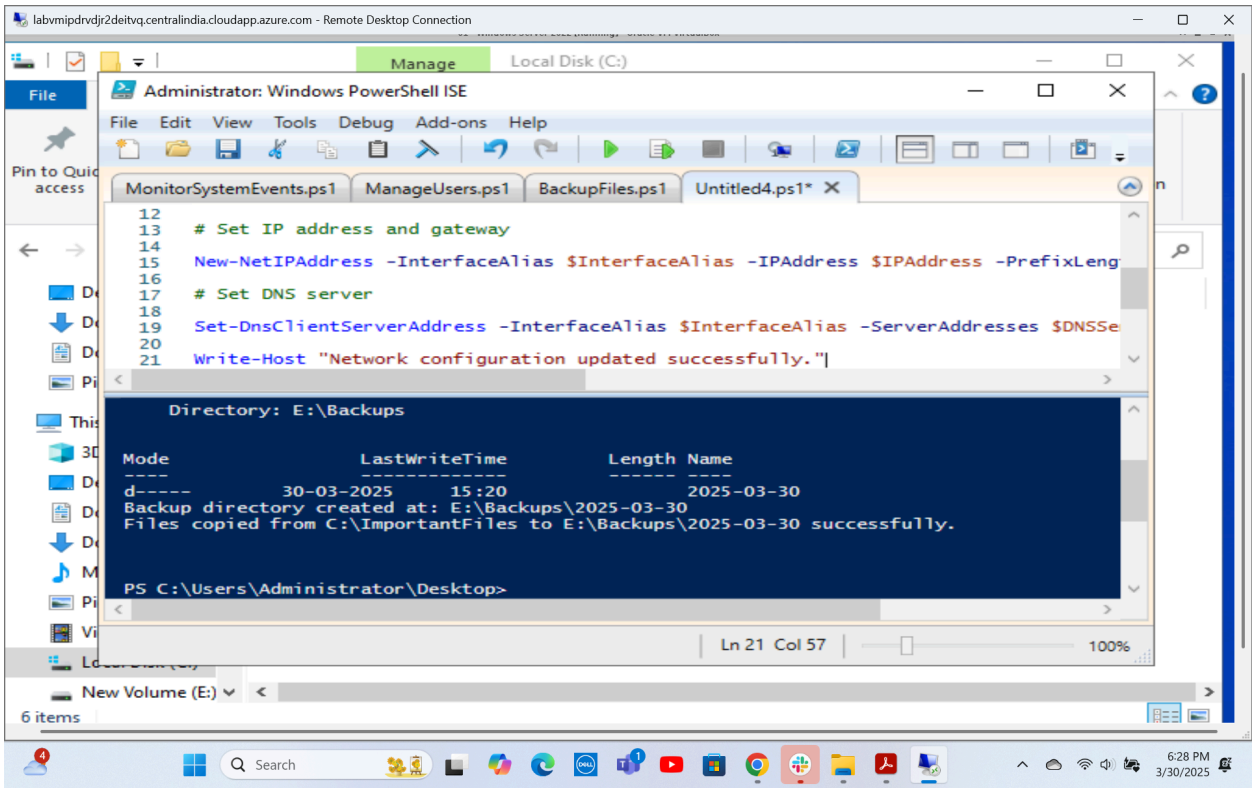


3.6 Executed the script of backing up files of the C drive to the D drive having the current date by running the following command: **.\BackupFiles.ps1**

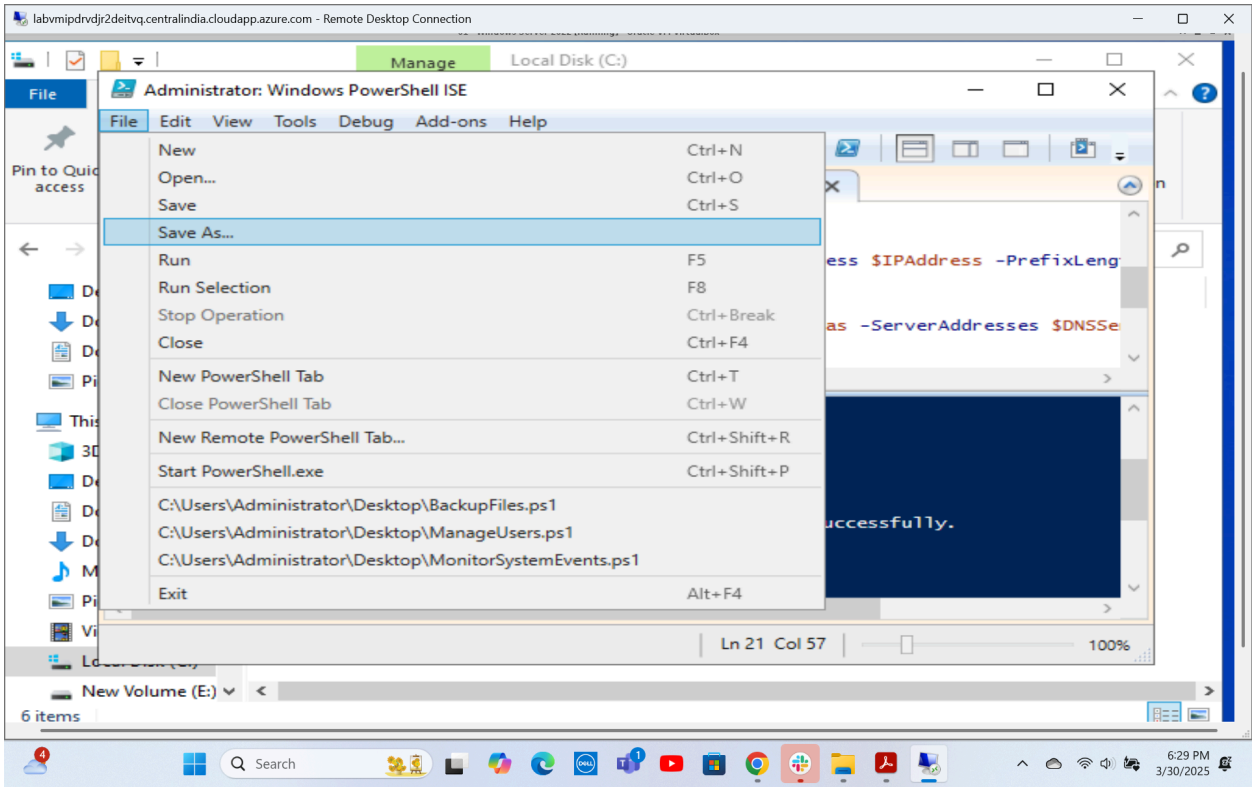


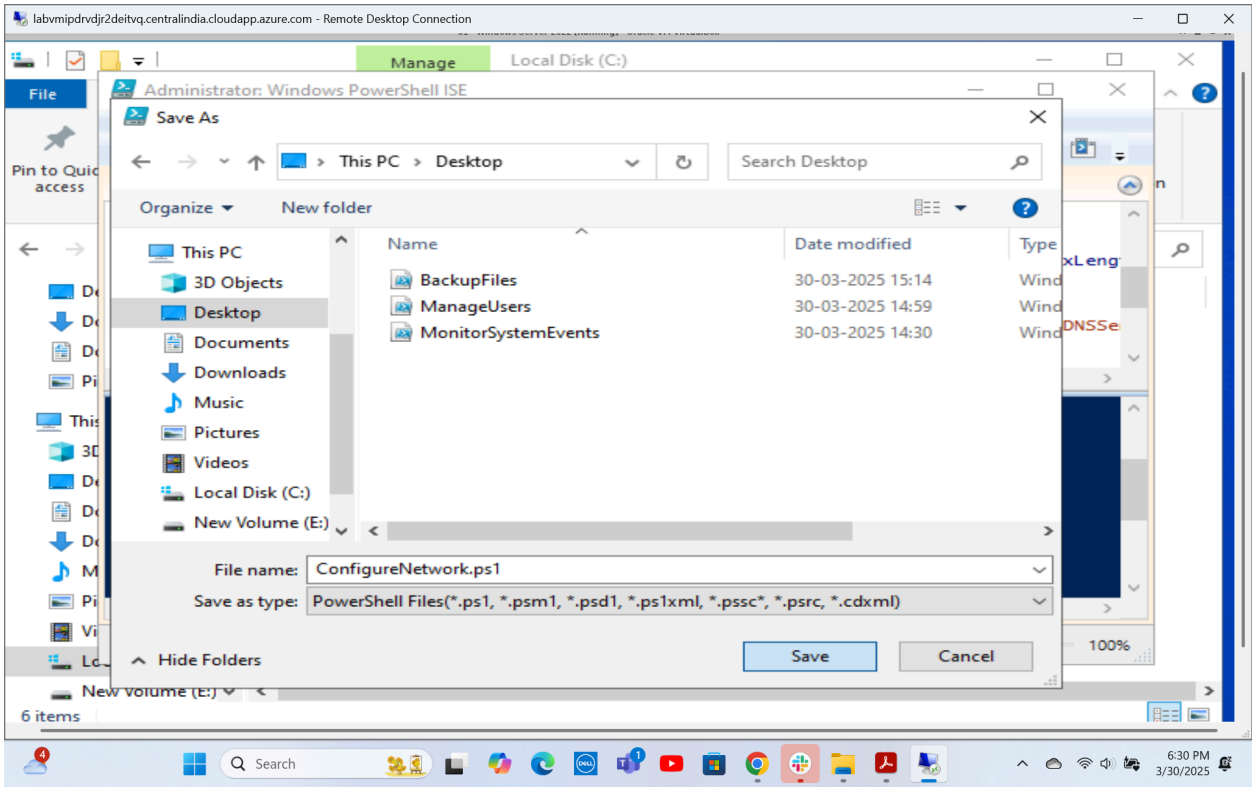
Step 4: Designed an approach for network configuration

4.1 Repeated **step 2.1** to write the script for performing **network configuration**

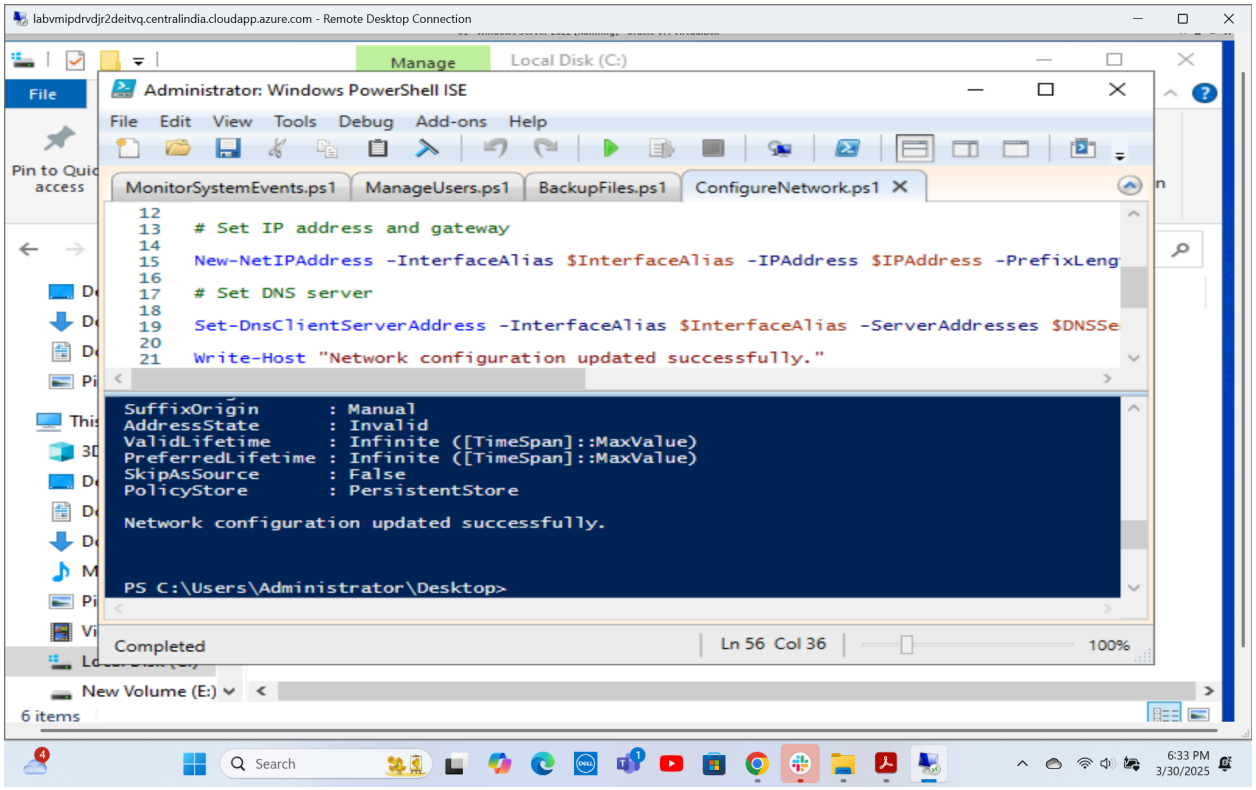


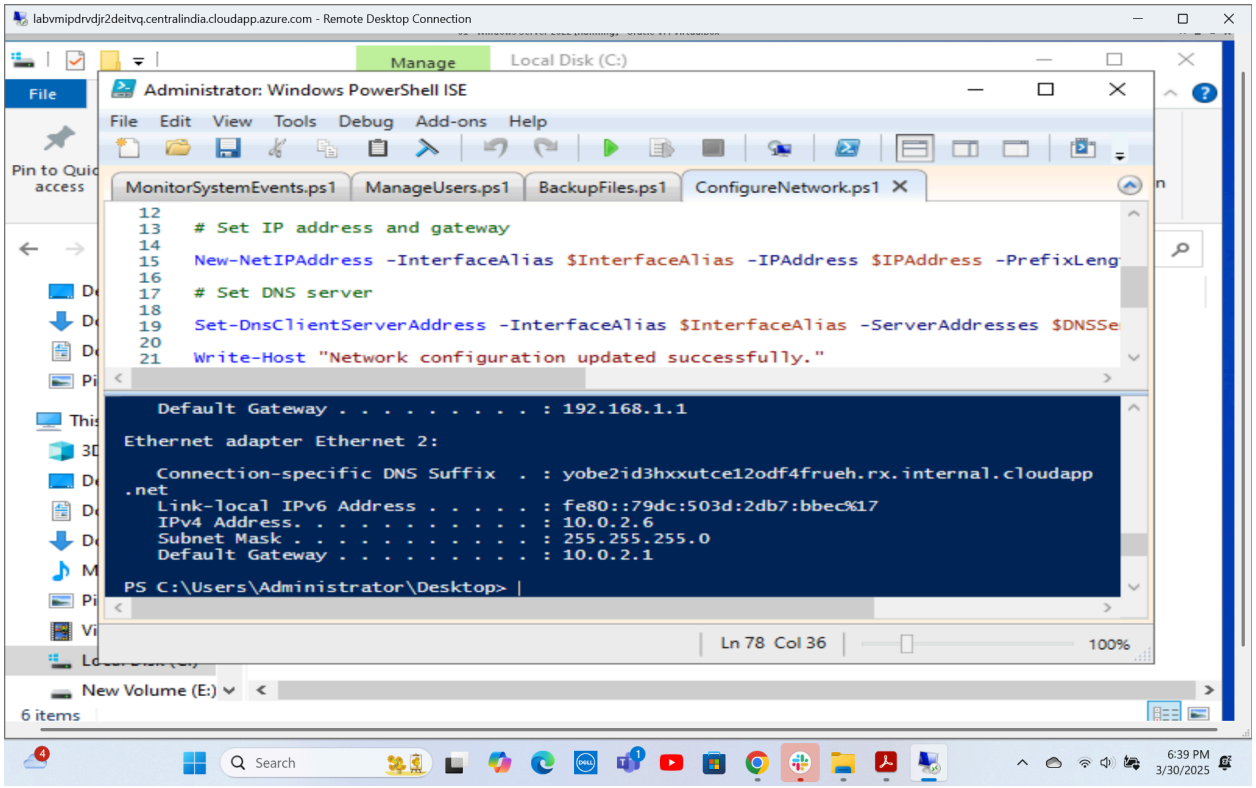
4.2 Repeated **step 2.3** and saved the file with the name **ConfigureNetwork.ps1** on the desktop



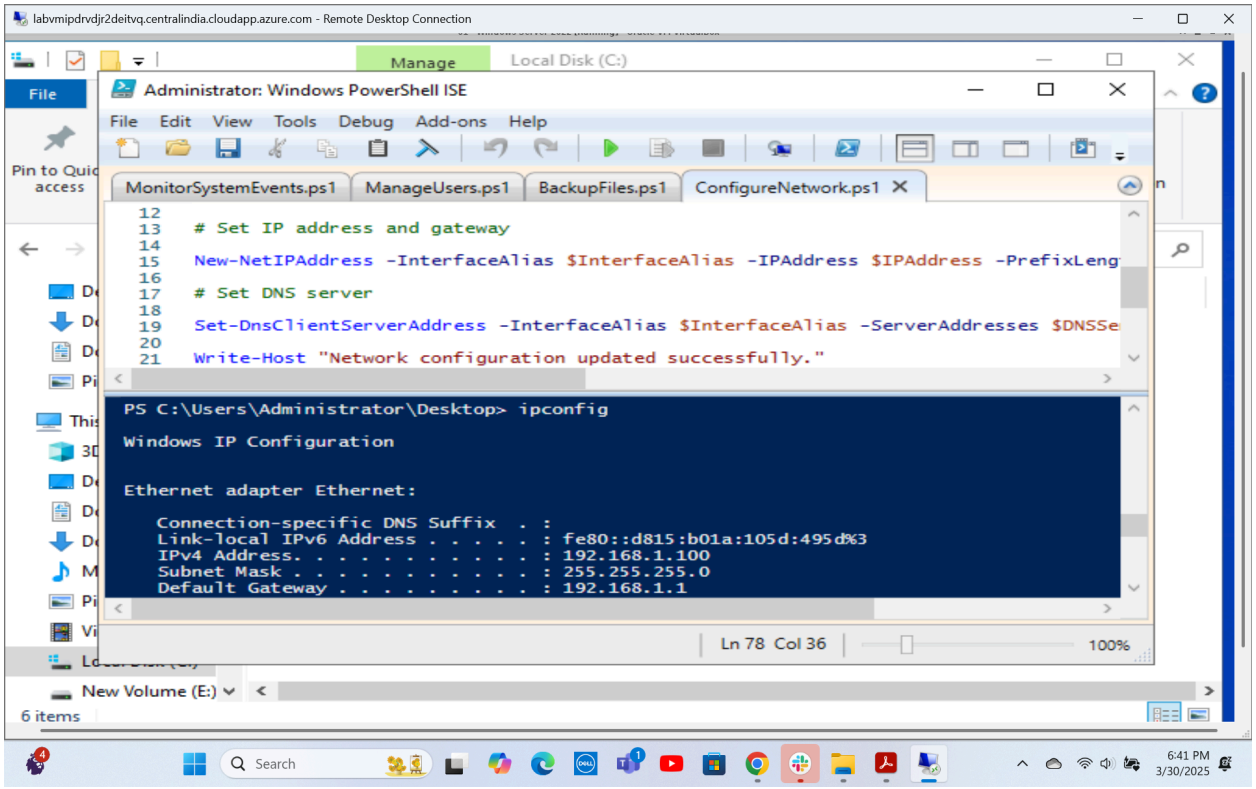


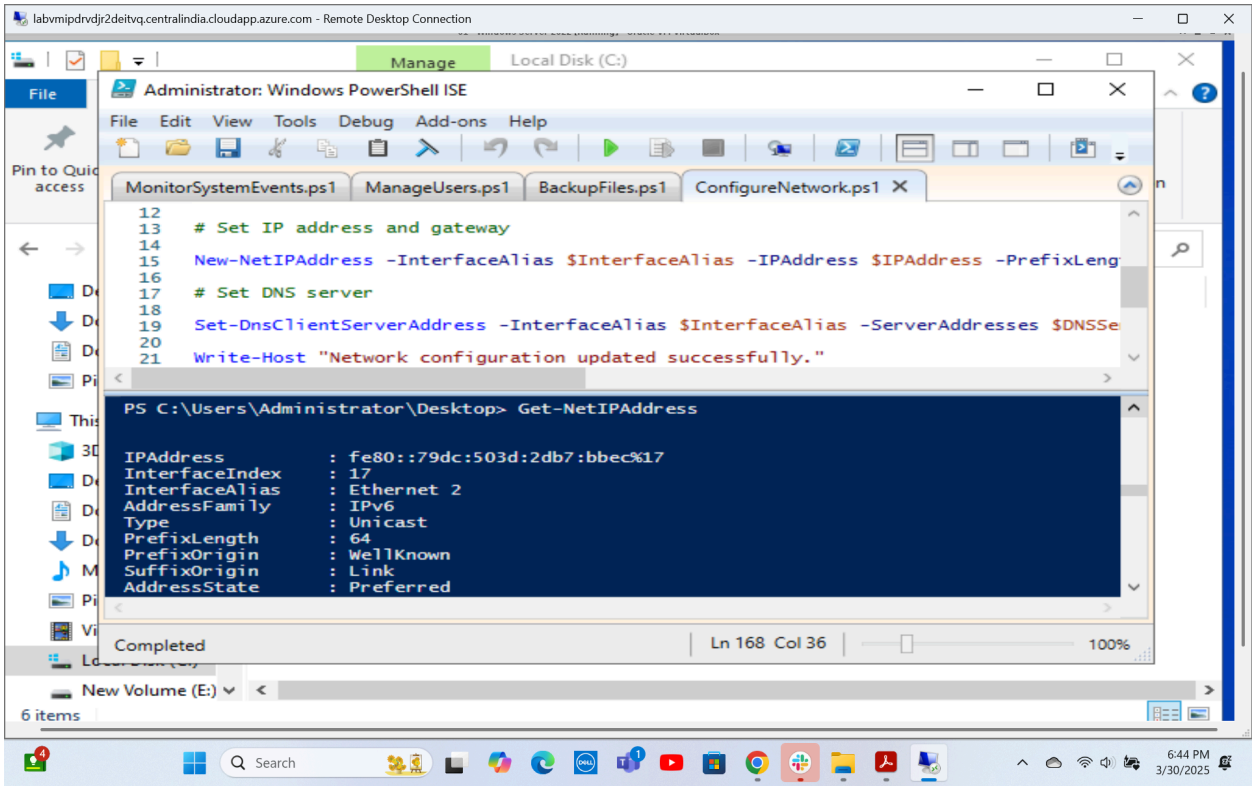
4.3 Executed the script that updates the network adapter settings with the new IP configuration by running the following command: **.\ConfigureNetwork.ps1**





4.4 Verified the new changes by running the following commands: **ipconfig**
Get-NetIPAddress




labvmipdrvdjr2deitvq.centralindia.cloudapp.azure.com - Remote Desktop Connection
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
MonitorSystemEvents.ps1
ManageUsers.ps1
BackupFiles.ps1
ConfigureNetwork.ps1
Set IP address and gateway
New-NetIPAddress -InterfaceAlias $InterfaceAlias -IPAddress $IPAddress -PrefixLeng
Set DNS server
Set-DnsClientServerAddress -InterfaceAlias $InterfaceAlias -ServerAddresses $DNSSe
Write-Host "Network configuration updated successfully."
PS C:\Users\Administrator\Desktop> Get-NetIPAddress
IPAddress : fe80::79dc:503d:2db7:bbec%17
InterfaceIndex : 17
InterfaceAlias : Ethernet 2
AddressFamily : IPv6
Type : Unicast
PrefixLength : 64
PrefixOrigin : WellKnown
SuffixOrigin : Link
AddressState : Preferred
Completed
Ln 168 Col 36
100%
New Volume (E:)
6 items
Search
6:44 PM
3/30/2025