LAB 04 – Windows

By :- Faraz Ahmed

Contents

1. Join Win10Client and IISServer VMs to Your Team Domain

- Go to Settings option in Win10Client, select “About” and then select “Rename this PC (advanced)” as highlighted in Figure 1.

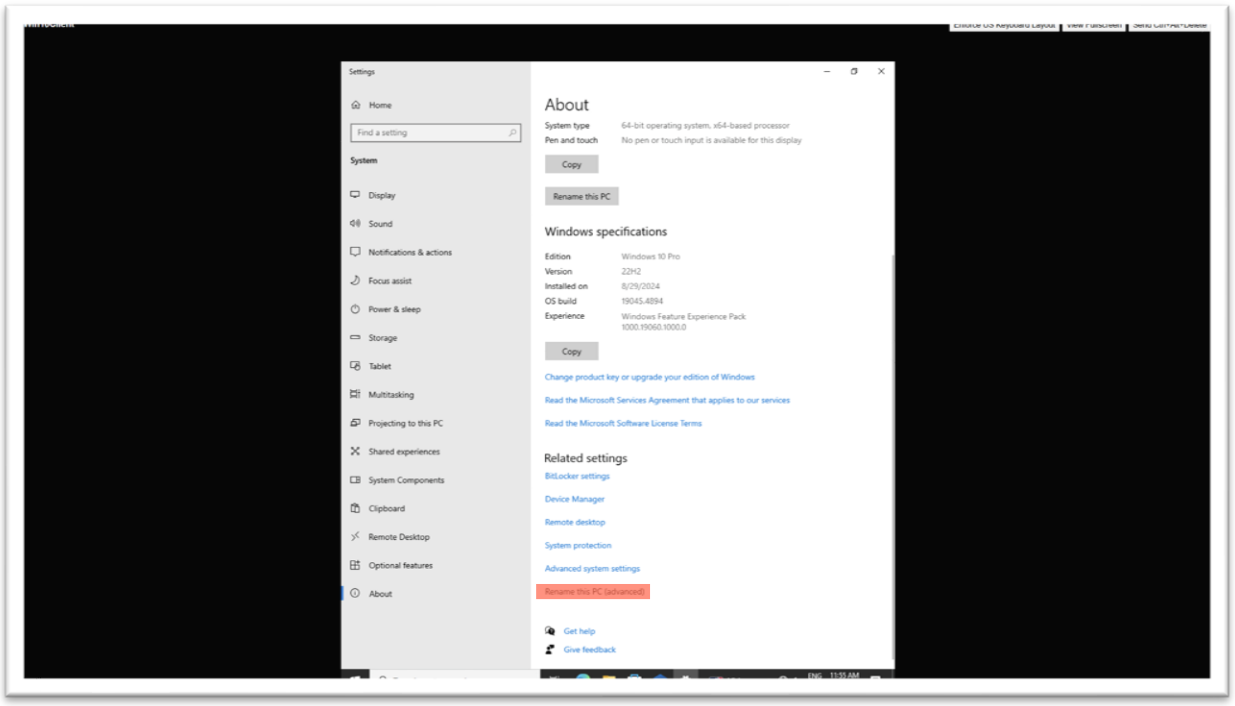

Figure 1: Screenshot of “Rename this PC option” in About section.

- Then write computer name to “Win10Client” and in member of domain put “team32.local” to make Win10Client join team domain as shown in Figure 2. Then press OK.

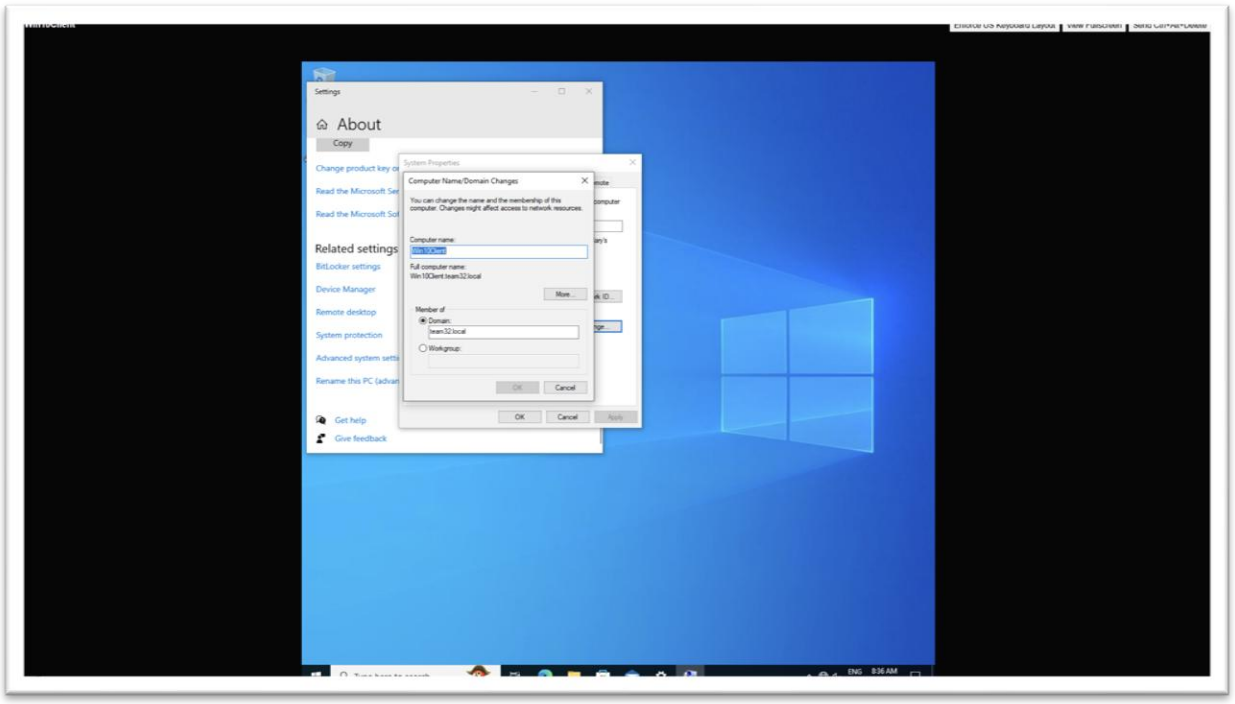

Figure 2: Screenshot of Computer name/domain changes window.

- As we can see the computer's name and the domain is changed which we can observe in Figure 3.

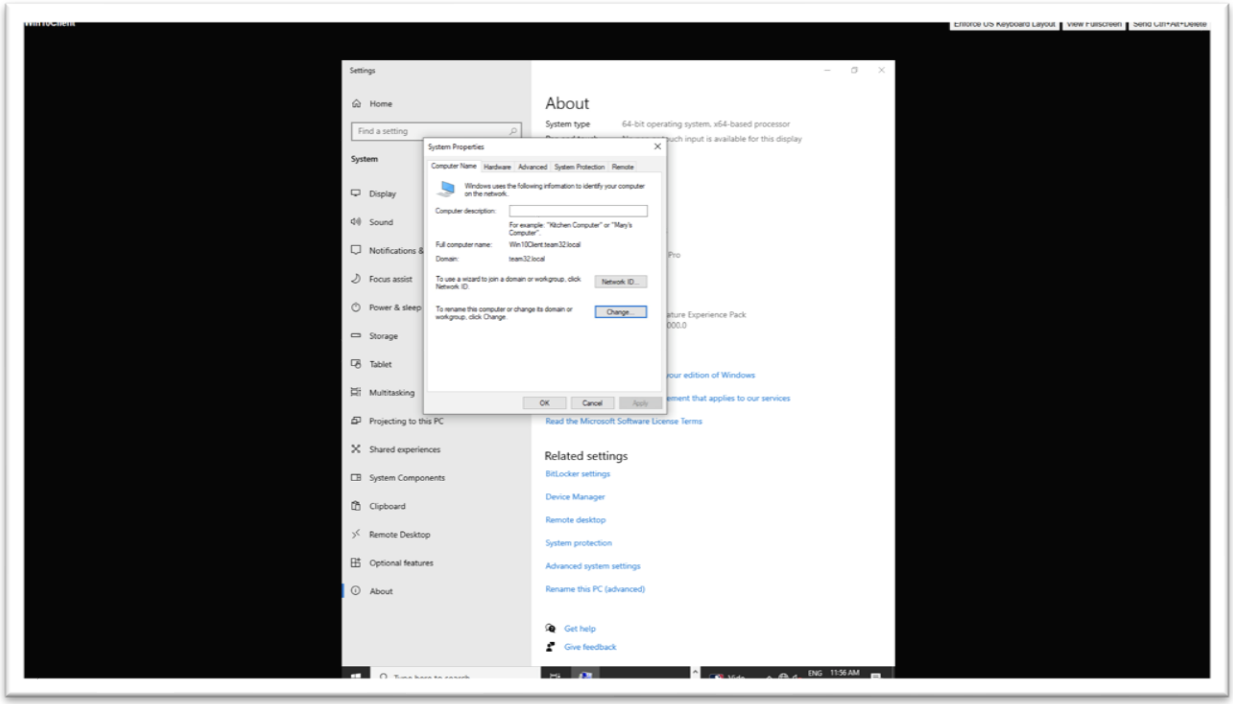

Figure 3: Screenshot of System Properties to check computer name and domain.

- Then we select "Properties" dialog in the "This Computer" to check the overall changes made to the name and domain of the Win10Client which we can observe changes as highlighted in Figure 4.

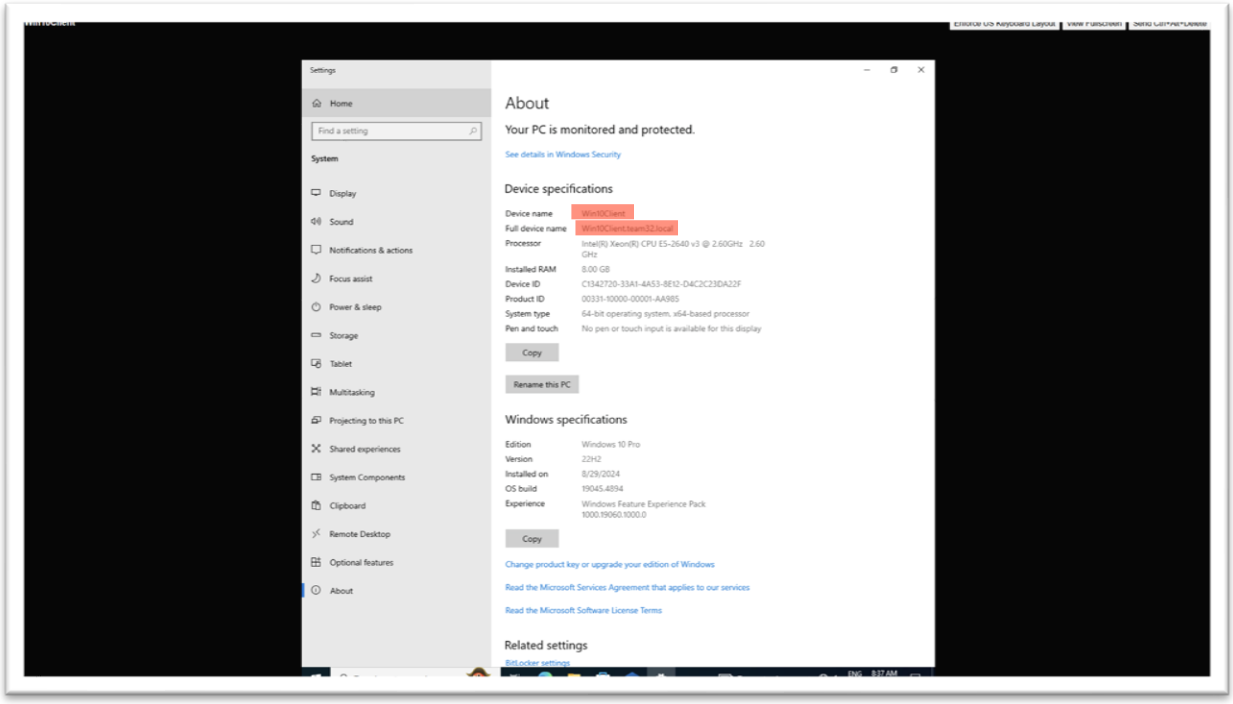

Figure 4: Screenshot of "Properties or About" section to confirm changes made.

- Below we can observe the properties or “SConfig” of IISServer VM where we can verify the changes made to “computer name and domain name” as highlighted in Figure 5.

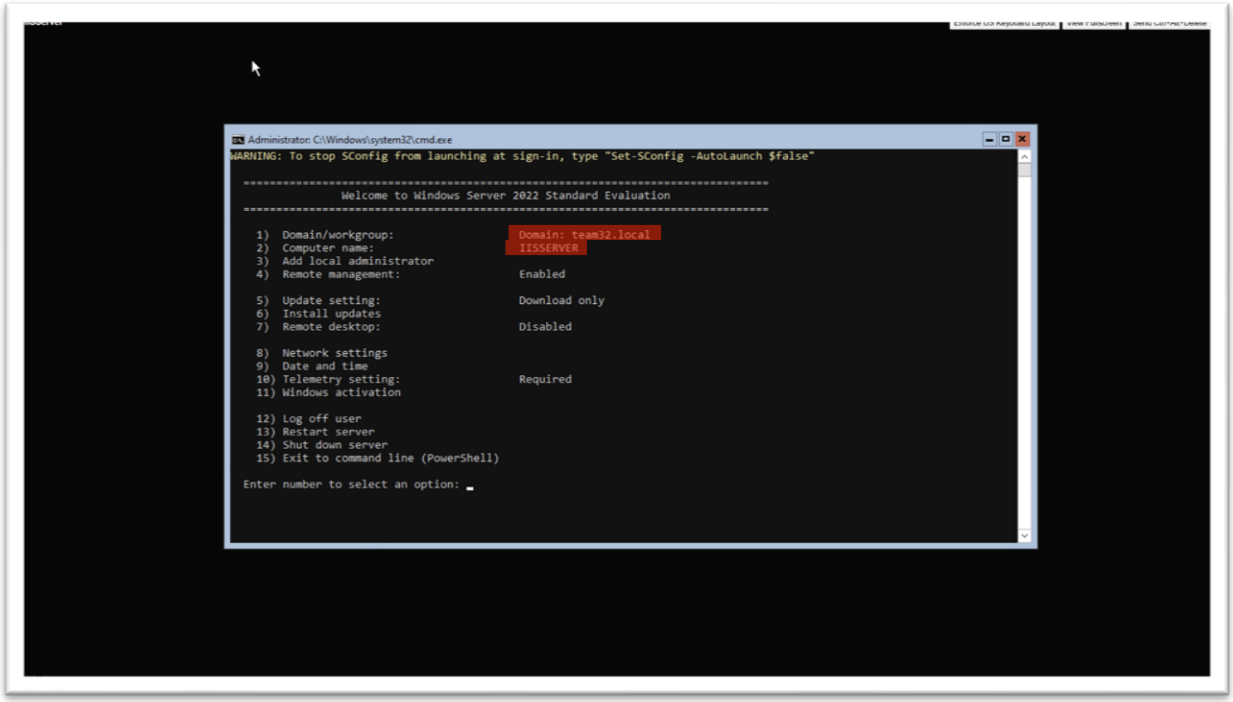

Figure 5: Screenshot of “SConfig” to check changes in Computer’s name and domain.

2. Create Two Users on Your Team Domain

- Go to search bar and type “Active Directory Users and Computers” and select it in ADServer as shown in figure 6.

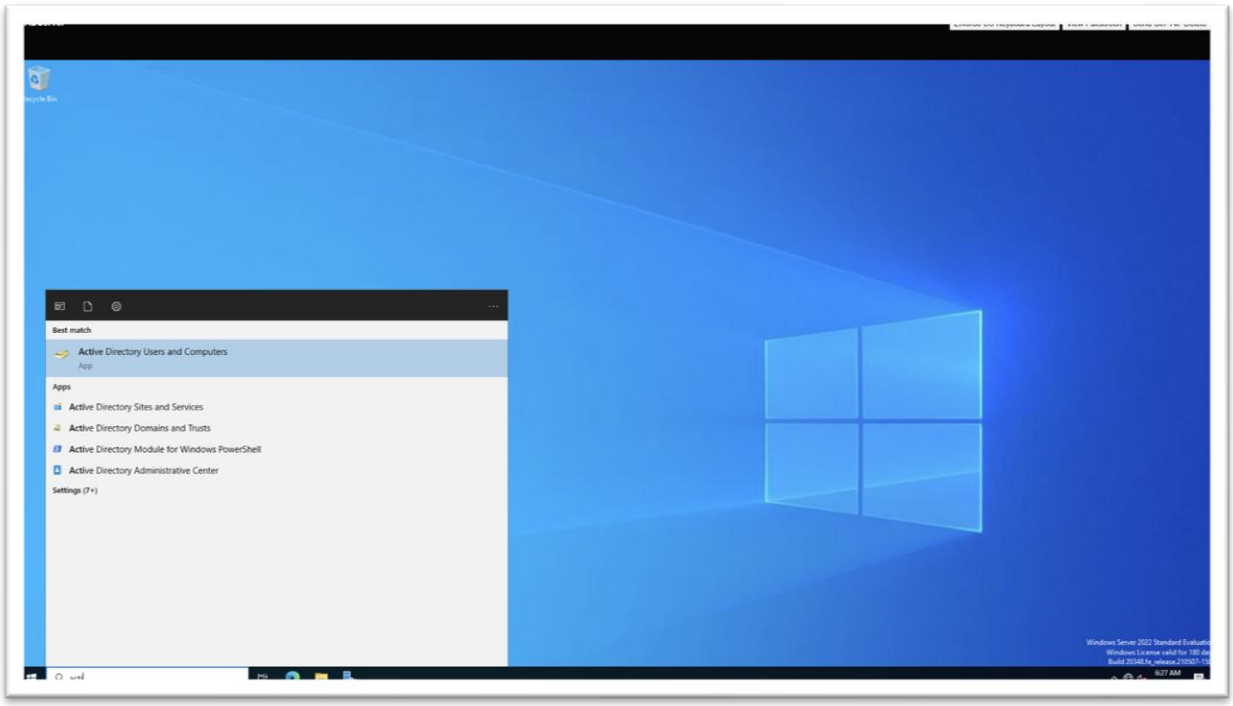

Figure 6: Screenshot of path to “Active Directory Users and Computers”.

- As we can observe the team domain “team32.local” on the left side, select it then go to “Users” and right click it then select “New” and then select “User”.

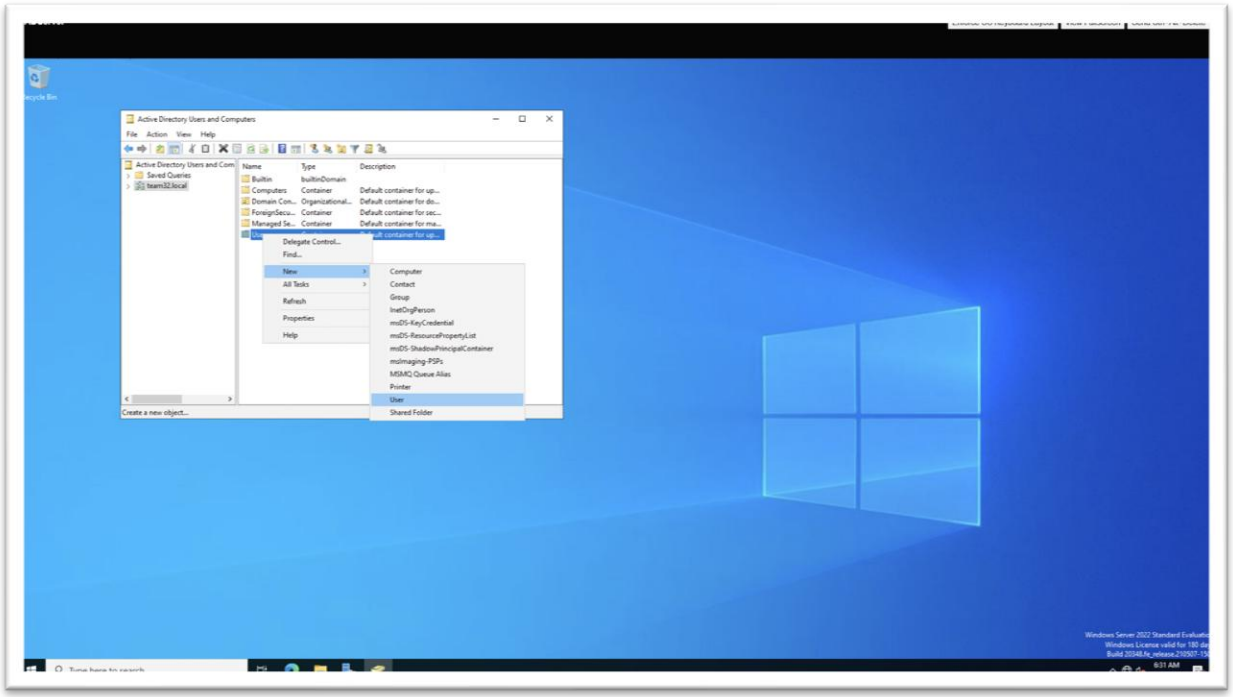

Figure 7: Screenshot of where to go to create a “New User” in team domain.

- Now enter “Kevin” in first name and also type “Kevin” in user login name as shown in Figure 8. Then press next.

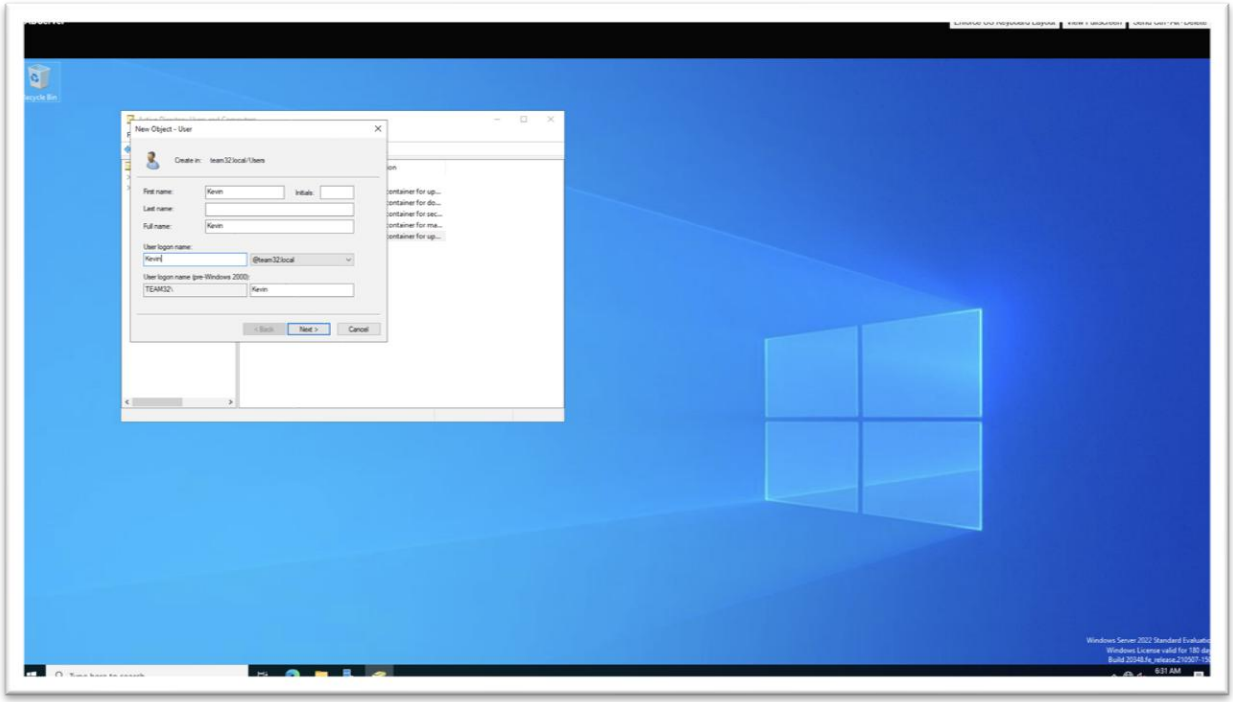

Figure 8: Screenshot of typing name and user login of new user “Kevin”.

- Then create the password “Change.me!” and uncheck “User must change password at next login” and press next.

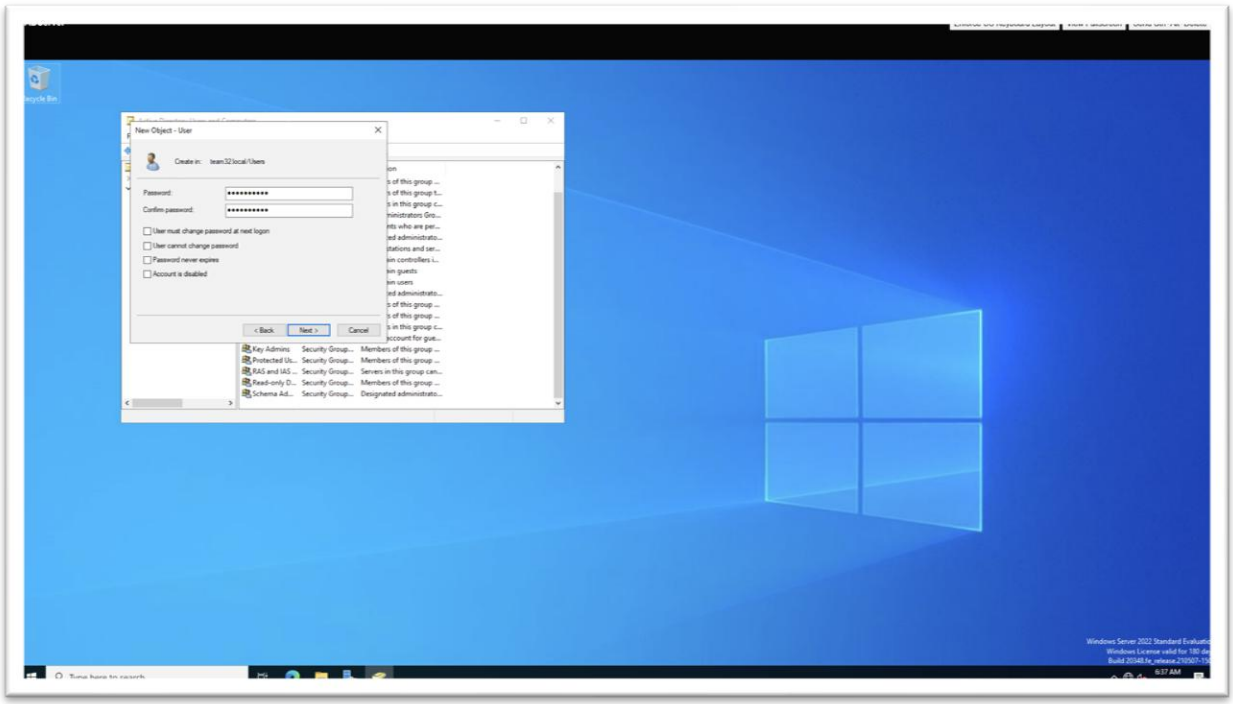

Figure 9: Screenshot of creating a new password “Change.me!”.

- As we can see in figure 10, the new user “Kevin” is created.

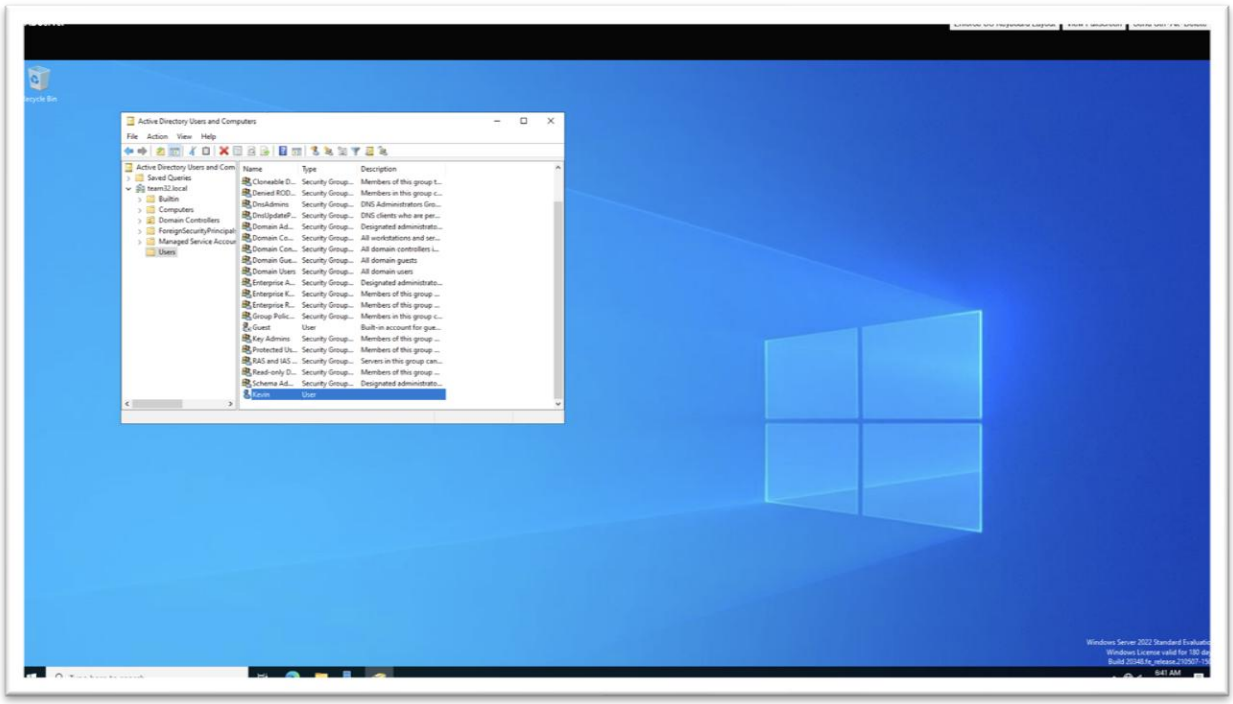

Figure 10: Screenshot of new user “Kevin” is created.

- Now to give admin control to “Kevin”, we will right click it and select properties as shown in figure 11.

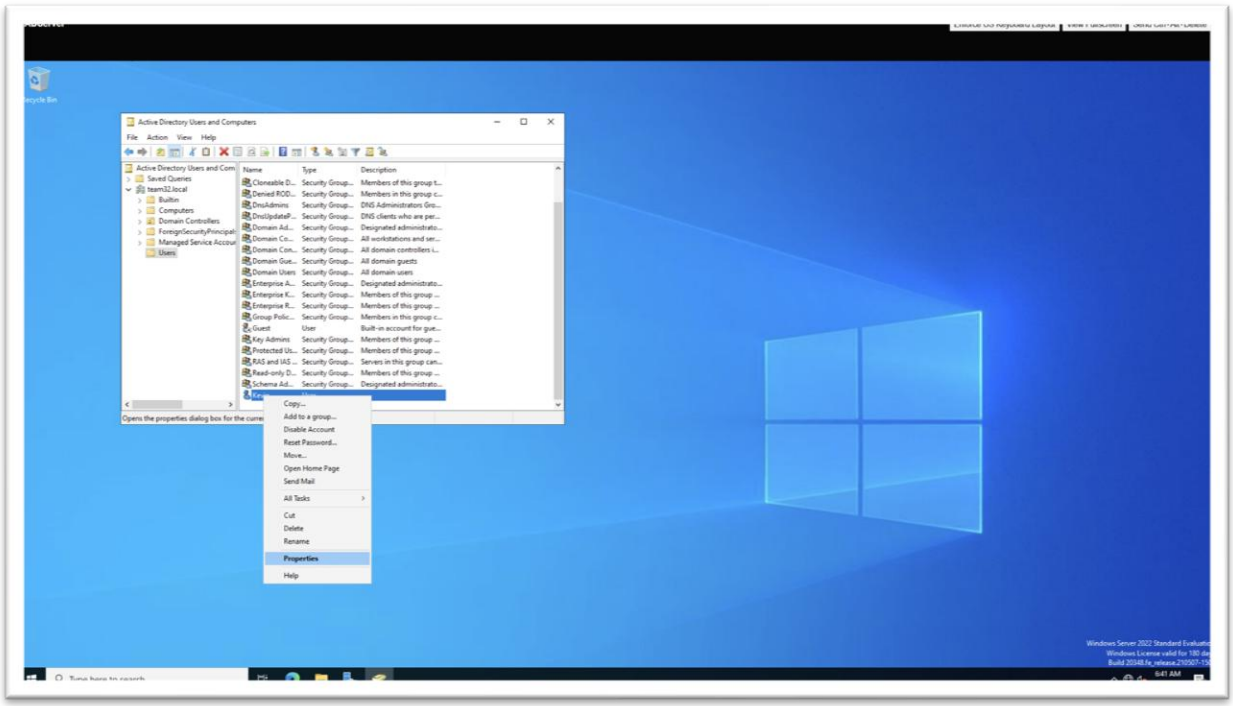

Figure 11: Screenshot of option of properties in Kevin.

- As we can see there is already domain users access to “Kevin” which we can remove as we will anyway give domain admin access. Now click “Add” .

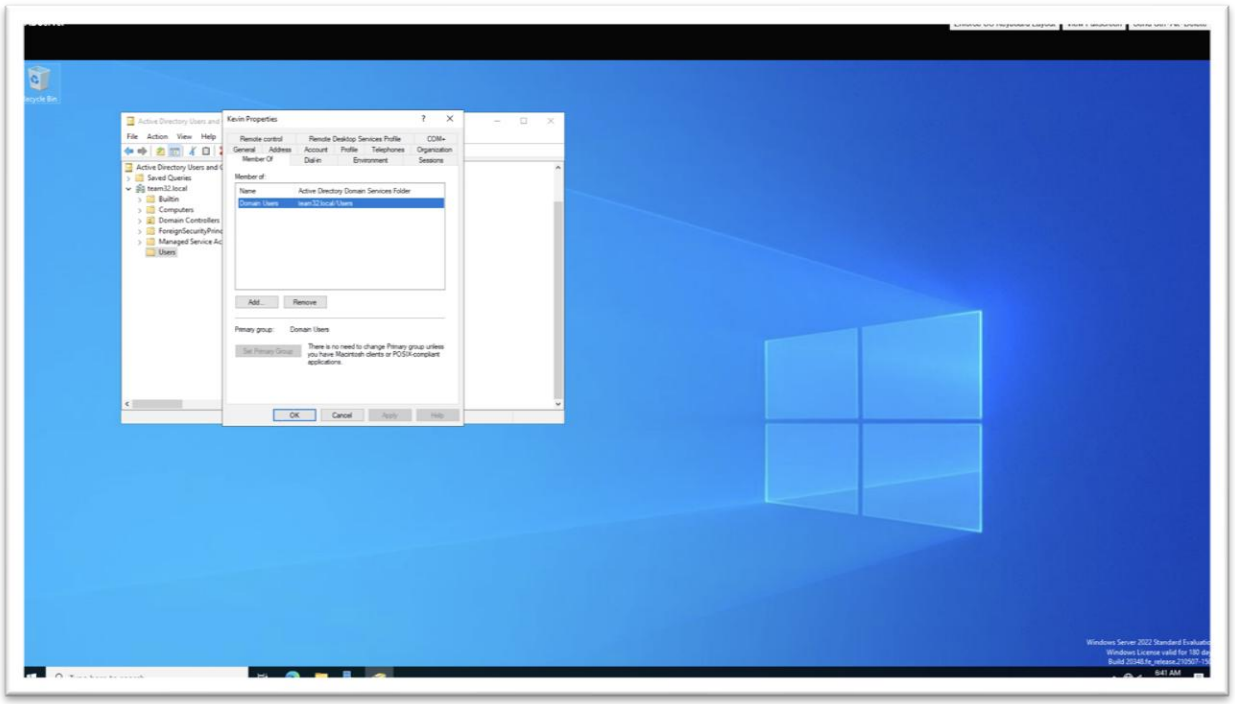

Figure 12: Screenshot of Kevin Properties to add domain admin.

- Now type “Domain Admins” and click “Check Names”. If the typed words gets “underlined” then it’s the right object name and we can select ok to proceed.

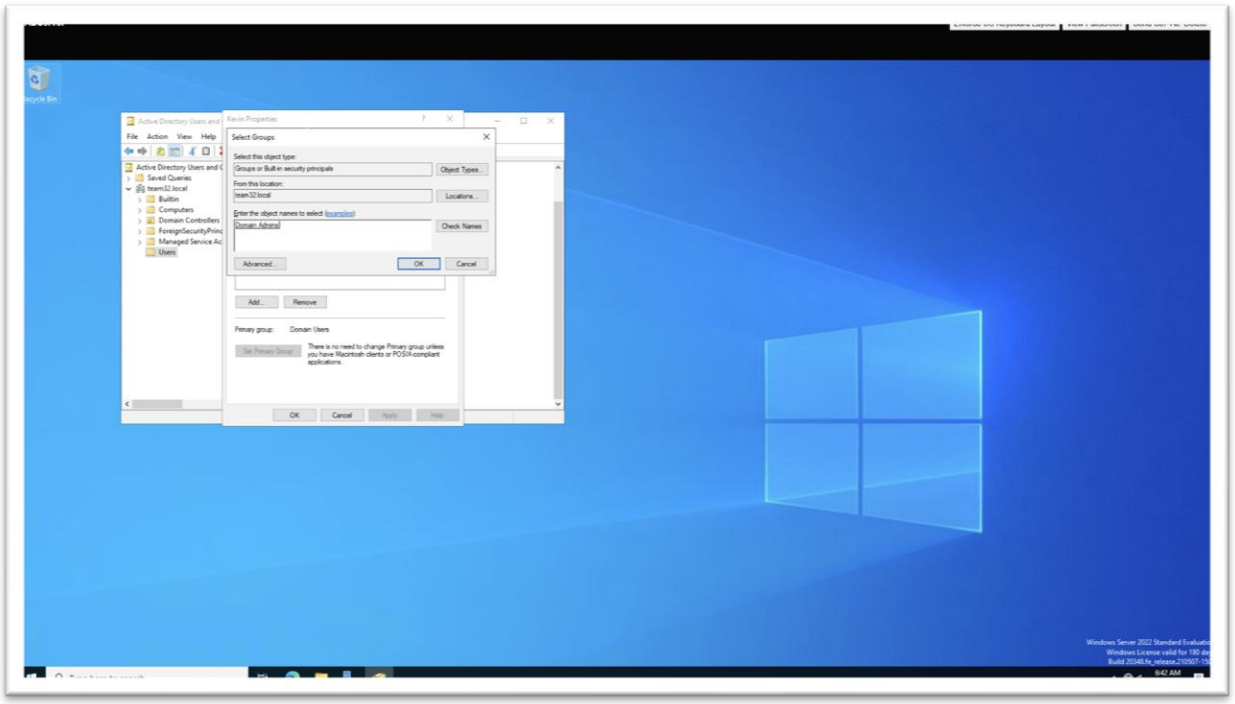

Figure 13: Screenshot of entering “Domain Admins” in object names.

- Now we can see “Domain Admins” in Members of. Now, click OK as in Figure 14.

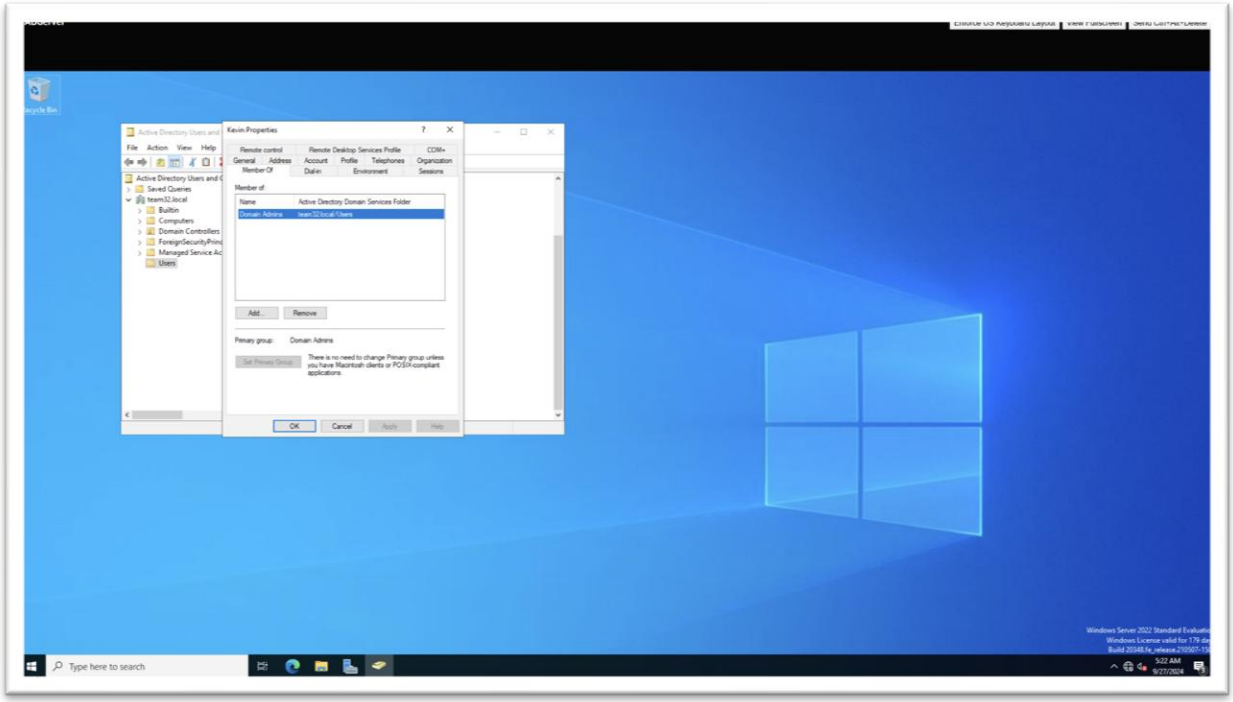

Figure 14: Screenshot of “Domain Admins” in Member of.

- Now follow the same steps which we used to create “Kevin” for creating “Dave CEO” as shown in figure 15,16 and 17.

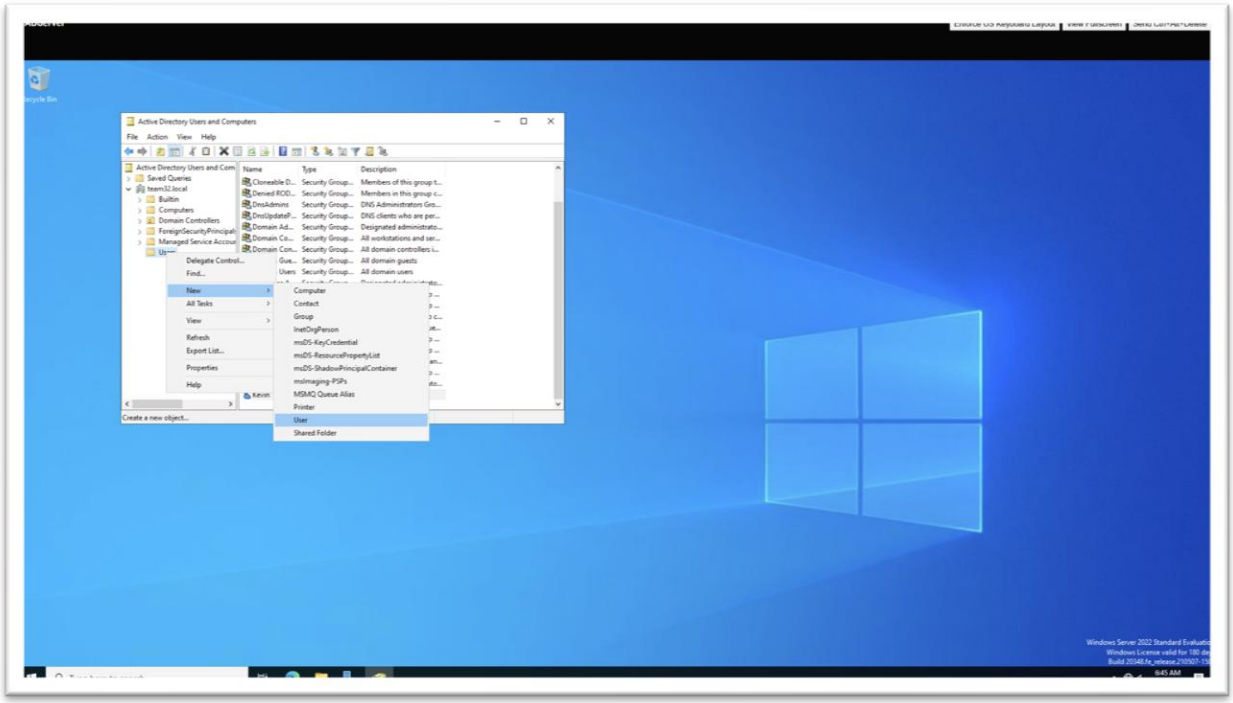

Figure 15: Screenshot of path to creating “New User”.

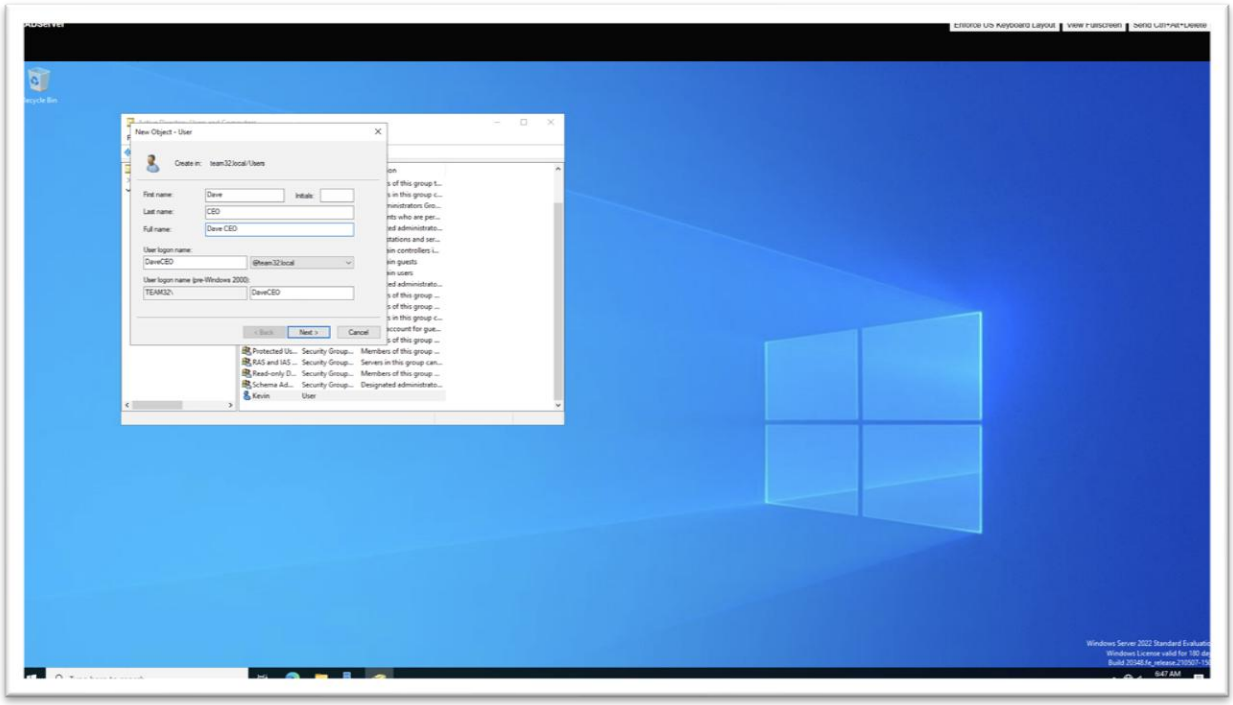

Figure 16: Screenshot of naming the name users as "Dave CEO".

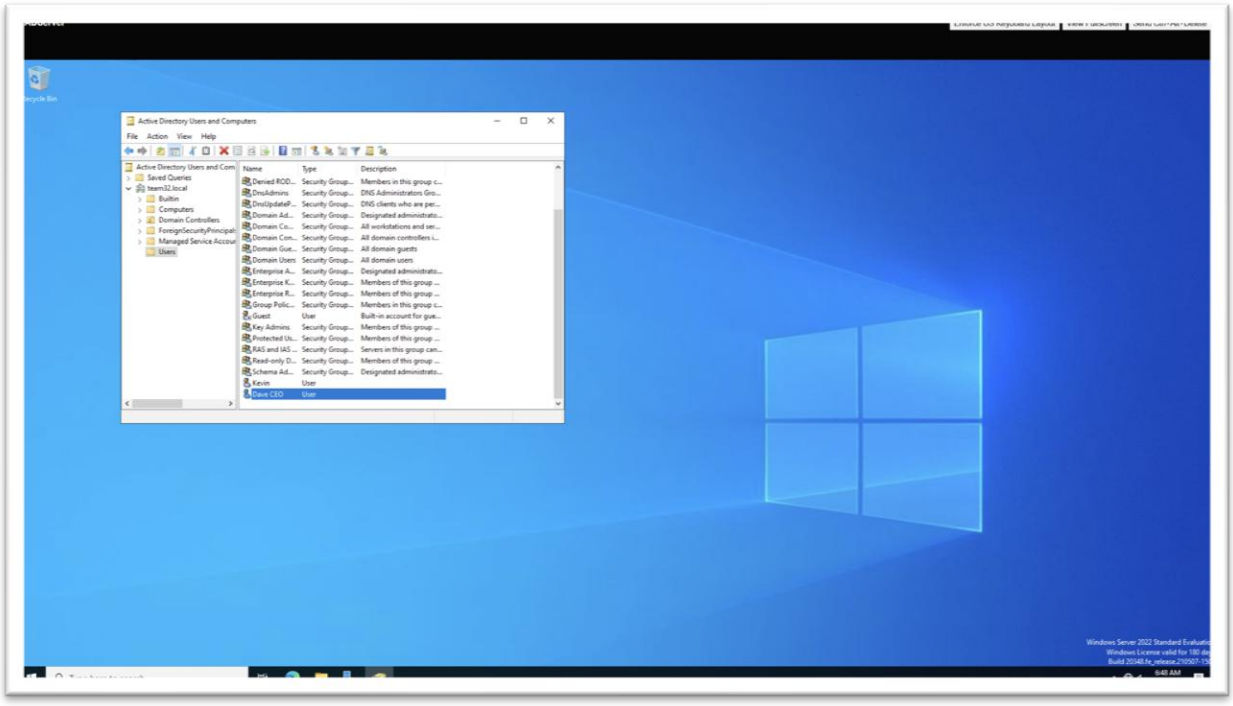

Figure 17: Screenshot of New User "Dave CEO".

3. Add IISServer to the ADServer Server Pool

- Open Server Manager, then select “Manage” on top right and then click “Add Server”.

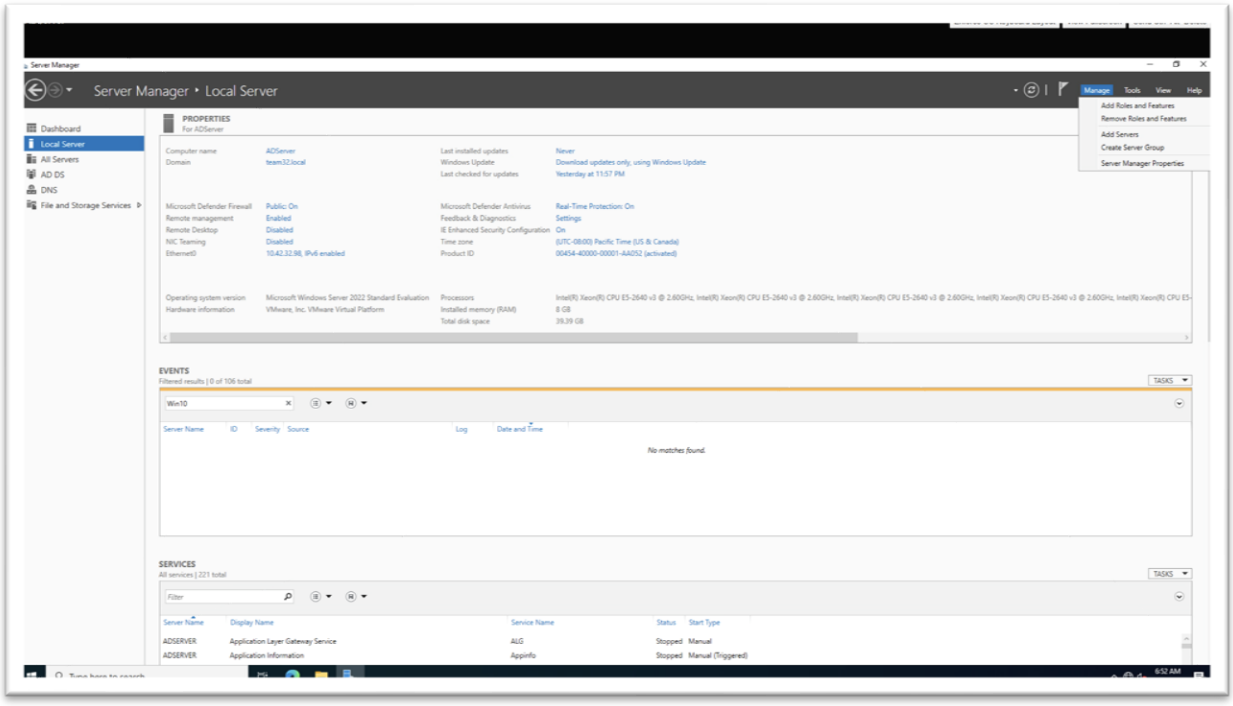

Figure 18: Screenshot of Server Manager

- Then select “IISServer” to add its server and press OK.

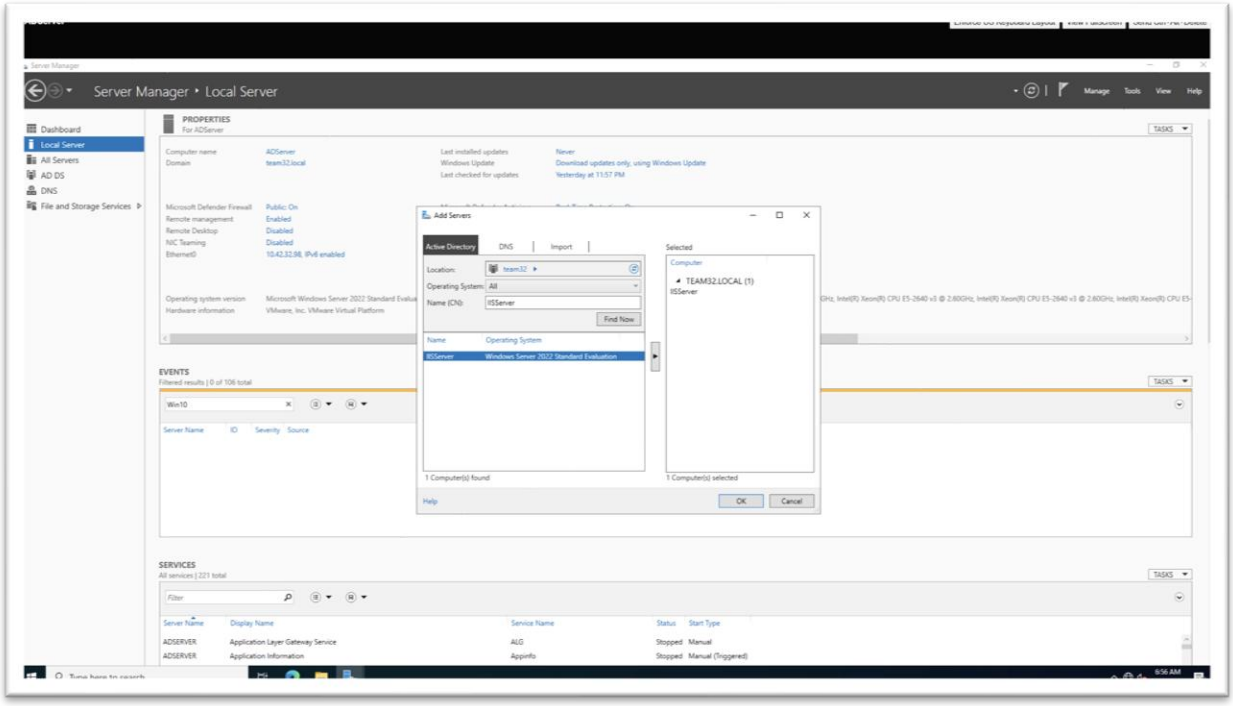

Figure 19: Screenshot of Add Server to add “IISServer”.

- Now we to go to “All Servers” and under servers we can check that “IISServer” servers is there or not. We can observe that it shows “Online” status as highlighted in Figure 20.

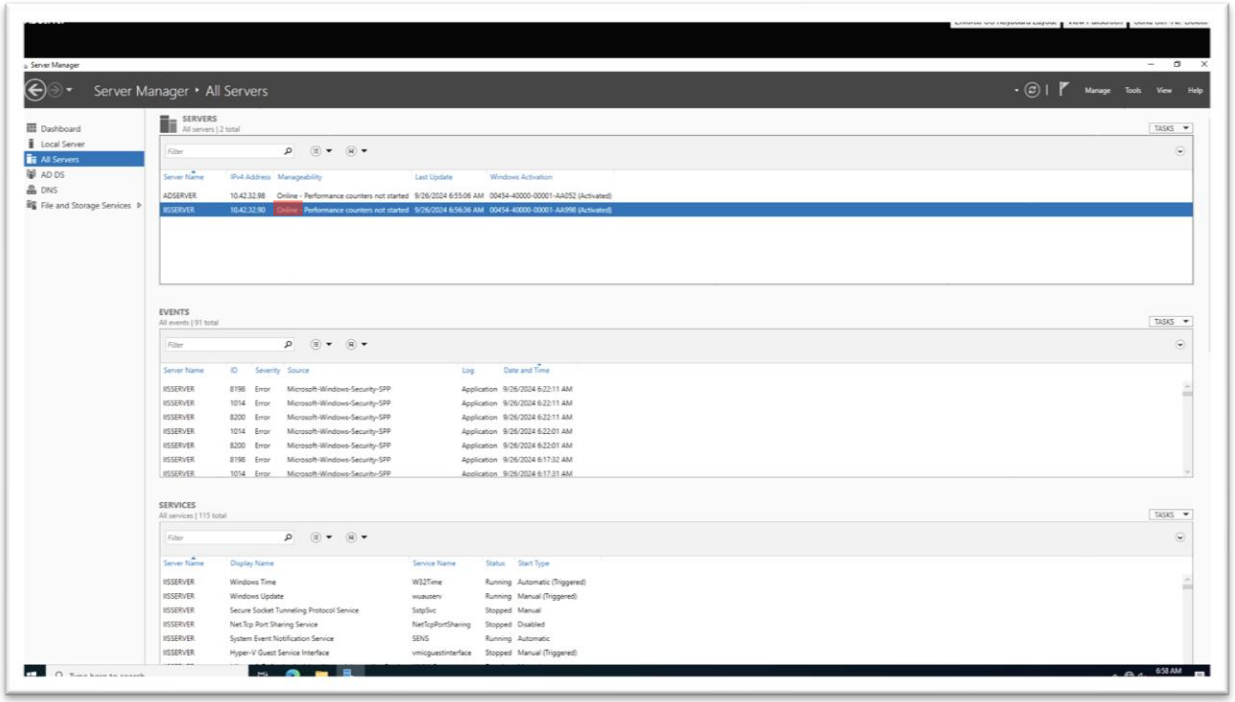

Figure 20: Screenshot of All Servers to check “IISServer server”.

4. Install an “Internet Information Services” Web Server on IISServer

- Open Server Manager and then select “Manage” from top right then click “Add Roles and Features” as shown in Figure 21.

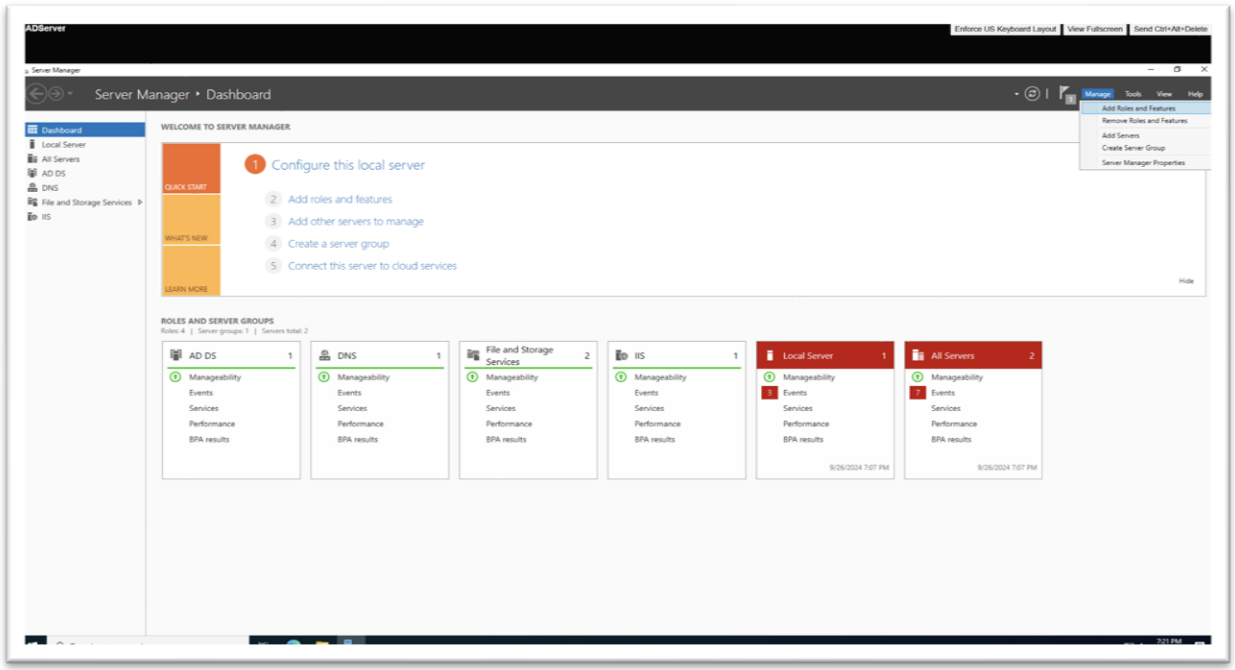

Figure 21: Screenshot of path to “Add Roles and Features”.

- Then click Next for first page. And on Installation Type, “Role-based or feature-based installation” then press next.

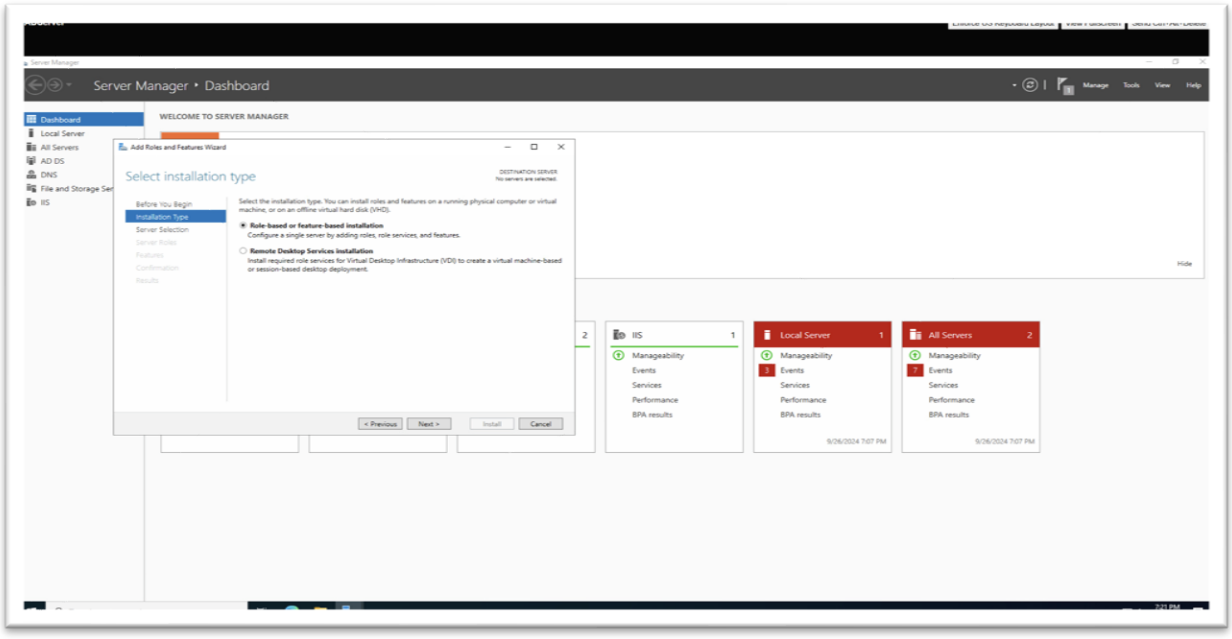

Figure 22: Screenshot of “Installation Type” and select Role based.

- Now, select “IISServer.team32.local” to configure “IIS on IISServer”.

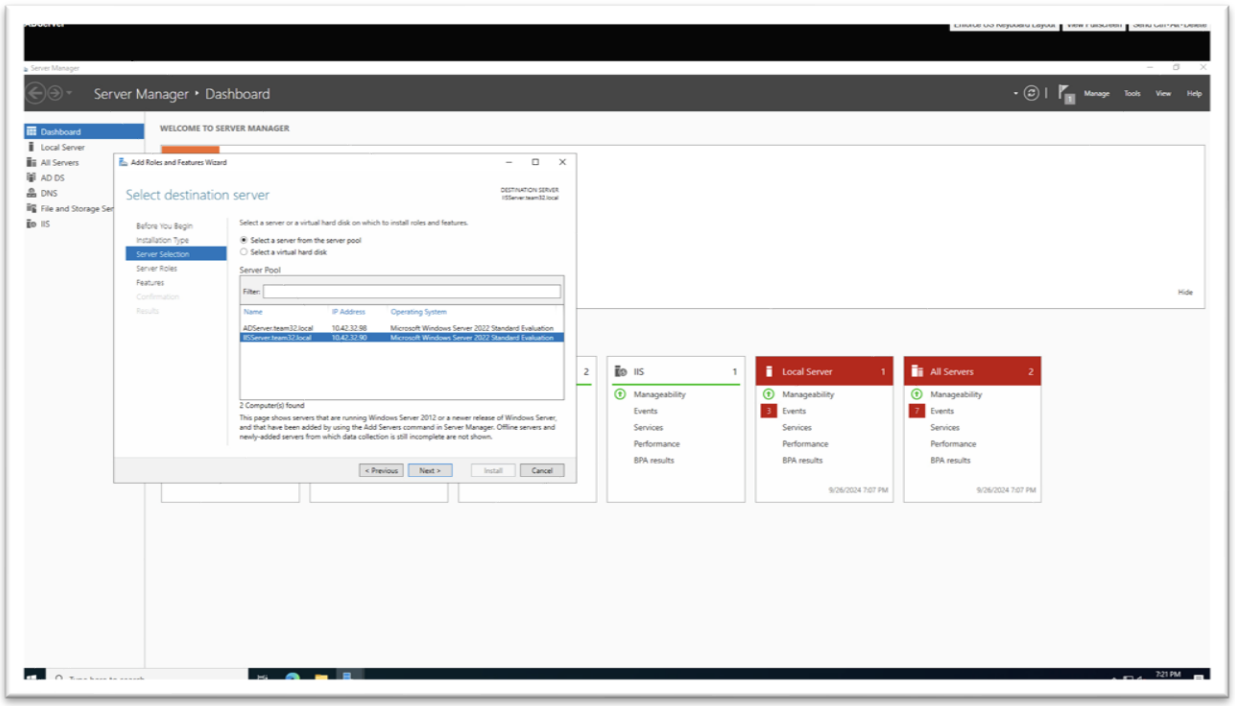

Figure 23: Screenshot of Server Selection to select “IISServer.team32.local”.

- Now in Server Roles, select “Web Server” check box and press next.

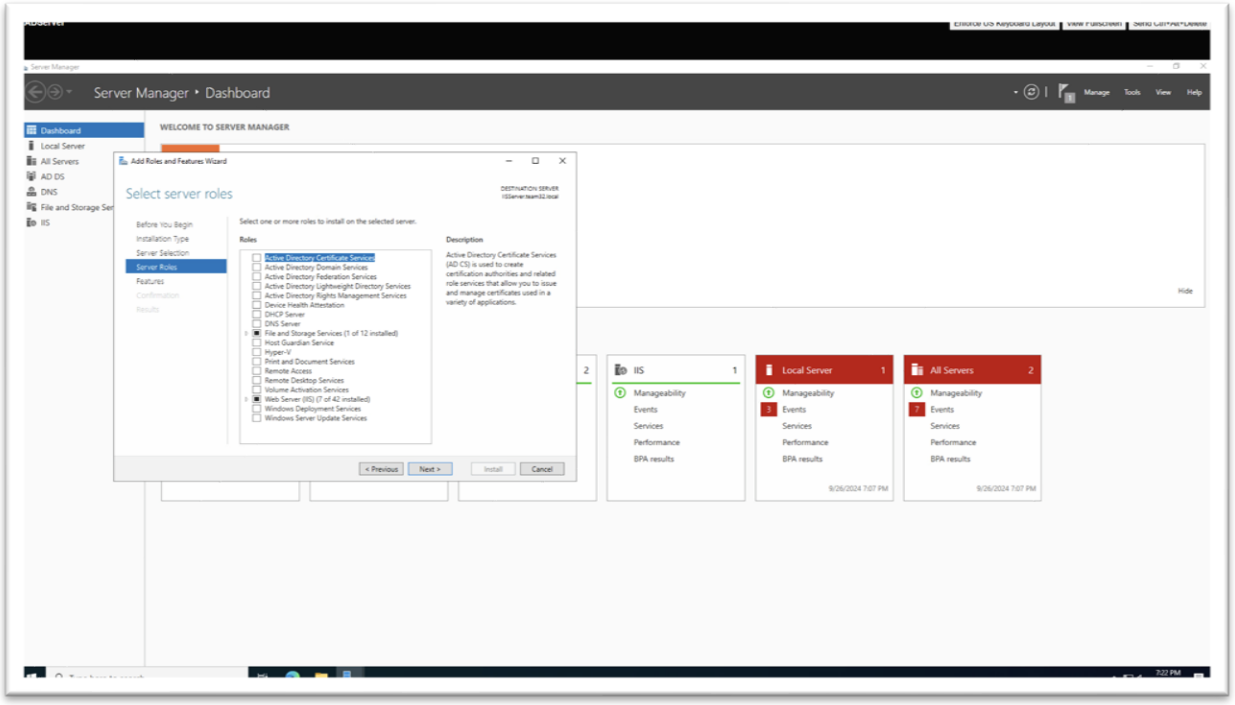

Figure 24: Screenshot of Server Roles to select “Web Server”.

- Now select “Install” option in features as highlighted in Figure 25.

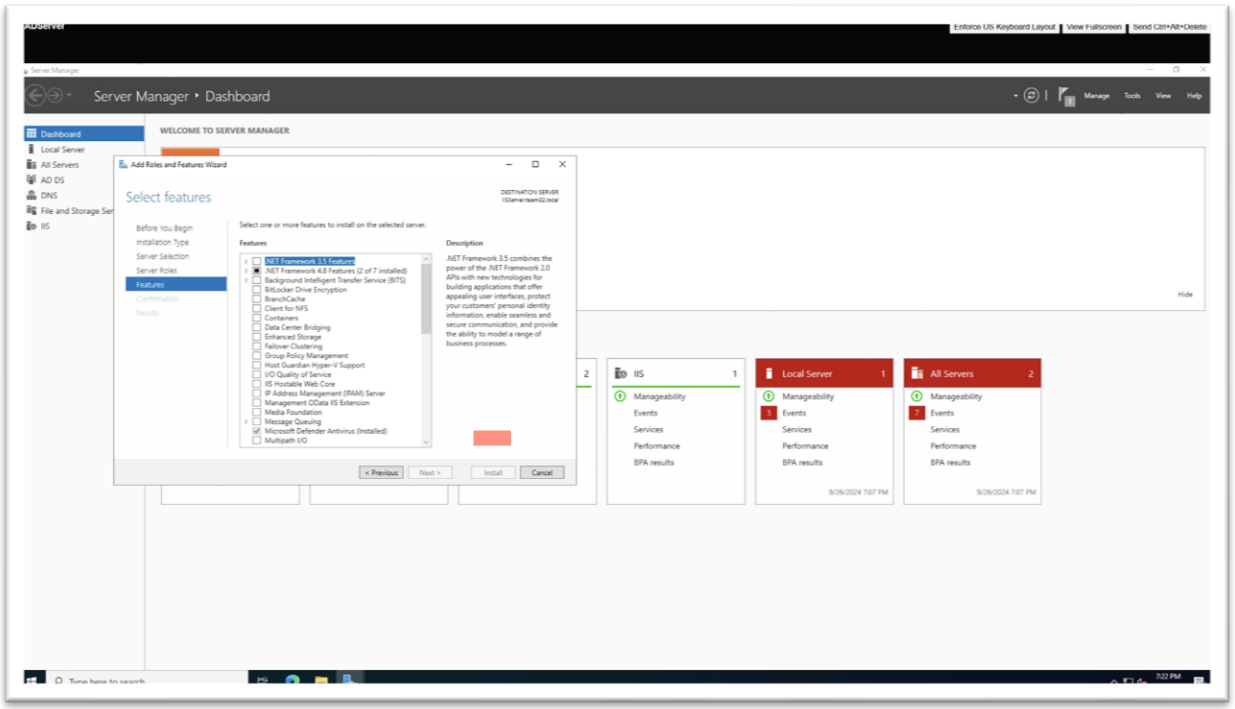

Figure 25: Screenshot of Features tab to start “Install”.

- As we can see in Figure 26, we can access webpage which is hosted by IISServer on OutsideDevice by entering “IP-10.42.32.90”.

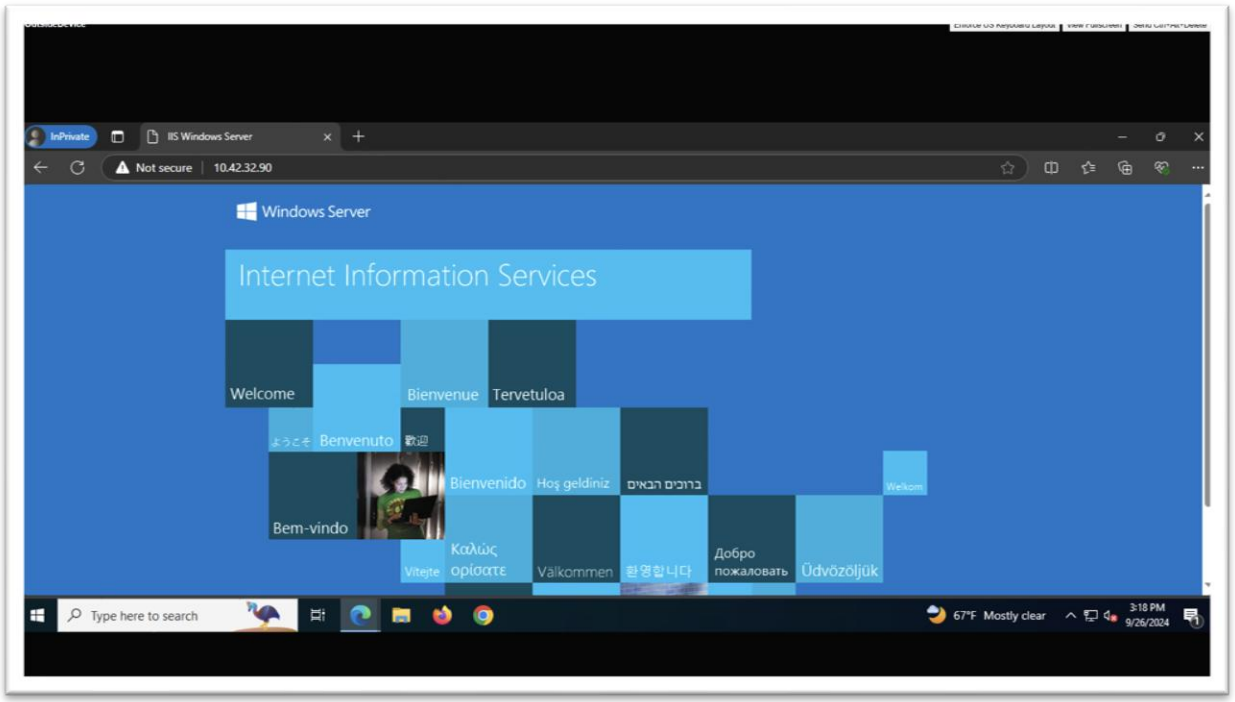

Figure 26: Screenshot of Webpage “hosted by IISServer” on OutsideDevice.

- As we can observe below in Figure 27, the firewall rule which helped us connect OutsideDevice to webpage hosted to IISServer.

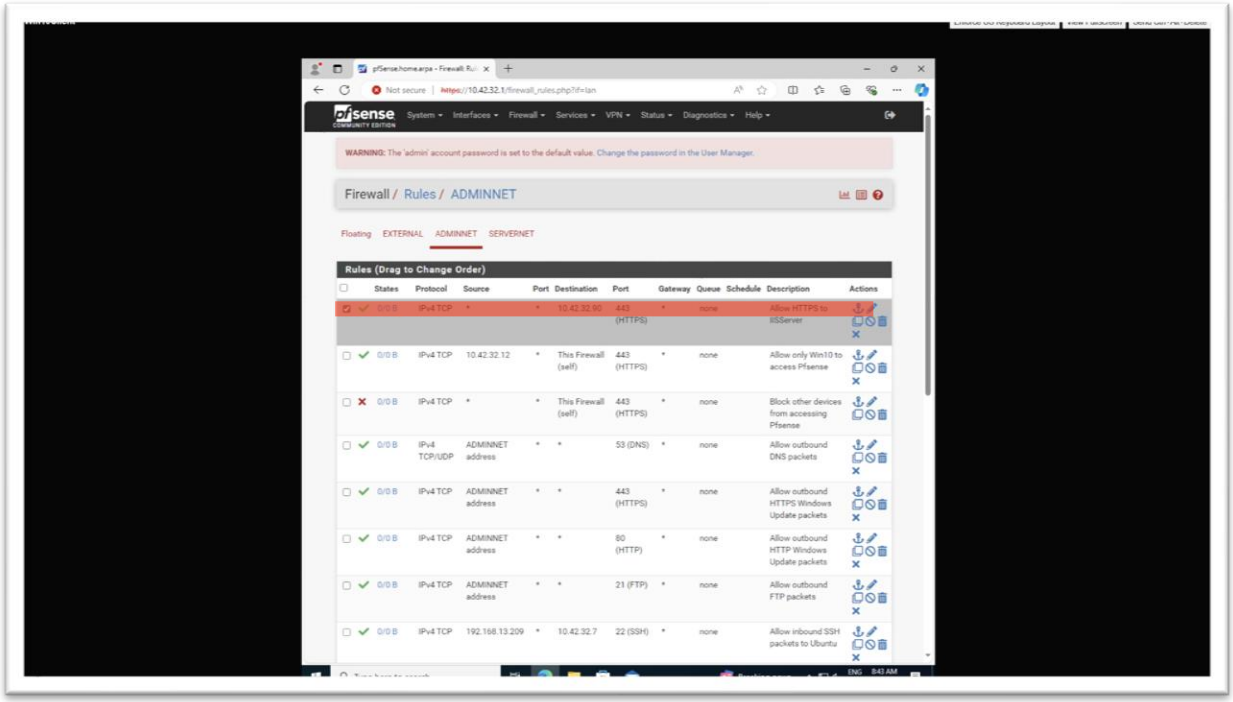

Figure 27: Screenshot of Firewall Rule to connect "OutsideDevice to webpage hosted to IISServer".

5. Create Groups

- Open “Active Directory Users and Computers” then select domain “team32.local” and right click on “Users” then click “New” and then “Group” as shown in Figure 28.

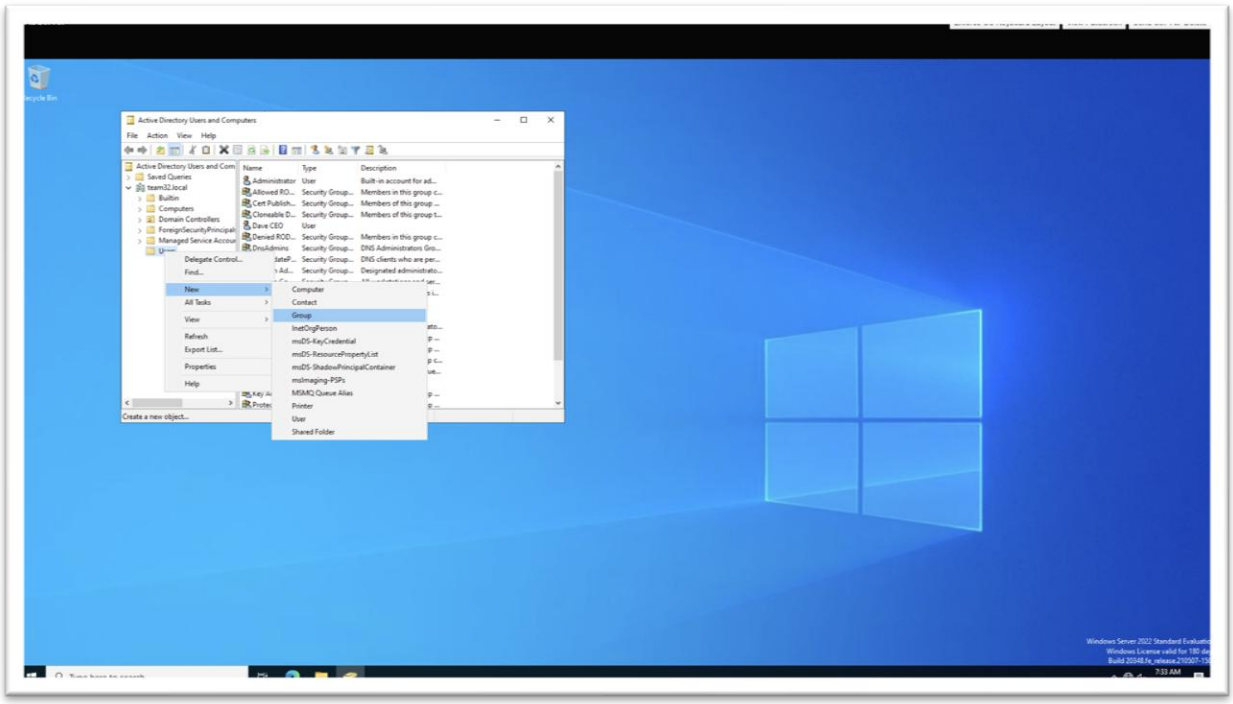

Figure 28: Screenshot of path to create “New Group”.

- Now enter the Group Name “UBFaculty” and select OK.

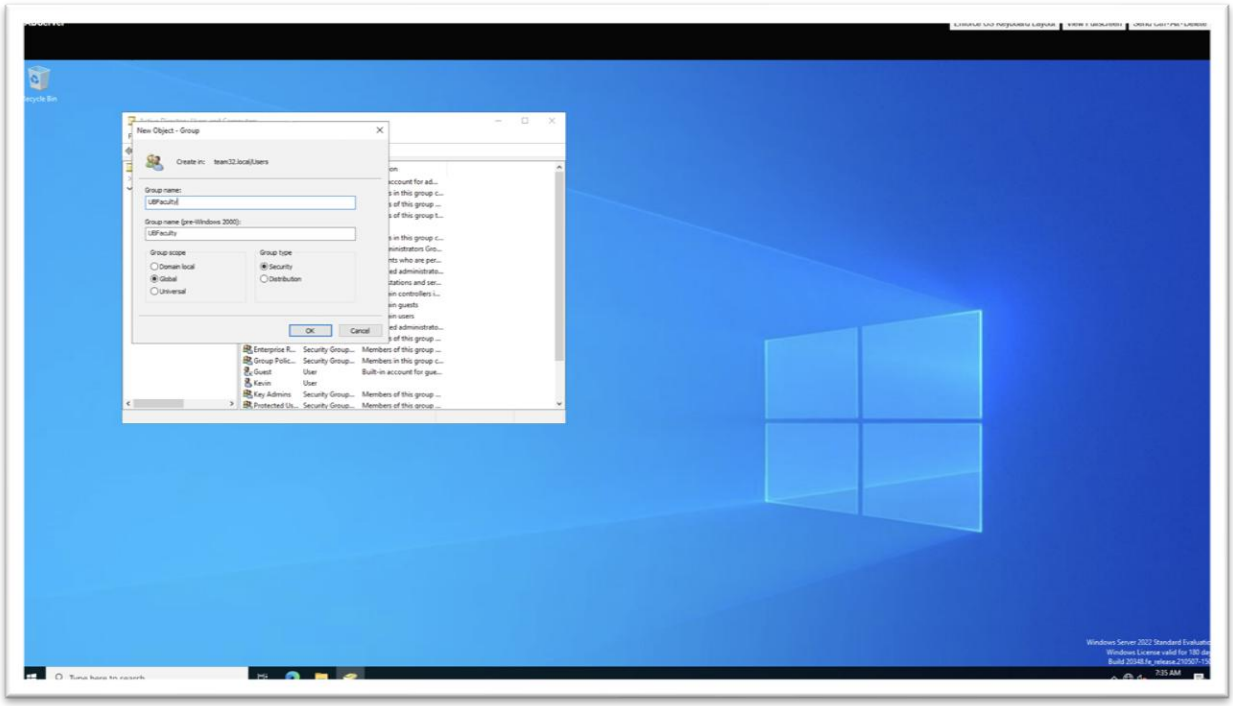

Figure 29: Screenshot of entering “Group Name- UBFaculty”.

- Now we have to find the newly created group “UBFaculty” and right click then select properties as shown in Figure 30.

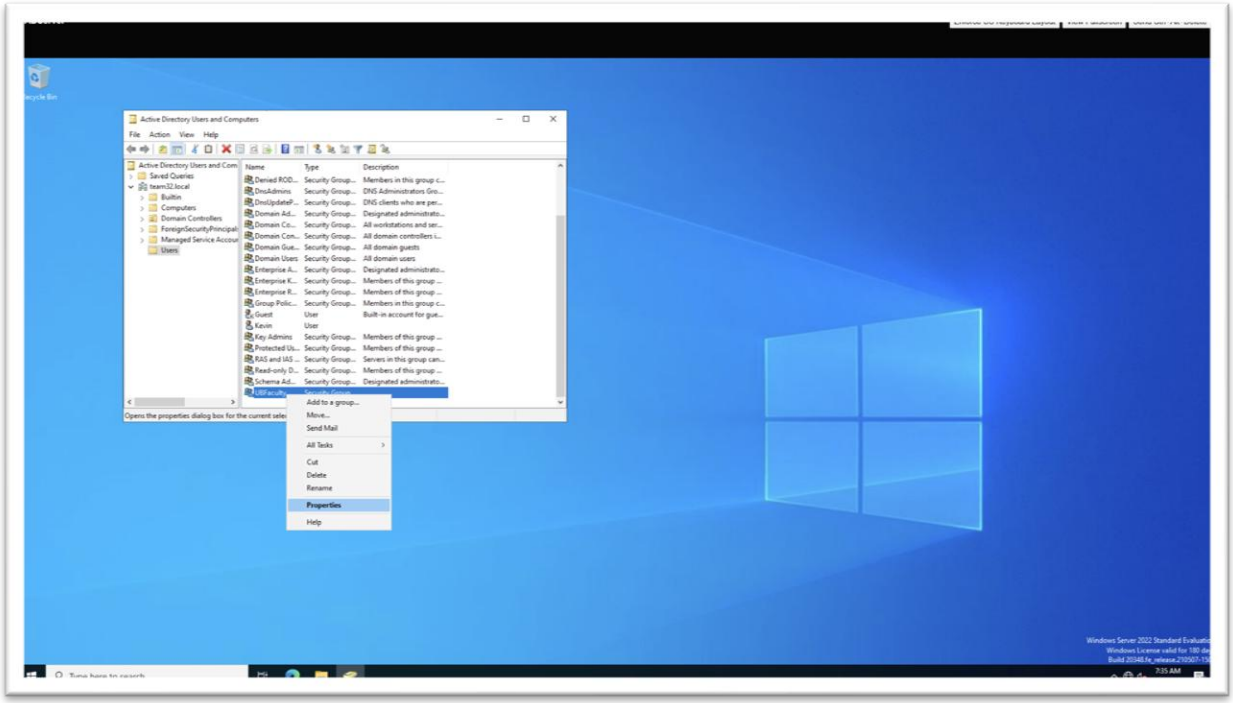

Figure 30: Screenshot of path to open properties for “New Group”.

- Now for this group we will allow “all the Domain Users” so we will type “Domain Users” in object names and click “Check Names”, if it outlines the object name then press OK as shown below in Figure 31.

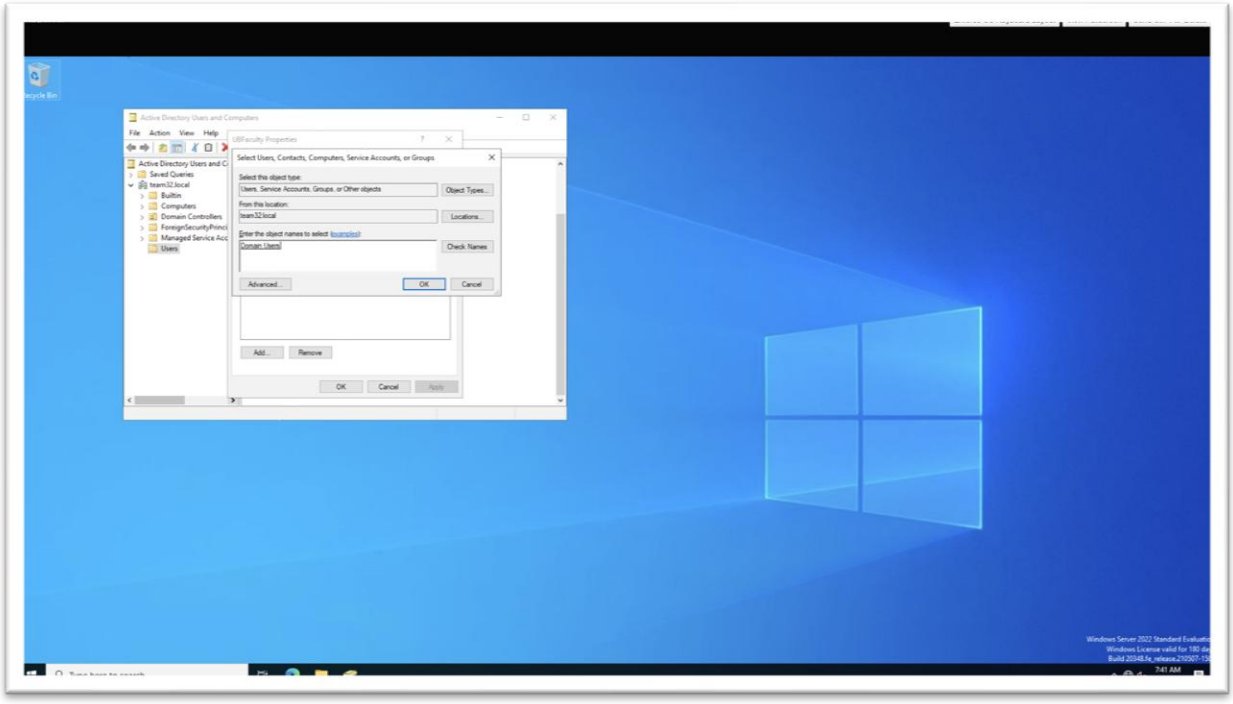

Figure 31: Screenshot of entering “Domain Users” in Object names.

- Now, do the same for other group- “Workstations”. (Figure 32 and 33)

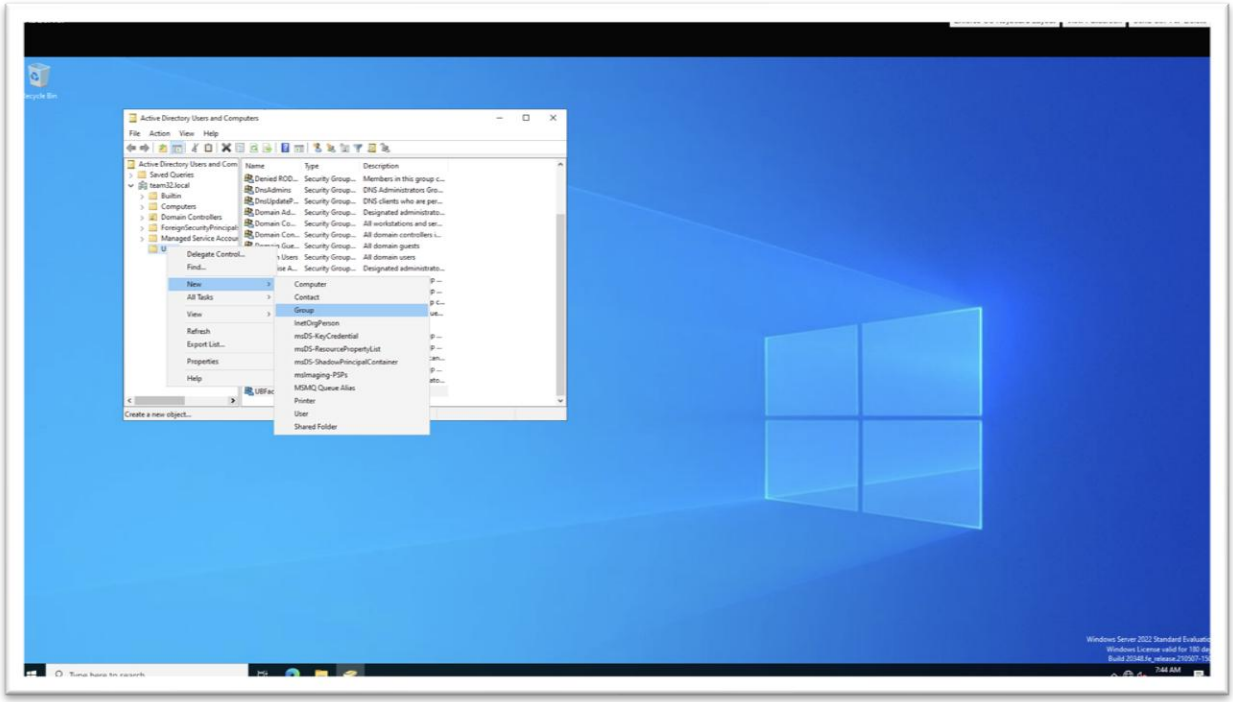

Figure 32: Screenshot of path to make “New Group- Workstations”.

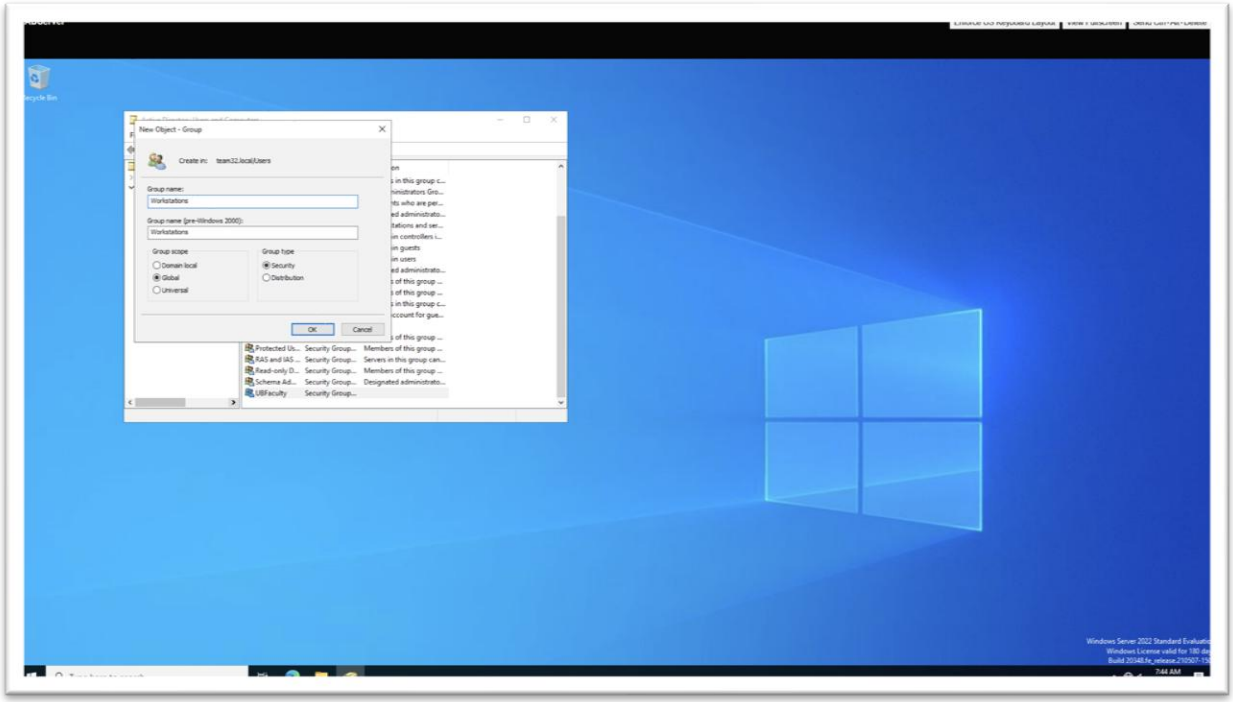

Figure 33: Screenshot of entering the Group Name- “Workstations”.

- Now we have to find the newly created group “Workstations” and right click then select properties as shown in Figure 34.

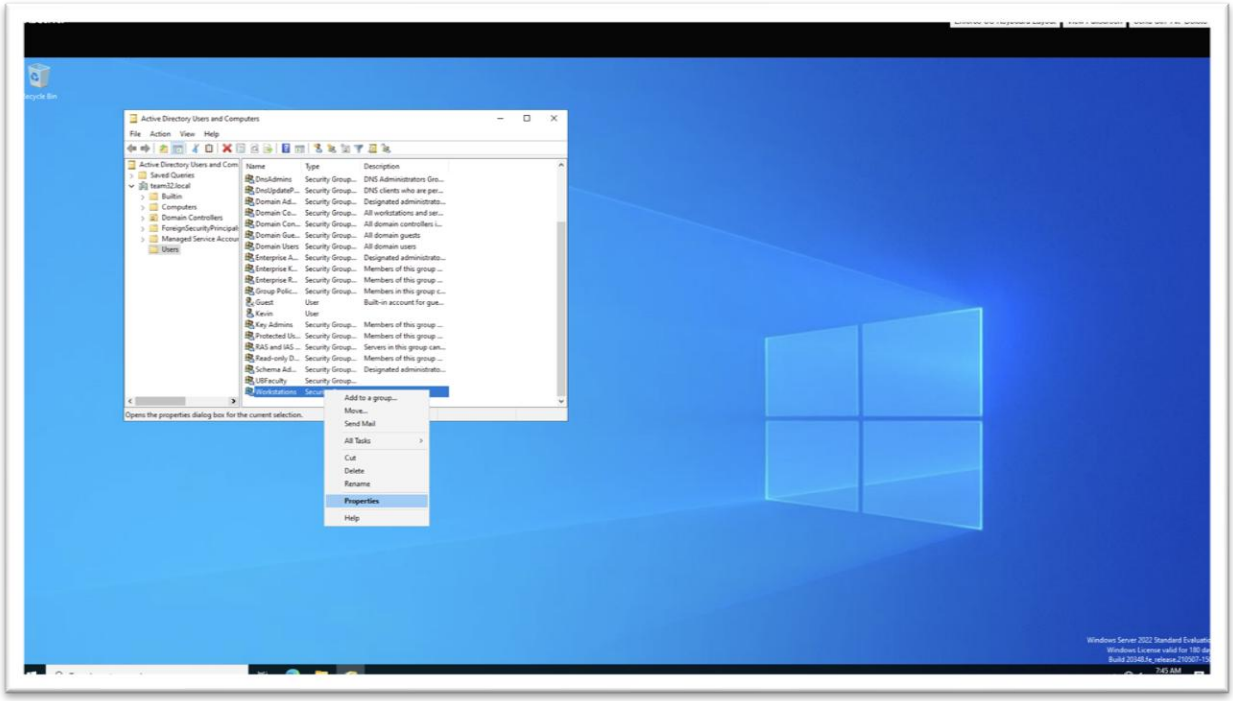

Figure 34: Screenshot of path to Properties of Workstations.

- Now, for Workstation we need “all domain devices” to be connected so for that we enter “Domain Computers” in object name and press “Check Names” and if we get outline on Object name then we select Enter as shown in Figure 35.

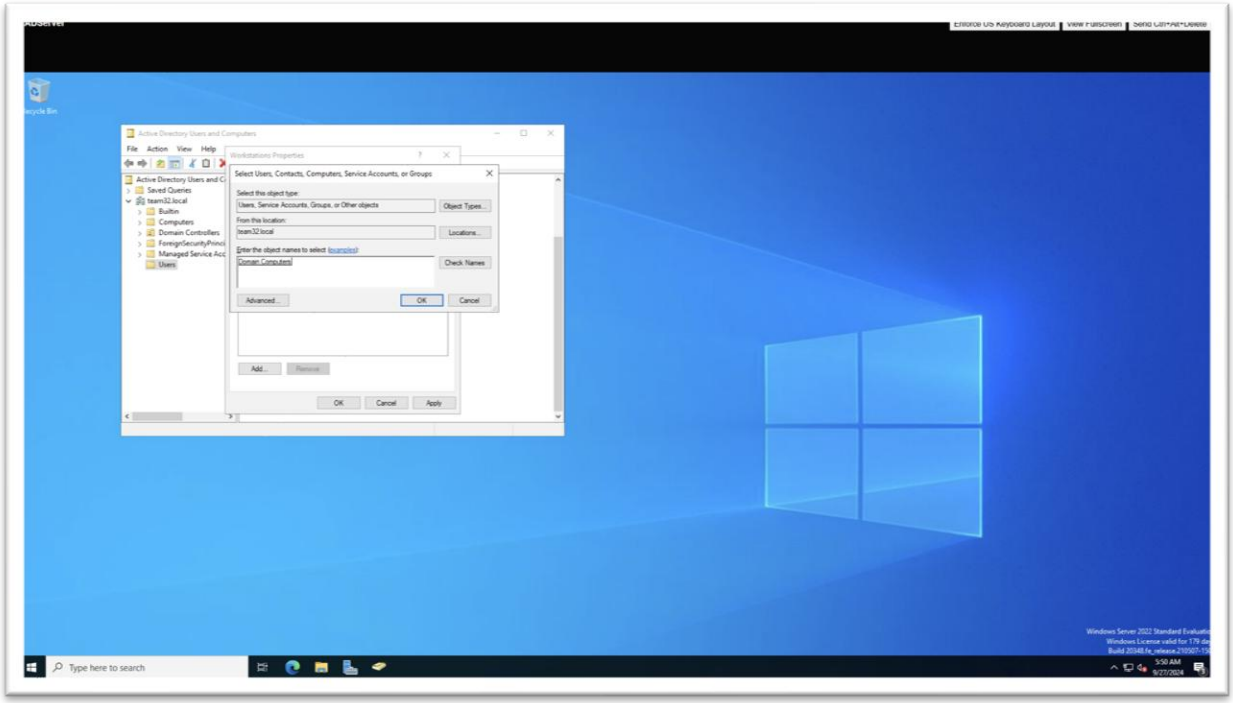

Figure 35: Screenshot of entering object name- “Domain Computers” for Workstations.

6. Enforce a Background Group Policy

- Create a “New Folder to store photo” anywhere (I did it in desktop) as shown in Figure 36 and save photo- logo.jpg inside it on ADServer as shown in Figure 37.

Figure 36: Screenshot of creating “New folder- Background Desktop Picss” on desktop.

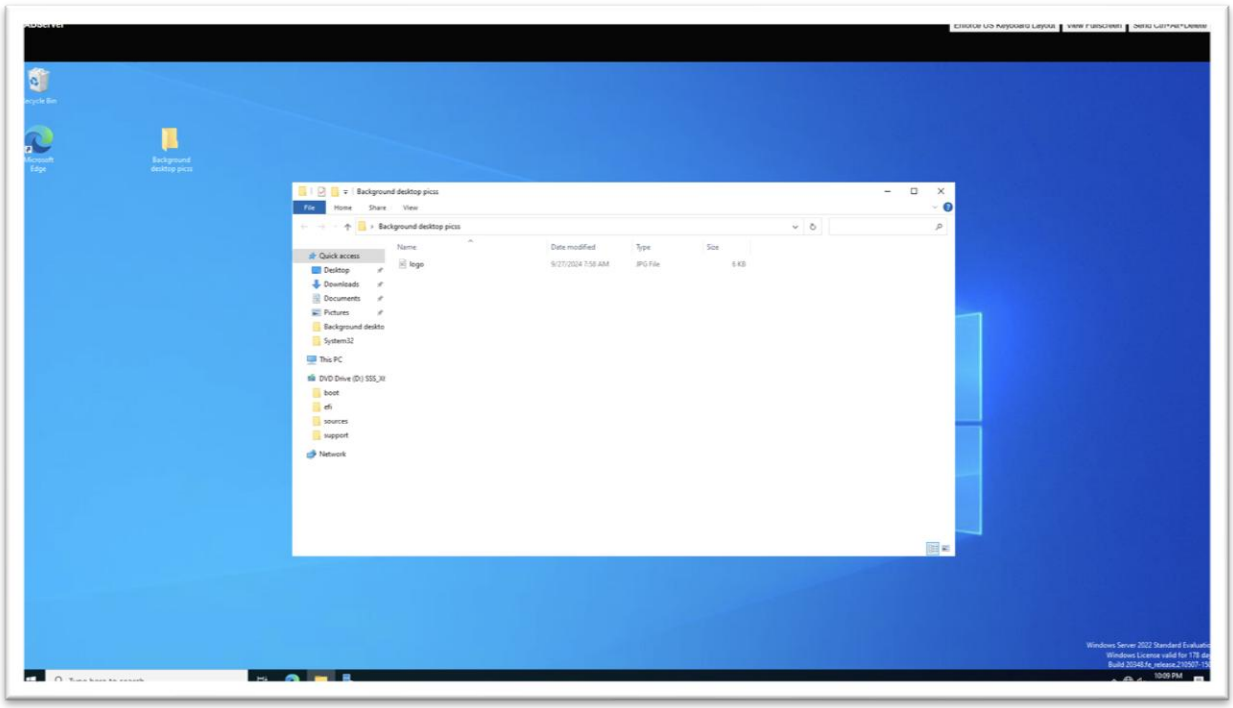

Figure 37: Screenshot of “logo.jpg in new folder.

- Now right click the folder and go to the properties, select sharing and select “Advanced Sharing…” .

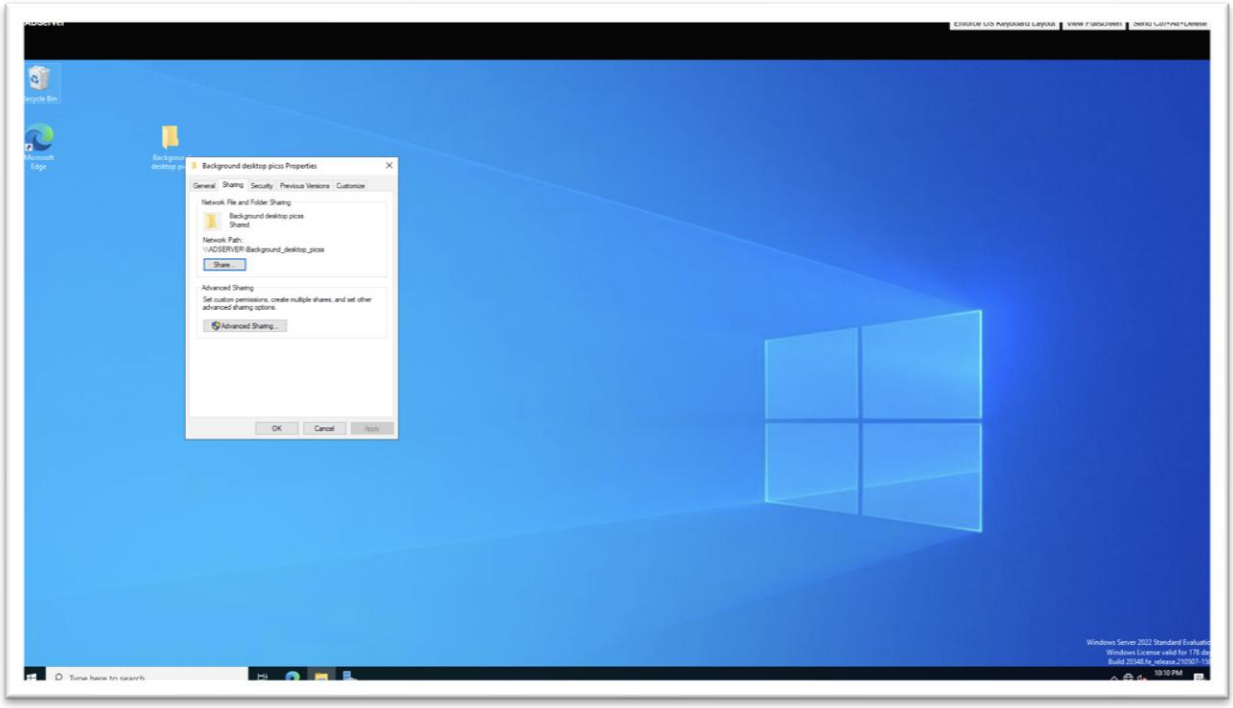

Figure 38: Screenshot of Sharing option in properties.

- Now type the “Share name” (use different name than original folder name) and then select “Permission” as shown below in Figure 39.

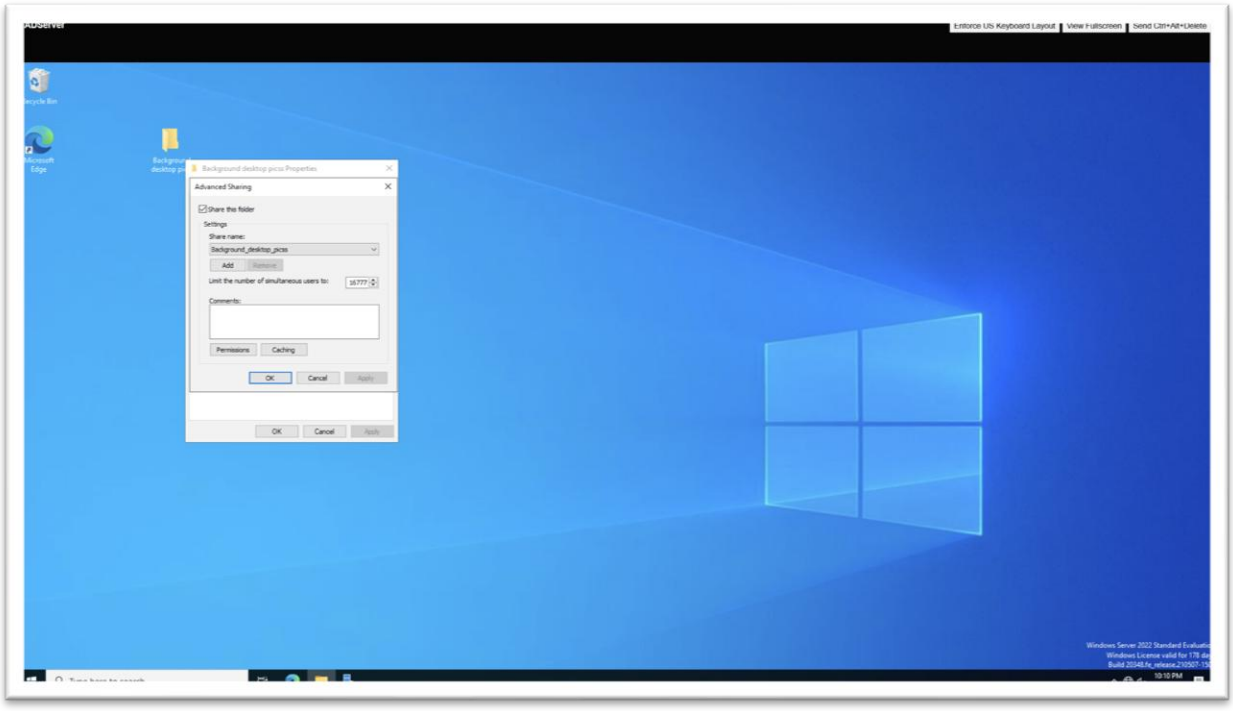

Figure 39: Screenshot of “Advanced Sharing and adding Permissions”.

- Now add “Domain Computer” to allow or give permission to all domain devices and then select apply and then OK.

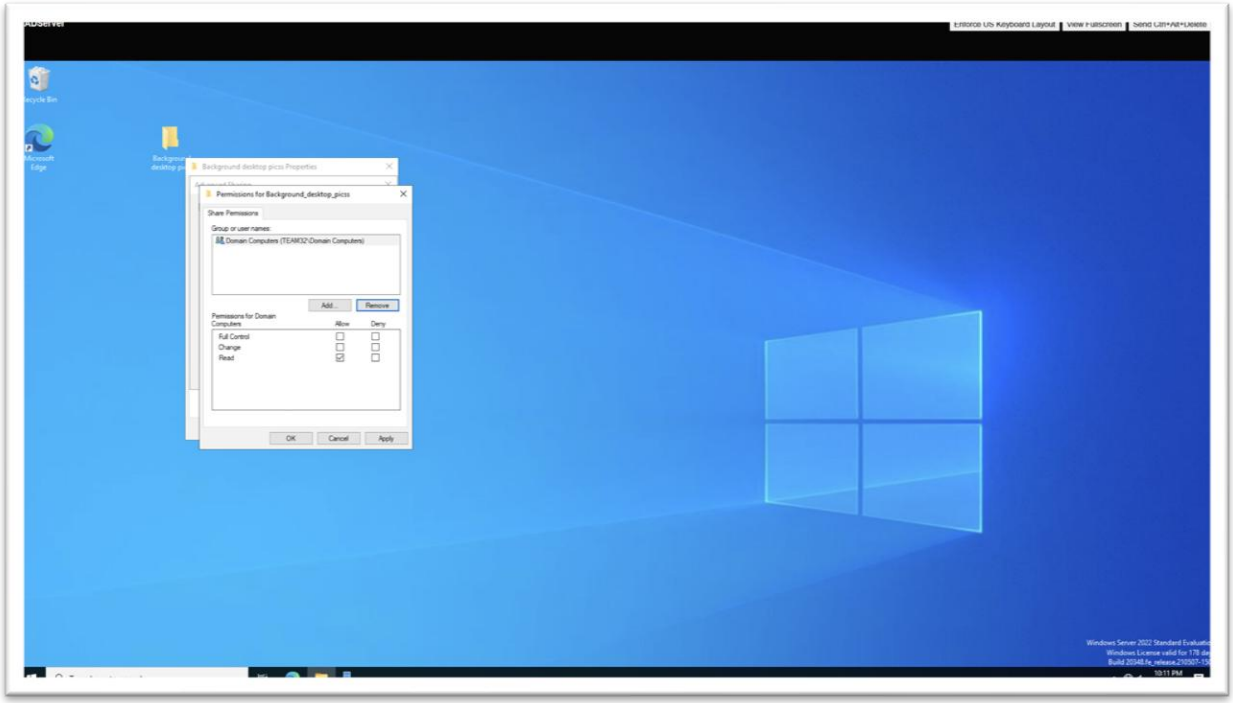

Figure 40: Screenshot of “Permissions to add domain devices”.

- Now Open “Group Policy Management” and select Team Domain “team32.local” and right click it to open “Create a GPO in this domain and link it here” as shown in Figure 41,

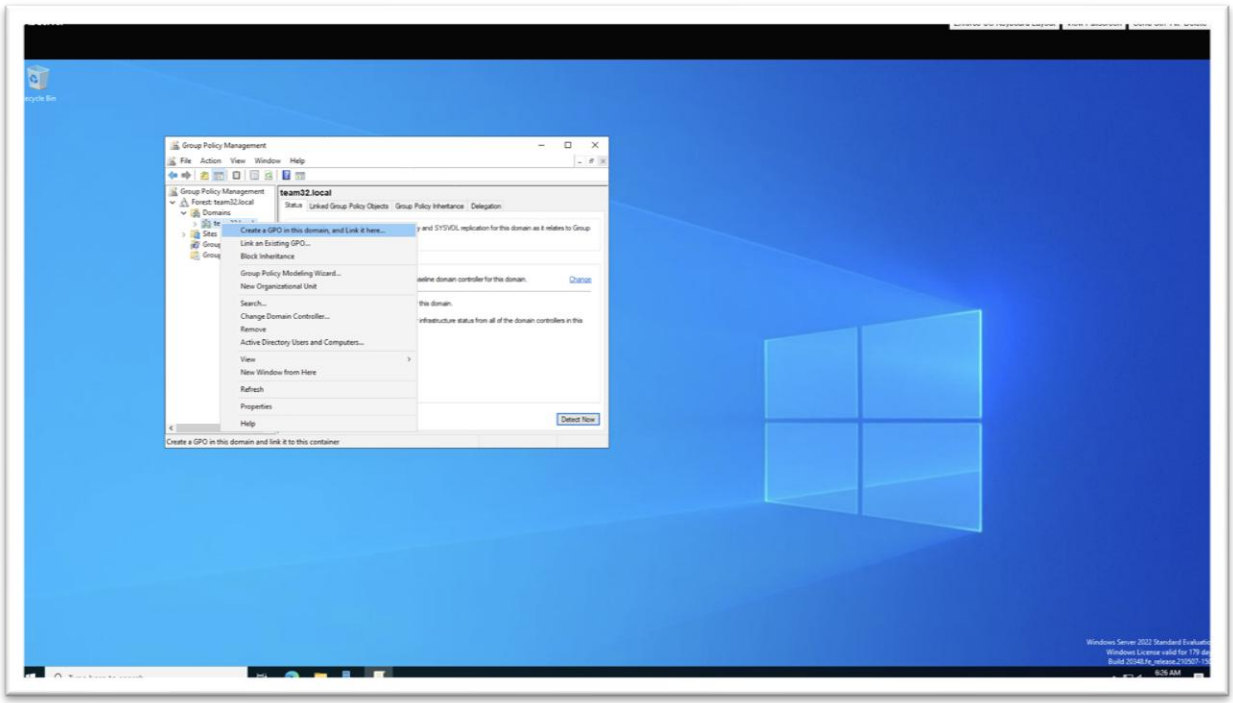

Figure 41: Screenshot of path to create “A GPO in team domain”.

- Now you have to name the “New GPO” and press OK.

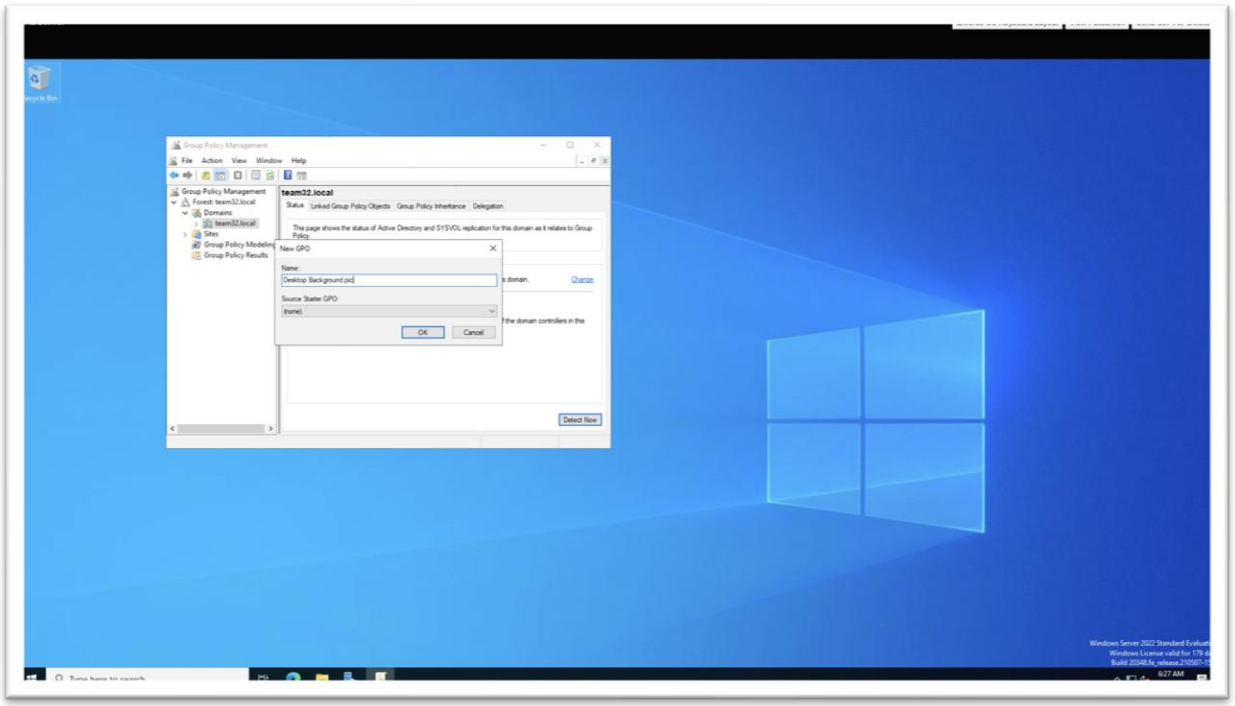

Figure 42: Screenshot of naming the “New GPO”

- Now right click that “New Desktop background GPO” and select “Edit”.

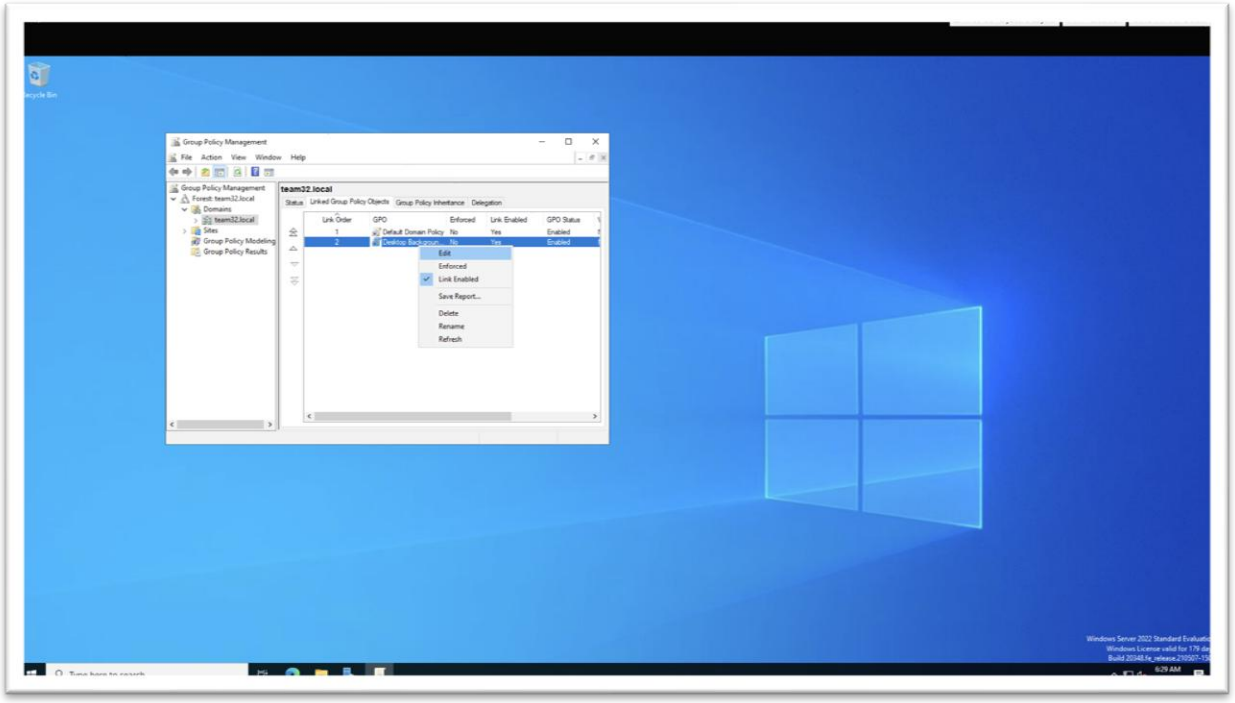

Figure 43: Screenshot of “Edit” of Desktop Background GPO.

- Now go to “User Configuration>Policies>Administrative Temp.>Desktop>Desktop” and select “Desktop Wallpaper” as shown in Figure 44.

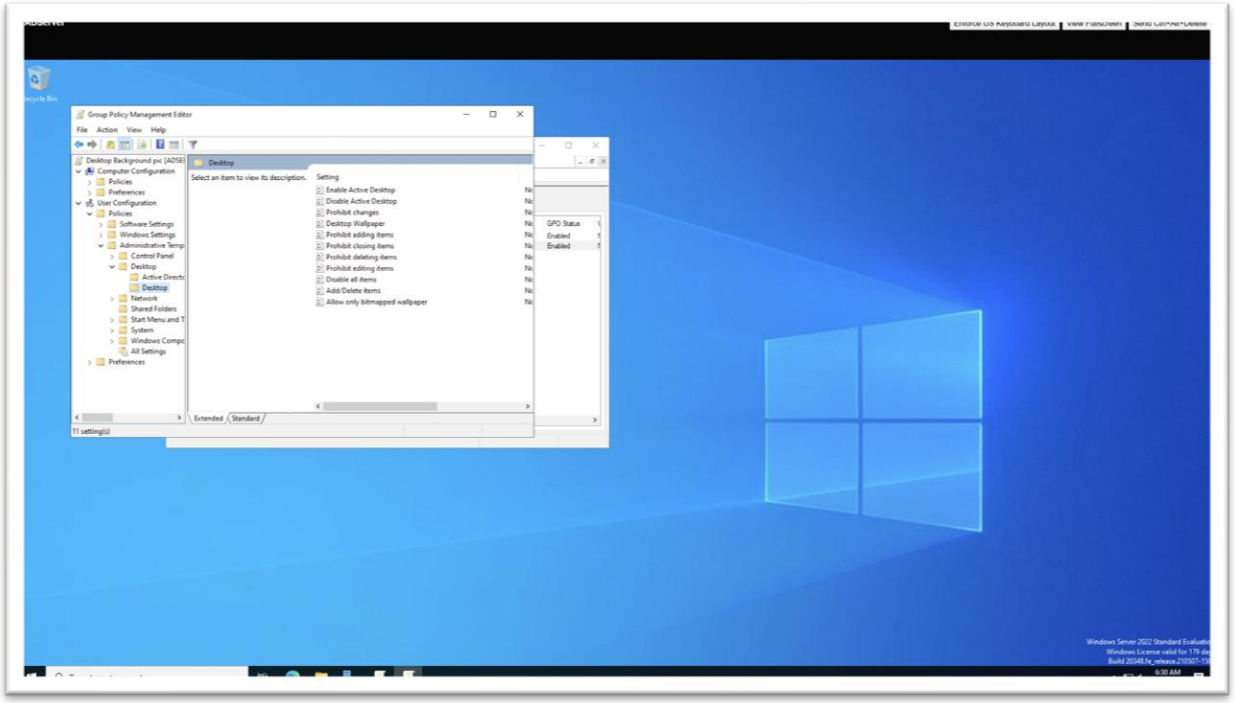

Figure 44: Screenshot of Edit the “Desktop Wallpaper”.

- Now click “Enabled” and under Wallpaper Name type “Network path” from Figure 38 and select wallpaper style -Fill to cover the whole screen and click OK.

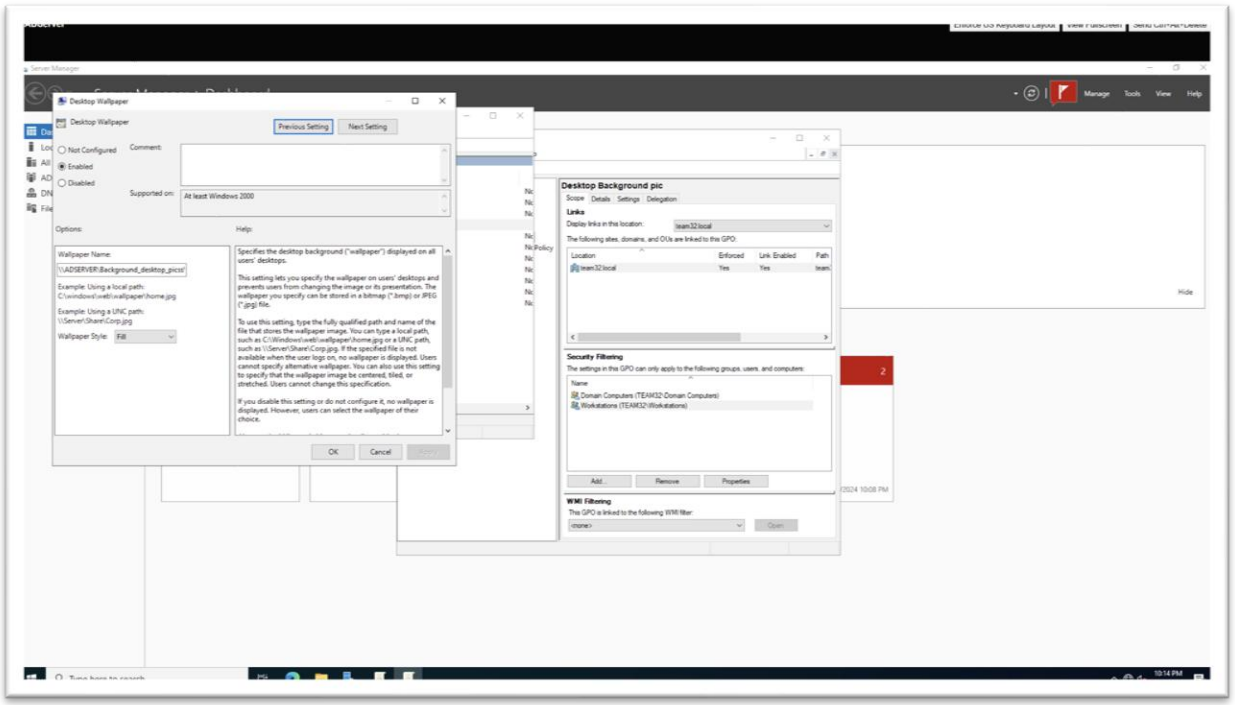

Figure 45: Screenshot of “Enabling Desktop Wallpaper and putting address”.

- Now add “Security Filtering” and put “workstations and domain computers” to only allow them to access as shown in Figure 46.

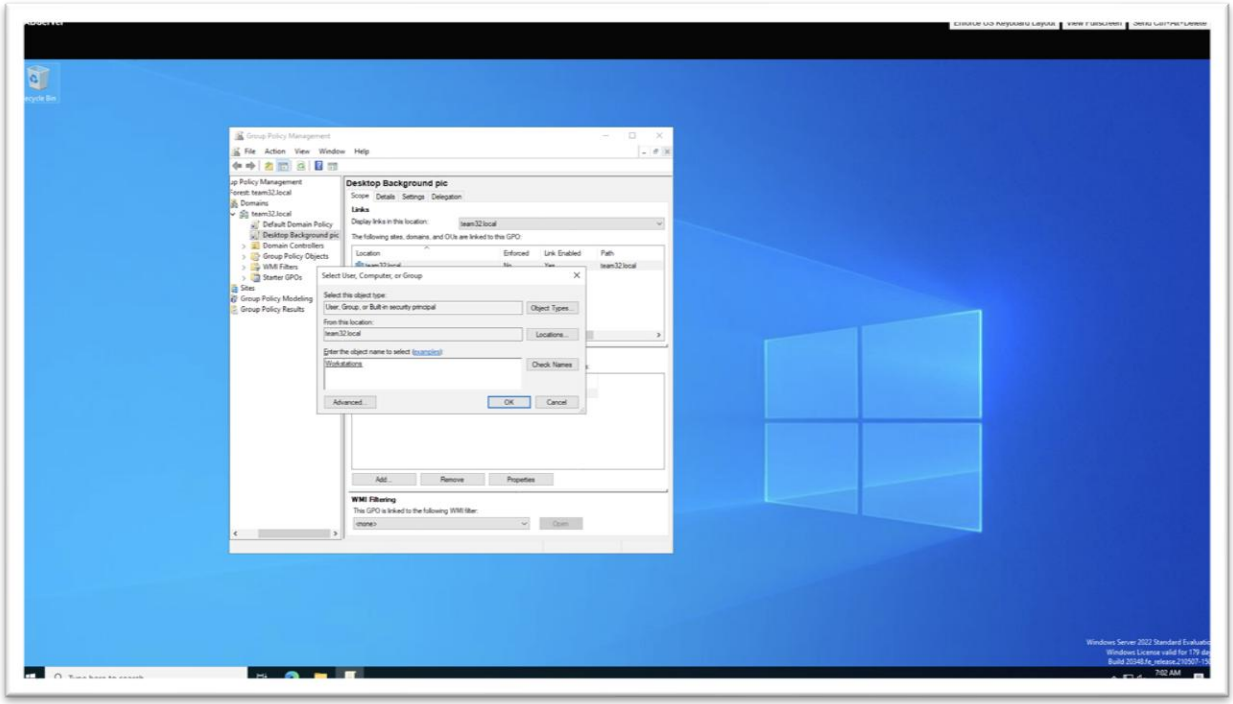

Figure 46: Screenshot of Adding “Workstations and Domain Computers” to Security Filtering.

- You can “Enforced” the GPO of Desktop Background if you want it to ignore all the conflicts and apply the policies. Also write “gpupdate /force” in Command prompt after policies are applied.

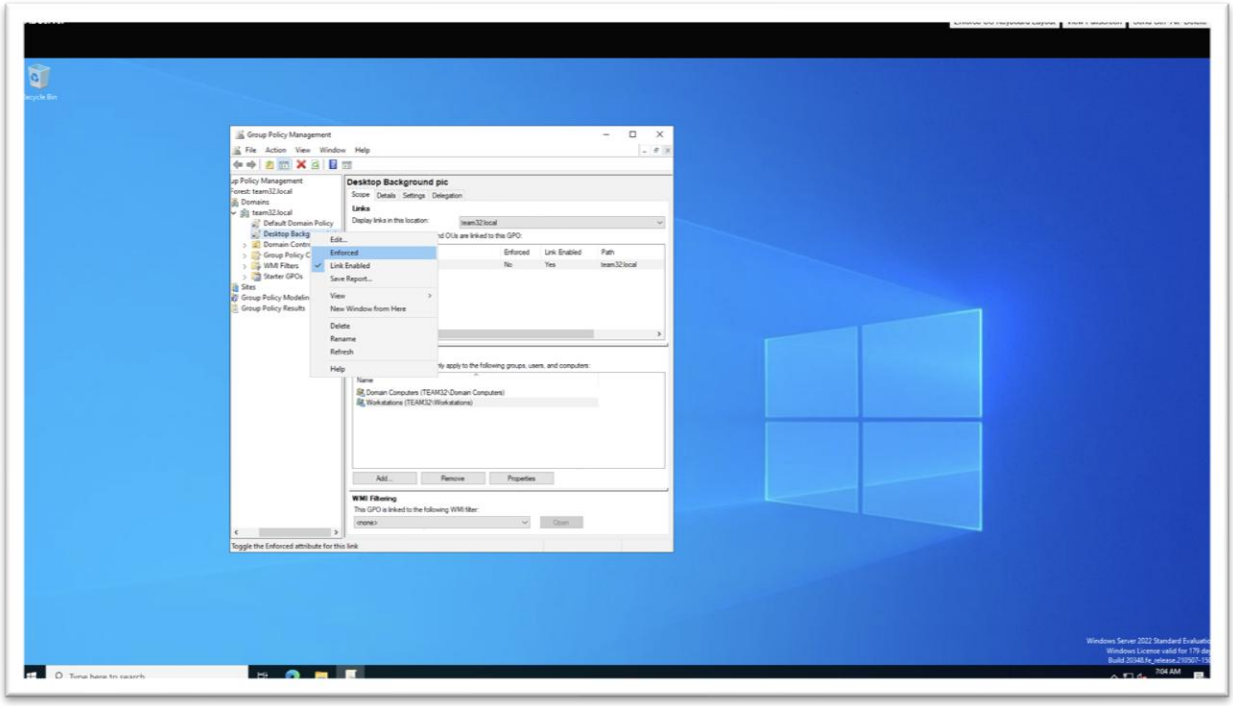

Figure 47: Screenshot of “Enforced” the GPO of Desktop Background.

- Now, either sign out or restart each VM to apply all the policies and we can see the results shown below in Figure 48 and 49.

Figure 48: Screenshot of Desktop Wallpaper change in ADServer.

Figure 49: Screenshot of Desktop Wallpaper change in Win10Client.

7. Setup PowerShell Transcription Using a Group Policy

- Open Group Policy Management, select “team32.local” and enter “New GPO- Powershell Transcription Policy” and press OK as shown in Figure 50.

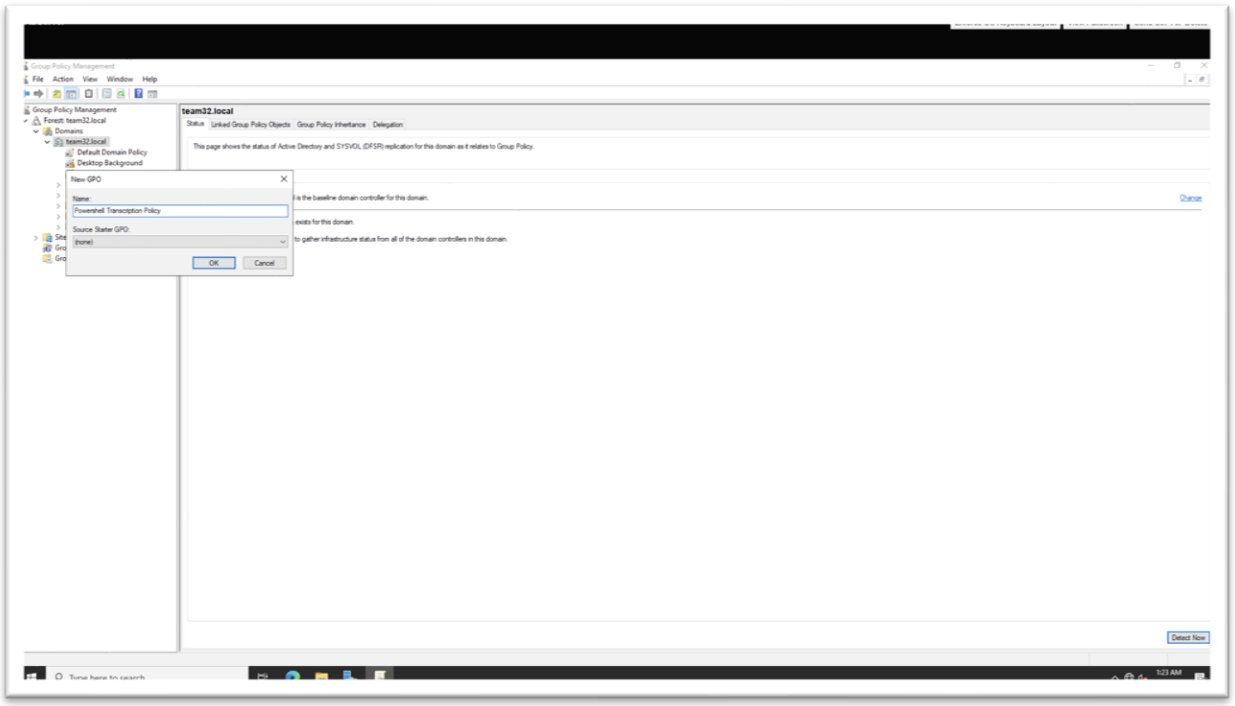

Figure 50: Screenshot of creating “New GPO” in team domain.

- Select Newly created GPO and right click it to open “Edit”.

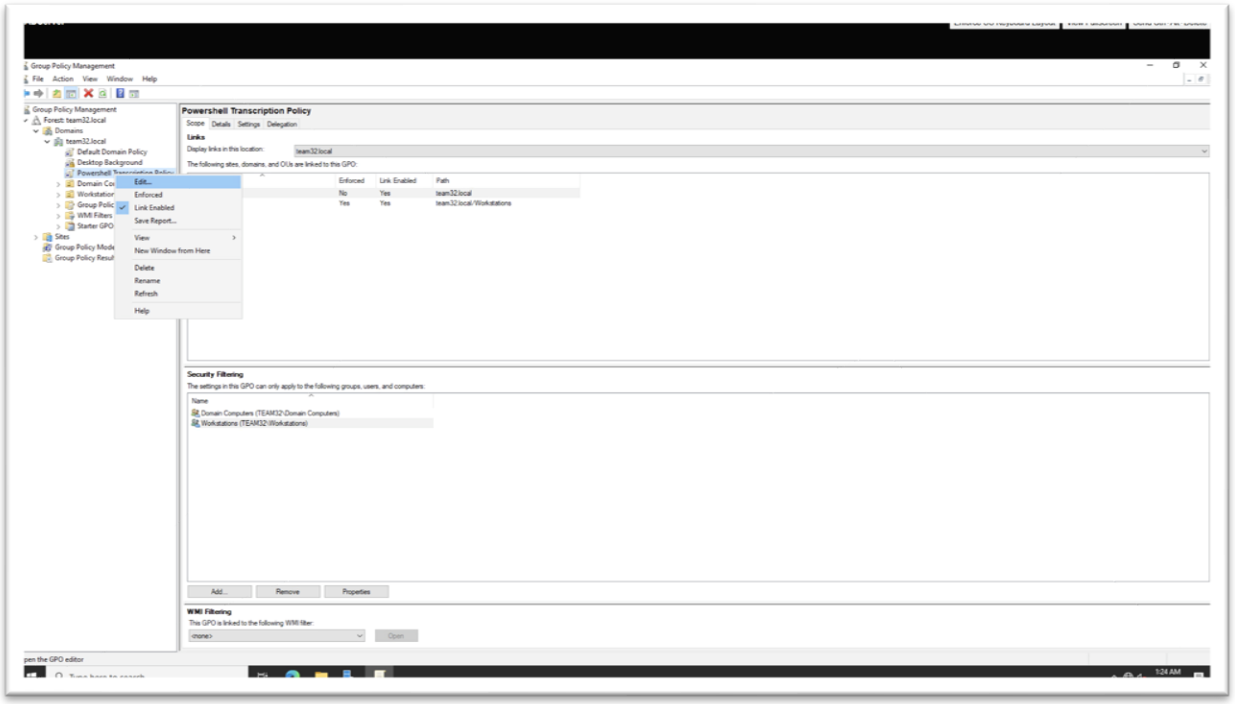

Figure 51: Screenshot of selecting “Edit” in New GPO.

- Now go to “Computer Configuration>Policies>Administrative Temp.>Windows Conf.>Windows Powershell” and select “Turn on Powershell Transcription”.

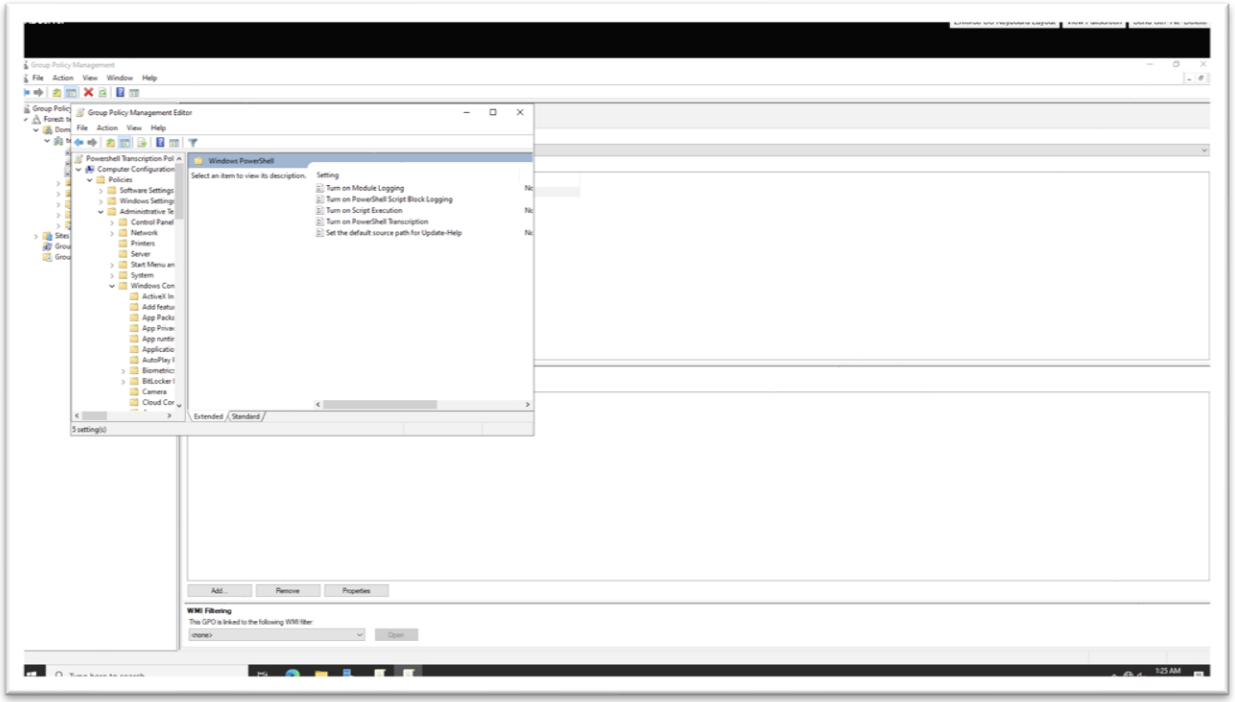

Figure 52: Screenshot of “Edit” of Powershell Transcription Policy.

- Now open “Turn on Powershell Transcription” and select “Enabled” and type network path for shared folder in “Transcript output directory” and press OK.

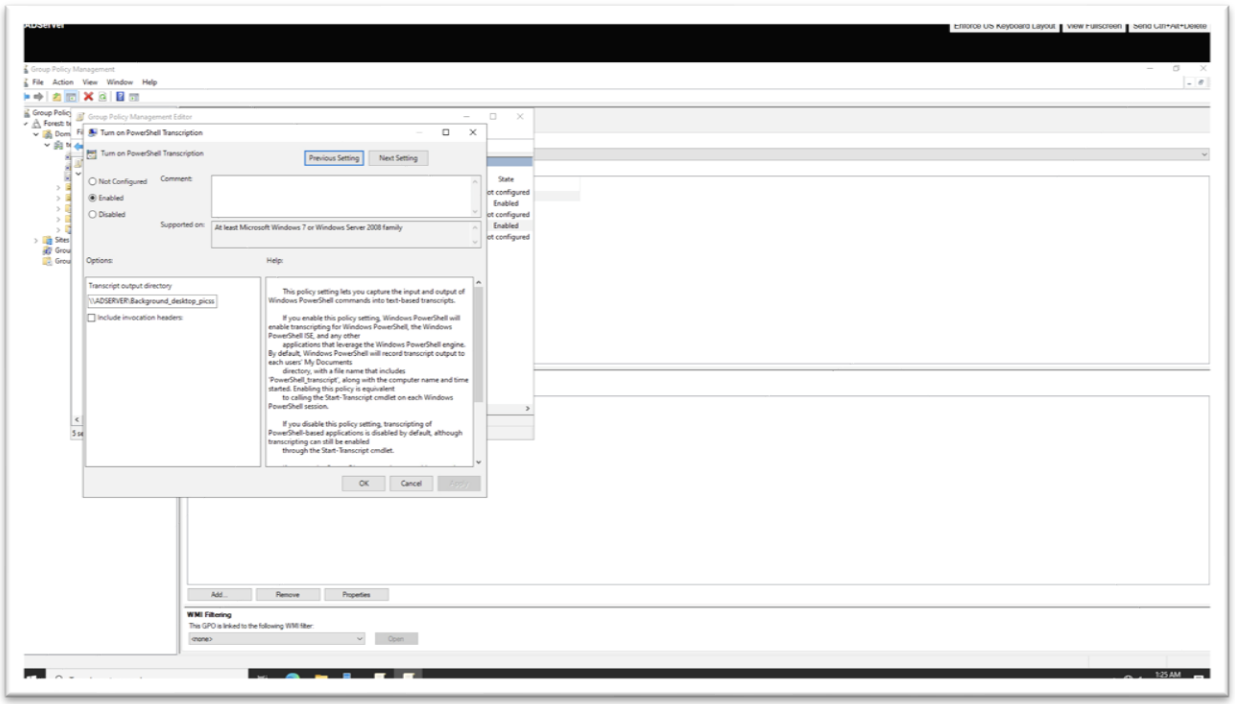

Figure 53: Screenshot of “Enabled and entering network path” in “Turn on Powershell Transcription”.

- Then after that select “Turn on Powershell Script Block Logging” and “Enabled” it. Then press OK.

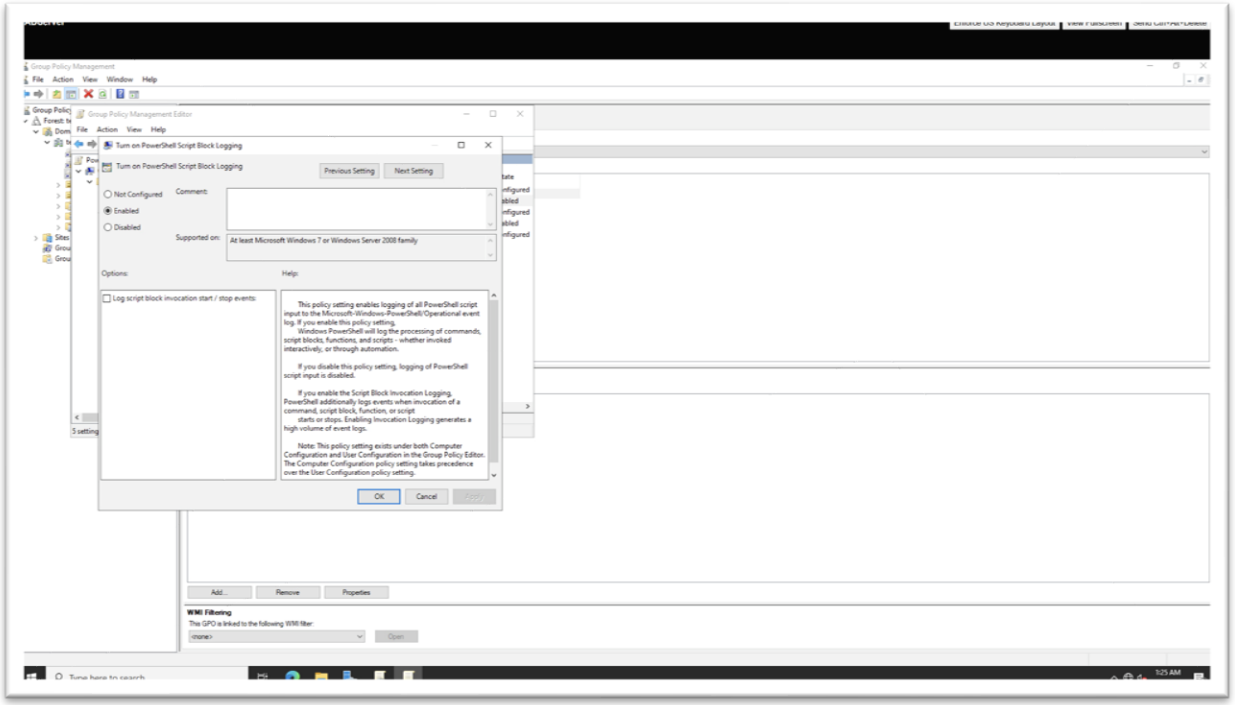

Figure 54: Screenshot of “Enabled” for “Turn on Poershell Script Block Logging”.

- You can “Enforced” the GPO of Powershell Transcription Policy if you want it to ignore all the conflicts and apply the policies. Also write “gpupdate /force” in Command prompt after policies are applied.

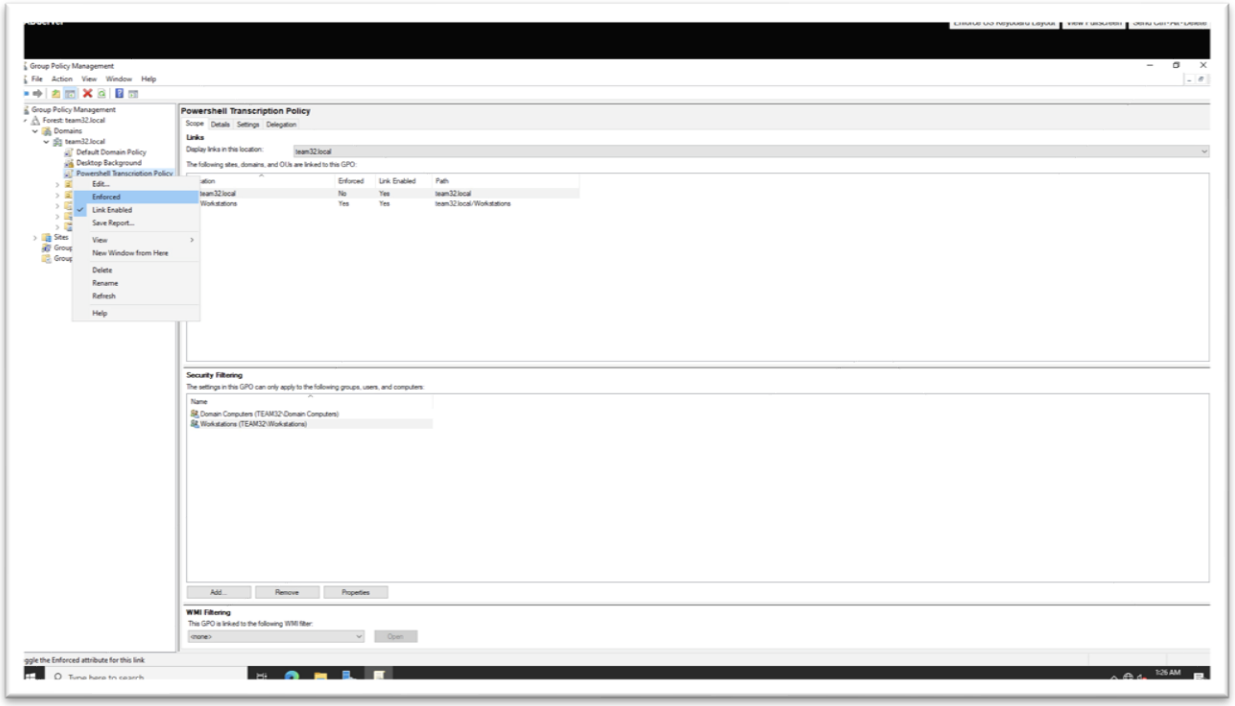

Figure 55: Screenshot of selecting “Enforced” in Powershell Transcription Policy GPO.

- Now on Win10Client, run Powershell and enter “pwd” command and enter then close it.

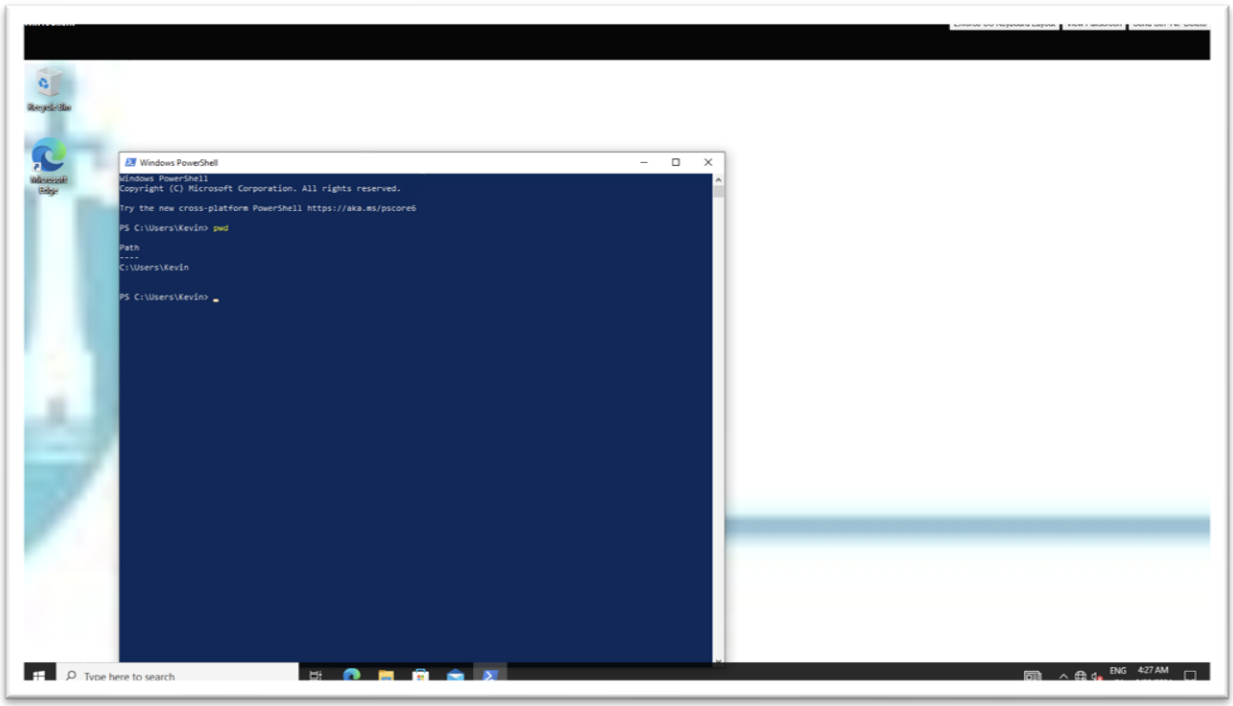

Figure 56: Screenshot of command “pwd” in Powershell.

- Now check “Shared Folder” on ADServer and observe a “New Folder as highlighted in Figure 57.

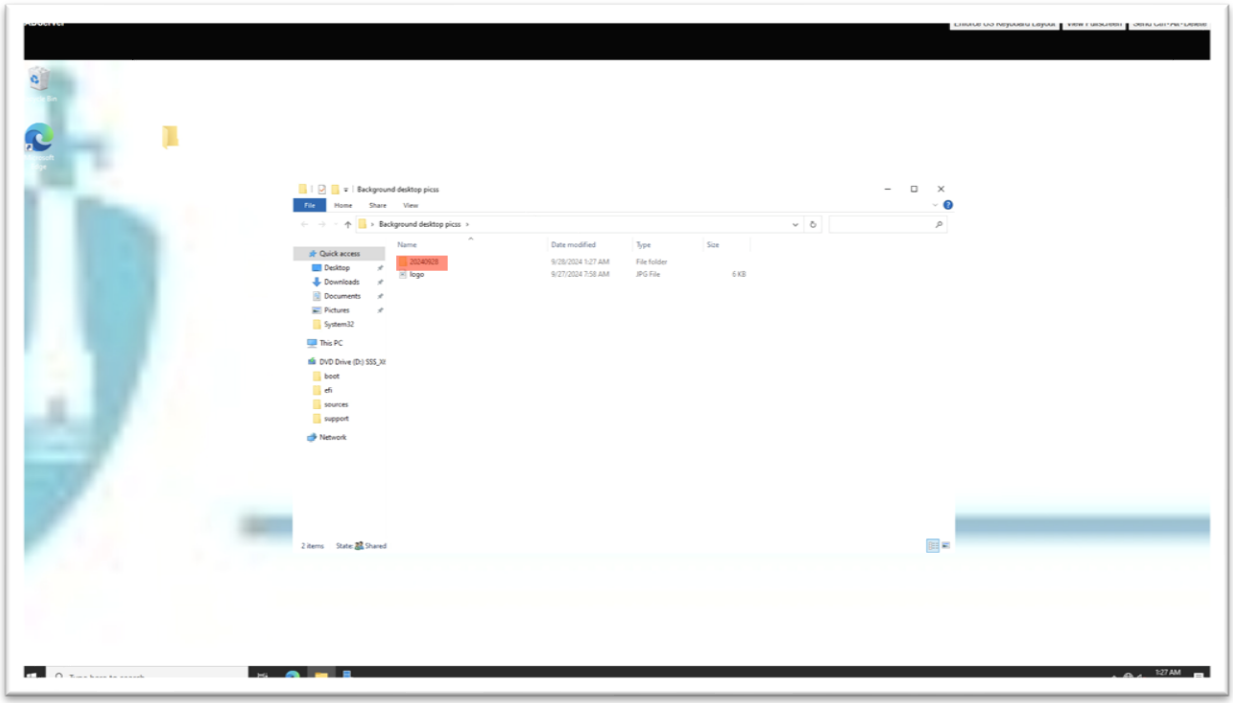

Figure 57: Screenshot of “New Folder” added to shared folder.

- We can see the content when we open the folder which is in Figure 58.

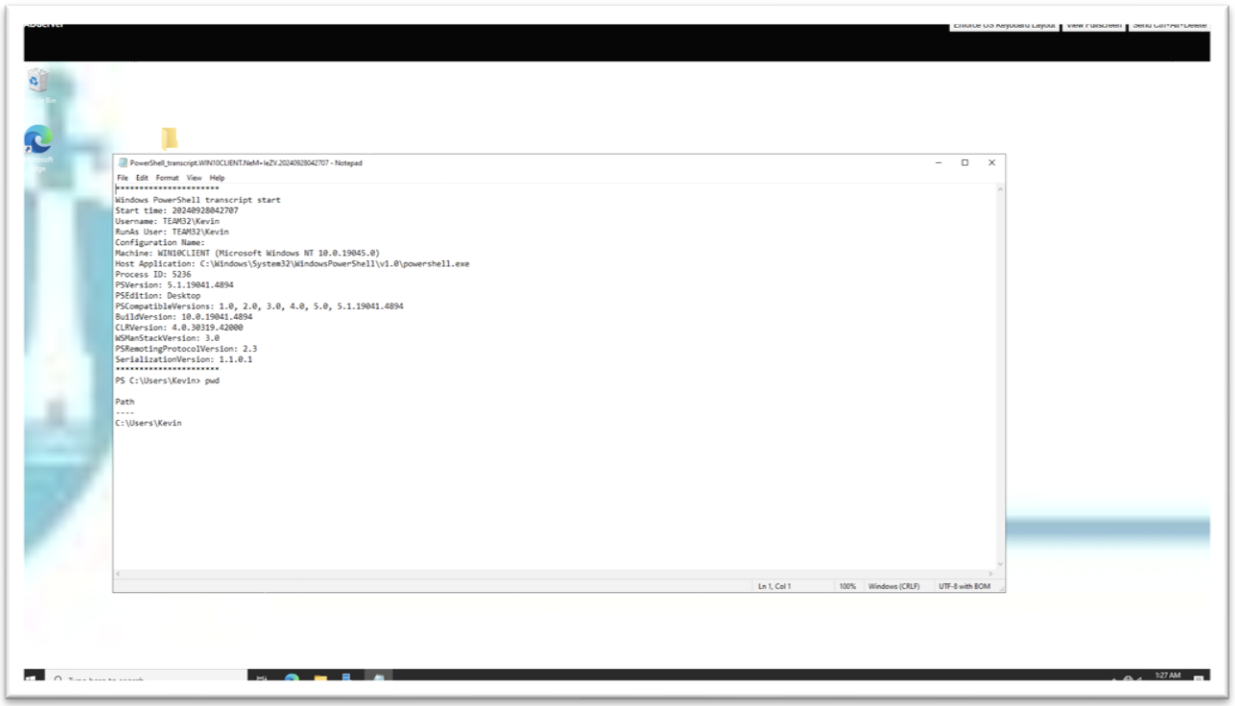

Figure 58: Screenshot of Output for New Folder.

8. Update Topology

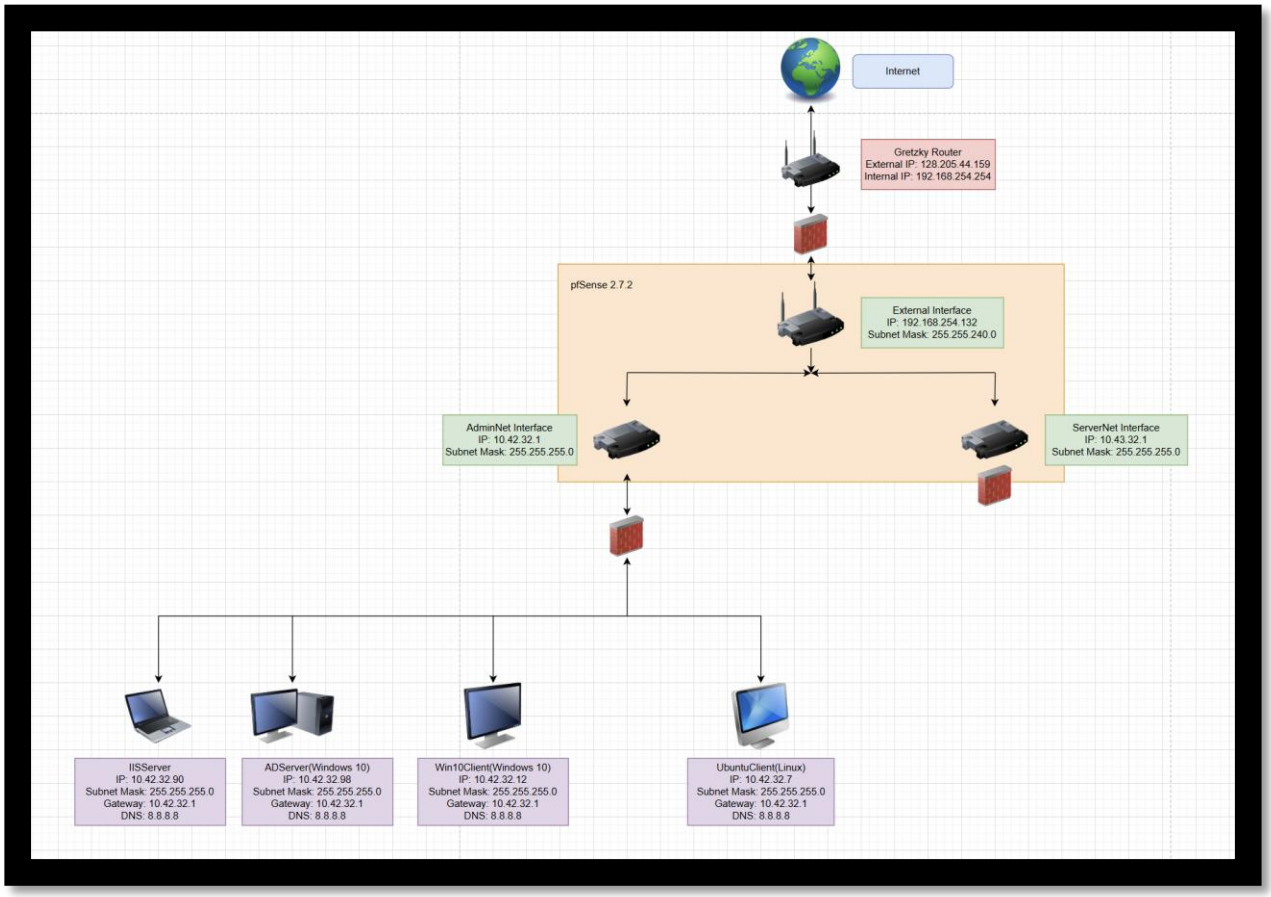

Figure 59: Screenshot of Updated Topology.

9. EAS 595 Additional Tasks

To: Kevin Cleary, CEO
From: Faraz Ahmed, Security Engineer
Date: September 26th, 2024
Subject: Implementation of the New Password Policy GPO

Dear Kevin,

As part of our ongoing efforts to increase security at UBNetDef, I propose the implementation of a new Group Policy Object (GPO) to enforce a strong and always available password policy across our organizational units (OUs). The configuration aims to address potential vulnerabilities and establish ideas of security awareness among our users.

- Creating of WinOUs (Organizational Units)- So we created WinOUs OU in Figure 60 and 61 and in figure 62 we add Win10Client and IISServer to WinOUs.

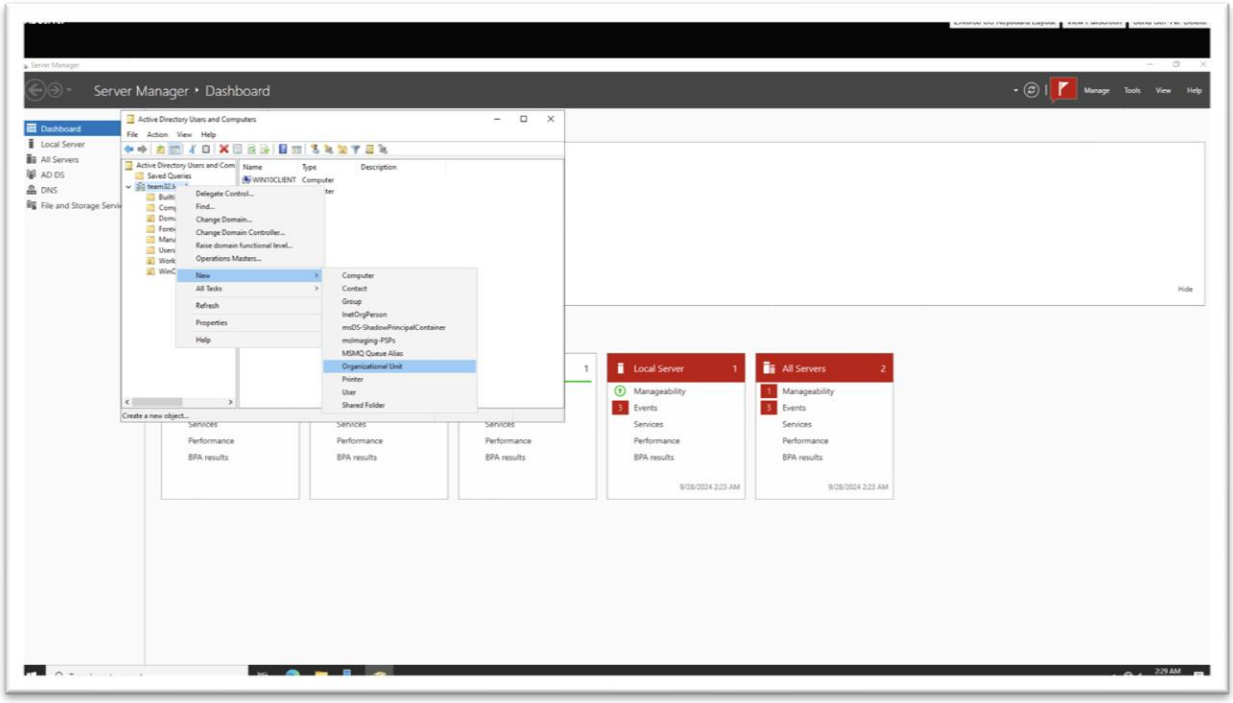

Figure 60: Screenshot of creation of WinOUs

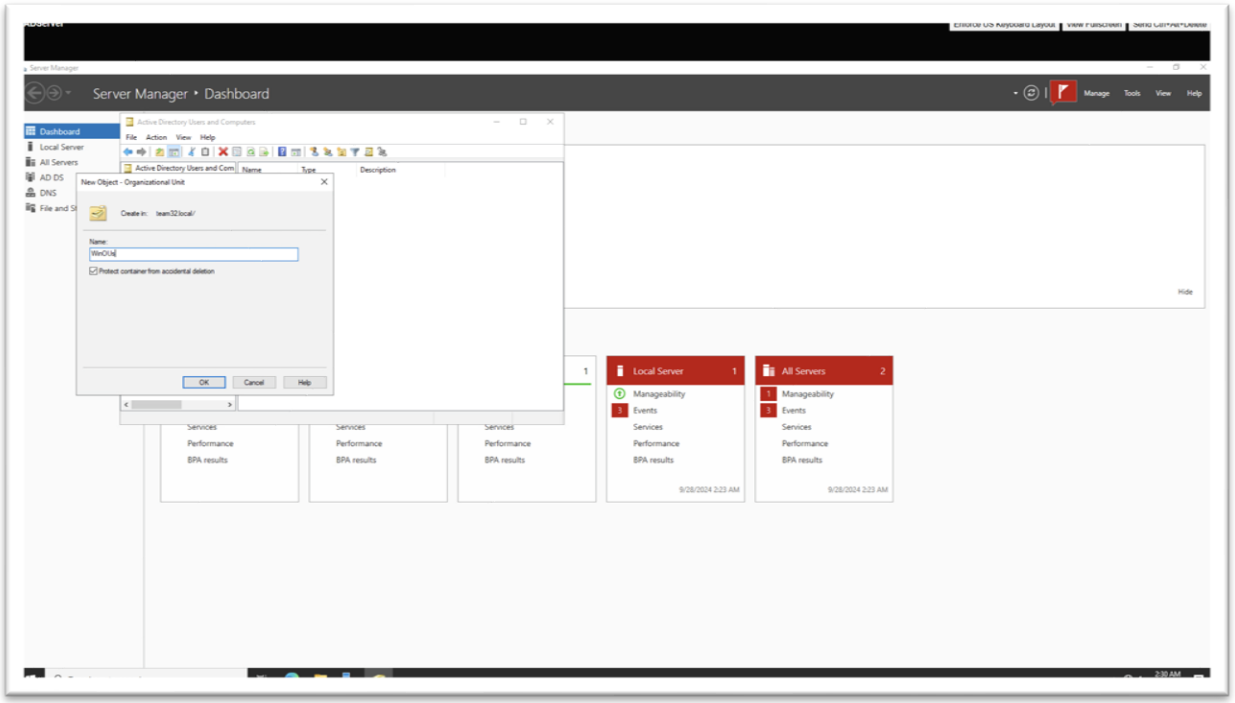

Figure 61: Screenshot of name of OU

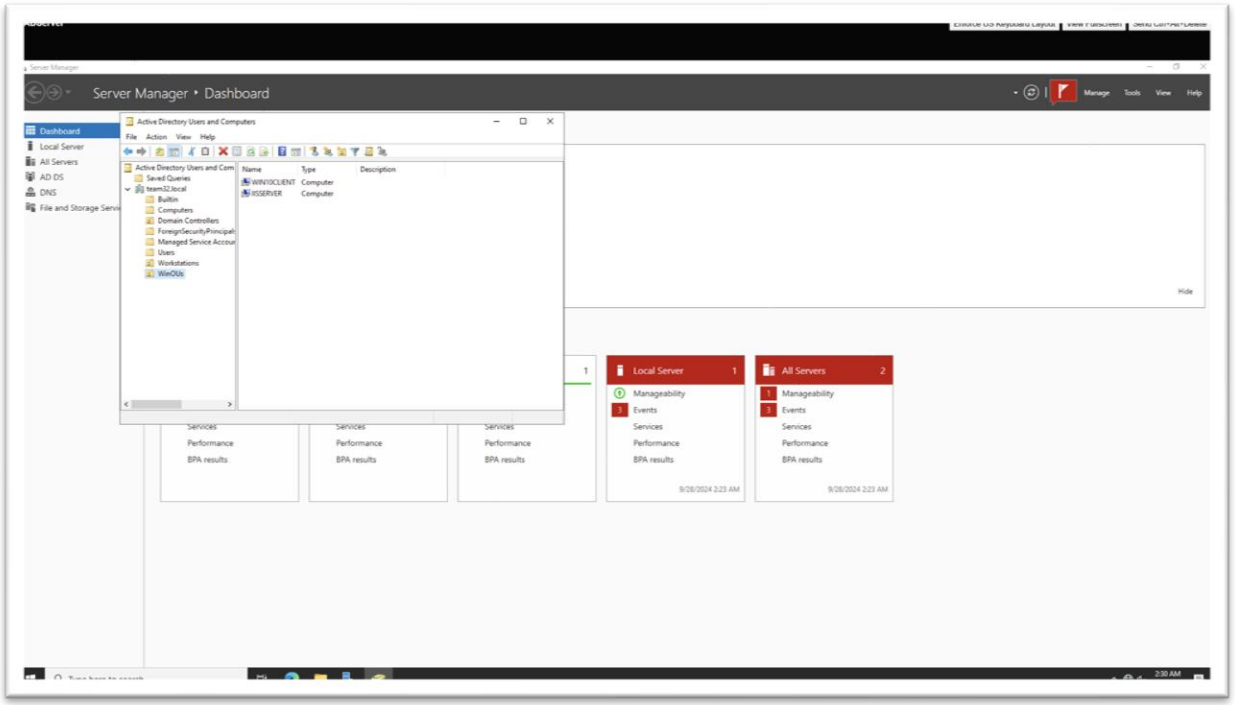

Figure 62: Screenshot of add "Win10Client and IISServer" to WinOUs.

- This is the finalized OU folder structure in Active Directory Users and Computers. (Figure 63)

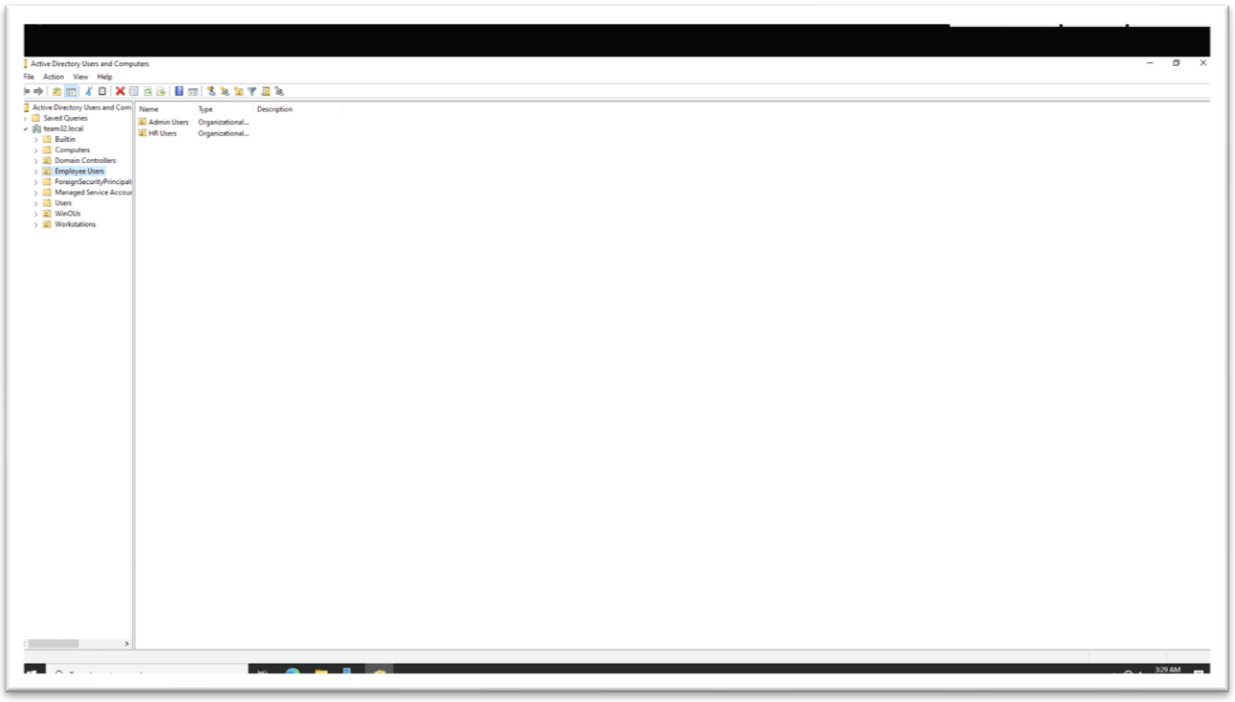

Figure 63: Screenshot of "Final OU folder in Active Directory Users and Computers".

- Error we get when we login through "Employee Users" which will stop us from entering.

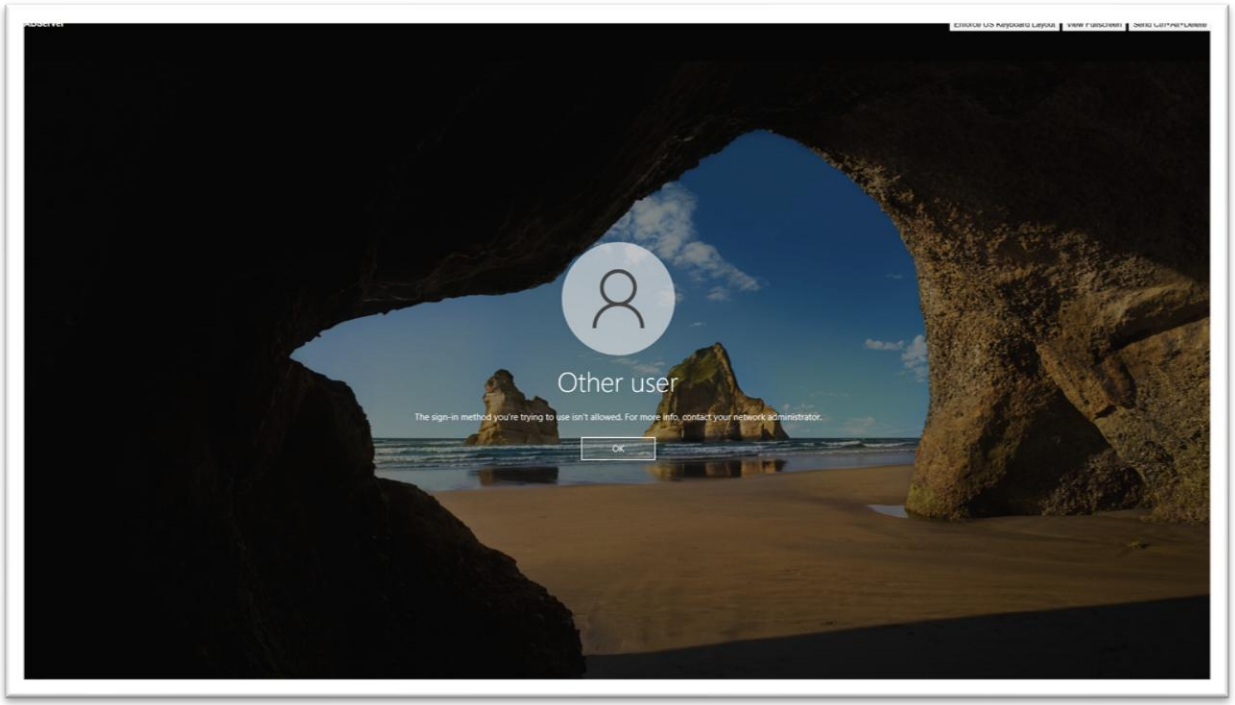

Figure 64: Screenshot of "Error Message to get when enter through Employee Users".

By using this password policy, we not only protect our sensitive information but also mantain a culture of security awareness among our employees. These measures align with industry standards and help avoid any security threats in the system.

I recommend proceeding with the creation of the GPO password policy for the WinOUs OU, as well as additional security measures such as logon prompts and restrictions on Remote Desktop and PowerShell usage for our user groups.

Please let me know if you have any questions and require further details regarding this proposal.

Best regards,

Faraz Ahmed
Security Engineer
fahmed29@buffalo.edu