Active Directory Pentesting: Lab Setup

Today in this article we will be learning how to set up an Active Directory Lab for Penetration Testing. Active Directory is Microsoft's directory-based identity-related service which has been developed for Windows Domain networks. Here we will see step-by-step methods to build an Active Directory in Windows Server 2016 on a virtual machine. So, let us get started with configuring the lab.

Table of Contents

Introduction to Active Directory

The role of a directory is to store information about the objects present within it, but the Active Directory not only stores data but also provides it to the Network Administrators and the users of that particular domain whenever it is requested. It generally stores important information about the users like their names, passwords, contact information, etc and provides it to other users with authority in the same network to make use of the available information.

It stores data in a structured form hierarchically. It can have upright security with logon authentications and by having access control over the objects present in the Active Directory. For easy management one can also implement policy-based administration.

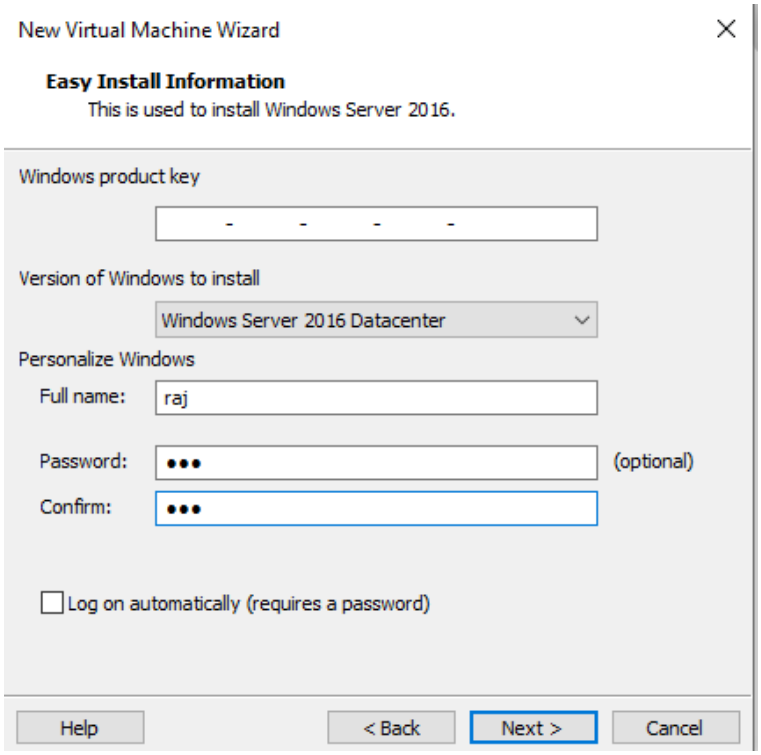
Lab Requirements

- Virtual Machine (VMware Work Station/Player)
- Windows Server 2016

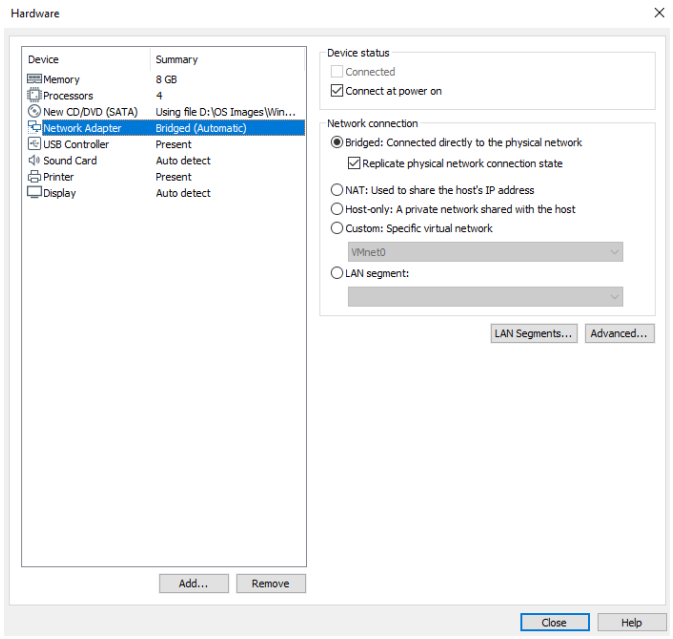
- Windows 10 Pro Operating System (Clientt)

Configuring Windows Server 2016

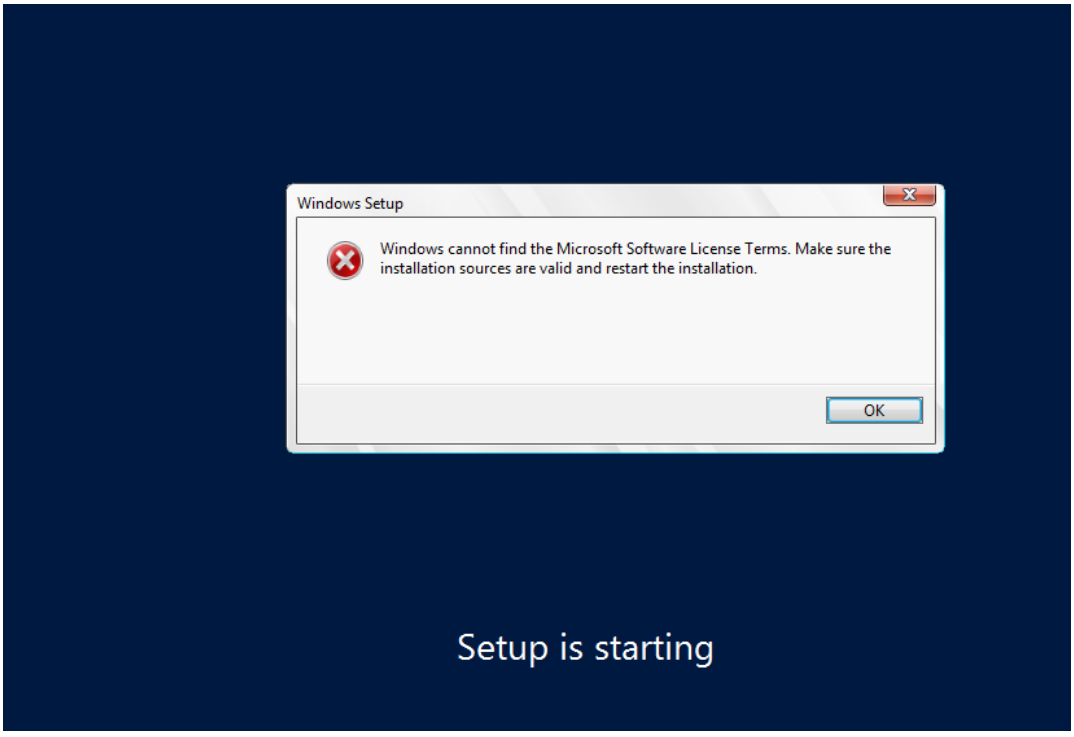
Power on your VMware, and let's begin with the installation by creating a new Virtual machine from the File option. Here you will personalise your Windows system by providing it with your username and the password that you want to set. Then click on Next to proceed.



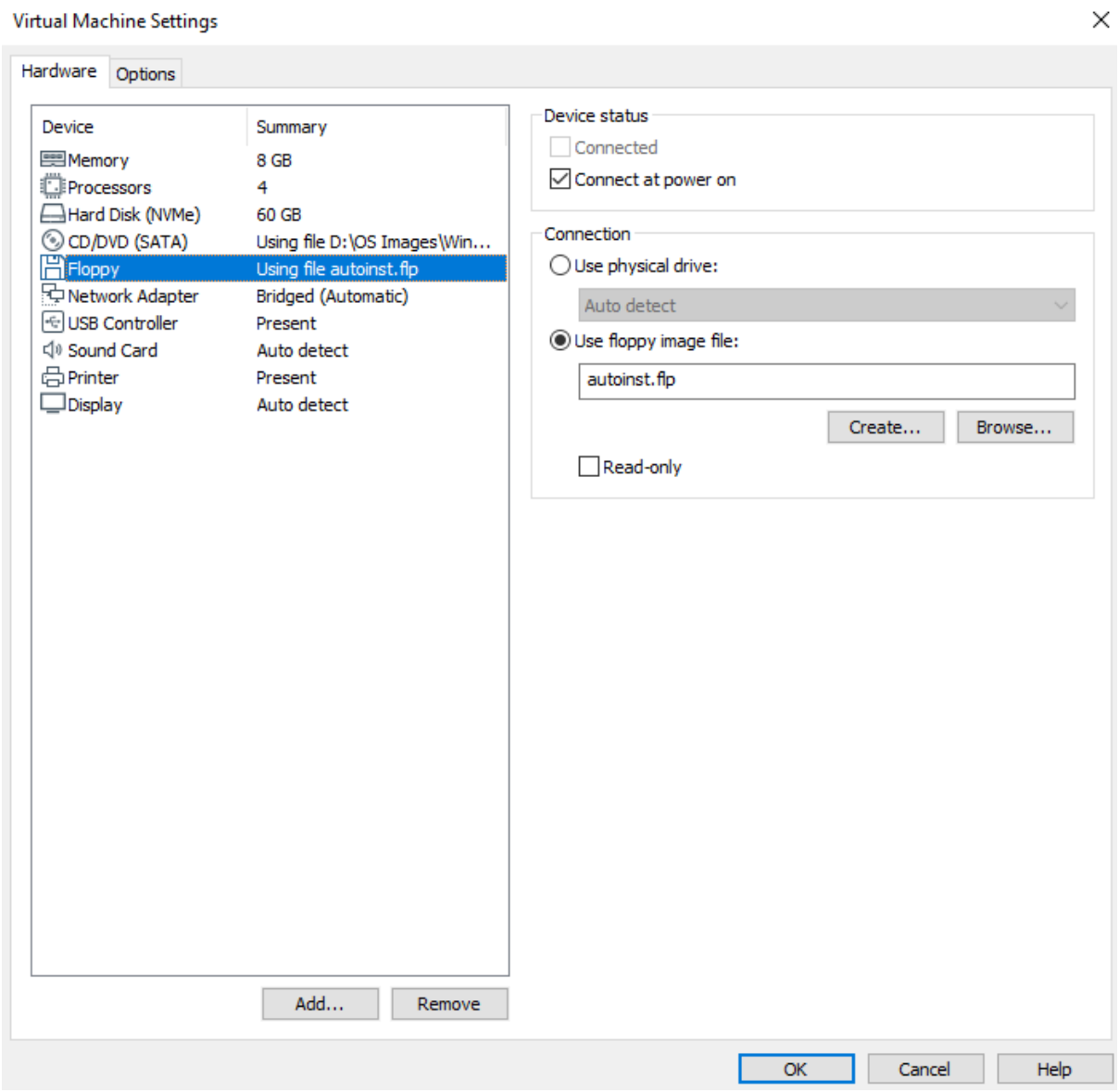
Now go to Virtual Machine settings and click on Network Adapter settings and make sure that there is a bridged connection where the host system's physical network connection will be replicated. Let's close this and move ahead.



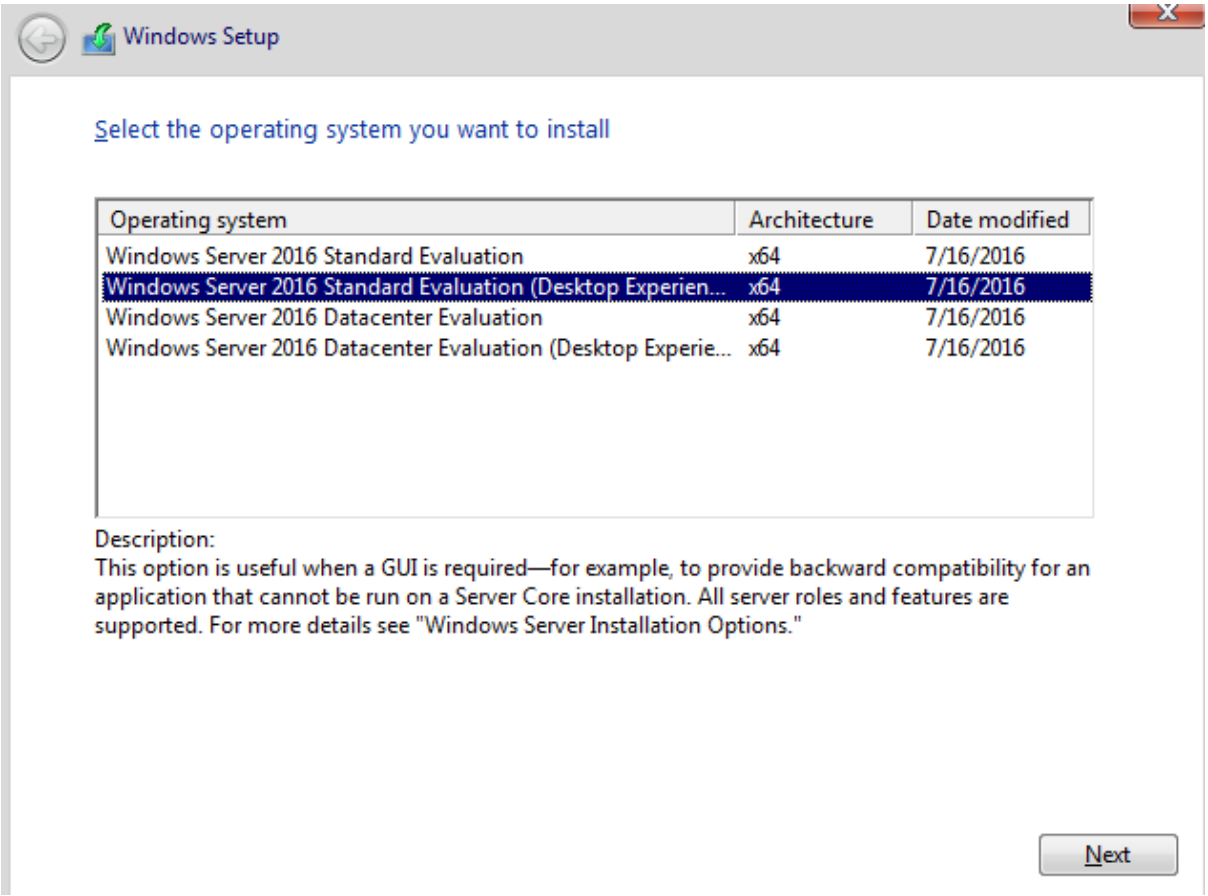
Here you see that the setup did not proceed, therefore let's go back and fix this error from occurring.



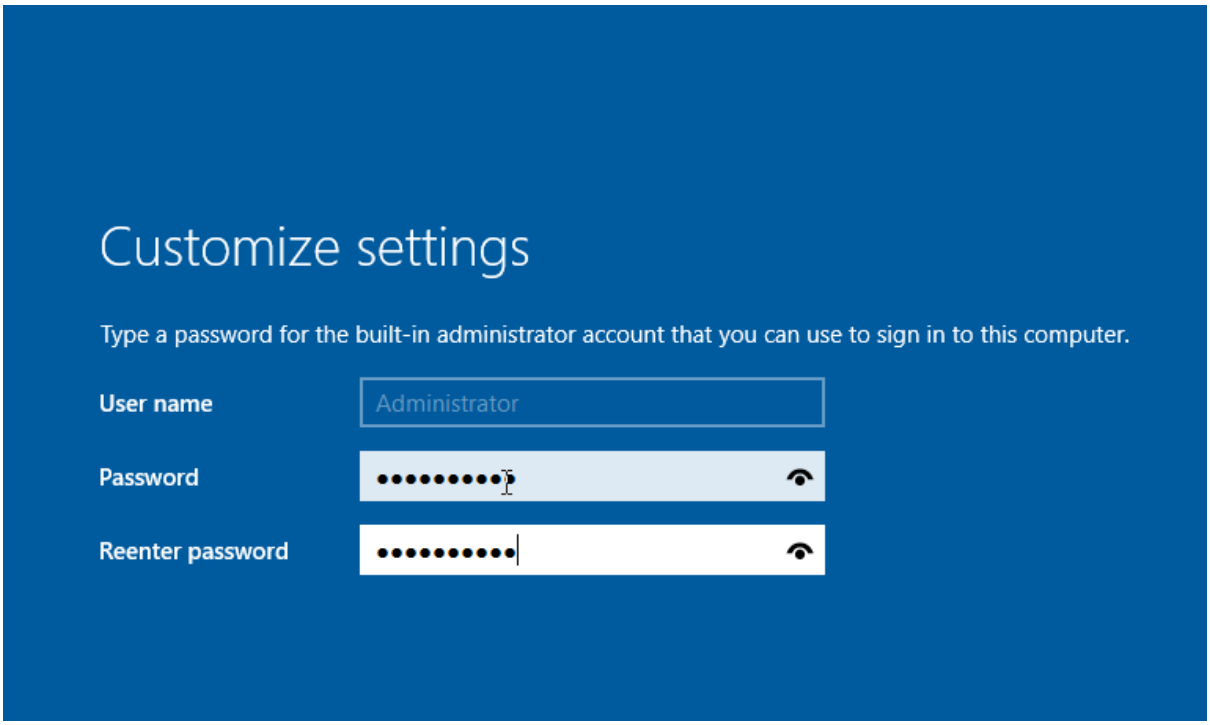
We will go back to Virtual Machine settings and click on Floppy, there under the connection option and choose the Use floppy image file option to make it work like a charm and proceed.



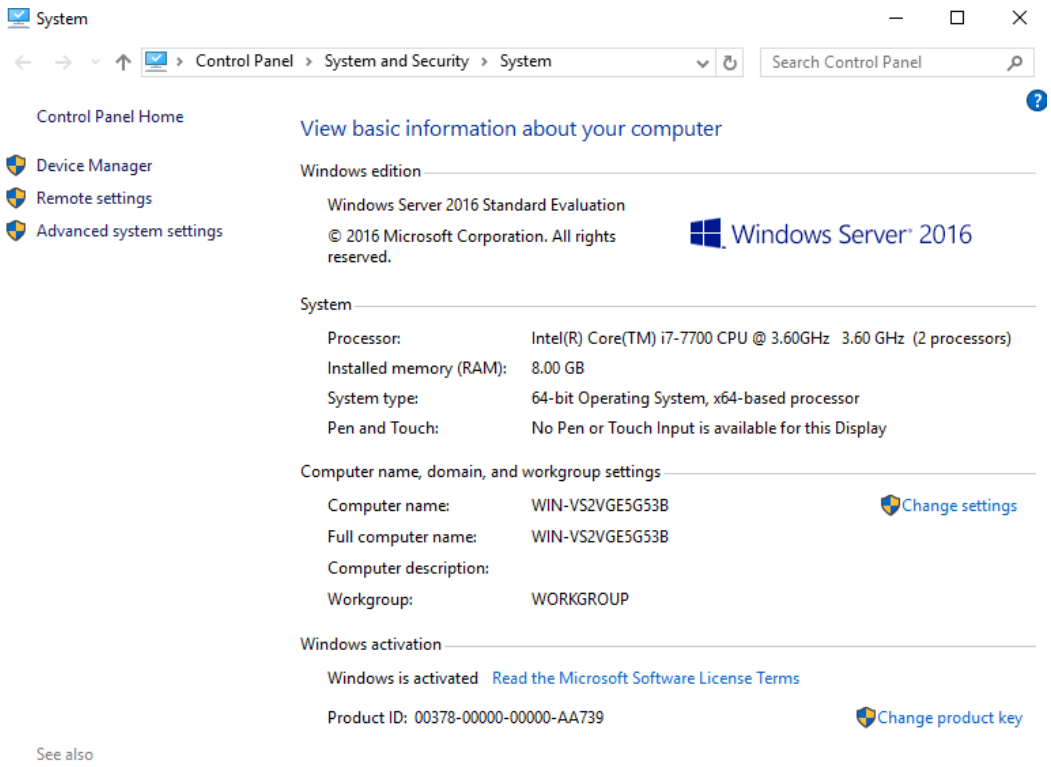
Now you will select the operating system to install from the four options given below. Here we use Standard Edition with the GUI to have a better user-interface. The Desktop Edition provides much better features as compared to the server-core as it has very limited functions. Click on next to proceed.



The operating system should start installing and under the customize setting option enter the password you want to put for the default administrator account.

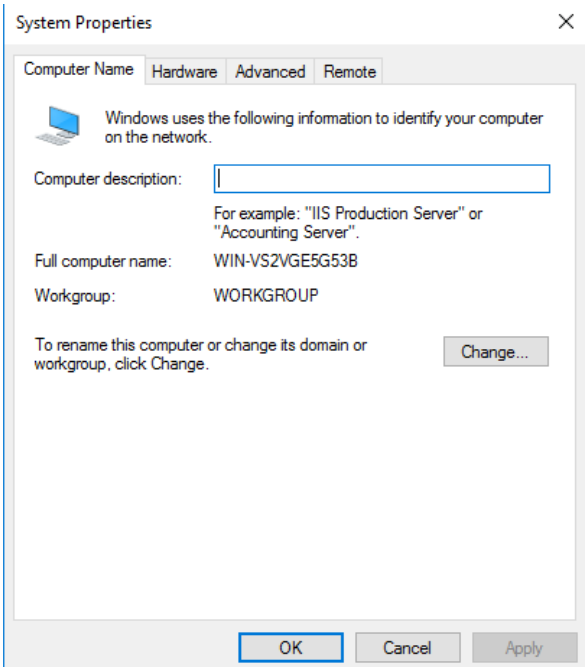


Now you see that your server is installed and ready to use and can find all the basic details on the server under the system option of the control panel.

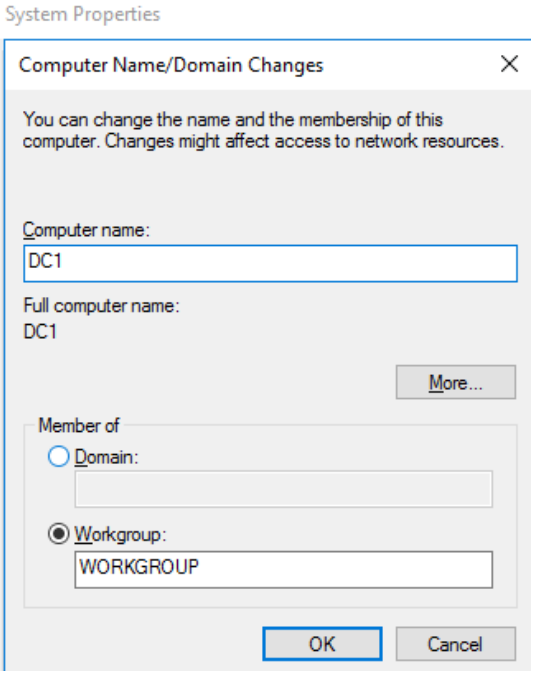


Installing AD DS

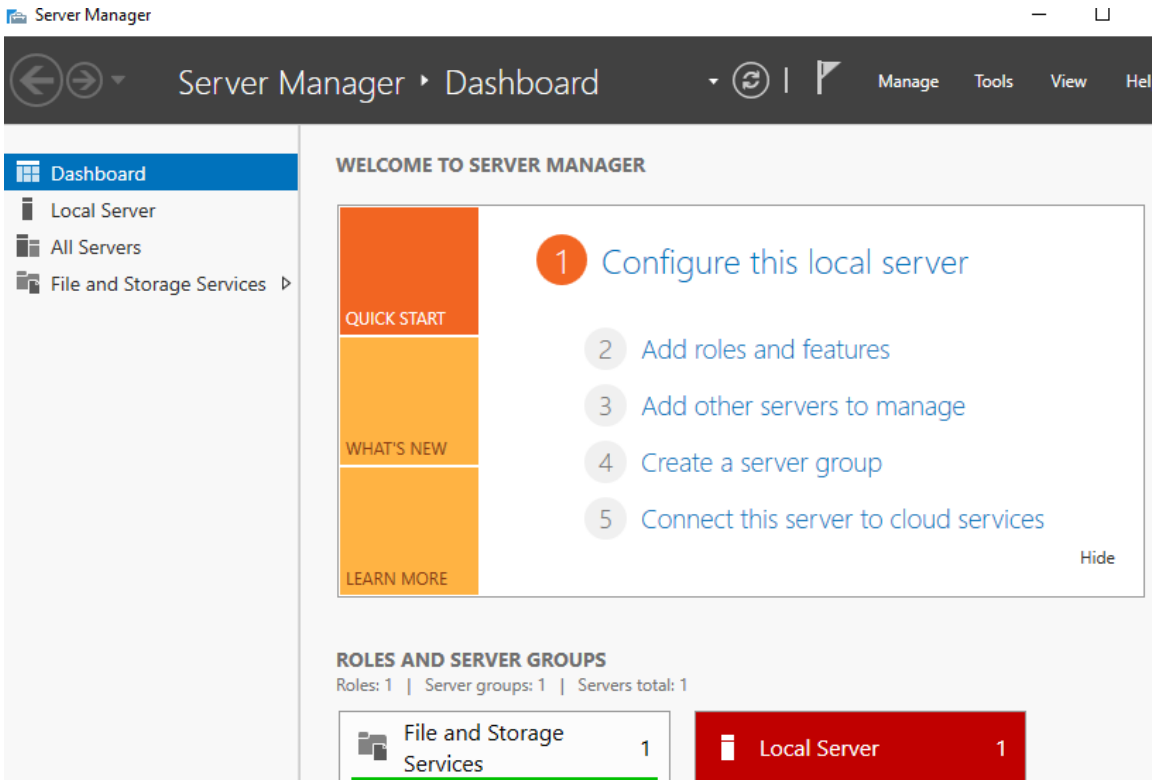
Now let us open the system properties from the 'Local Server' option and let us make changes to the domain name.



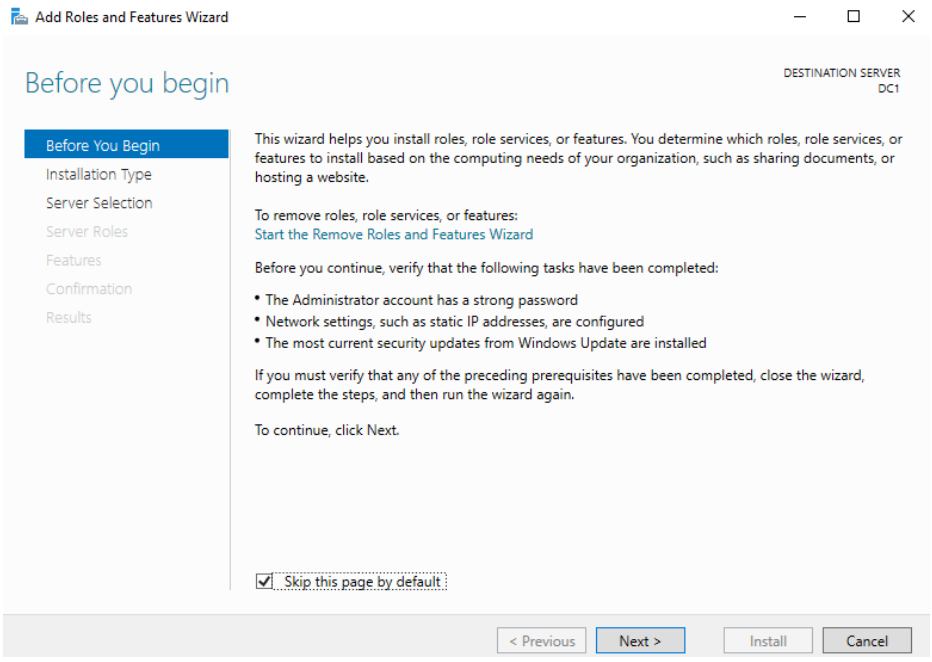
Let's keep the computer name as DC 1 and make it the member of the workgroup with the name 'WorkGroup'. On finishing this, click on 'OK' to proceed.



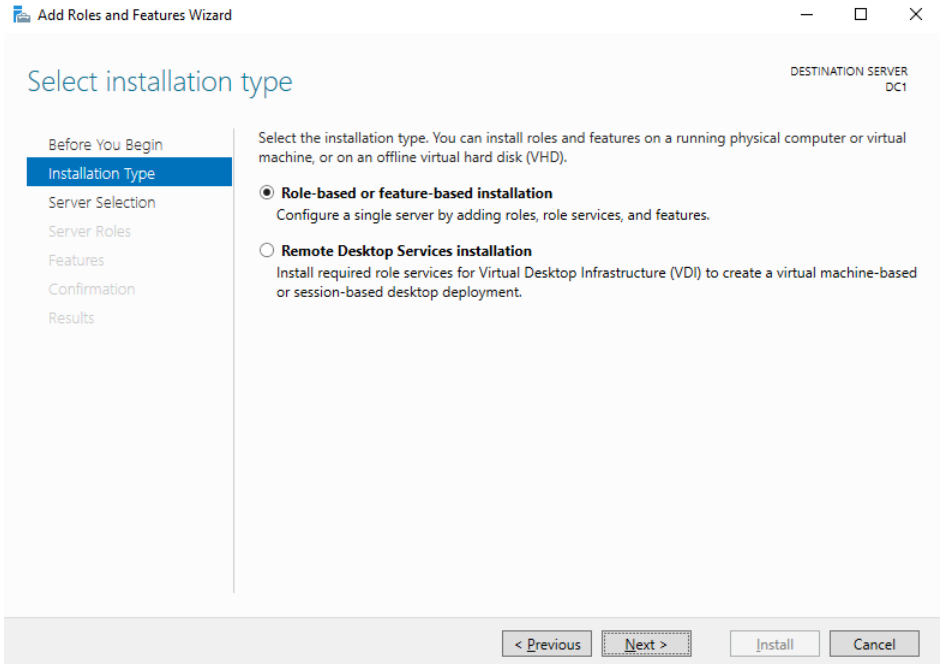
Come back to the dashboard and now let's begin with configuring the Active Directory role. Click on the Manage option at the top of the Dashboard. Then click on 'Add roles and features.



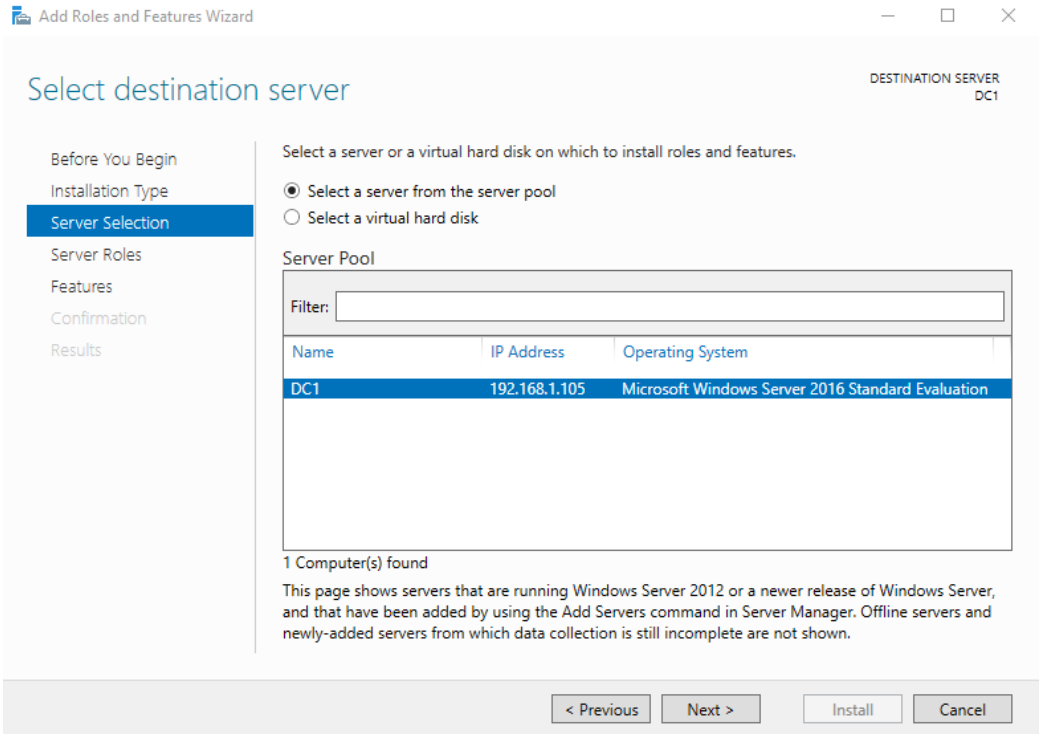
You see the installation wizard before you and click on 'next' to proceed.



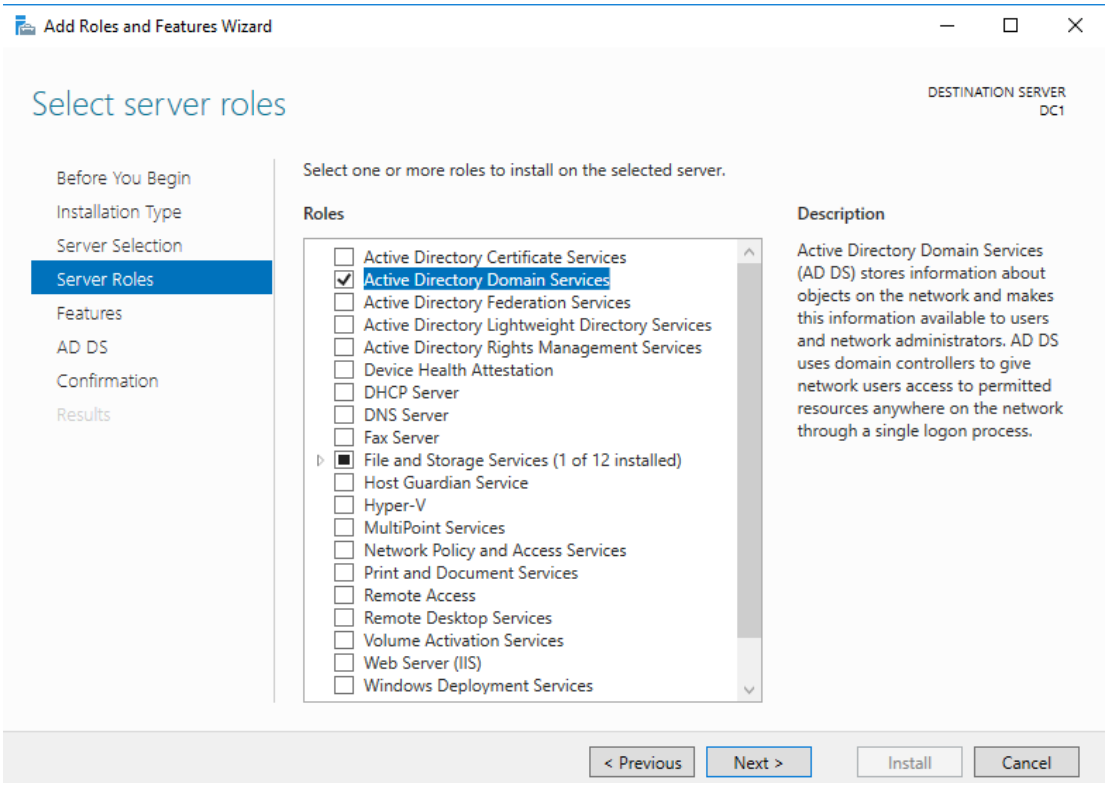
Then select Role-based or feature-based installation as it allows you to manually configure all the prefered roles at your convenience.



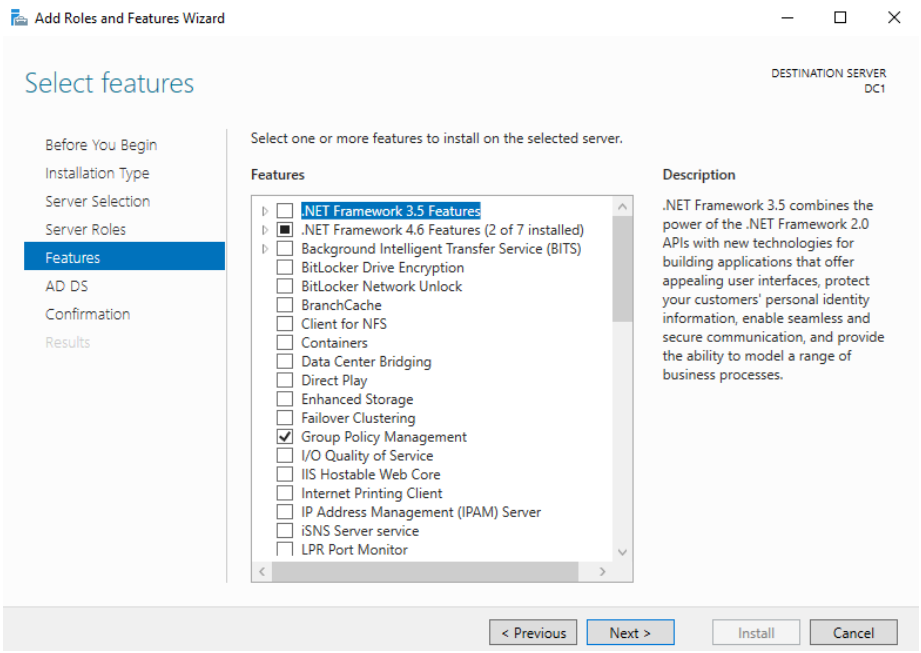
Choose the server you have created from the server pool that is available before you.



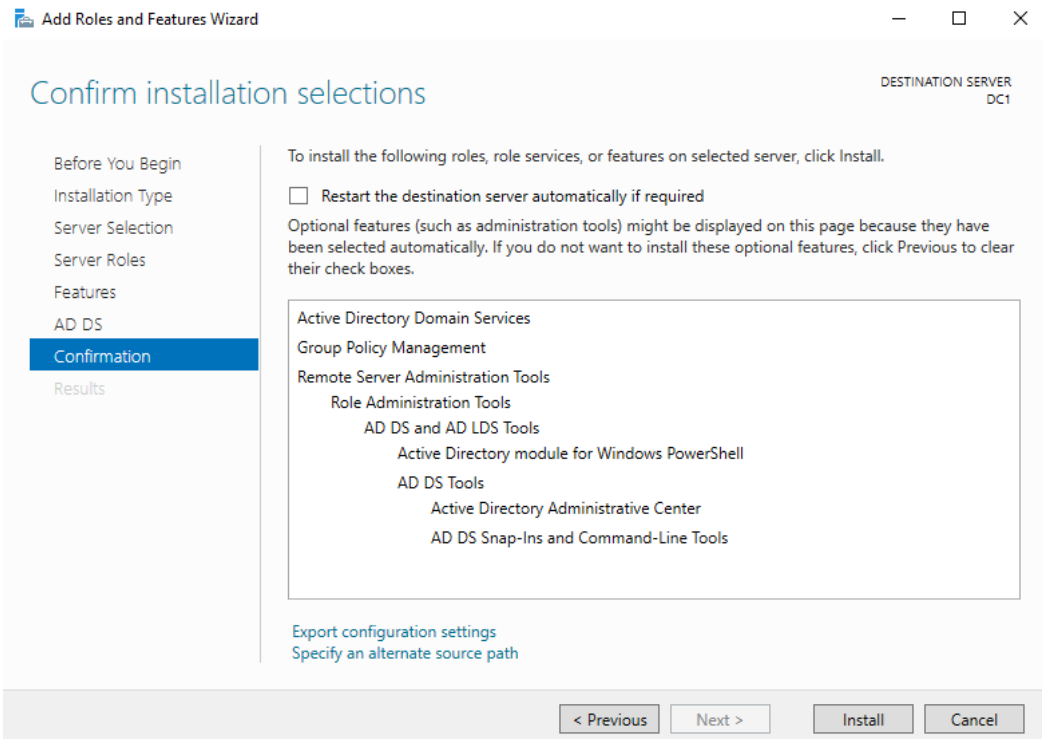
Now choose the server roles you want to add. Here we require Active Directory Domain Services. We check that option and click next to proceed.



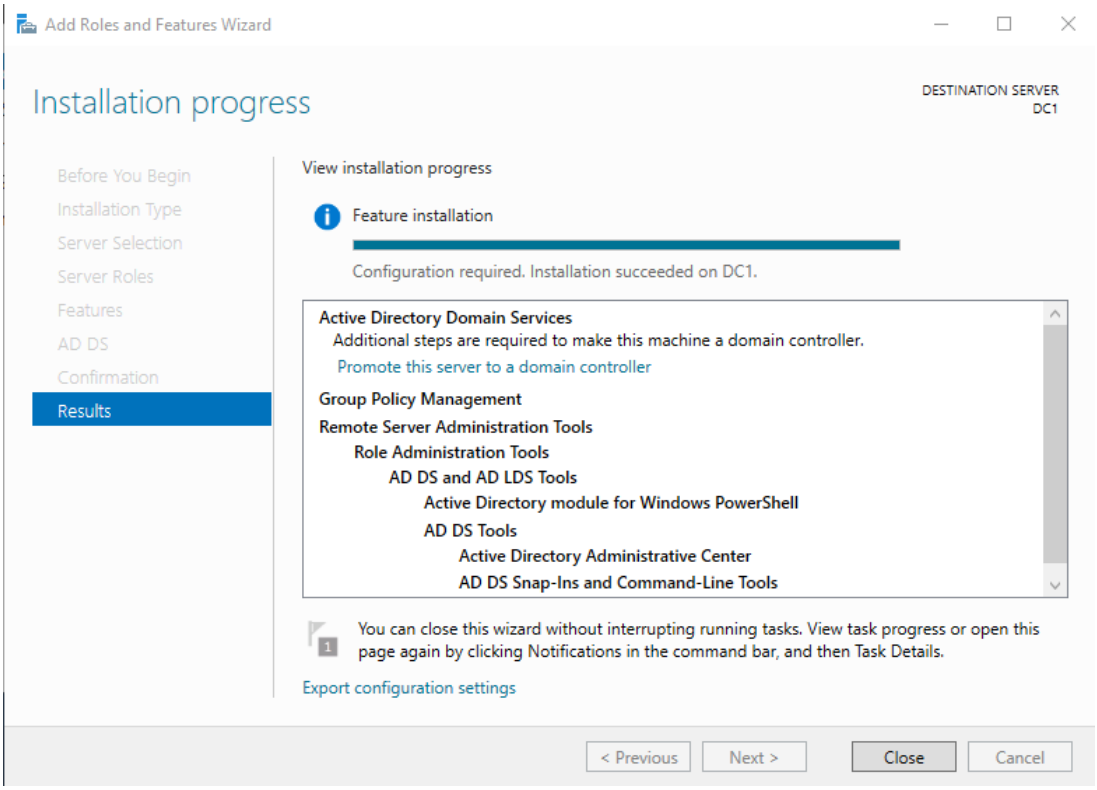
In features installation Choose Group Policy Management. It is a management feature in Windows that allows you to control multiple users and computer configurations present in an Active Directory environment. Click on Next to proceed.



Now let us confirm the selections you have made for the installation of the Active Directory Domain Server and proceed.

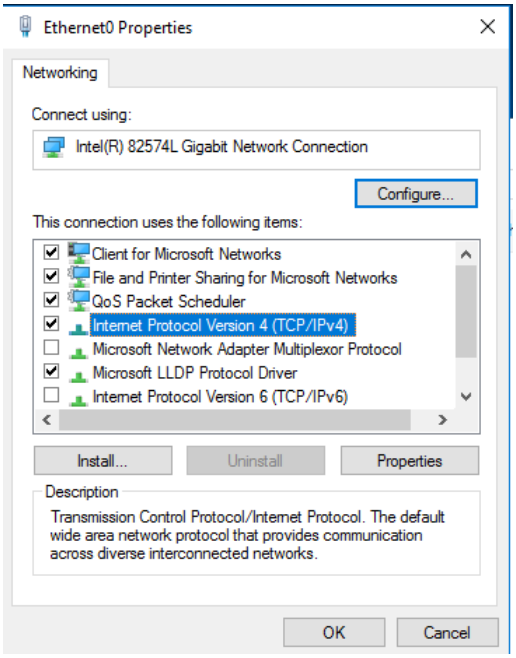


Let us wait for the installation to complete and close the window when it is ready.

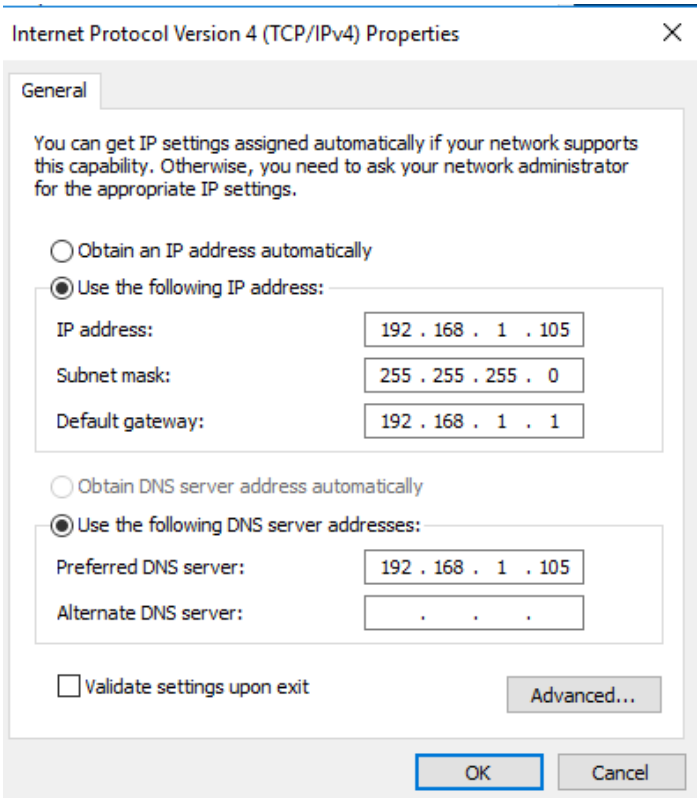


Network Configurations

Enable the ethernet connection and click on Properties. Double click on Internet Protocol Version TCP/IPv4.

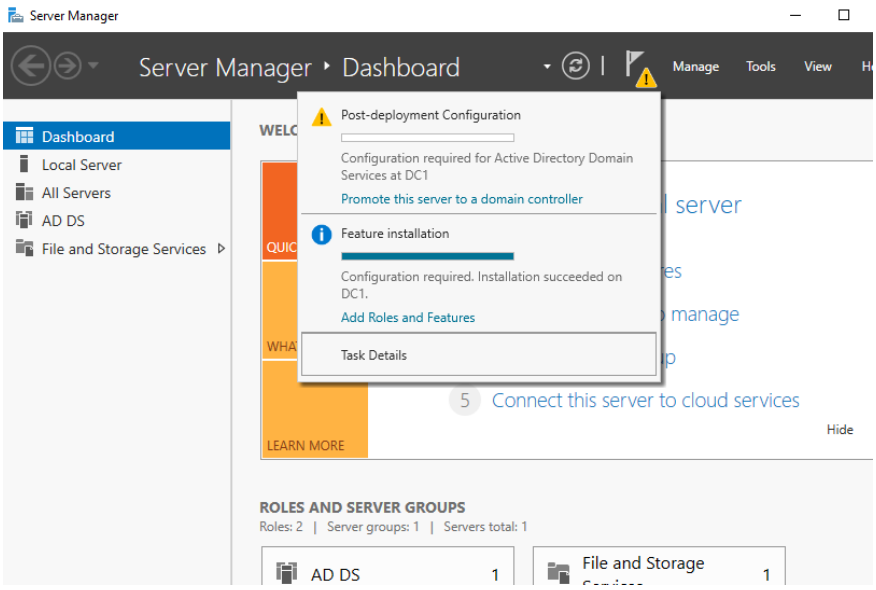


Now assign the Static IP address and the subnet mask will be automatically be assigned. Also, assign the default gateway. Then assign DNS Server address.

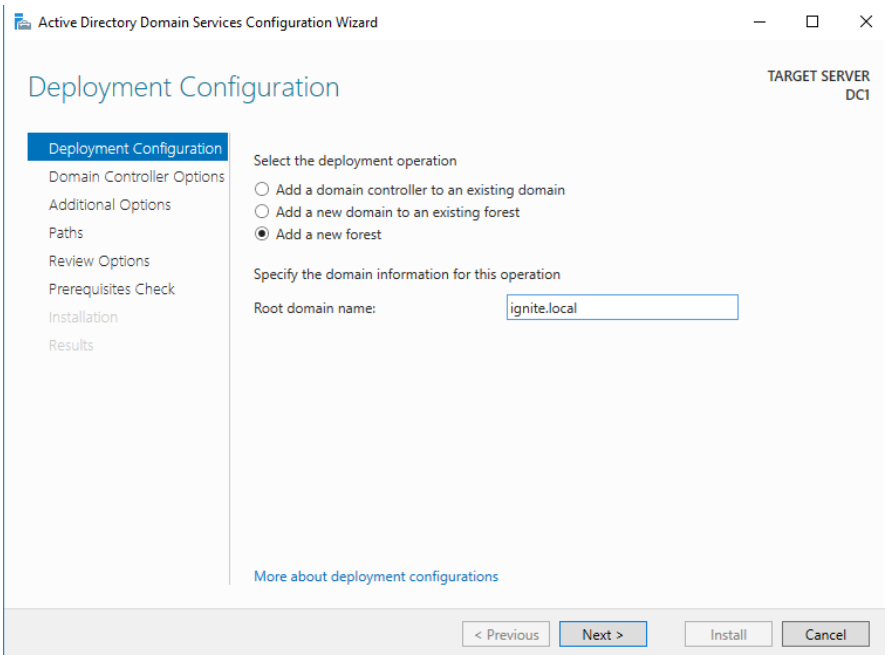


Post-Deployment Configurations

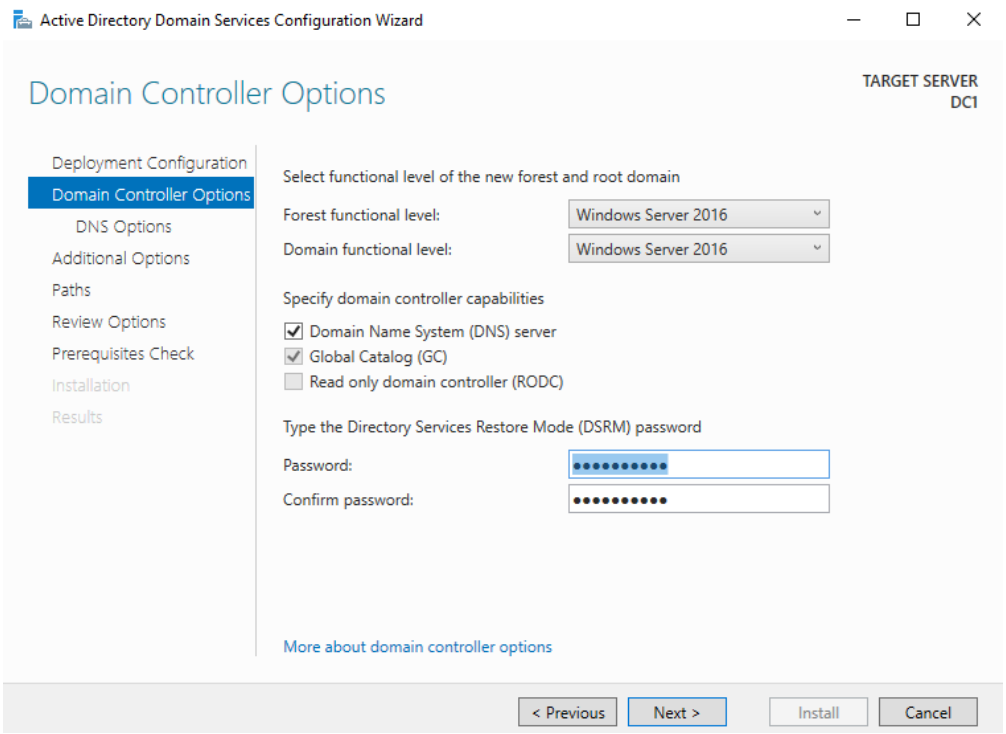
Once the AD DS feature installation is completed you see a flag notification, so let us move on to the configurations that are required in the post-deployment phase. Click on Promote this server to a domain controller to proceed.



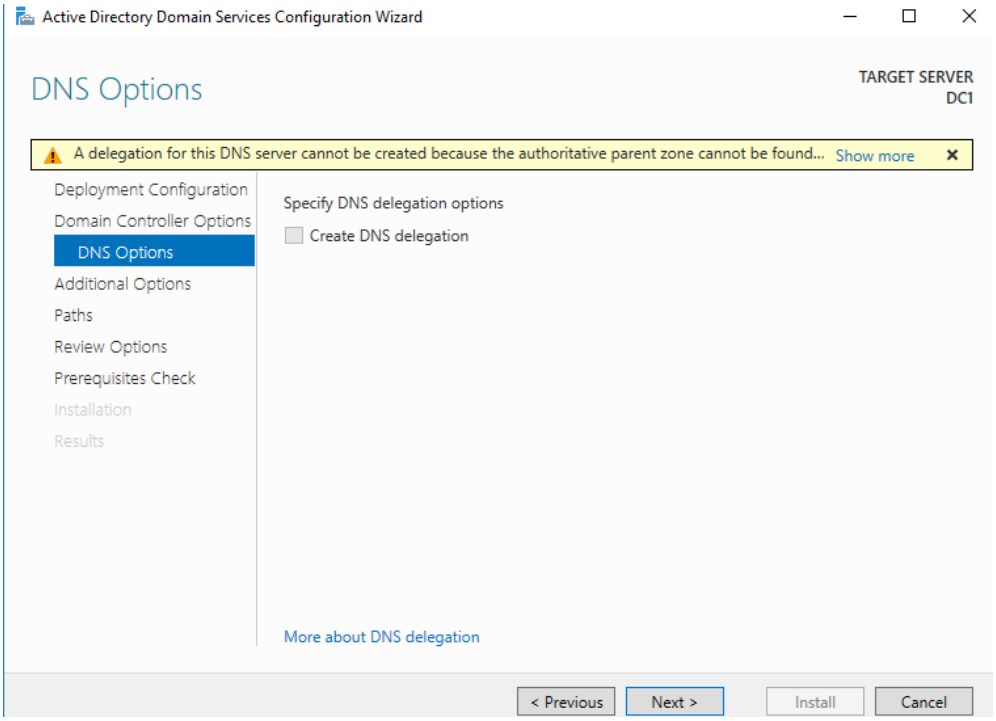
In Deployment Configuration let's create a new forest with the root domain name as ignite.local. A forest in the Active Directory is of the highest level of organisation. Each forest has the potential to share a single database, a global address list and security boundaries. Therefore, by default one use or even for that matter an administrator belonging to one forest cannot make us of another forest.



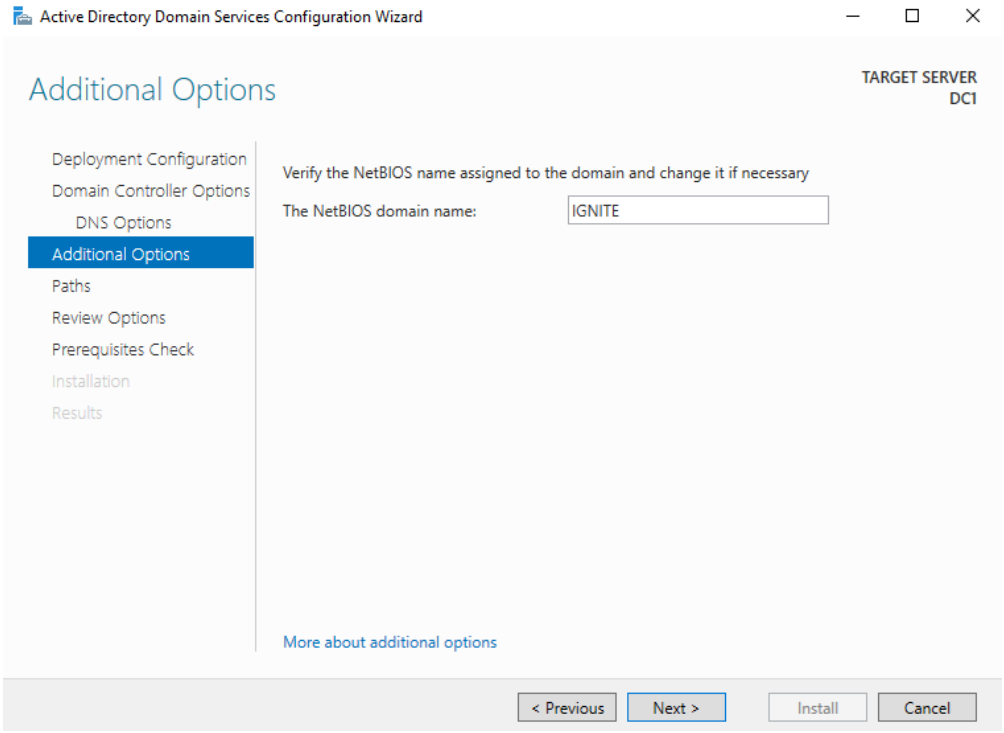
Now let's configure the domain controller capabilities by checking the first two boxes which allow DNS server and Global Catalog. Also, enter the Directory Services Restore Mode password which is a safe mode booting method for windows server domain controllers. The Domain functional level will depend on the forest functional level. Click on Next to proceed.



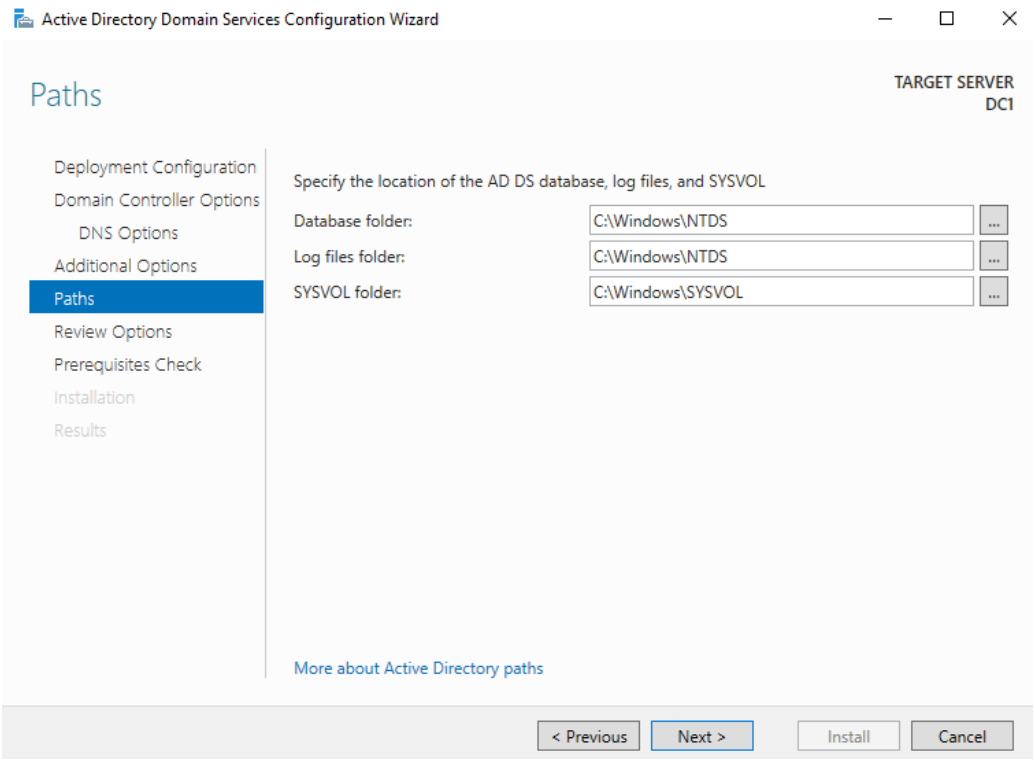
You can skip this option and click on Next.



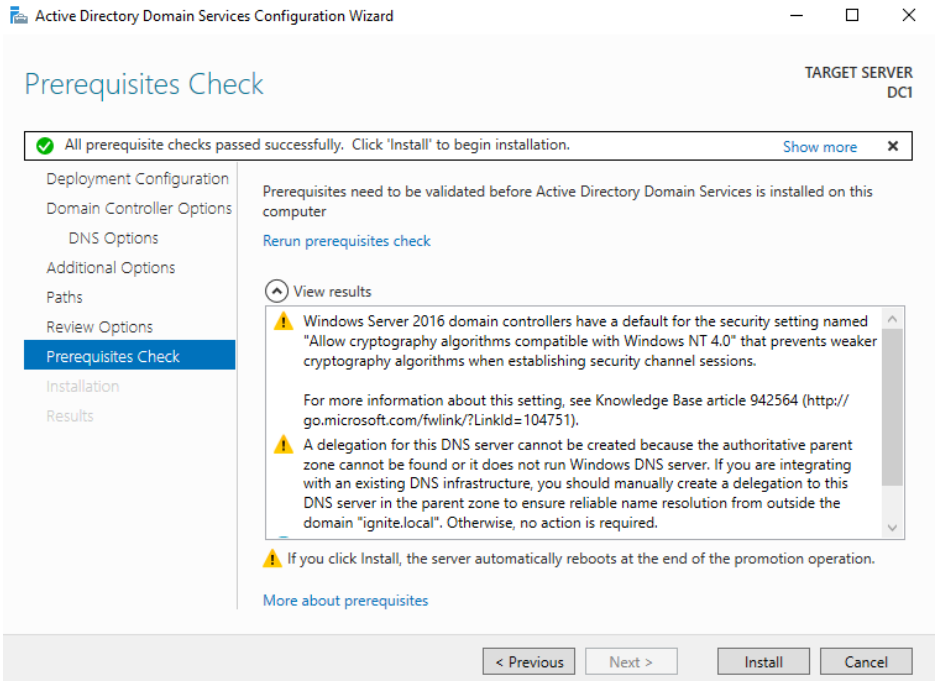
In the additional option, you can verify your NetBIOS name as entered prior and proceed.



Mention the path for creating AD DS database, log files and SYSVOL storage and proceed.

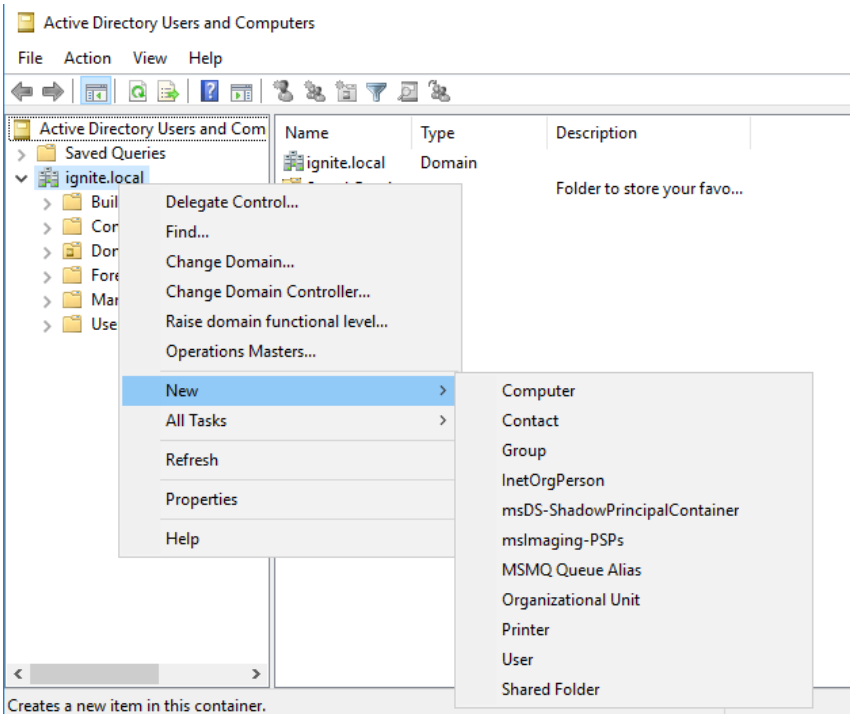


Check all the specifications that you have set are correct and Install the configuration. On finishing the installation, the server will reboot itself and ask you to login again.

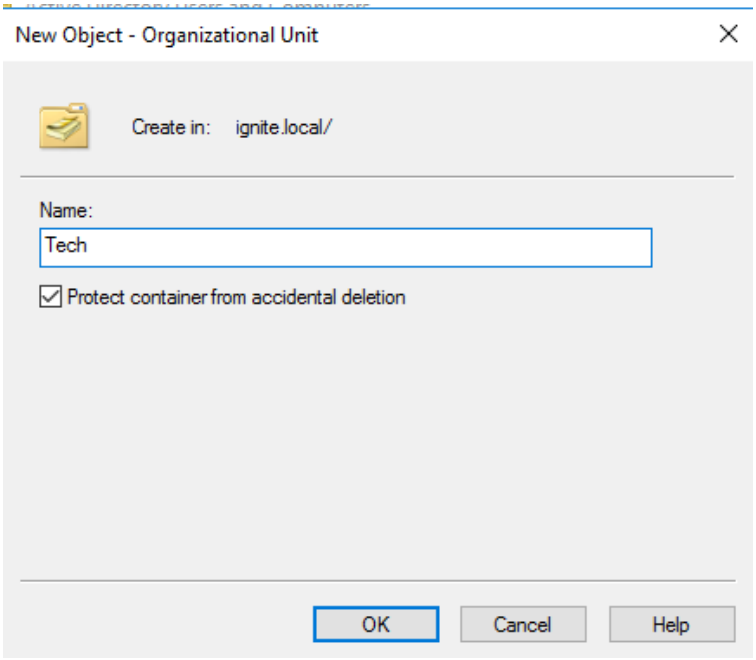


Configure User Account

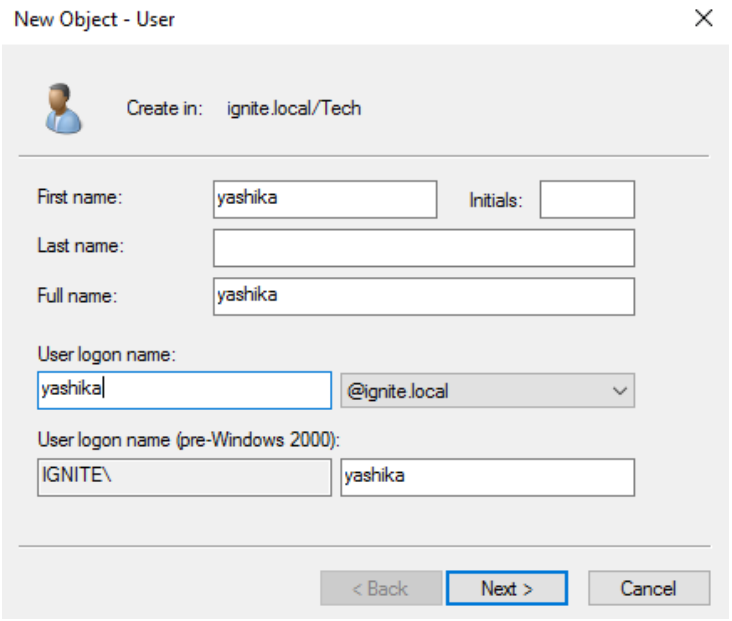
Now let us proceed to create users in our Active Directory by clicking on **Tools/Active Directory Users and Computers.** It will open a new window; click on the domain name you have created and then click on **New/Organisational Unit**.



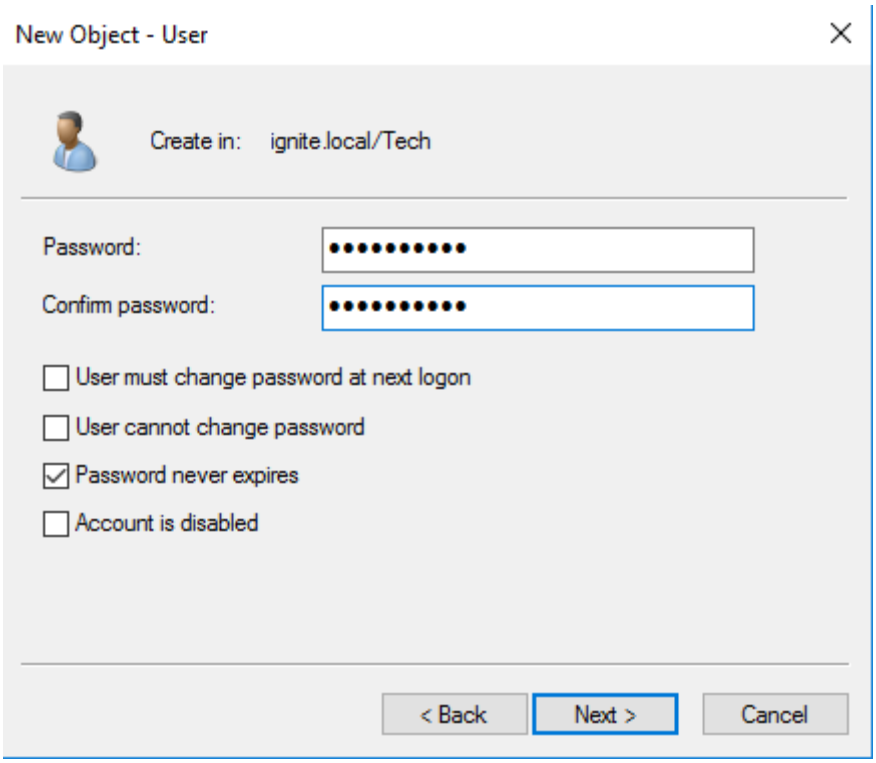
A new window will appear for creating a new object. You can name it as per your requirement and proceed.



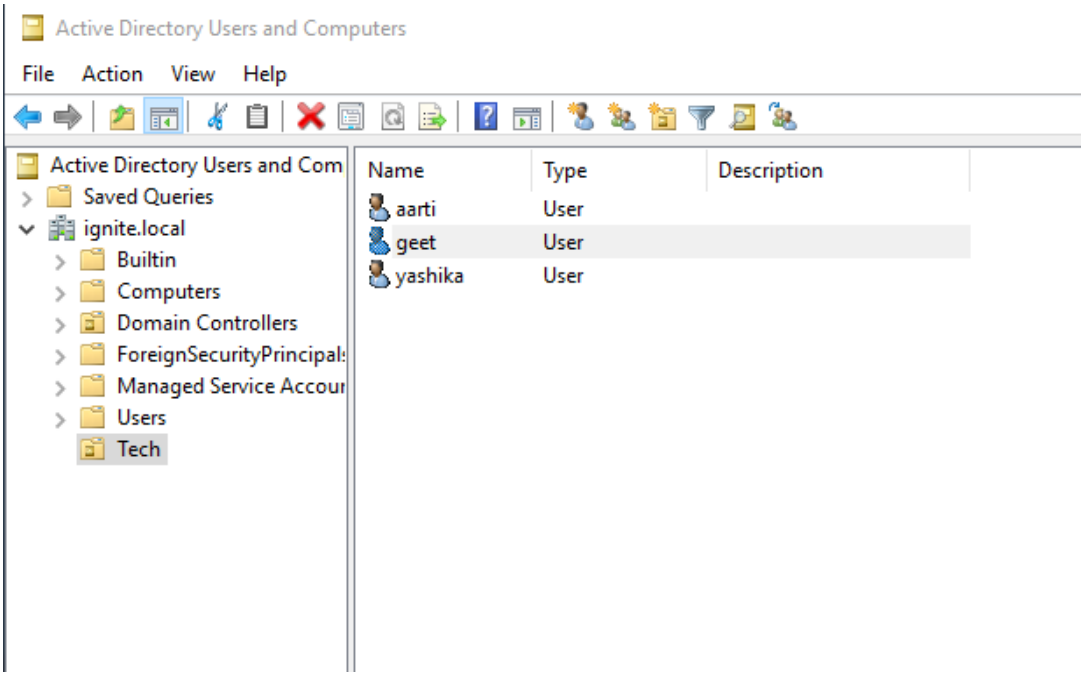
A window to create a new object which is a user will appear. Enter all the required details of the user and proceed.



Enter the password for the newly created user and then proceed ahead. Voila! Your user has been created.

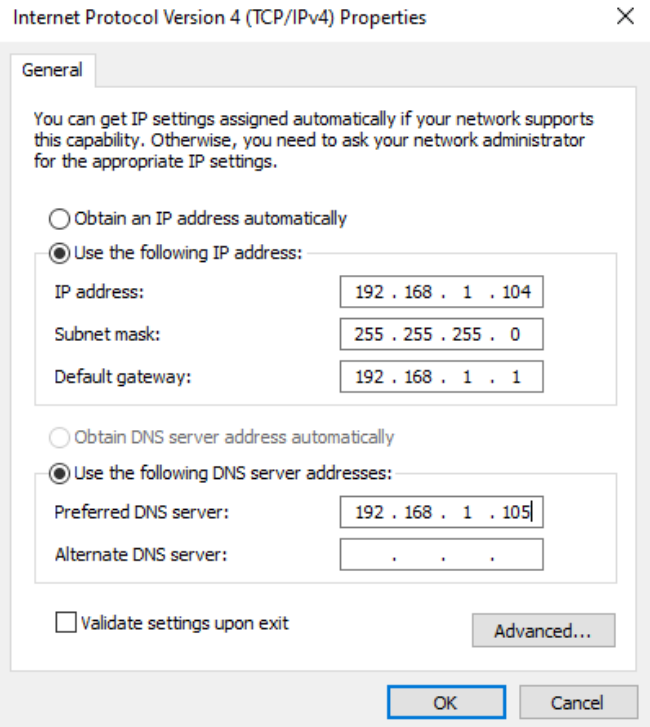


Subsequently you can create multiple users under an organisational unit.

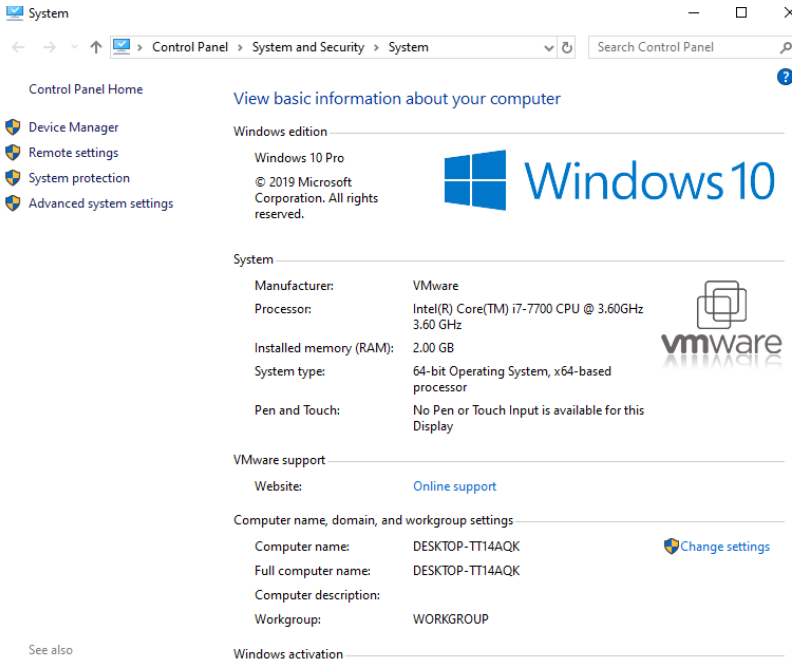


Add Client to the Domain

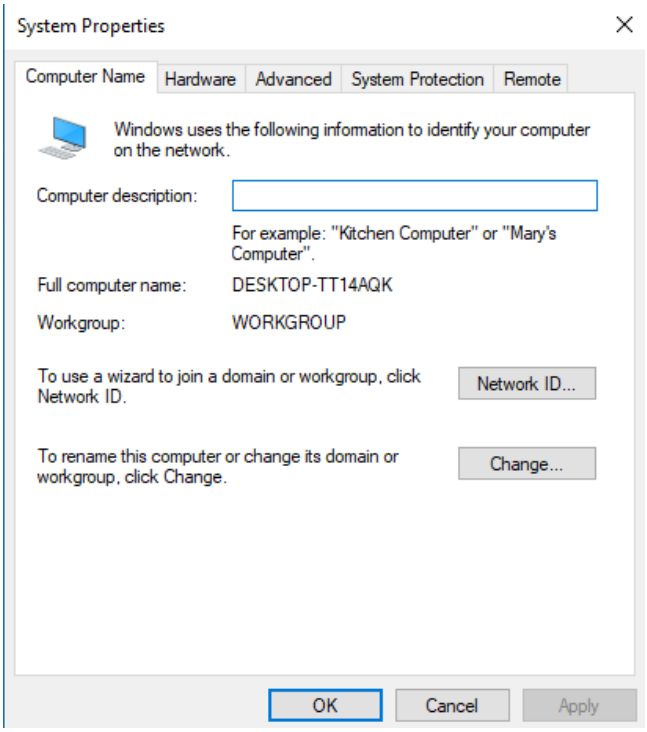
Here in the Windows 10 system before connecting it to the domain, we have to set a Static IP for the system and mention the IP address of the Domain Controller in the DNS server address.



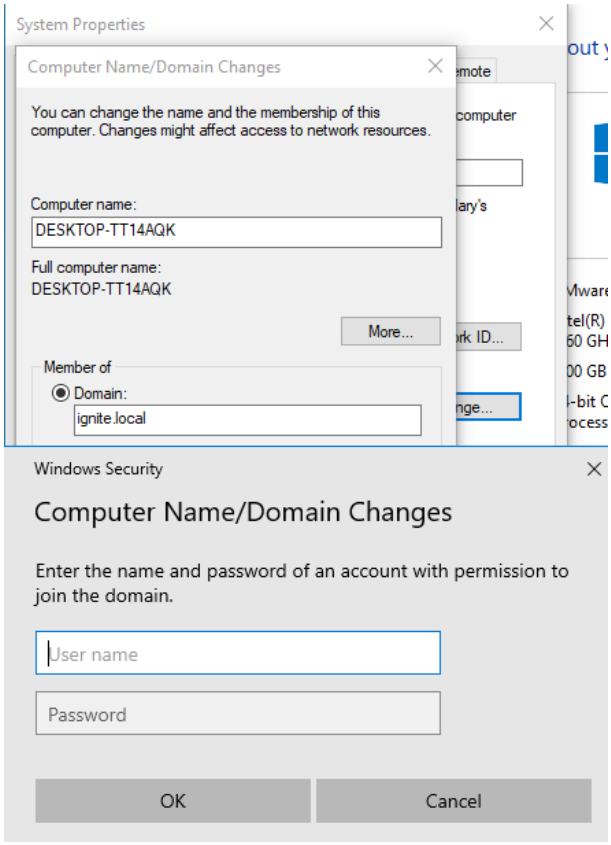
Go to control panel and check the basic information of your system and change the computer name settings.



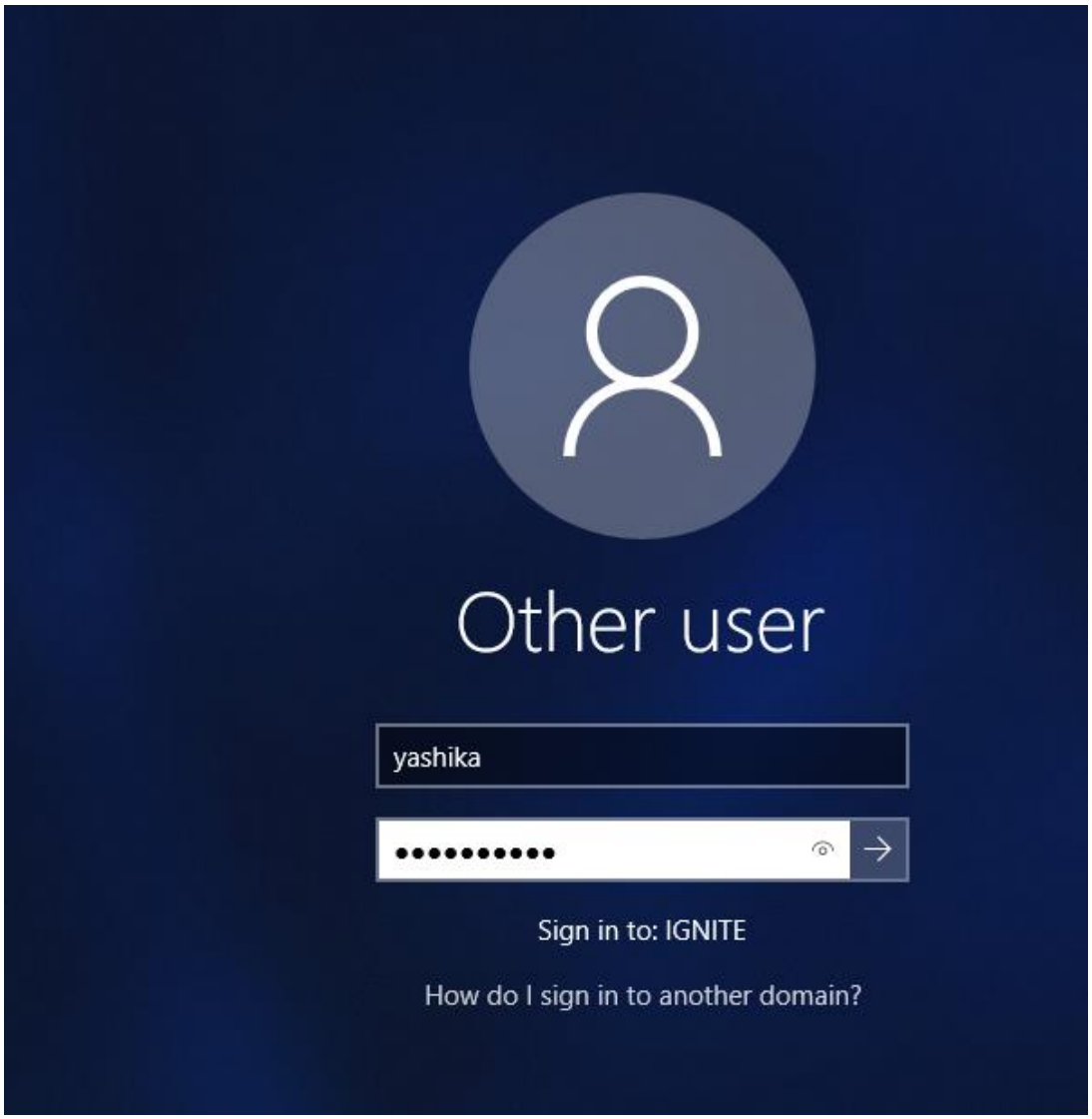
Now click on change option to join the domain.



It will display your computer name and click on domain under the member and you will be prompted to enter the username and password of the domain changes that you are making.



Once, you are done with this, restart your system and you can login with your username and password to sign in under the domain that you had previously created.



After logging in you can open the command prompt and go too the directory in which your user is present. Make use of the net user command and mention the user's name with domain. You will get details about the user

net user yashika /domain

```
C:\Users\yashika>net user yashika /domain
The request will be processed at a domain controller for domain ignite.local.

User name                    yashika
Full Name                    yashika
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            ⌈7/⌈5/⌈2020 4:01:49 AM
Password expires             Never
Password changeable          ⌈7/⌈6/⌈2020 4:01:49 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   ⌈7/⌈5/⌈2020 4:07:02 AM

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Domain Users
The command completed successfully.


C:\Users\yashika>
```

Hence here your Active Directory Pen testing Lab is setup and ready to use. Happy Pen testing!