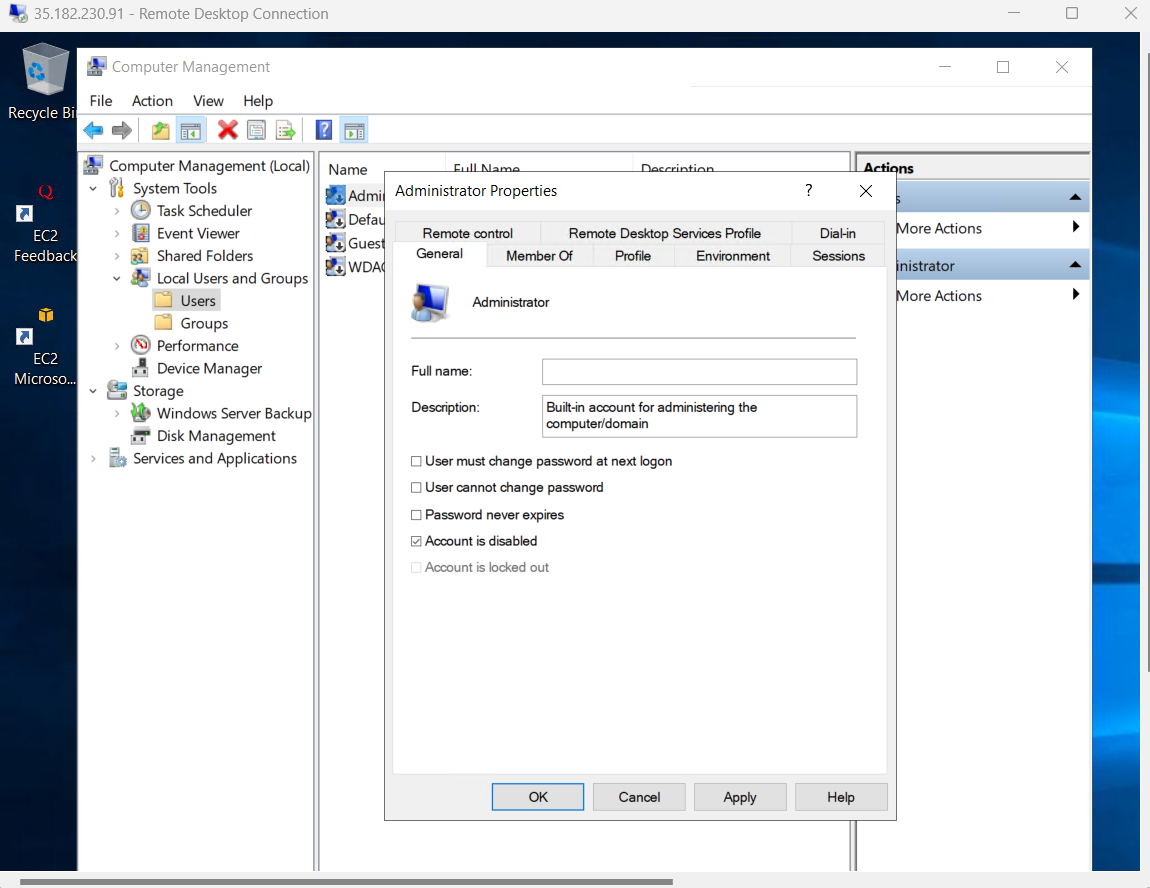
|  | **Durham College** |
| --- | --- |
| **Course** | INFT 1103 |
| **Professor** | Ida Leung |
| **Student Name**  **Student ID** | Maisha Khatoon  100899259 |
| **Lab3** | Hardening Window Servers |

For this lab, we will be working with both the OshawaDC and the FileServer. First power on your OshawaDC server, then power on your FileServer.

For screenshots, ideally use the *snipping tool* to take a screenshot of the relevant information to each question. Normal print screen must shown the focus point for each activity. Either insert your sc

**User Configuration**

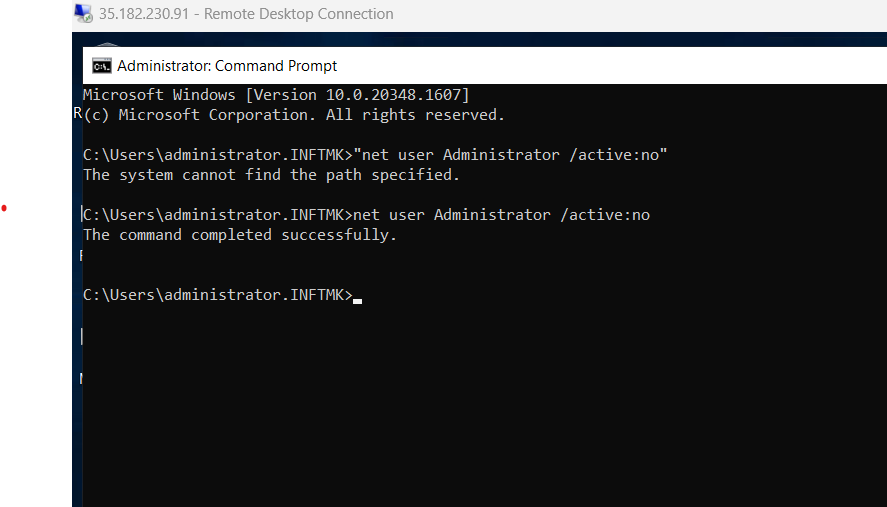
1. On your **FileServer** PC open Windows Administrative Tools > Computer Management
2. Expand Local Users and Groups > Users
3. Find the Administrator account > right click > Properties
4. Under the general tab put a check beside “Account is disabled”
   1. Take a screenshot and place it here



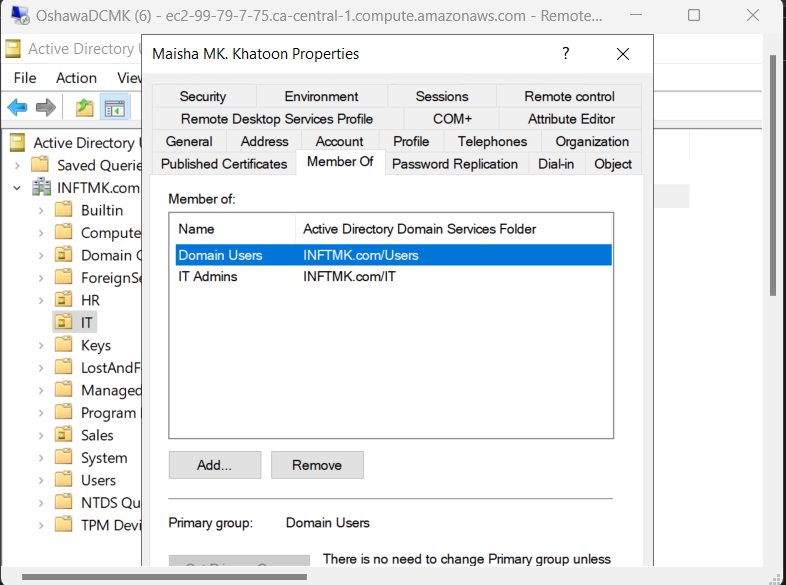
If your window server does not support “local users and groups” GUI, how can you achieve the same goal? Please describe briefly from below space and paste the screenshot here.

Ans: You can use either PowerShell or Command line to do this. Below is the command to do in to run in CMD. Make sure you in elevated mode “run as administrator”.

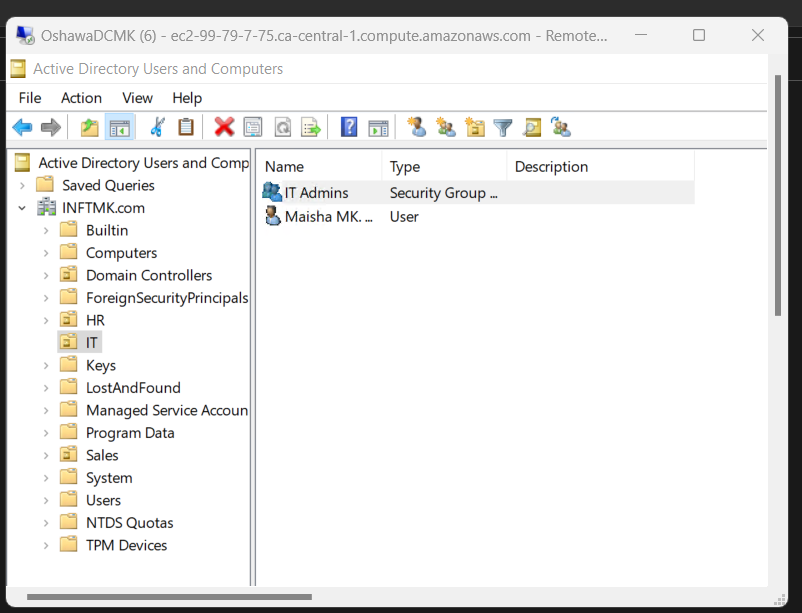
“net user Administrator /active:no”



1. Press Apply and close the window
2. On the **OshawaDC** open Active Directory Users and Computers
3. Locate the user account that you created for yourself in the Week 4 lab (step 9)
4. Right click > Properties
5. Click on the **Member Of** tab
   1. Take a screenshot and place it here

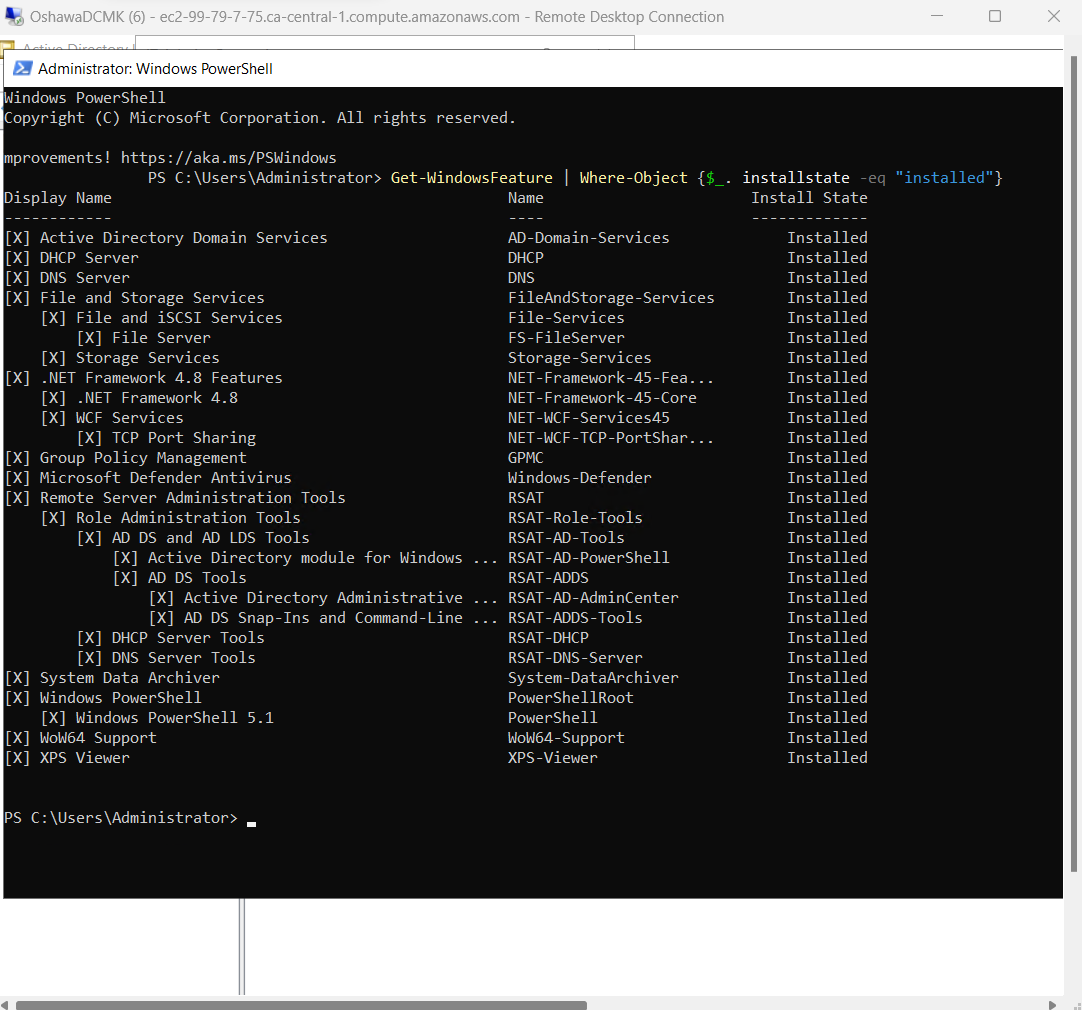


1. Close the user properties window
2. Open the **Groups** OU
3. Right click on the **IT Admins** group > Properties
4. Click on the **Members** tab
   1. Take a screenshot and place it here



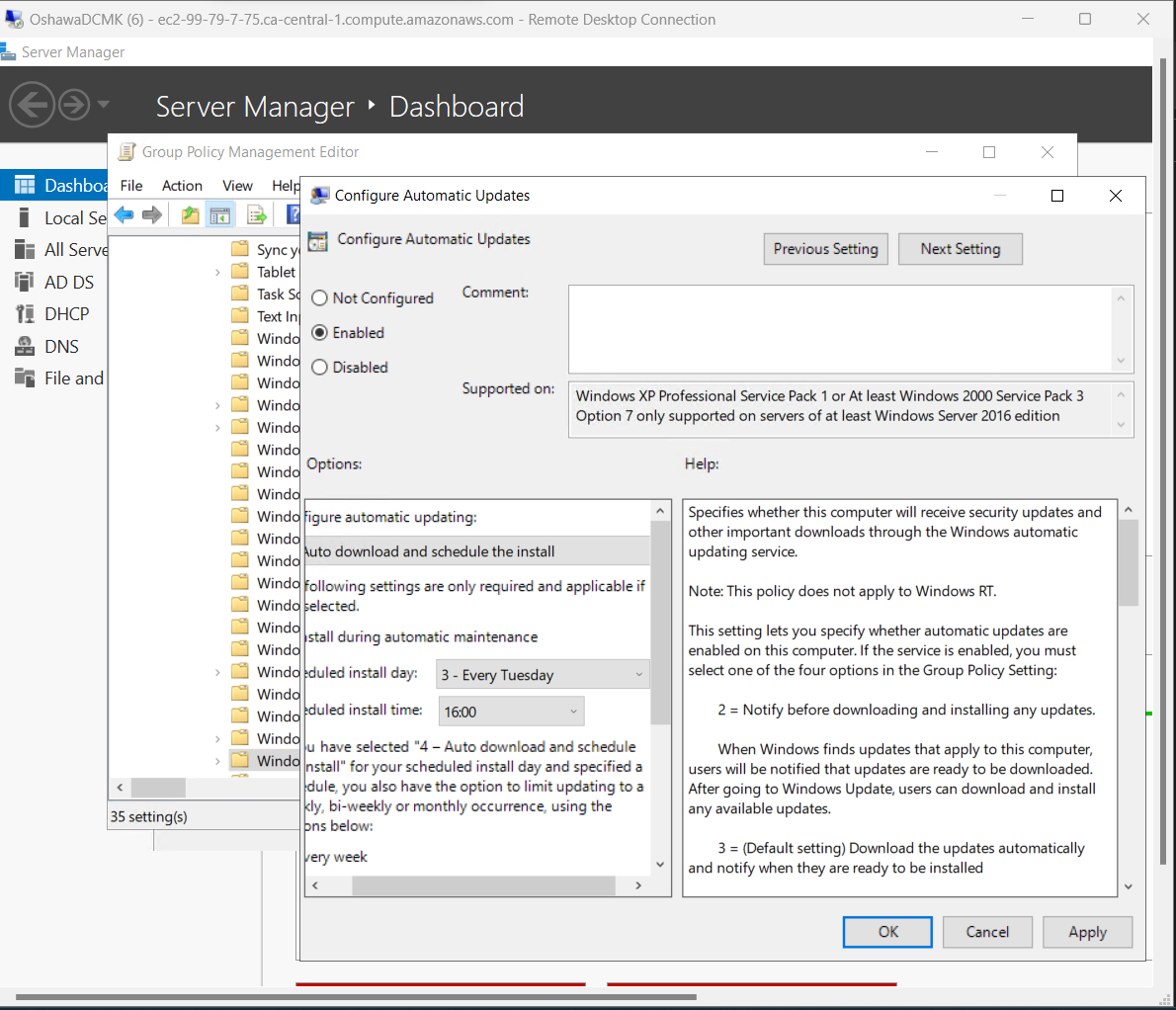
**Features and Roles Configuration**

1. On the OshawaDC open PowerShell
2. Run the following command: Get-WindowsFeature | Where-Object {$\_. installstate -eq "installed"}
   1. Take a screenshot and place it here

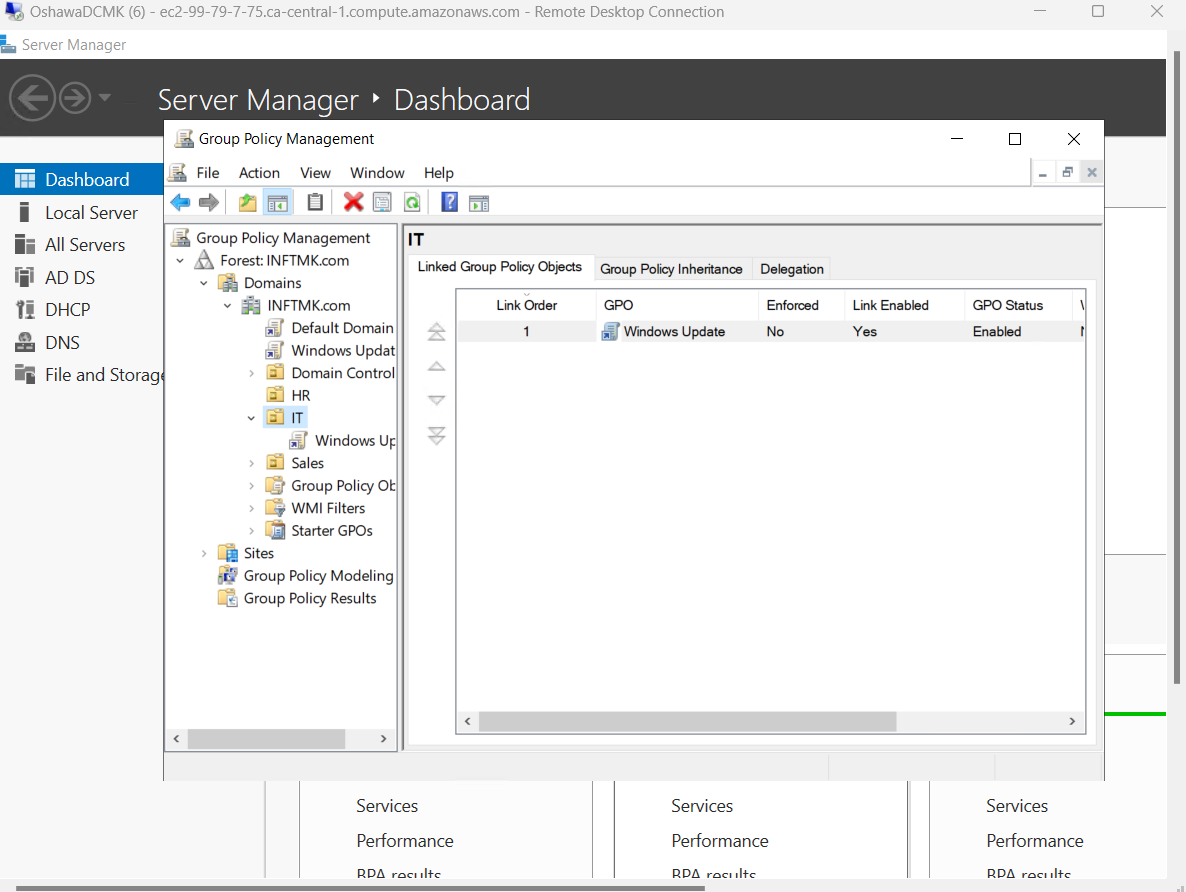


**Manage Server Updates**

1. On the OshawaDC open Group Policy
2. Under Group Policy Objects create a new policy objected called **Windows Update**
3. Right click the Windows Update policy and select **Edit**
4. Expand the following path: *Computer Configuration > Policies > Administrative Templates > Windows components > Windows Update*
5. Find the *Configure Automatic Updates* policy setting
6. Right click > Edit
7. Select **Enabled**
8. Configure the policy to *Auto Download and Schedule the Install*
9. Choose **Every Tuesday** at **16:00**
   1. Take a screenshot of your policy settings and paste it here

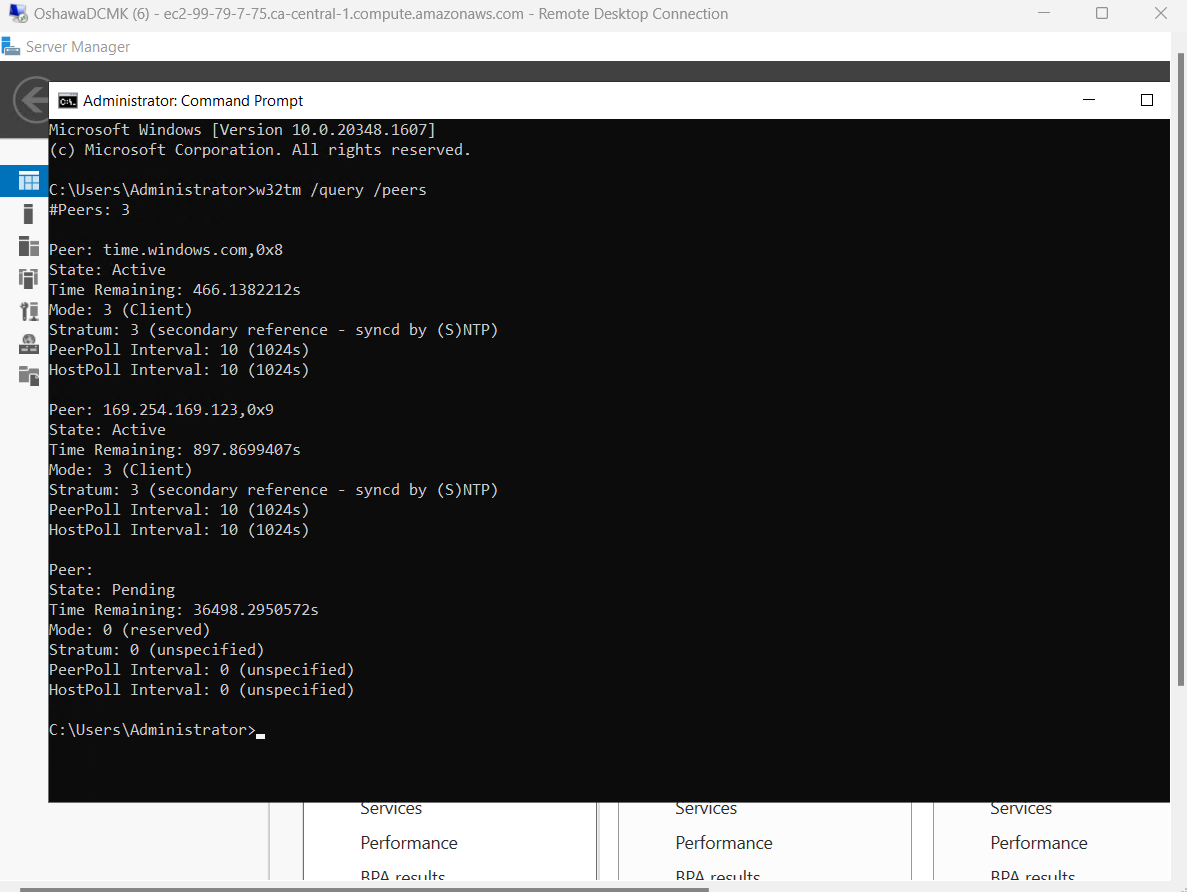


1. Find the OU containing the **FileServer** PC
2. Right click the OU and select “Link an Existing GPO….”
3. Select the Windows Update GPO and click OK
   1. The GPO should now show below the OU. Take a screenshot and paste it here



**NTP Configuration**

1. On the **OshawaDC** open command prompt (cmd)
2. Run the following command: *w32tm /query /peers*
   1. Take a screenshot of the response and paste it here

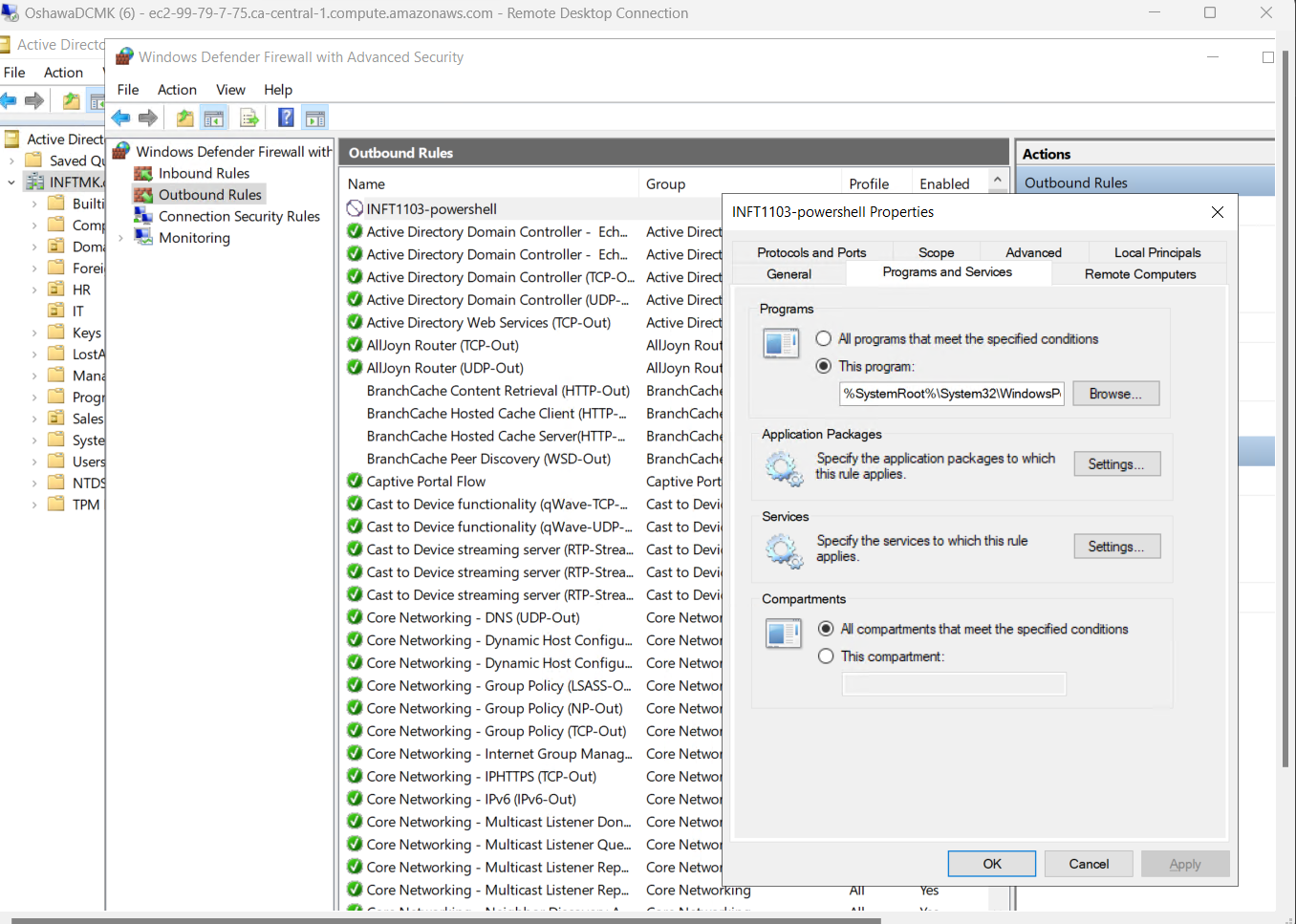


1. What is the output of your command prompt command indicated?

Ans: The command is used to display the list of time servers that a computer is configured to use for time synchronization. The output of the command will display the IP addresses or domain names of the time servers, along with their Stratum level and whether they are currently reachable.

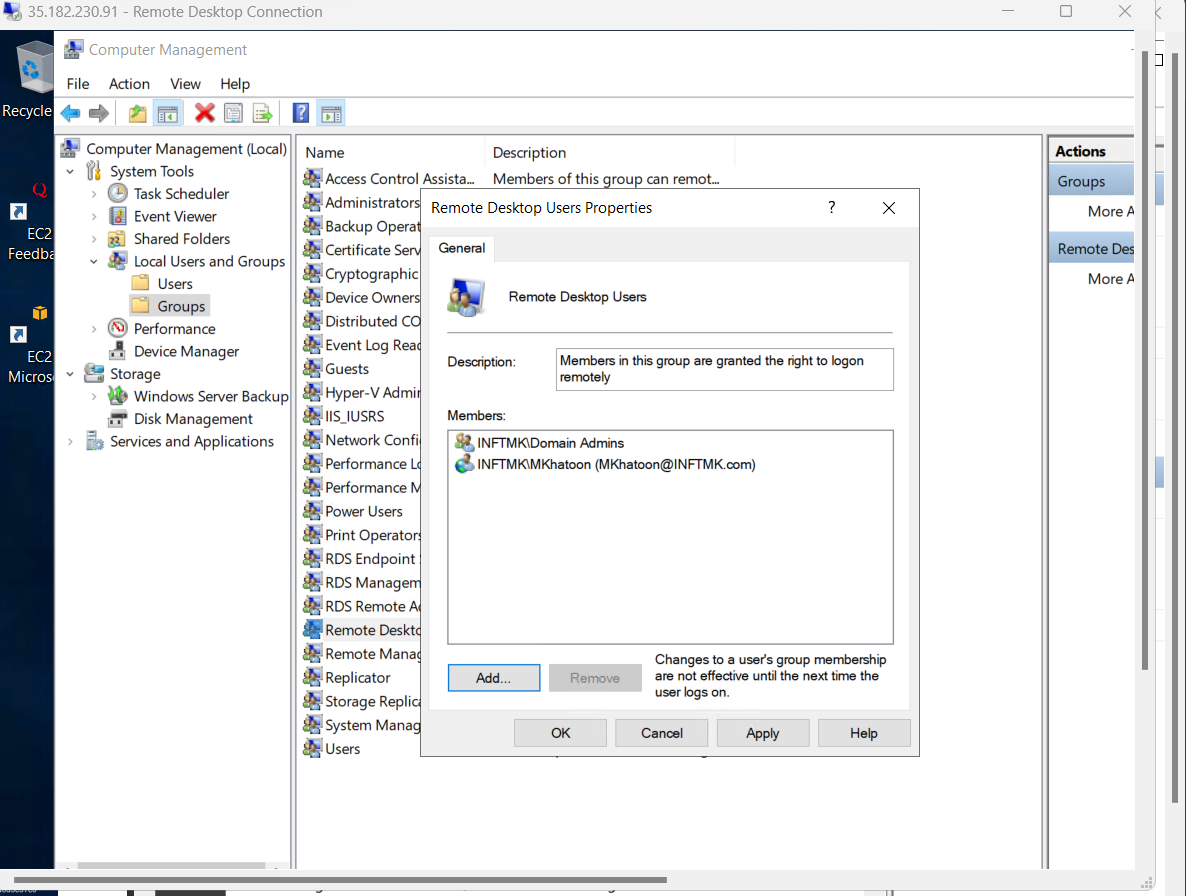
**Windows Firewall Configuration**

1. On the **OshawaDC** open server manager and ensure that your firewall setting is set to **Domain**
   1. If it is not, you may need to restart your NIC
2. Open **Windows Firewall** and select *Advanced Settings*
3. Right click **Outbound Rules** and select New Rule…
4. Select **Program**
5. Under *Program Path* select *Browse…* and browse to: *C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe*
6. Select *Block the connection*
7. Make sure that *Domain* is checked under the *When does this rule apply?* window
8. Under *Name* type: INFT1103-powershell
9. Select *Finish*
10. Right click on the *INFT1103-powershell* rule in your Outbound rule list and select *Properties*
11. Click on the *Programs and Services* tab
    1. Take a screenshot and paste it here



**Remote Access Configuration**

1. On the **FileServer** PC open *Computer Management*
2. Expand *Local Users and Groups* and select the *Groups* folder
3. Open R**emote Desktop Users** group and select *Add…*
4. Add *Domain Admins* group
5. Add the user account that you created in the Week 4 Lab (Question 9)
   1. Take a screenshot and paste it here

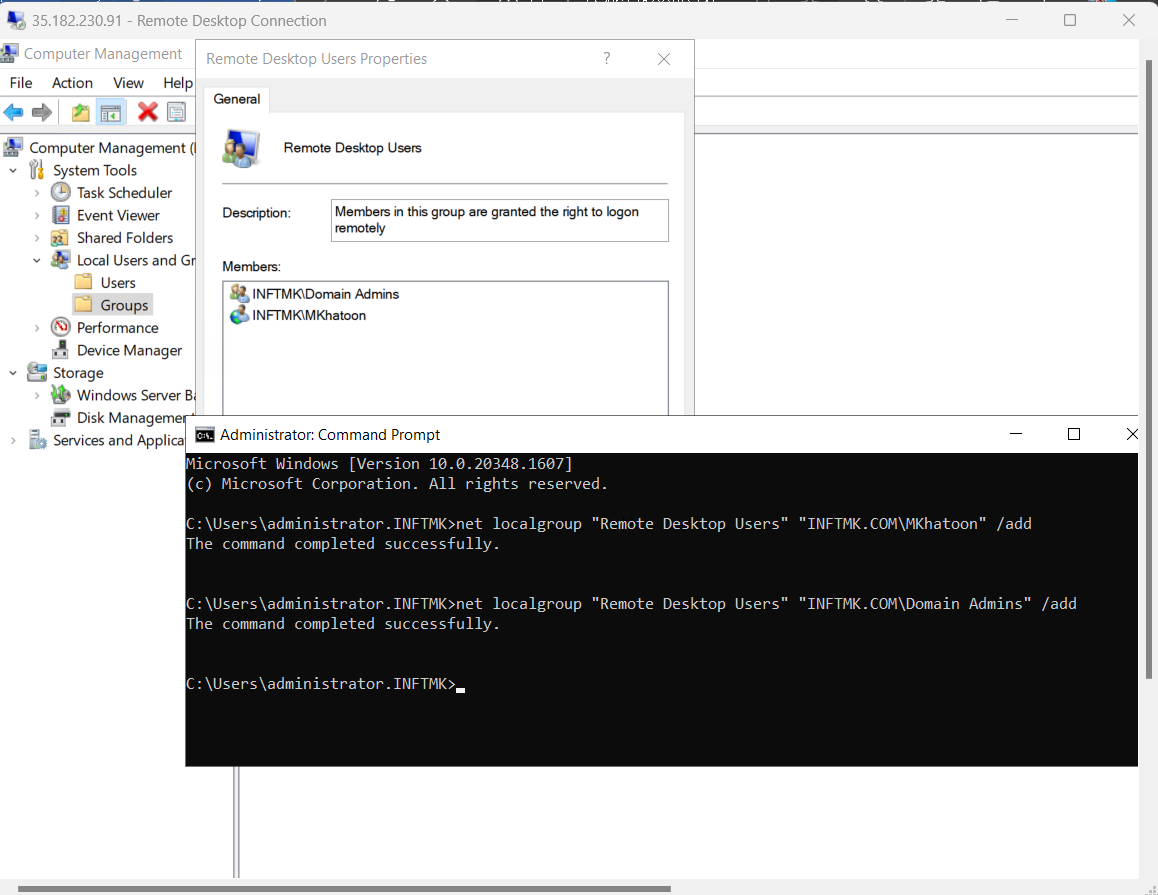


If your window server does not support “local users and groups” GUI, how can you achieve the same goal? Please describe briefly from below space and paste the screenshot here.

Ans: You can use the command line to add users to the group. (Run in elevated mode)

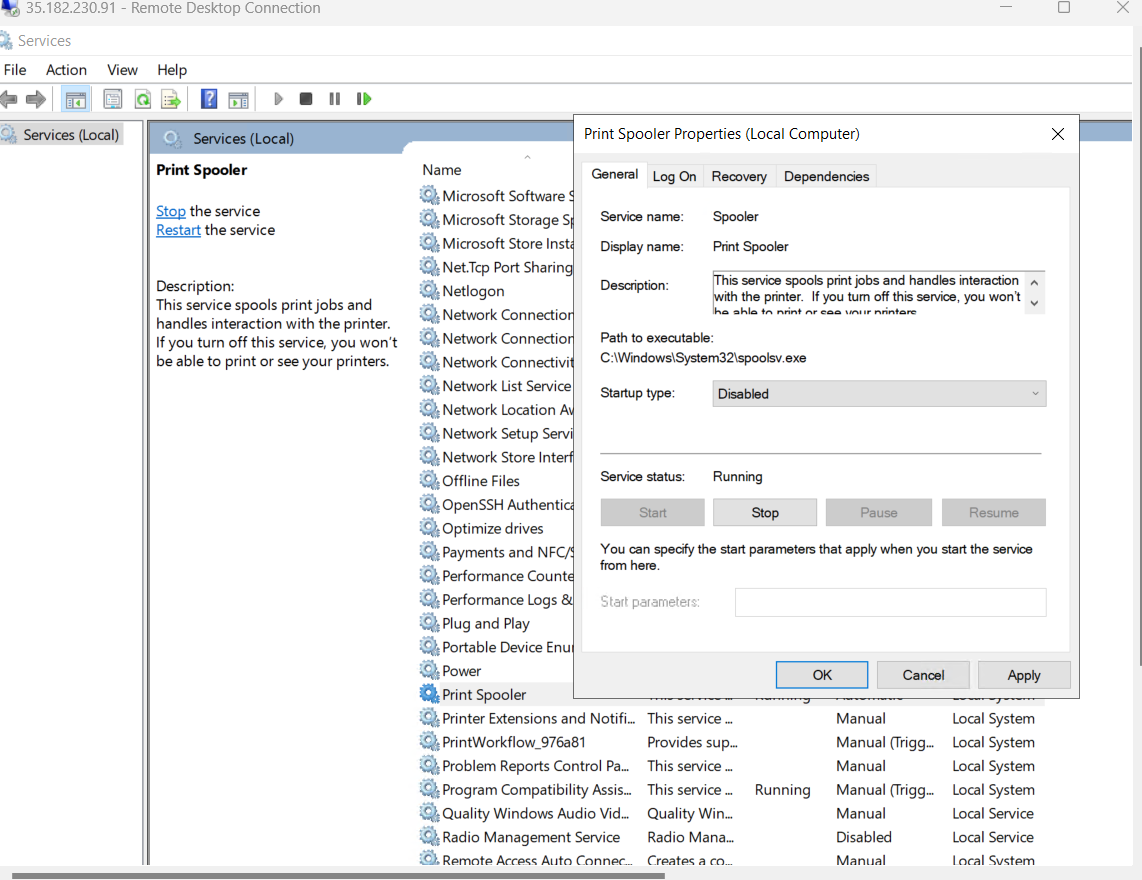
net localgroup "Remote Desktop Users" “INFTMK.COM\MKhatoon” /add

net localgroup "Remote Desktop Users" "INFTMK.COM\Domain Admins" /add



**Service Configuration**

1. On the **FileServer** PC, open *Services*
2. Find the *Print Spooler* service and right click and select *Properties*
3. Change the startup type to *Disabled*
   1. Take a screenshot and paste it here



**Logging and Monitoring**

1. On the **OshawaDC** open *Event Viewer*
2. Expand *Windows Logs*
3. Right click *Application* and select Properties
4. Change the Maximum log size to: **30480**
   1. Take a screenshot and paste it here

