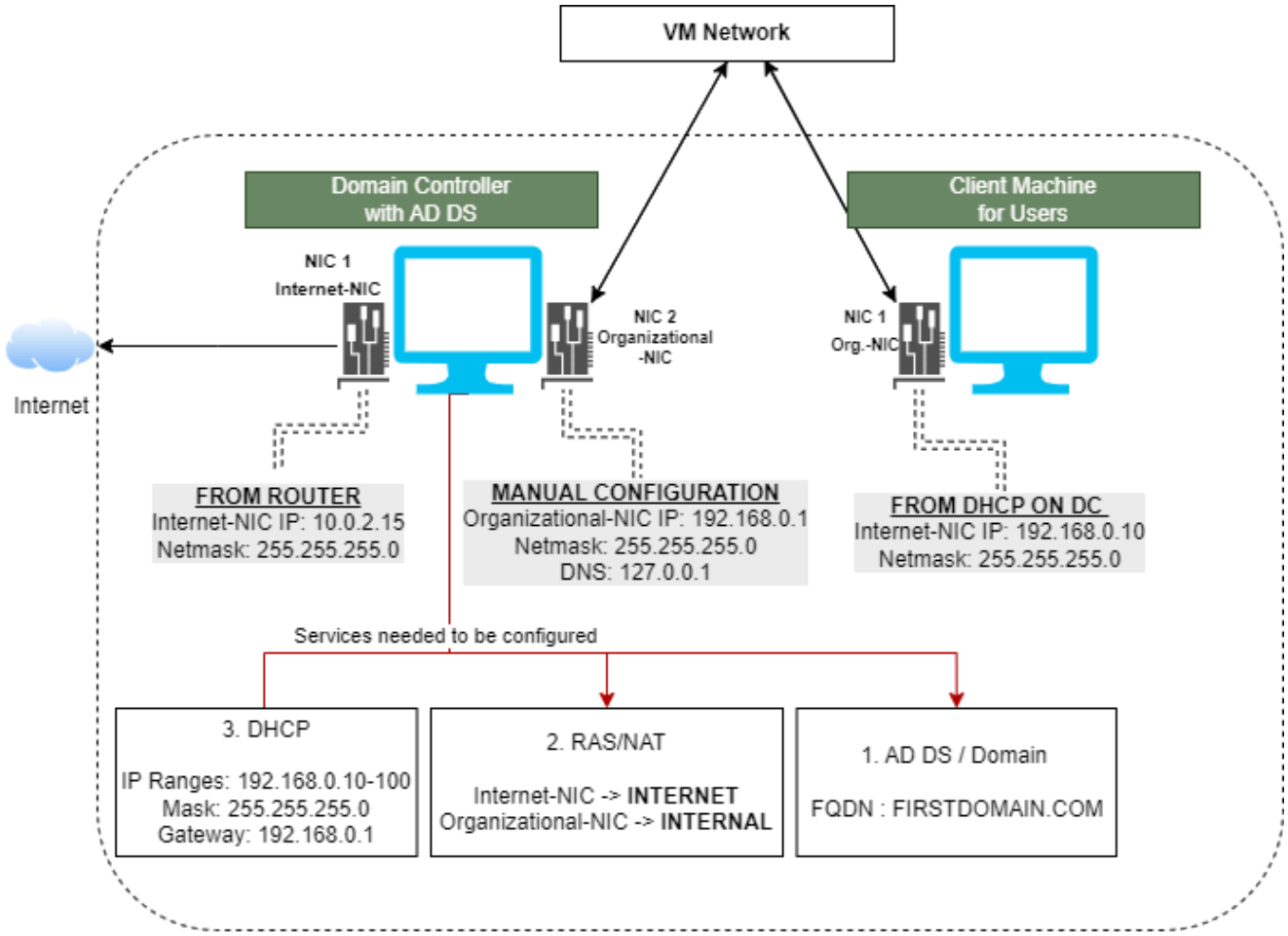
Active-Directory-Project

Project Overview

In this project setting, I aim to emulate a mini organizational IT setting where accounts are created and restricted based on organization requirements, using Microsoft Active Directory Services. We have an internal organization network where the domain controller on which Windows Server 2019 is up and running, the client machine that will be used by employees in the office and several user accounts for different users to log in and work.

Our primary objective is to automate the creation of 100+ users in the Microsoft Active directory, using Powershell. For this purpose, the following organizational network setting is assumed and we configure our services based on the following setting.

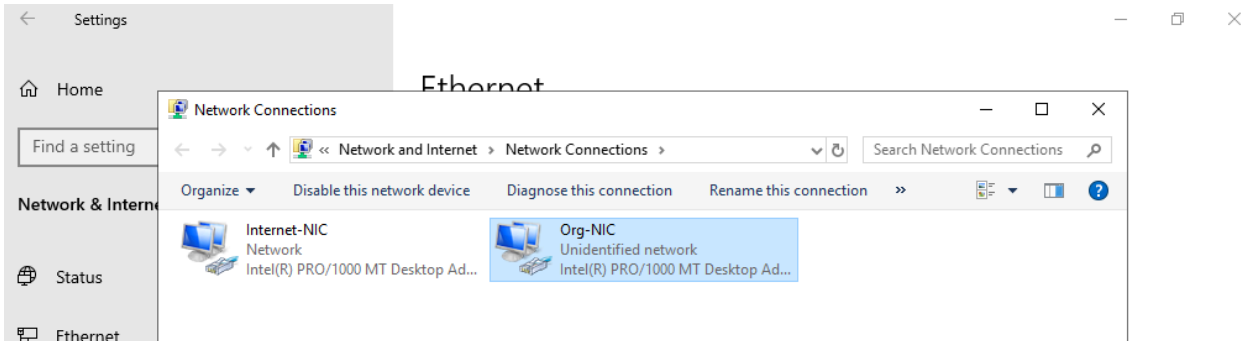


Setting up required OS in VirtualBox:

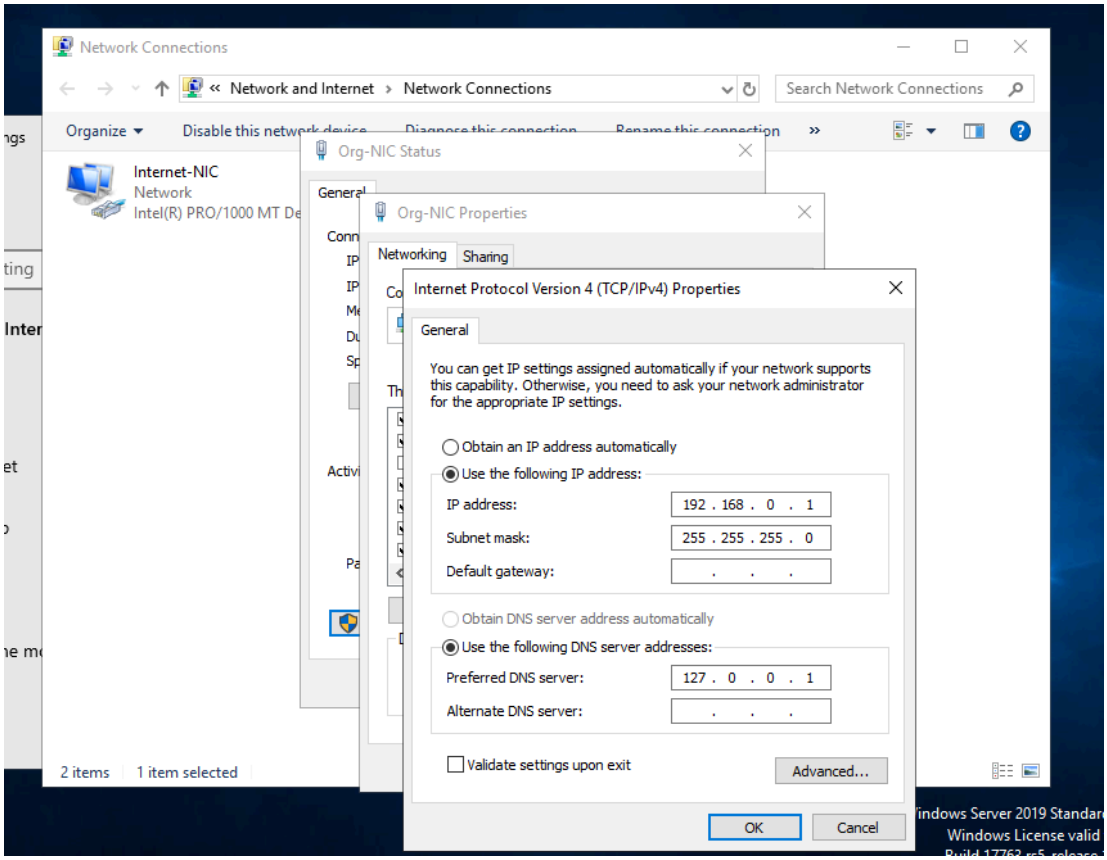
1. Install VirtualBox, it's pretty easy, just follow the steps for installation: https://www.virtualbox.org/wiki/Downloads
2. Download windows 10: https://www.microsoft.com/en-us/software-download/windows10
3. Download windows19 server (takes some time): https://www.microsoft.com/en-us/evalcenter/download-windows-server-2019
4. Meanwhile, go get ready with the VMs in VirtualBox for Windows server 2019
    4.1. Add a VM, give a name and select ‘other windows-64 bit’ from the dropbox
    4.2. Choose at least 2GB for Ram, Processors 2 (1 also works)
    4.3. Choose around 10 to 15 GB for hard disk
    4.4. Ensure VDI is chosen and hit Enter!
    4.5. For additional configuration of the domain controller, go to settings of the VM and choose 3 or 4 processors to speed things up and importantly in the networks tab, enable the 1st adapter to NAT and enable the 2nd adapter to internal network, click done. VM is ready
5. Click on the VM, when a pop up appears, select the windows 19 server we downloaded earlier. Follow the prompts and choose the custom section while asking for installation.
6. Wait for a while until the OS is installed and reboot it
7. Give a password you can remember
8. To unlock, Click on Input -> Keyboard -> insert Ctrl-Alt-Del and enter your password
9. We want to add guest additions to make smoother operations on our OS. Go to devices tab at the top in the virtual box window of the machine and select 'insert guest additions CD image'
    9.1. Go to File Explorer and click my PC, click on CD Drive D: and select VBoxWindowsAdditions-amd64
    9.2. Keep clicking next and once all additions are loaded, reboot your system.

Installing & Configuring Active Directory Domain Services:

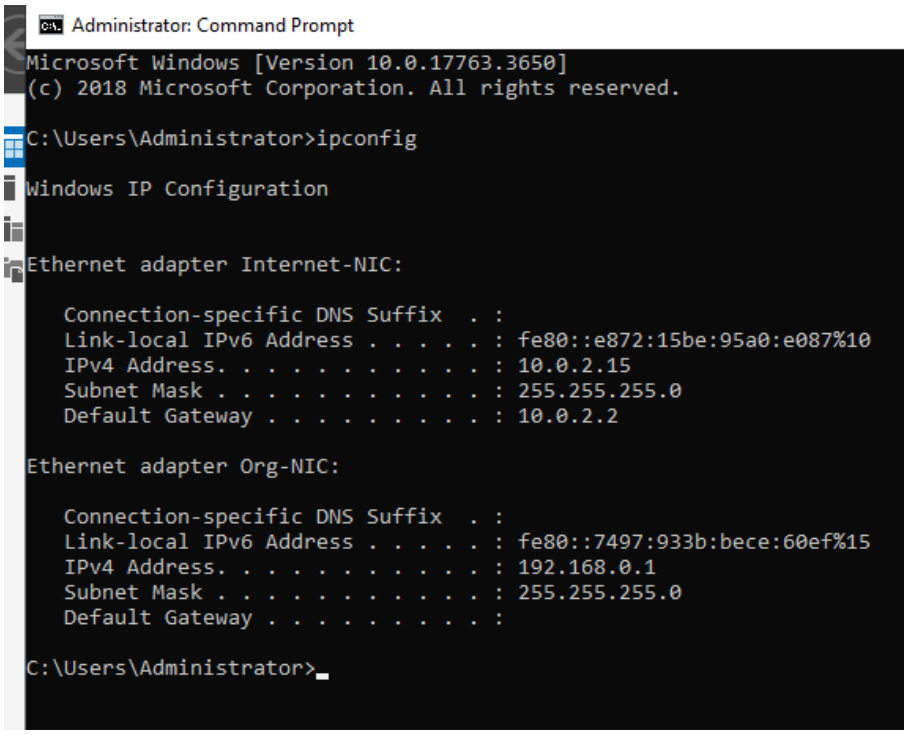
10. Go to settings -> network and ethernet -> Ethernet-> Change adapter options
11. Double click on either Ethernet options and figure out which one is connected to the internet. (Most probably Ethernet1 connected to the internet with IP 10.0.2.15.
12. This is the ethernet adapter that will be connected to the internet. Another adapter is connected to the internal network of the organization.
13. Rename both NICs so you can figure out which one is which. Following is how mine looks: Internet-NIC connects internet and Org-NIC connects to internal organization network



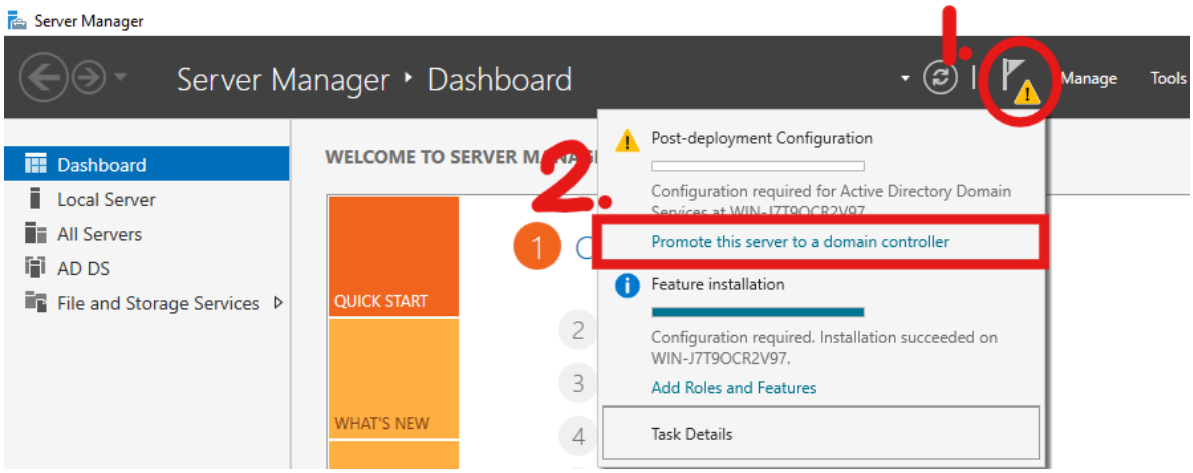
14. An important step here, we are assigning an IP address to Org-NIC ethernet. Click on it -> Properties -> Select Internet Protocol Version 4 (TCP/1Pv4).
15. Before entering the details, you need to figure out how many devices are in the internal network and base your subnet mask accordingly. Here for demonstration purposes, there is only one device in the internal network so we use a subnet mask of 255.255.255.0 that can contain 254 hosts, which is more than enough. As for the IP, choose any from the private ranges
16. I entered the IP address as 192.168.0.1. The domain controller itself will act as the default gateway, so this field will be empty
17. As for the DNS section, when we install Active directory, it automatically installs DNS, so the domain controller will itself serve as the DNS server. We can use the loopback IP address or the address we just assigned in step 16. Following is the setup



18. To ensure the settings have been saved, we can go to Start, type ‘cmd’ and hit enter. Type in the command ‘ipconfig’. Following is how my NICs are set up



19. Next, go on to start and open Server Manager application, click on Add Roles and Features, a wizard will open. Click next twice and ensure that our server is selected (if you have more than one server, otherwise it's already selected), click next and choose ‘Active Directory Domain Services’ in Server Roles. If another Add Roles and Features Wizard opens, click on ‘Add Features’.
20. Click on next thrice and, select install in the final step. The installation takes a while to finish. On successful installation close the window.
21. We must now configure Active Directory Domain Service (AD DS). Click on the warning sign on the Server Manager dashboard shown in the screenshot:



22. In the wizard that opens, select ‘Add a new forest’. Give a domain name (firstdomain.com in my case). Click next and give a password.
23. Keep selecting Next, until Install. Wait for All prerequisite checks to pass and select install. Upon installation, the device will automatically restart to apply configured changes.

Creation & Configurations of Admin account with AD DS

24. Instead of working with the built in administrator account, we are going to create our own dedicated admin account. Login with your credentials in the server, notice the domain name is added along with the username.
    - 24.1. Go to start -> Windows Administrative tools -> (carefully select) Active Directory services Users and Computers.
    - 24.2. We will create an organizational unit in our domain, and then add our admin account in it. Right click on the domain, click on ‘New’, then

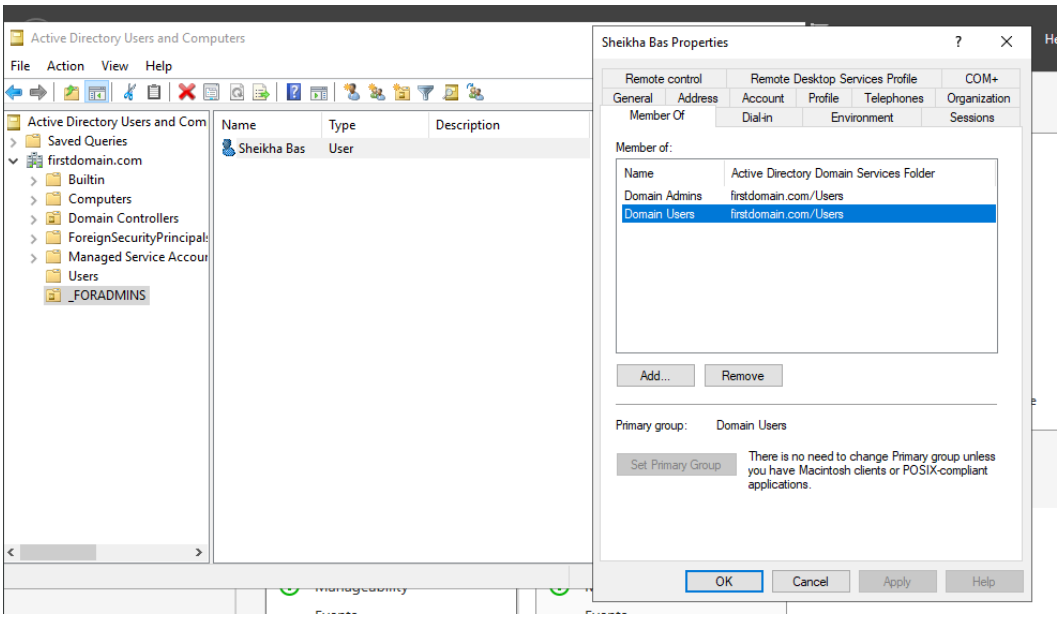
Organization Unit, give a decent name. You can also consider this as a folder in Active directory (_FORADMINS in my case).

24.3. Right click on the folder, go to new and select ‘user’. Fill in the details, a conventional method to use for a logon name is starting with a-<yourname>

24.4. Click on next and give a password. Since we are not dealing with password policies, we select the option ‘password never expires’ only and click on next.

24.5. The account is still not admin yet, go to properties -> member of -> add. Under the ‘Enter the object name..’ Type in Domain Admins and click check names. An underline appears on Domain Admins, click ok. Click apply and then okay.

24.6. Now we have our own domain admin account. See following:

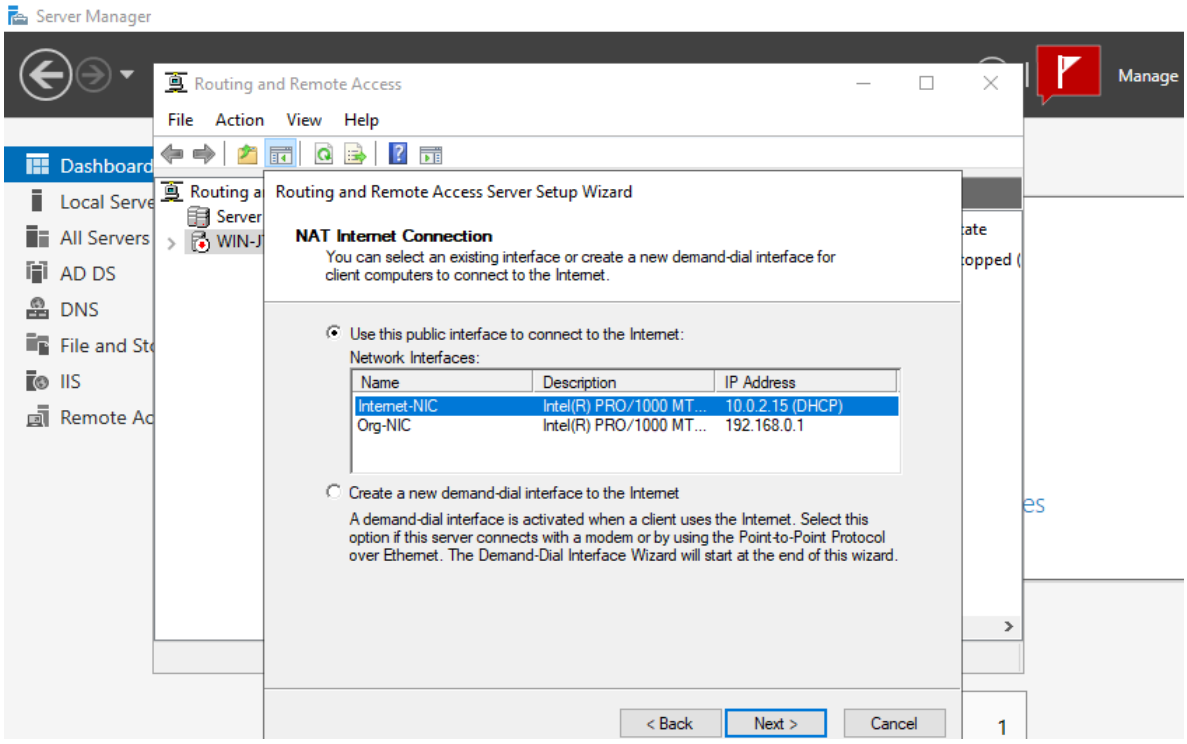


25. Sign out from the current account, instead of logging into ‘FIRSTDOMAIN\Administrator’ account, we will log into the above account we just created.

26. Click on ‘other user’, enter the user logon name you gave in step 24.3, and the password. Now you are in your admin account for your domain controller, yay!

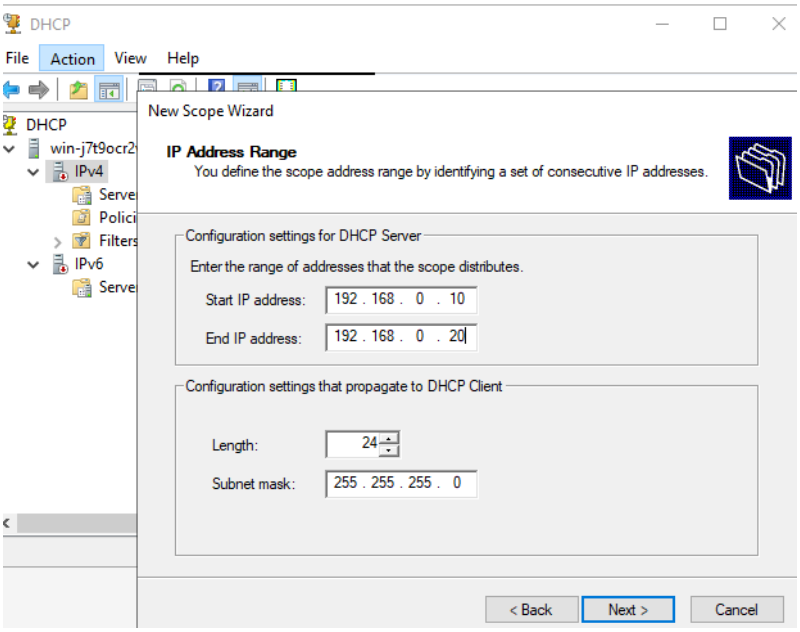
Install RAS/ NAT and DHCP configurations on Domain Controller

27. This section helps the clients that connect to our domain access and browse the internet. Click on start -> Server Manager
28. Click Add features or roles, selecting next except in the ‘Server Roles’ section, select ‘Remote Access’ and keep clicking next until ‘Role Services’ and check on ‘Routing’ option. When a wizard opens, click on ‘Add Features’. Keep clicking next, all the way through the install, wait till installed
29. After installation, go to -> Tools, select ‘Routing and Remote Access’. Right click on the server that appears in the new wizard open and click on the first option ‘Configure and Enable Routing...’.
30. Click Next and for Configurations, choose the service NAT and click next. This is because our domain controller acts as the medium through which the internal organizational systems can access the internet. NAT is required to convert private IP addresses to public ones so systems can browse the internet, but in a very controlled fashion since NAT is on the domain controller itself.
31. In the NAT Internet connection window, click on the interface that is configured to connect to the internet in step 13. In my case, I renamed it as ‘Internet-NIC’ (See following). Choose that and click on next and then finish. A warning might pop up indicating a user action to manually open ports on the firewall to enable routing and remote access, this is expected. By this step, RAS/NAT have been successfully installed and configured.



32. In the coming steps, we will install DHCP services and configure the service, similar to how RAS/NAT is done.
    - 32.1. Click on 'Add Roles & features' in the Server Manager Dashboard.
    - 32.2. Keep clicking next until Server Roles section, double click on DHCP server, click on Add features in the new wizard open.
    - 32.3. Keep clicking next all through install, once finished, go to tools -> DHCP
    - 32.4. Click on the server node in the wizard, under which IPv4 must be selected
    - 32.5. Now click on Action menu and select New scope
    - 32.6. Give a name that you can easily identify the scope. I will name this as the IP ranges distributed in the internal network. In step 16, verify your IP ranges.
    - 32.7. Accordingly, my IP ranges can be anywhere from 192.168.0.2 to 192.168.0.254, as the subnet mask is 255.255.255.0. IP 192.168.0.1 can be used as network address and 192.168.0.255 as broadcast IP address
    - 32.8. In my case - **Name** : 192.168.0.10-20 **Description**: Only 10 IPs available.

32.9. In the next wizard, enter starting IP address and ending IP. Enter the mask length as 24 and as subnet mask 255.255.255.0.(See following). Click next.

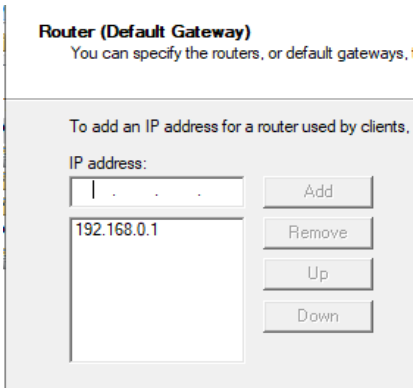


32.10. If specific IPs need to be excluded you can add that in the next wizard.

32.11. You can configure how long IPs can be leased before they disconnect and assign another IP. I am going to keep on 5 days, this can be 5 hrs depending on use case. Click next and next again.

32.12. To add an IP as a router used by clients, we need to route the traffic from the internal organizational network via internal NIC to the external NIC that has connected to the internet and this is why we have configured NAT and DHCP on the domain controller. So, the internal NIC IP address (step 16) acts as router to internal network clients. Enter that IP and click on add.

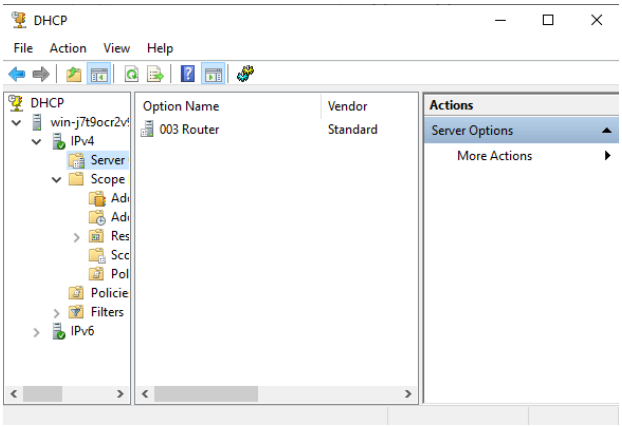
32.13. The setup looks like the following: Click next.



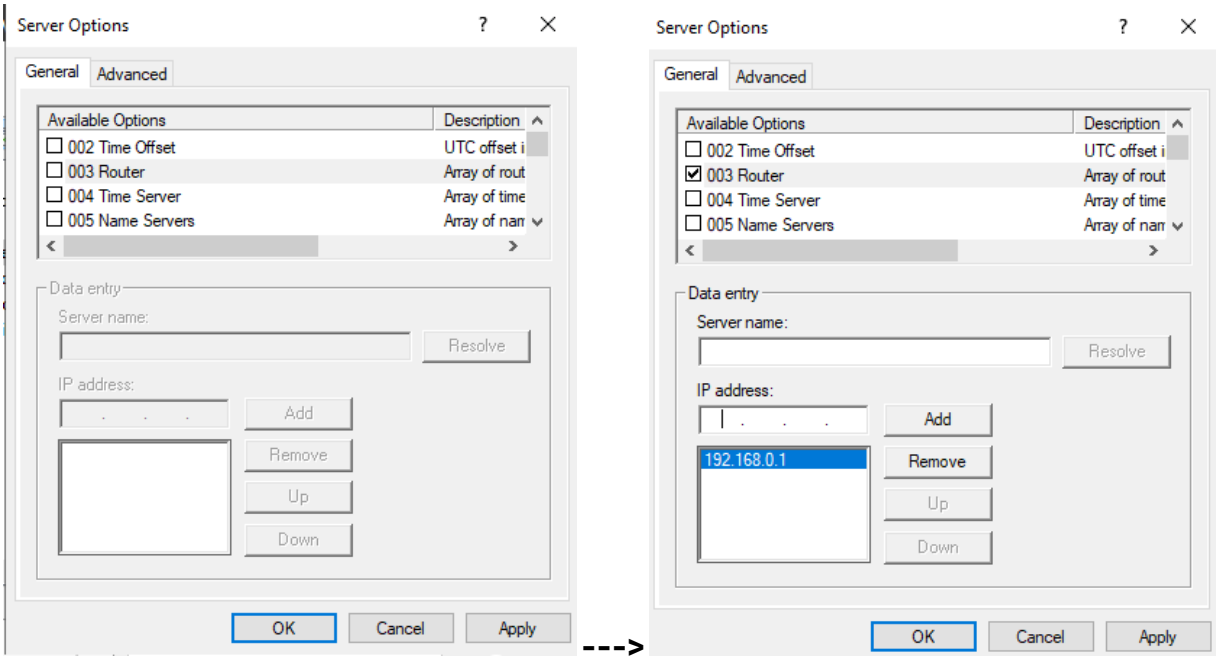
32.14. DNS is configured with Active Directory, click next, next again for WINS and check on ‘Activate now’ , click next and finish the setup.

32.15. Now right click on the server node and click authorize and right click again to refresh. Green checkmarks should appear on both IPv4 & IPv6 icons.

32.16. Finally, once everything is set up, go to tools -> DHCP click on the server node, click on IPv4 node and select ‘Server’. If the router information appears as shown below, leave it as it is. If not, follow 32.17.



32.17. Go to the ‘Action’ tab at the top of the window and choose ‘Configure Options’. If your setting looks like the following screenshot, then check on the Router, enter your Internal NIC IP and click ‘Add’, ‘Apply’ and ‘OK’.

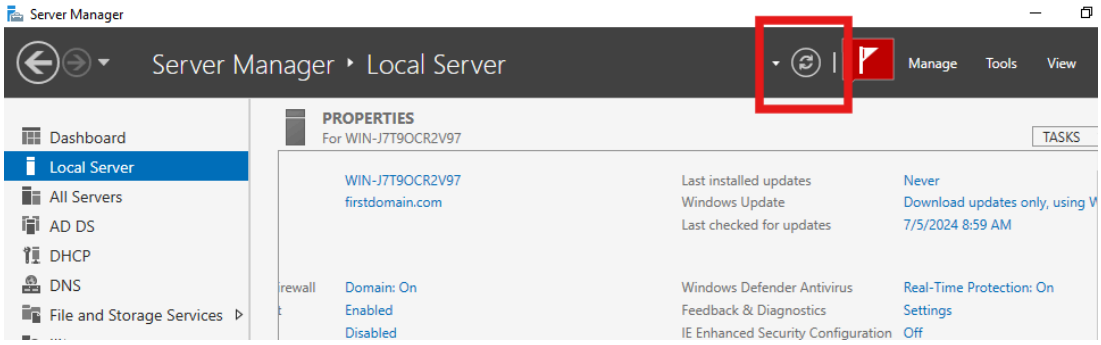


Powershell Script to create 100+ users in Active directory.

By now, we have gone through the complete steps to set up an Active directory and create a user in it. We cannot always follow the same while creating thousands of users in an organization. We might need to automate and create user accounts more efficiently.

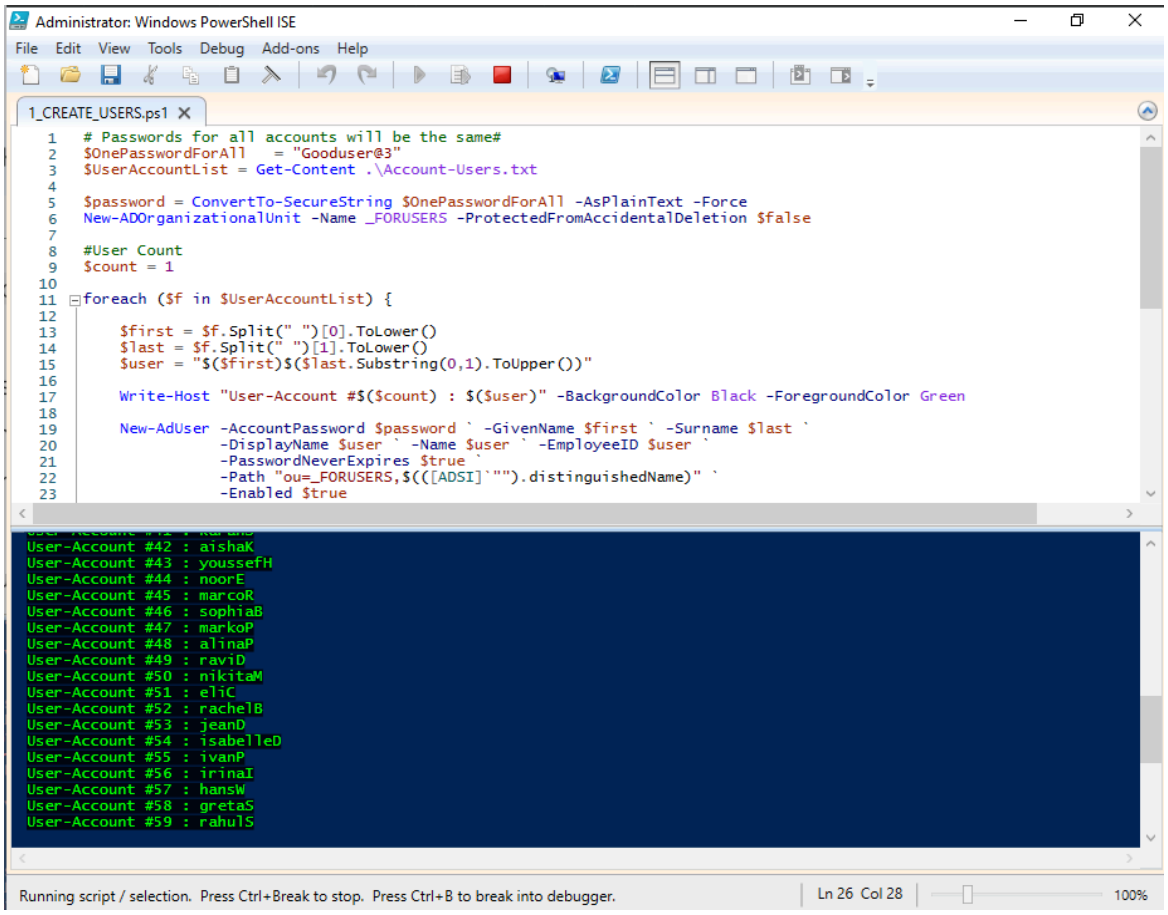
For this purpose, we will utilize Windows Powershell to create a script that creates the specified number of user accounts in the Active Directory. The script takes the list of accounts that needs to be created and a password for all the accounts. The script is available on my github.

To enable downloading the script, you need to switch off enhanced security. Normally this is not advised, only trusted sites should be listed and allowed to view. Since this is a lab, we will skip this and get to work with the script. In the ‘Server Manager’, click on configure the local server and find ‘IE Enhanced Security Configuration’. Click on ‘ON’ next to it and select off for both and click the refresh button.

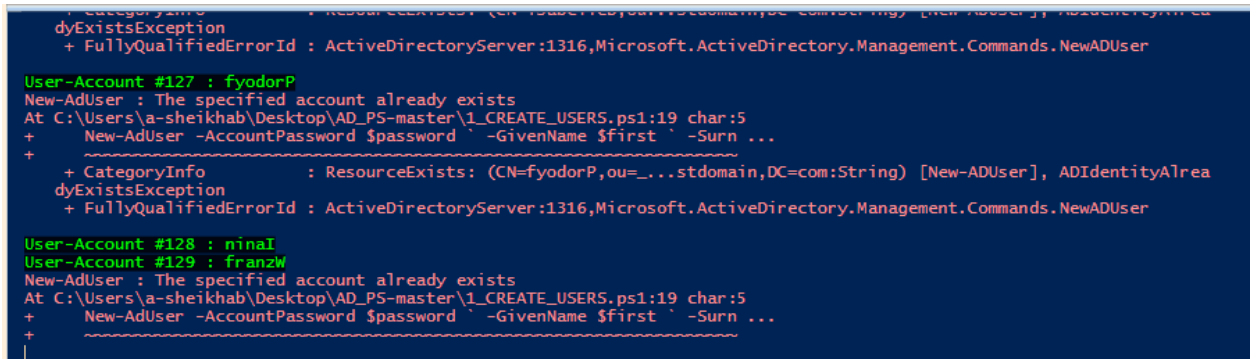


33. Download the script from: github.com/oliv6
34. Save and extract to Desktop.
35. Go to -> Start -> Windows Powershell ISE -> right click open as Administrative.
36. At the top of the window, select open file and open the powershell script
37. Type in the command line:
    37.1. `Set-ExecutionPolicy unrestricted` and select yes in the window that appears and run the script.
38. The code is scripted to take the first name and initial of the second name from the accounts-list folder. Just like in the step 24.2., `New-ADOrganizationalUnit` in the script creates an organizational unit in the directory for regular users without any admin privileges.
39. The name list was created using Gemini AI, you can also create your own list based on your requirements or copy the same list as mine.

40. Click on the green play button to run the script



You might find as few errors as the following, this is due to repeating names in the list and if you provide a bad password, errors might pop up as well.

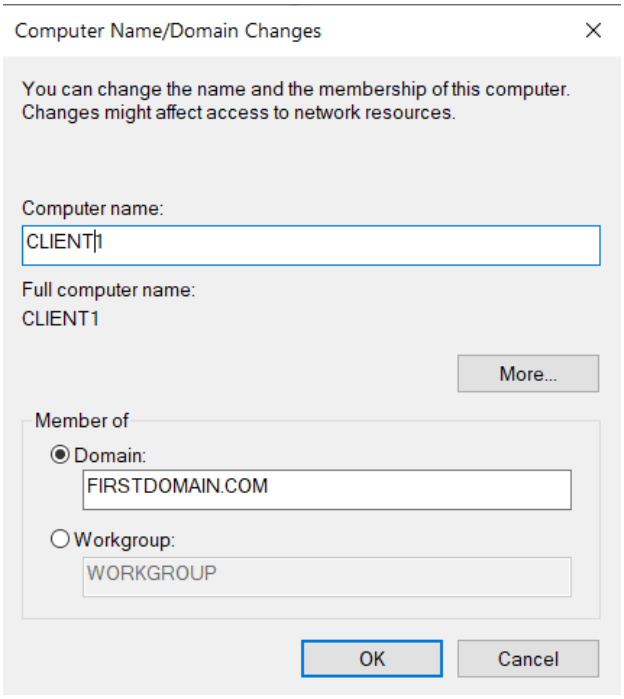


41. Go to Server Manager -> Tools -> Active Directory Users and Computers, you will find _FORUSERS organizational unit (folder in the directory), click on it to view all the users that were just created.

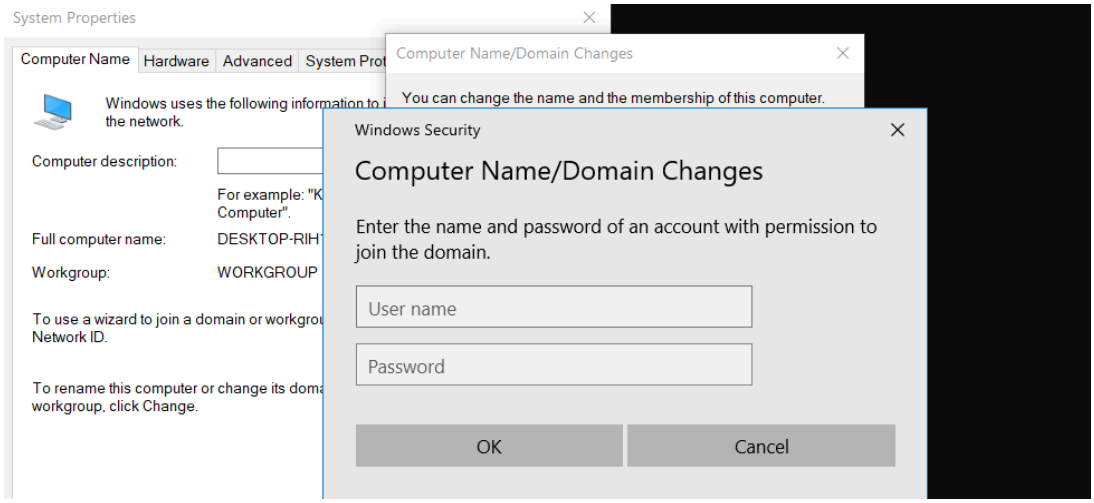
Therefore, we effectively added several users in the directory with Powershell within a short span of time. Instead of manually creating users with GUI which is also error prone, with Powershell, this was automated efficiently.

Connecting Windows Clients to the Domain Controller

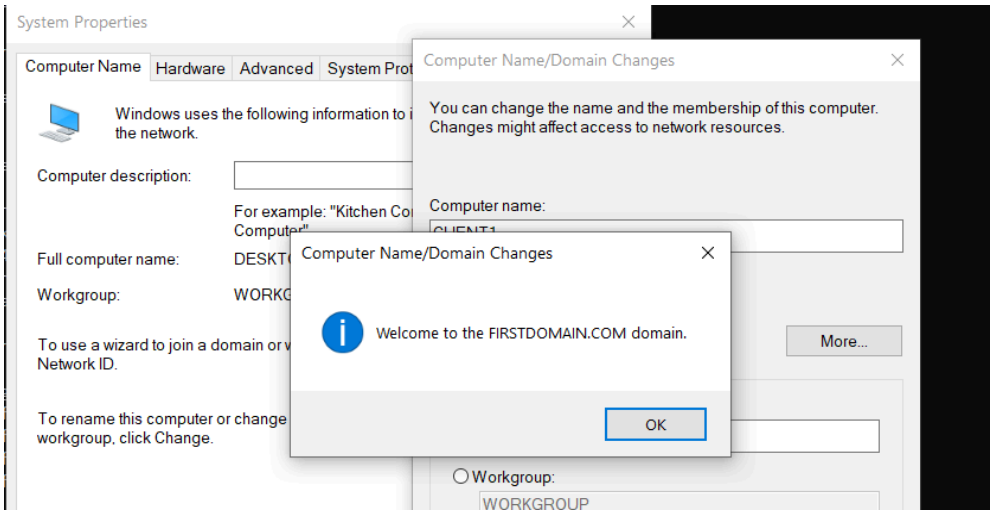
42. Go to the link https://www.microsoft.com/en-us/software-download/windows10 and download the tool and then download windows10 ISO image.
43. Follow the same steps you implemented to create the domain VM in step 4, except for 4.1. where you need to choose Windows 10 from the dropbox and 4.5. where select only one adapter and choose Internal Network.
44. After all the installation steps, the VM is up and running, go to -> start and type hostname. Some name of the machine is shown, let's change this and add the machine to the active directory by using one of the accounts we created.
45. Go to Start -> Settings -> About -> Rename this PC (advanced). In the 'To rename this computer...' section click 'Change..' and give a hostname and at the same time, select the domain option and enter the domain name, click OK.



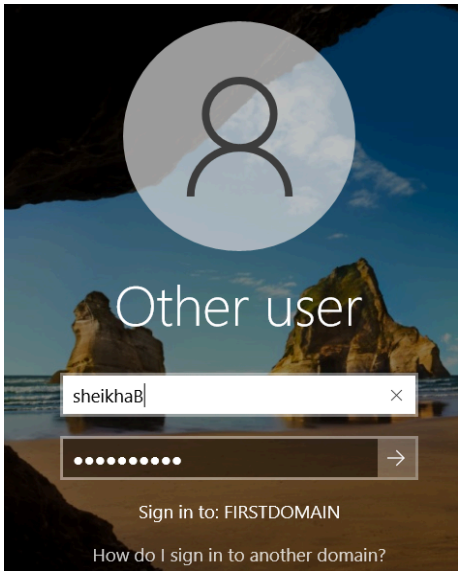
46. When prompted, enter the username from one of the 100 accounts we created in the domain and the password mentioned in the powershell script:



47. Upon successful joining, the prompt shows as follows and restart your VM.



48. Before logging in, change the user to the account you just added and enter



Thus, we successfully added a client to the domain with the authorized account on the active directory domain controller. With the client machine, we can enter with any credential we added in the active directory domain.

Summary

In a nutshell, we installed, configured, and set up active directory service on the domain controller within the Windows server 2019 virtual machine. All virtual machines were created using VirtualBox. We also configured other necessary network services like NAT, DHCP and Admin accounts. Most importantly, the most fun part of all, we automated the creation of over 100 regular user accounts in the microsoft directory using PowerShell. Atlast, we also joined a client host to the domain and logged in using the created user accounts.

Overall, this was a very comprehensive, detailed and hands-on experience with PowerShell and Active Directory services. It was a very fun and enjoyable experience to effectively use technology and see how task complexity can be reduced exponentially!

THIS MARKS THE END OF THIS PROJECT, THANK YOU!