

Active Directory Pentesting: Lab Setup

 hackingarticles.in/active-directory-pentesting-lab-setup

Raj

March 9, 2021

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**
- **Lab Requirements**
- **Configuring Windows Server 2016**
- **Installing AD DS**
- **Network Configurations**
- **Post-Deployment Configurations**
- **Create OU and user**
- **Add Client to the Domain**

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 (Client)

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.

New Virtual Machine Wizard ×

Easy Install Information
This is used to install Windows Server 2016.

Windows product key

Version of Windows to install

Personalize Windows

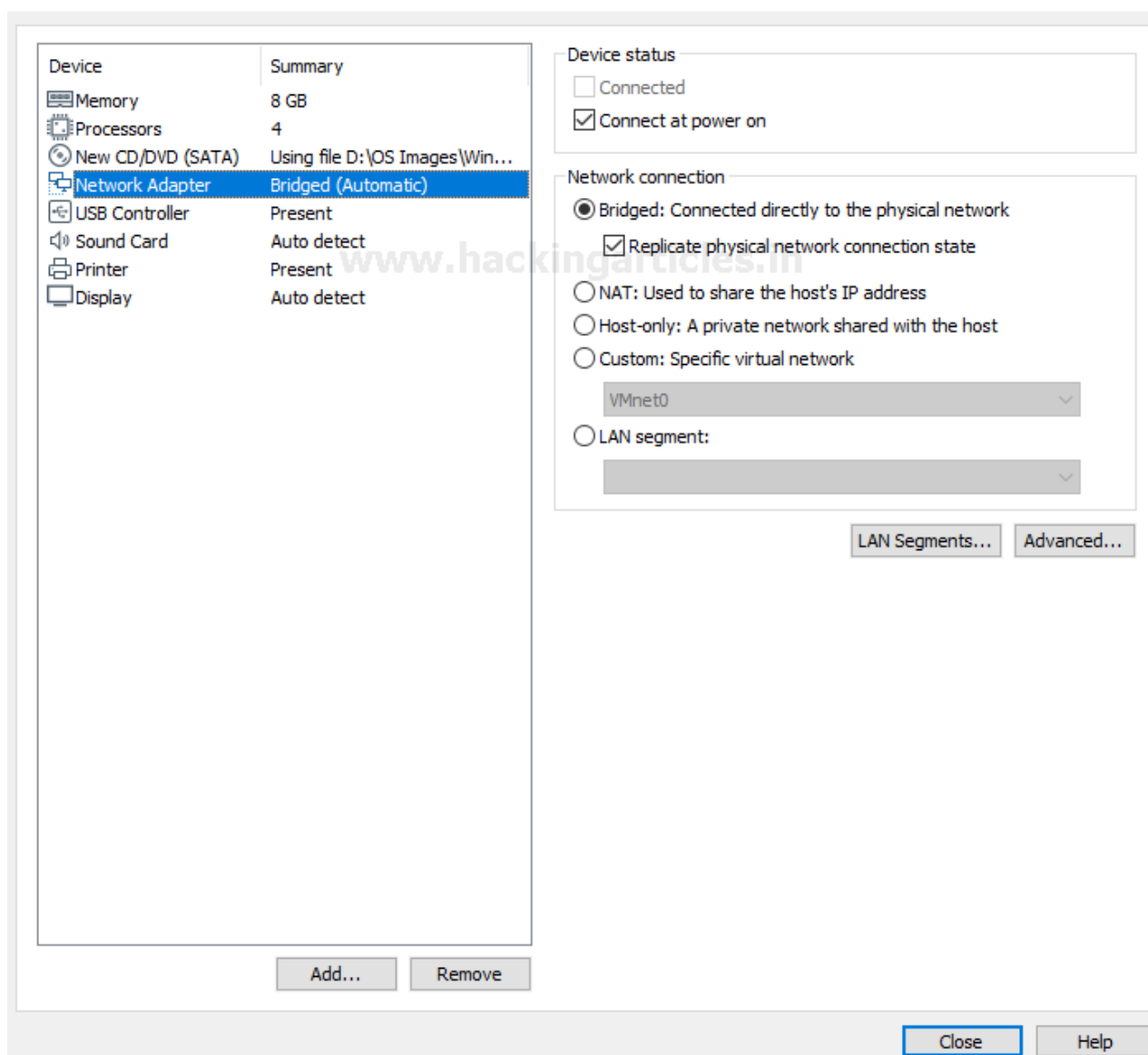
Full name:

Password: (optional)

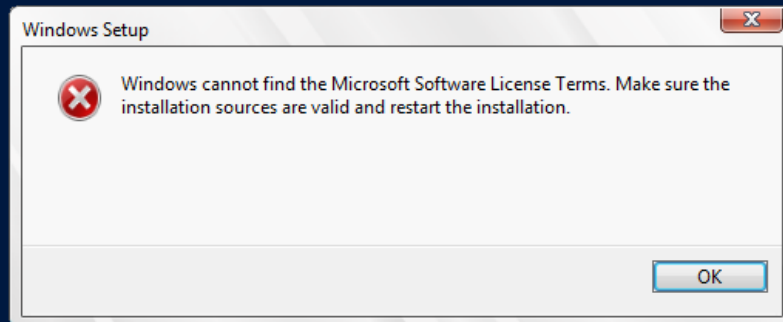
Confirm:

☐ Log on automatically (requires a password)

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.

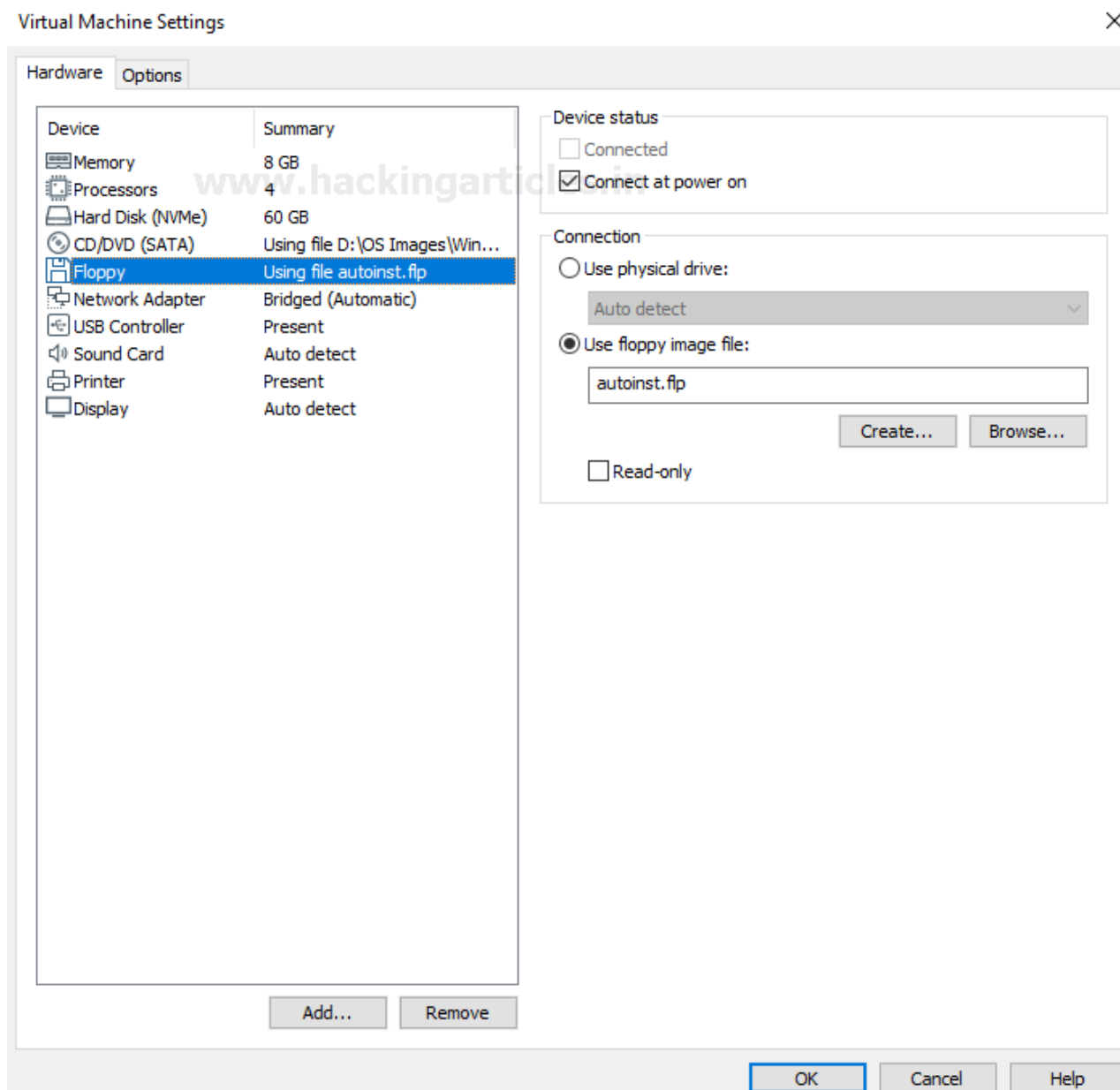


Here you see that the setup did not proceed, therefore let's go back and fix this error from occurring.

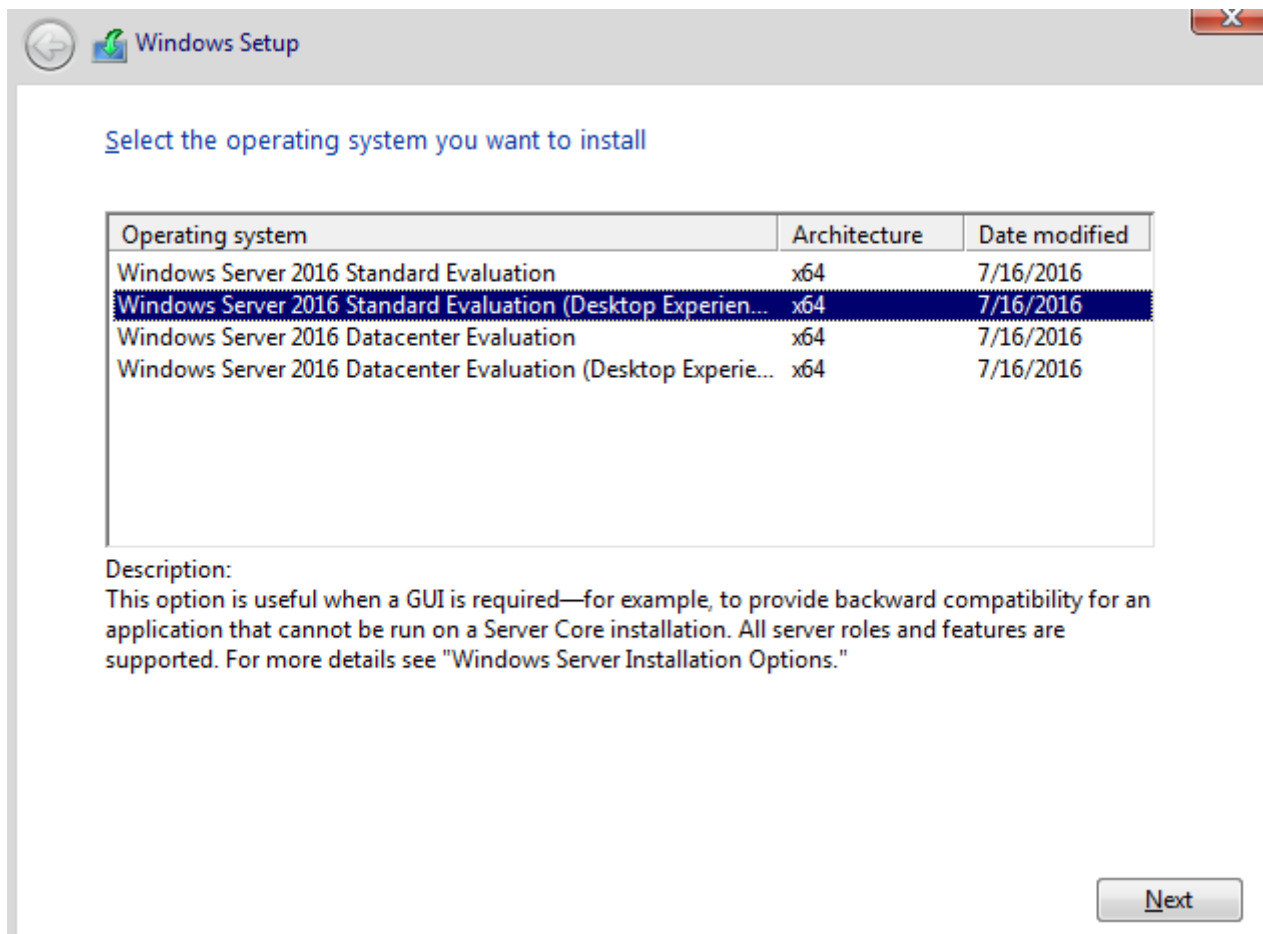


Setup is starting

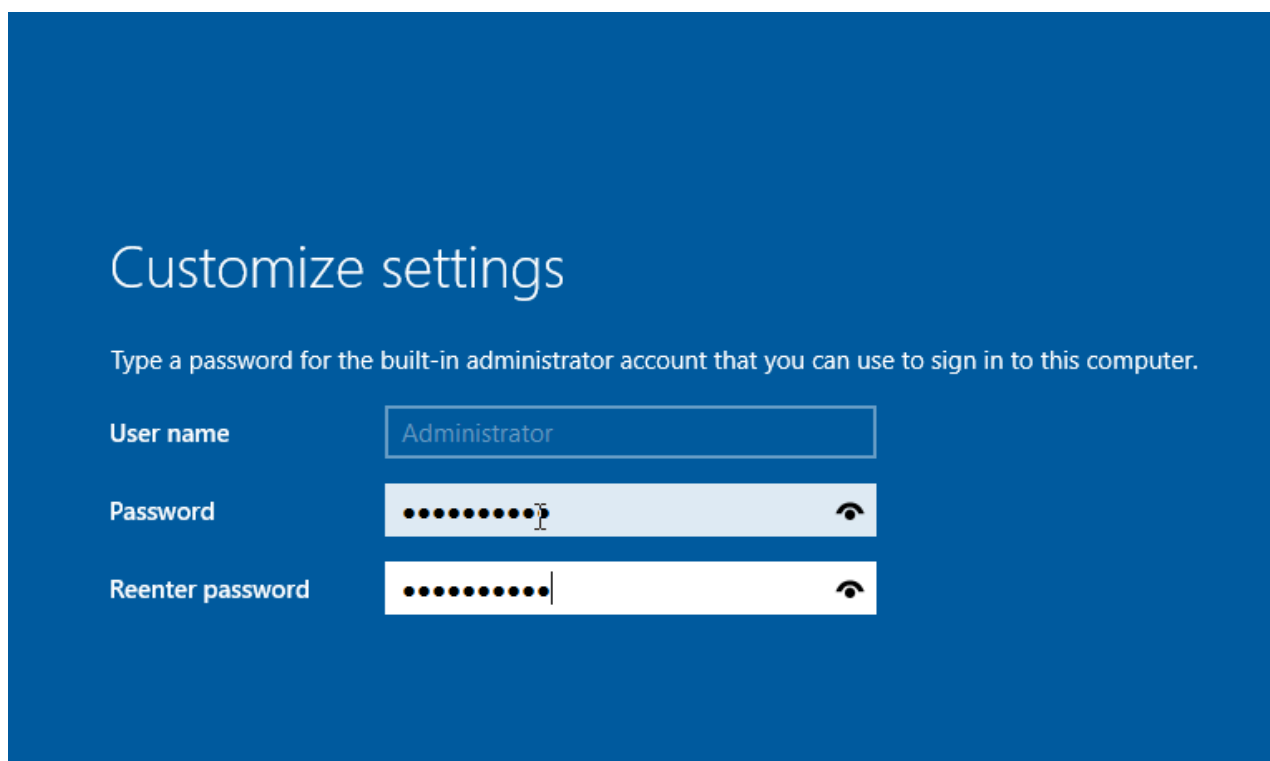
We will go back to Virtual Machine settings and click on Floppy, there under the connection option and choose the Use floppy image file option to make it work like a charm and proceed.



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.

System

Control Panel > System and Security > System

Control Panel Home

View basic information about your computer

Device Manager
Remote settings
Advanced system settings

Windows edition

Windows Server 2016 Standard Evaluation
© 2016 Microsoft Corporation. All rights reserved.

Windows Server® 2016

System

Processor: Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz 3.60 GHz (2 processors)
Installed memory (RAM): 8.00 GB
System type: 64-bit Operating System, x64-based processor
Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: WIN-VS2VGE5G53B
Full computer name: WIN-VS2VGE5G53B
Computer description:
Workgroup: WORKGROUP

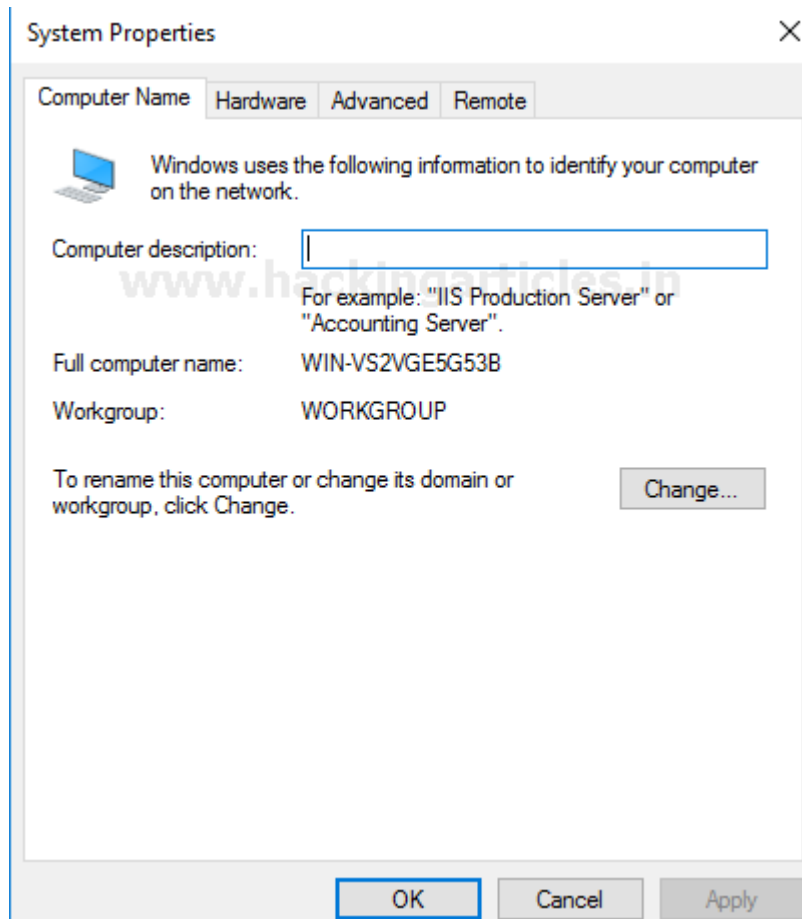
Windows activation

Windows is activated [Read the Microsoft Software License Terms](#)
Product ID: 00378-00000-00000-AA739

See also

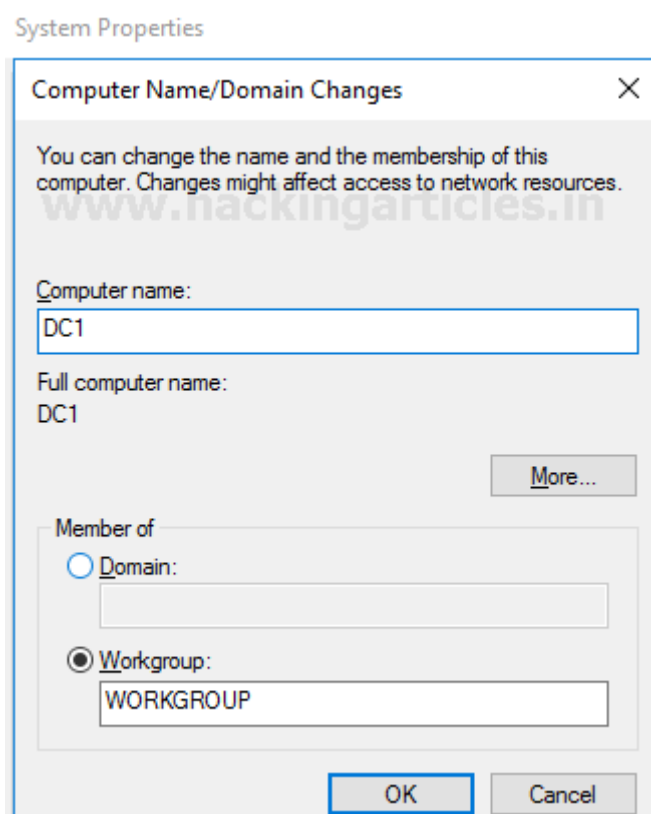
Installing AD DS

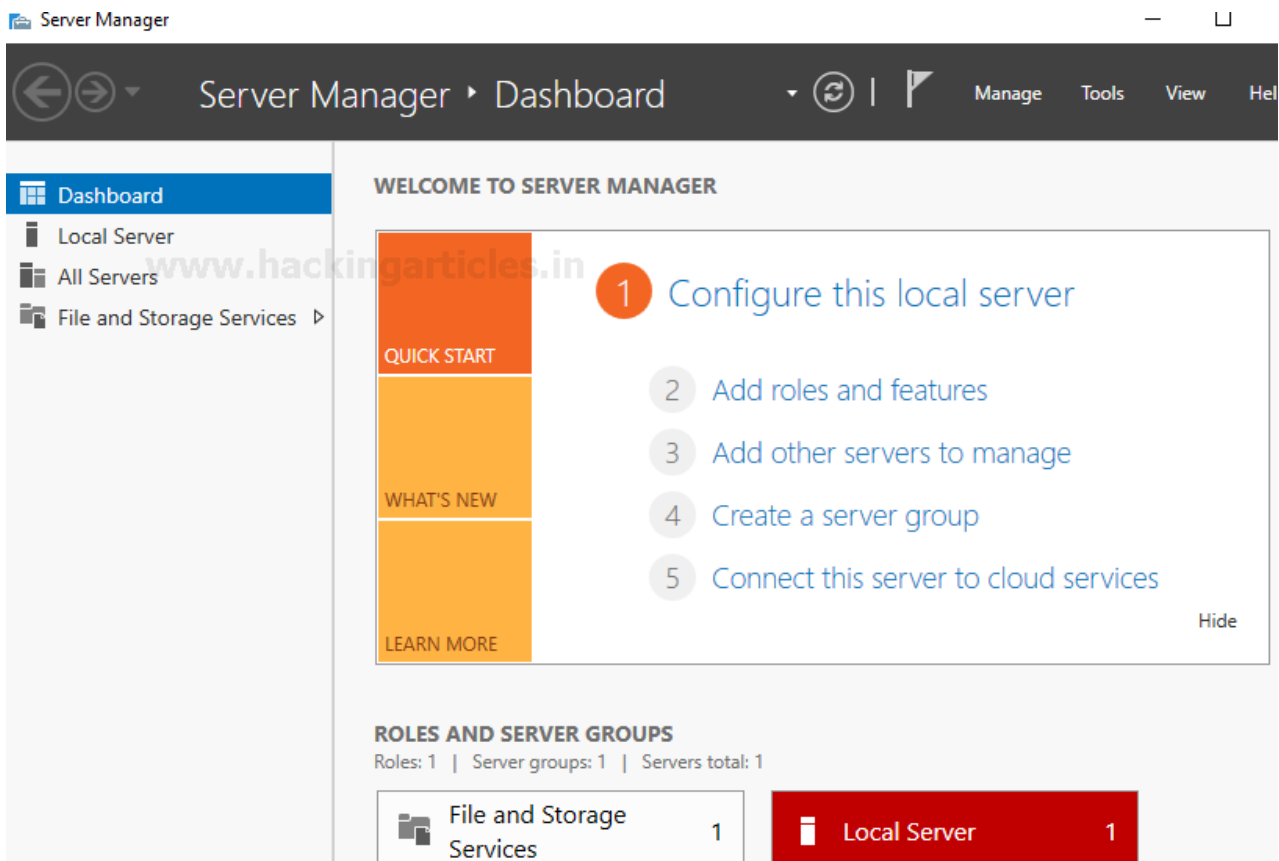
Now let us open the system properties from the 'Local Server' option and let us make changes to the domain name.



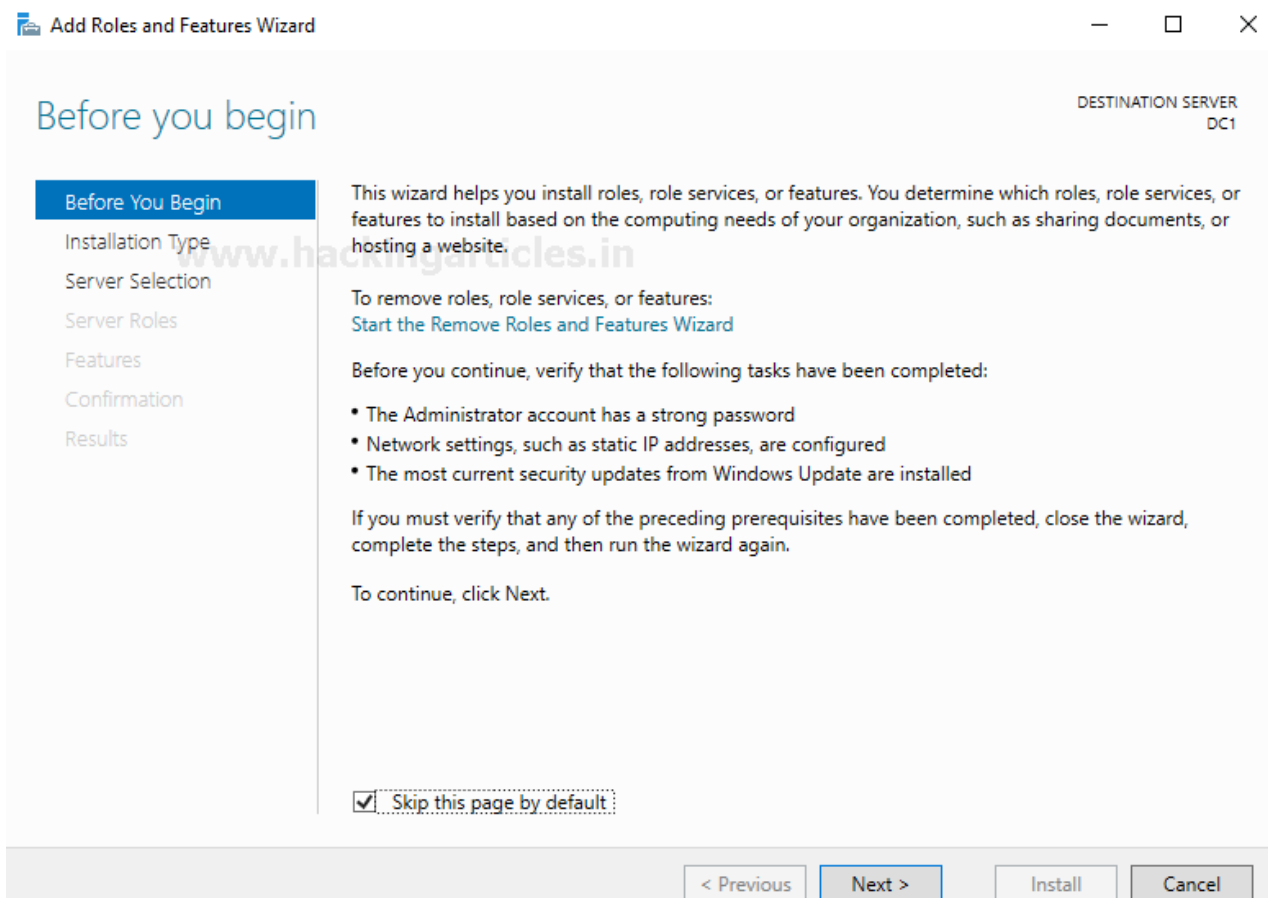
Let's keep the computer name as DC 1 and make it the member of the workgroup with the name 'WorkGroup'. On finishing this, click on 'OK' to proceed.

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'.

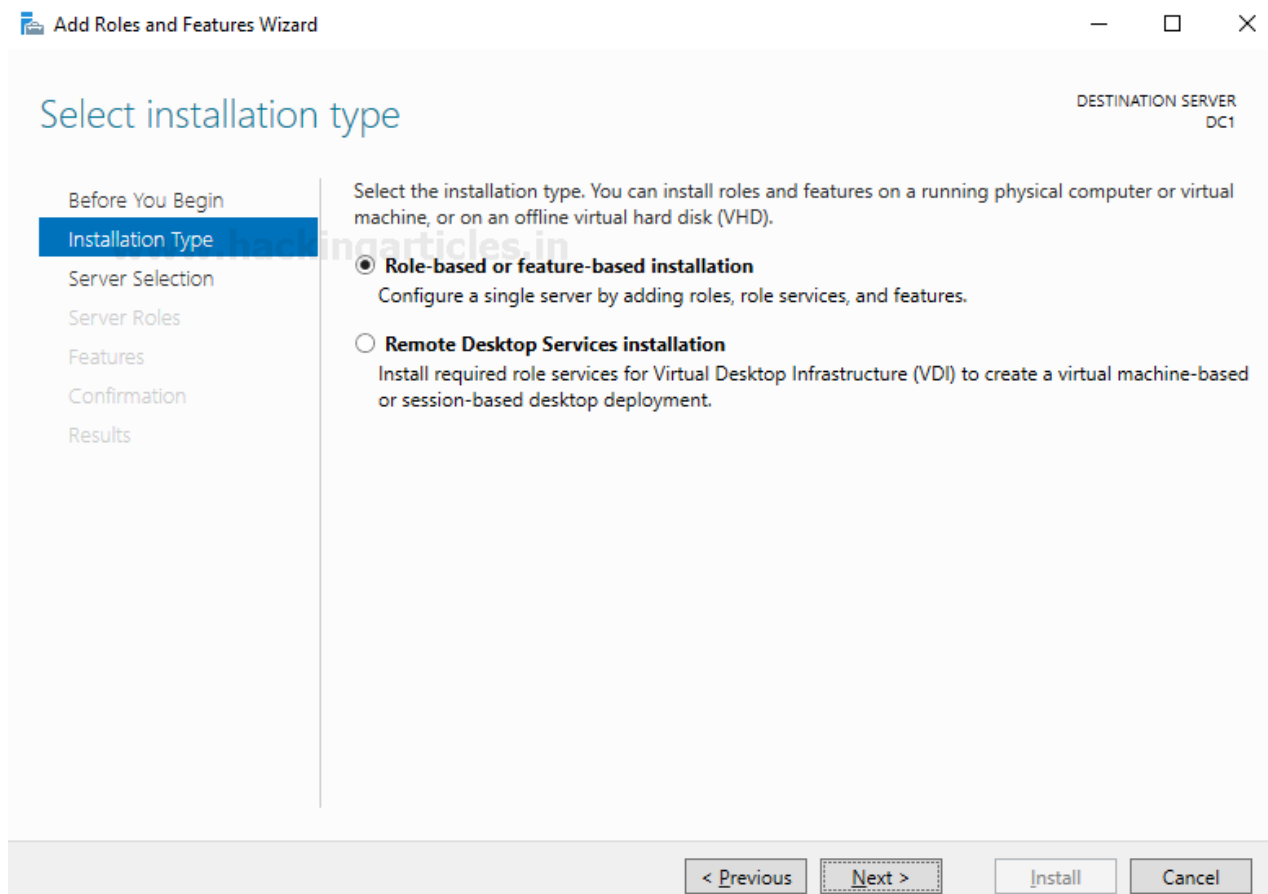




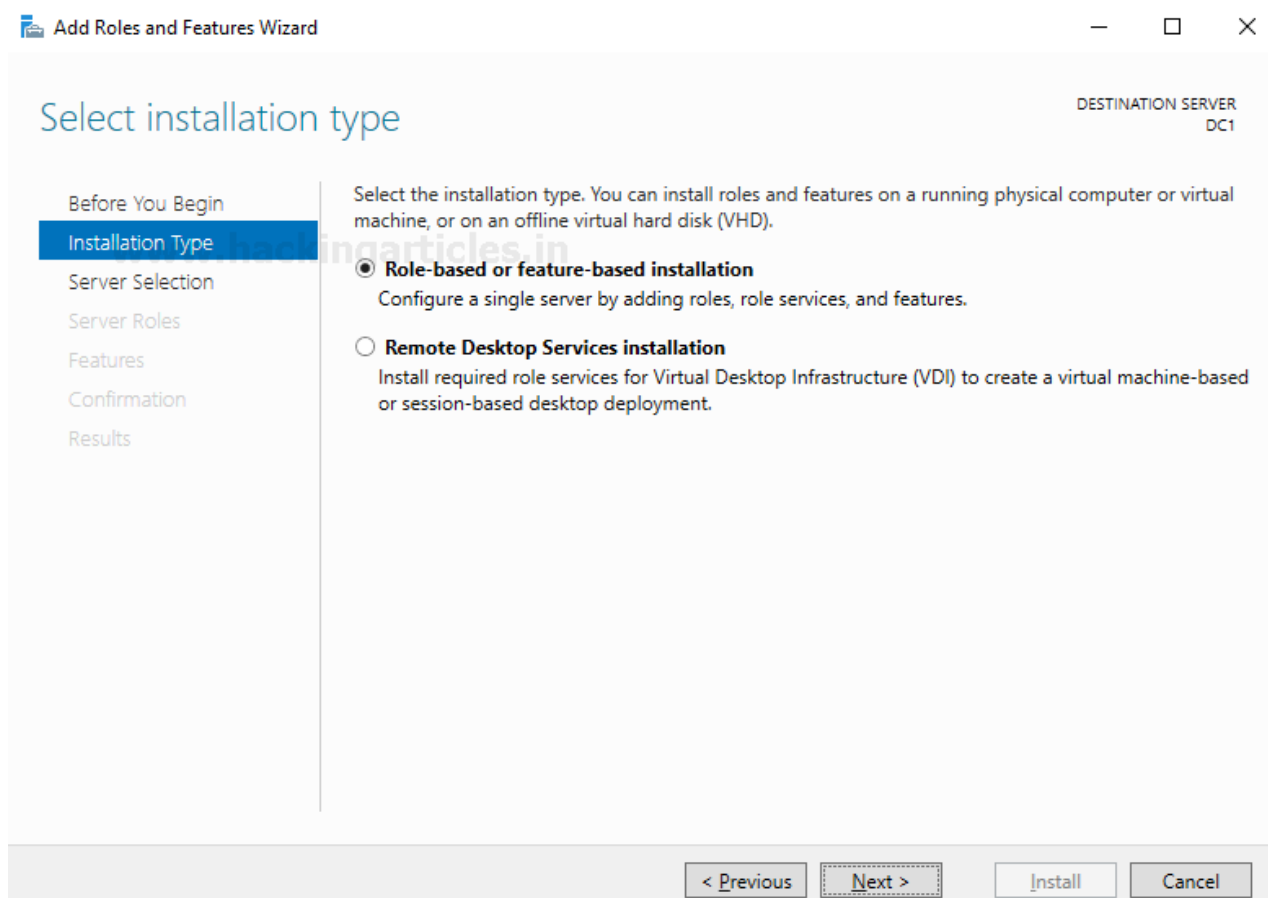
You see the installation wizard before you and click on 'next' to proceed.



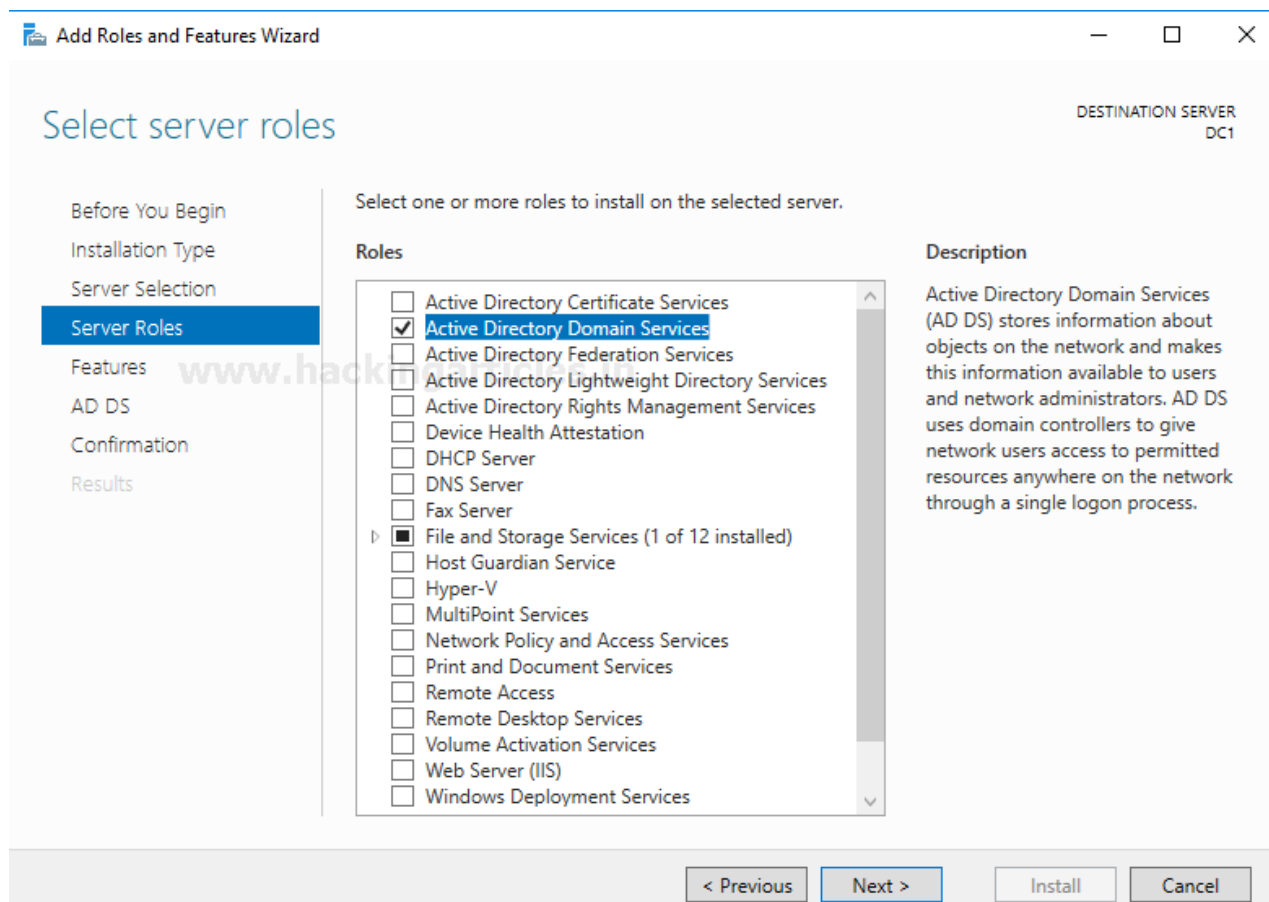
Then select Role-based or feature-based installation as it allows you to manually configure all the preferred roles at your convenience.



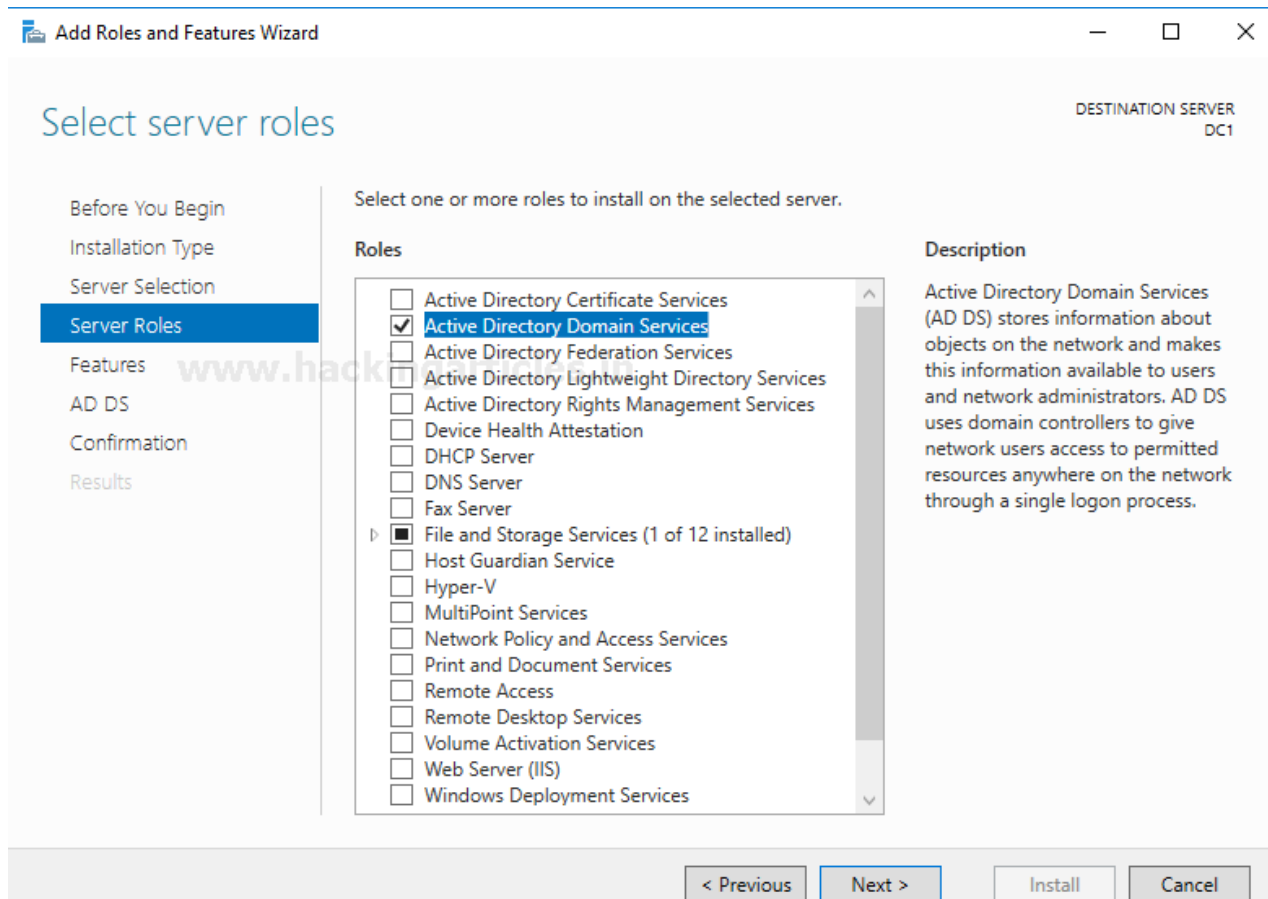
Choose the server you have created from the server pool that is available before you.



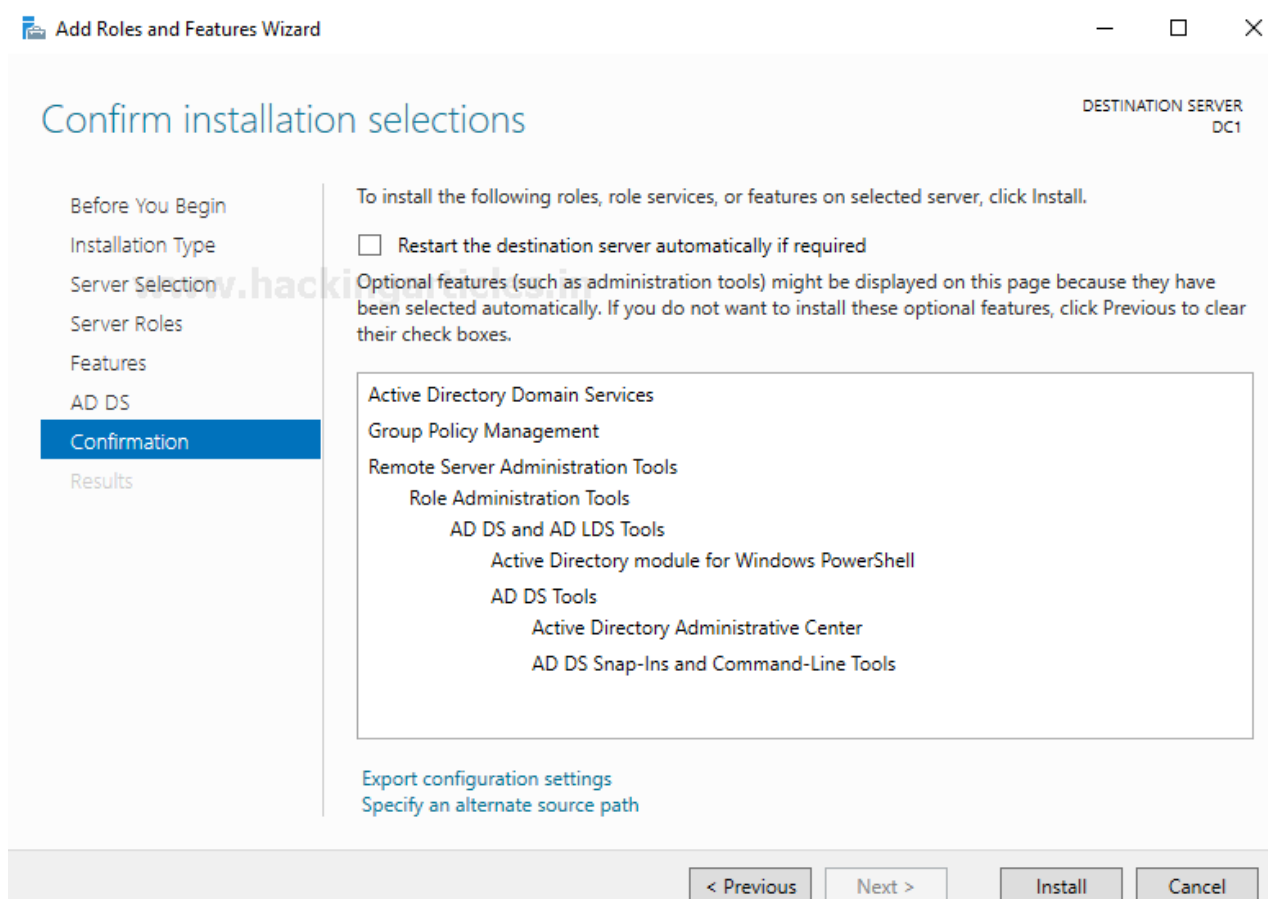
Now choose the server roles you want to add. Here we require Active Directory Domain Services. We check that option and click next to proceed.



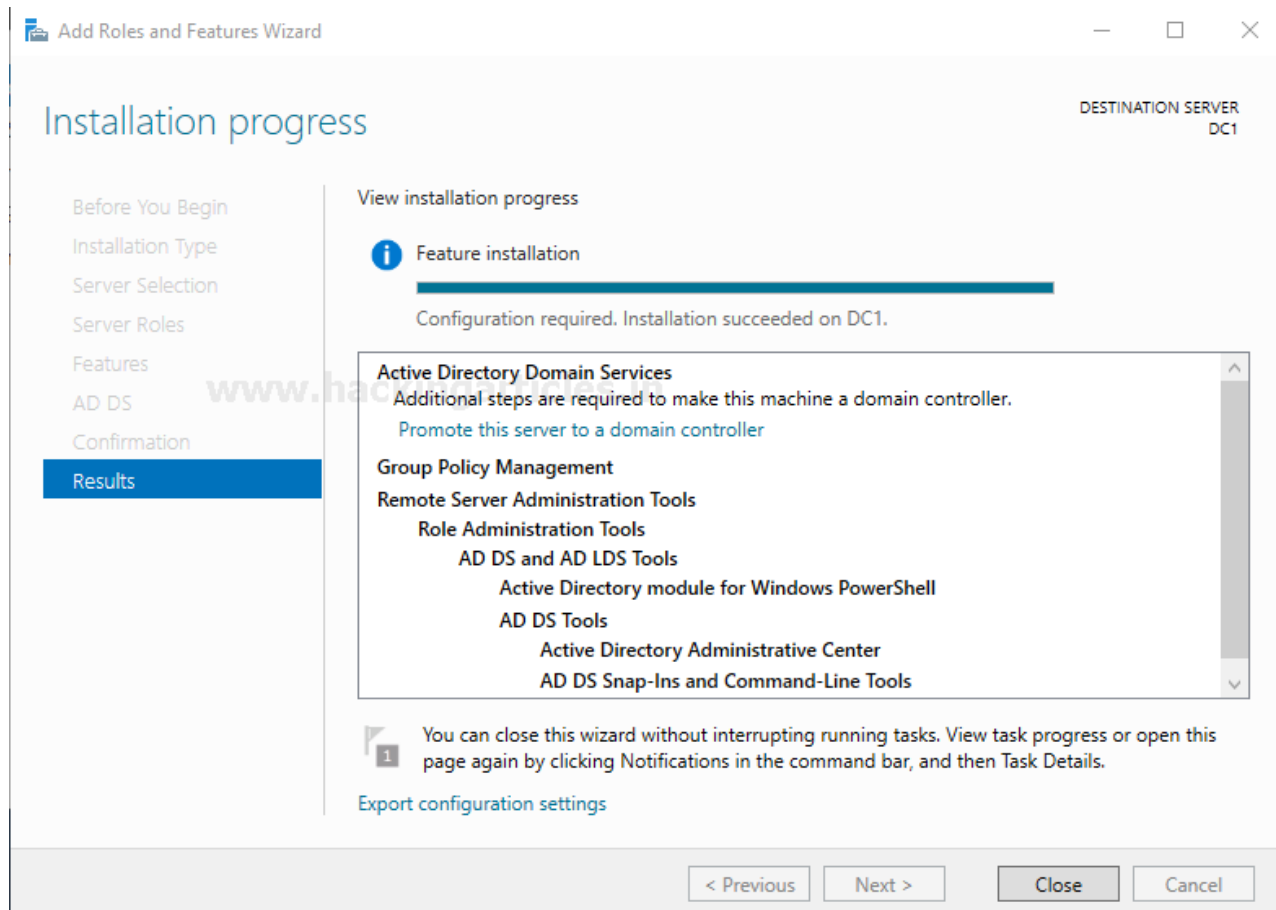
In features installation Choose Group Policy Management. It is a management feature in Windows that allows you to control multiple users and computer configurations present in an Active Directory environment. Click on Next to proceed.



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



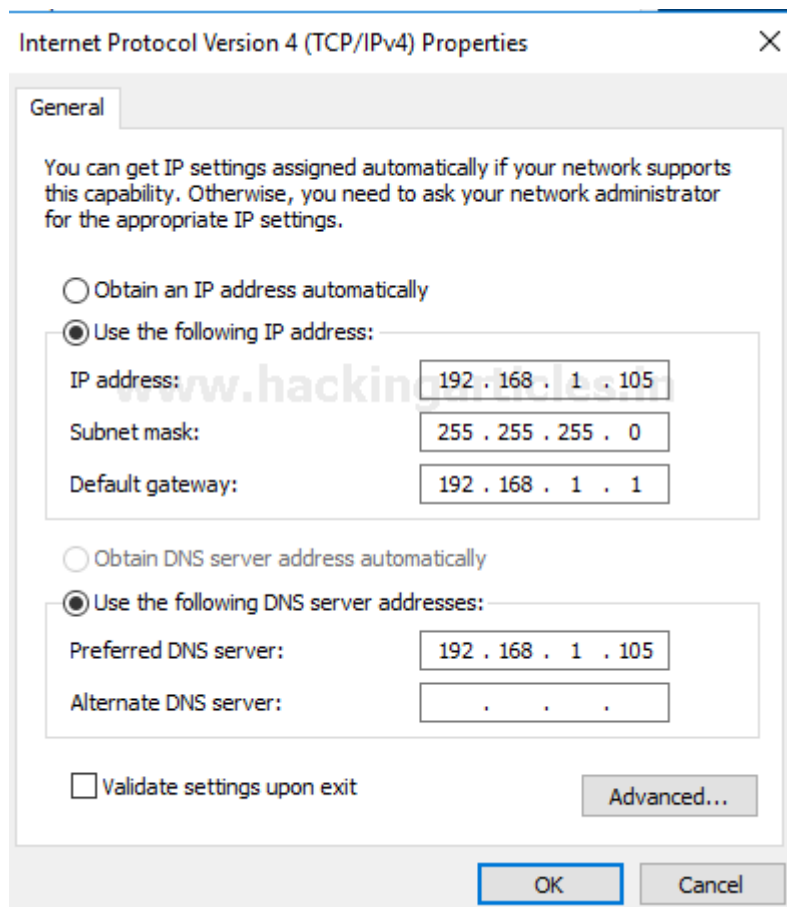
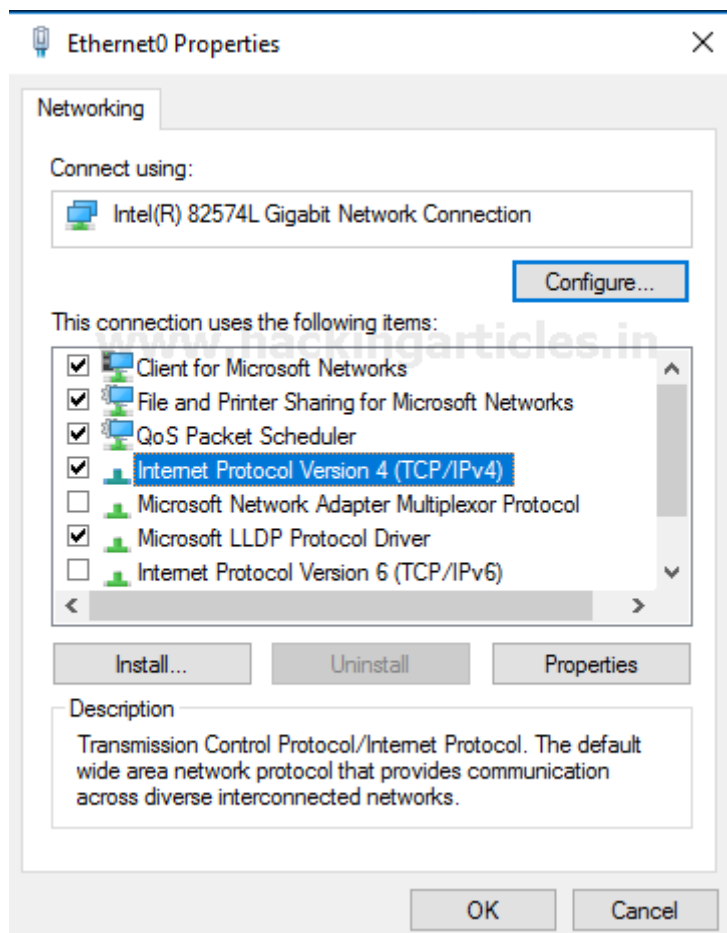
Let us wait for the installation to complete and close the window when it is ready.



Network Configurations

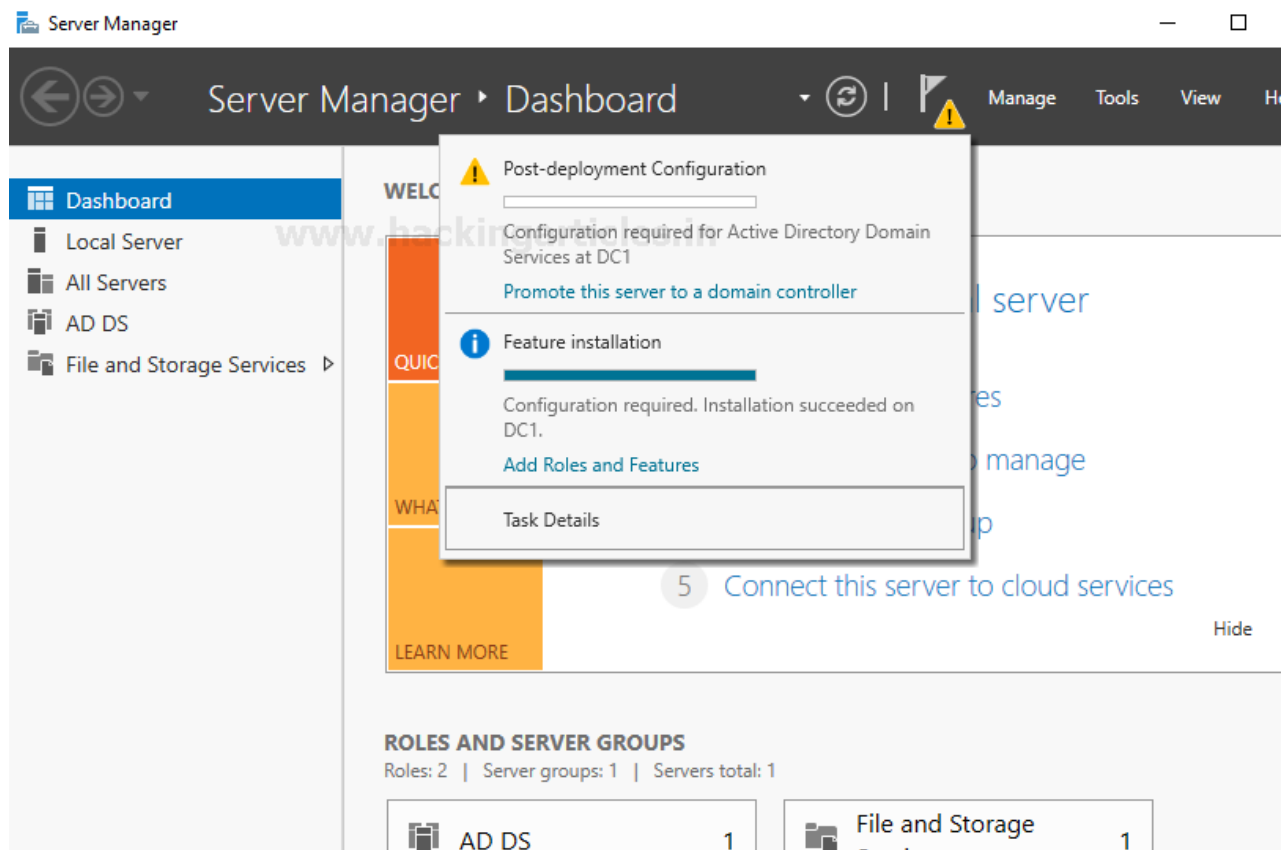
Enable the ethernet connection and click on Properties. Double click on Internet Protocol Version TCP/IPv4.

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 user or even for that matter an administrator belonging to one forest cannot make use of another forest.

Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
DC1

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

☐ Add a domain controller to an existing domain

☐ Add a new domain to an existing forest

☒ Add a new forest

Specify the domain information for this operation

Root domain name:

[More about deployment configurations](#)

< Previous Next > Install Cancel

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.

Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
DC1

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☒ Domain Name System (DNS) server

☒ Global Catalog (GC)

☐ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel

You can skip this option and click on Next.

Active Directory Domain Services Configuration Wizard

DNS Options

TARGET SERVER
DC1

A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found... [Show more](#) X

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Specify DNS delegation options

☐ Create DNS delegation

[More about DNS delegation](#)

< Previous Next > Install Cancel

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

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the Windows logo, the text 'Active Directory Domain Services Configuration Wizard', and standard window controls (minimize, maximize, close). The main window has a light gray background. On the left, a vertical navigation pane lists the steps: 'Deployment Configuration', 'Domain Controller Options', 'DNS Options', 'Additional Options' (highlighted in blue), 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main area is titled 'Additional Options' in blue. In the top right corner, it says 'TARGET SERVER DC1'. The main content area contains the text 'Verify the NetBIOS name assigned to the domain and change it if necessary' and 'The NetBIOS domain name:' followed by a text box containing 'IGNITE'. At the bottom of the main area is a link 'More about additional options'. The bottom of the window features a gray bar with four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Active Directory Domain Services Configuration Wizard

Additional Options

TARGET SERVER
DC1

Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name:

[More about additional options](#)

< Previous Next > Install Cancel

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

Paths

TARGET SERVER
DC1

- Deployment Configuration
- Domain Controller Options
- DNS Options
- Additional Options
- Paths**
- Review Options
- Prerequisites Check
- Installation
- Results

Specify the location of the AD DS database, log files, and SYSVOL

Database folder: C:\Windows\NTDS ...

Log files folder: C:\Windows\NTDS ...

SYSVOL folder: C:\Windows\SYSVOL ...

[More about Active Directory paths](#)

< Previous

Next >

Install

Cancel

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.

Prerequisites Check

TARGET SERVER
DC1

✓ All prerequisite checks passed successfully. Click 'Install' to begin installation.

[Show more](#) ×

- Deployment Configuration
- Domain Controller Options
- DNS Options
- Additional Options
- Paths
- Review Options
- Prerequisites Check**
- Installation
- Results

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

[Rerun prerequisites check](#)

⬆ View results

⚠ Windows Server 2016 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

⚠ A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "ignite.local". Otherwise, no action is required.

⚠ If you click Install, the server automatically reboots at the end of the promotion operation.

[More about prerequisites](#)

< Previous

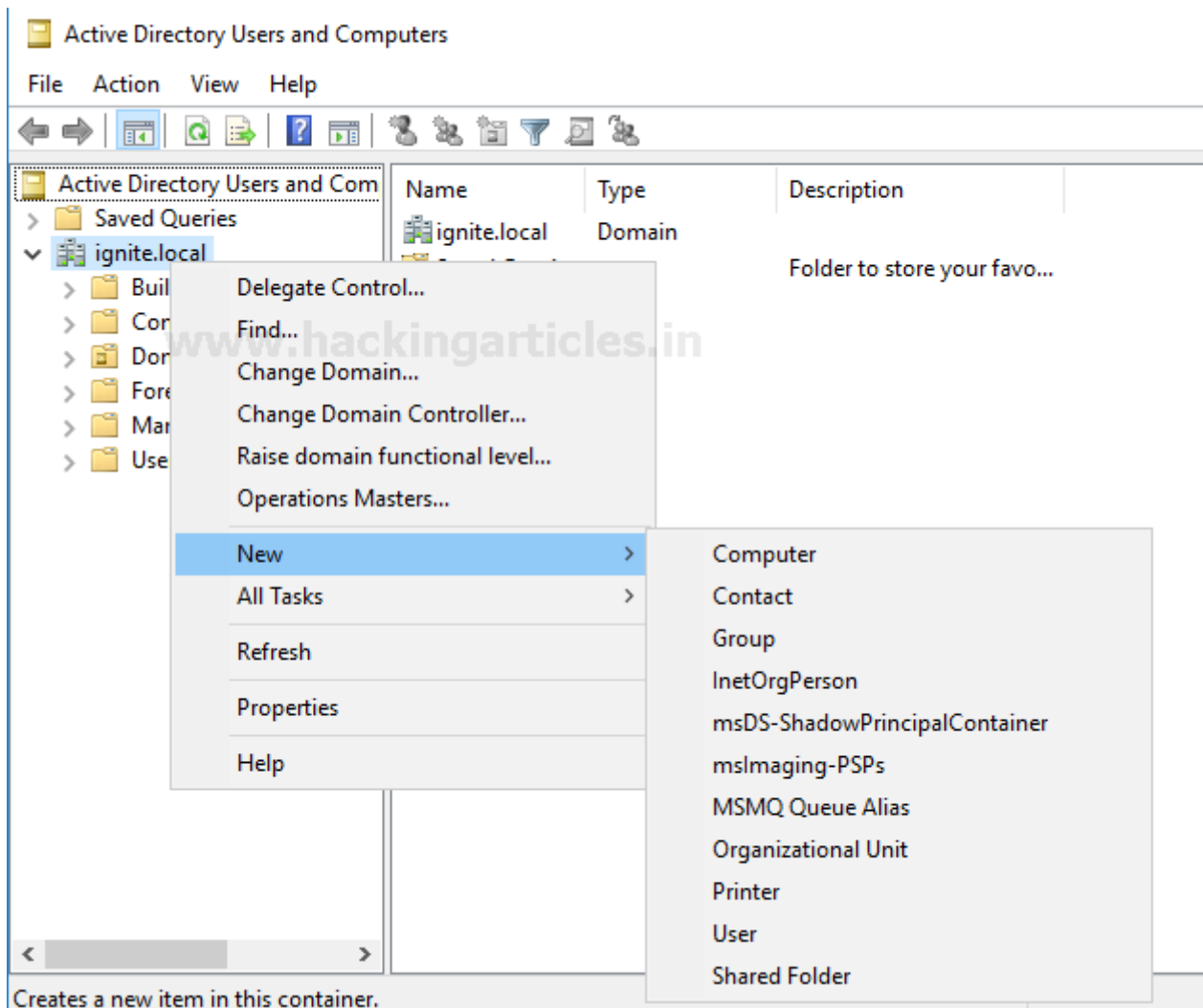
Next >

Install

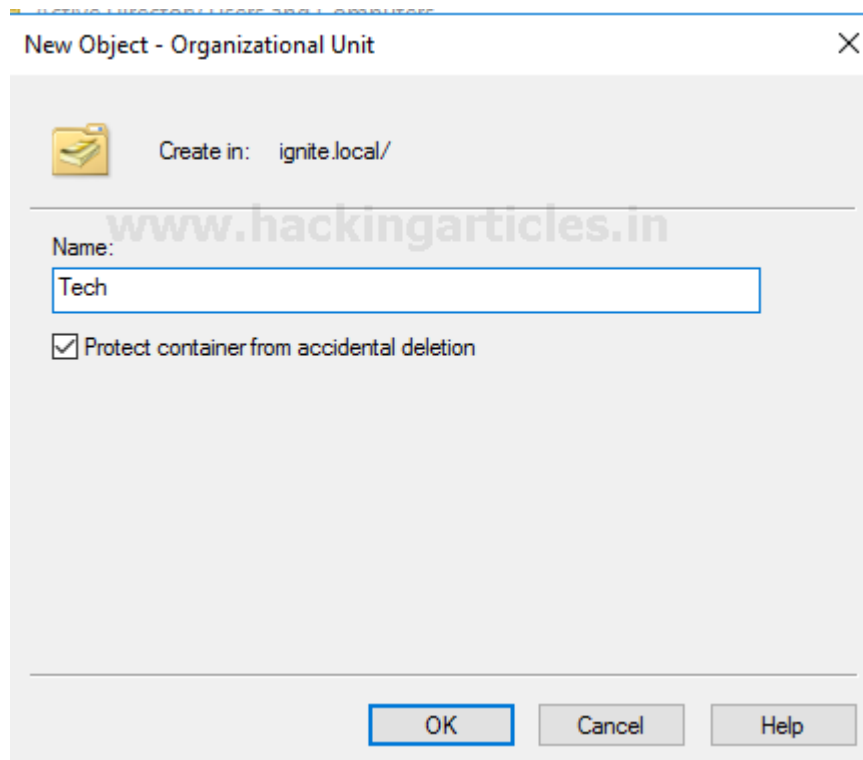
Cancel

Create OU and user

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.



The dialog box is titled "New Object - Organizational Unit" with a close button (X) in the top right corner. It features a folder icon and the text "Create in: ignite.local/". A "Name:" label is followed by a text box containing "Tech". Below this is a checked checkbox labeled "Protect container from accidental deletion". At the bottom are three buttons: "OK", "Cancel", and "Help".

New Object - Organizational Unit

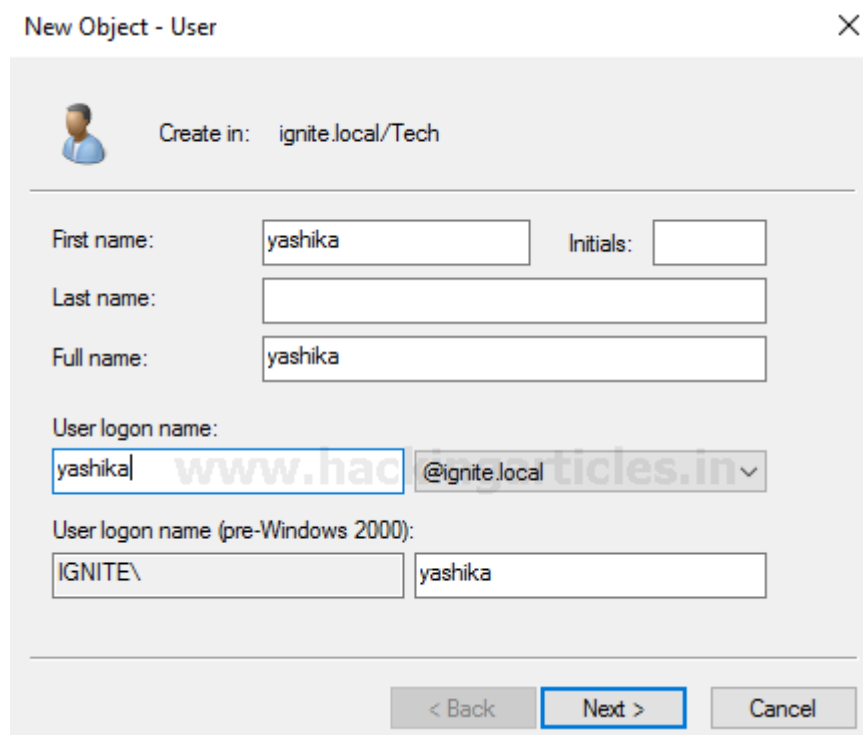
Create in: ignite.local/

Name: Tech

☒ Protect container from accidental deletion

OK Cancel Help

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



The dialog box is titled "New Object - User" with a close button (X) in the top right corner. It features a person icon and the text "Create in: ignite.local/Tech". It contains several input fields: "First name:" with "yashika", "Initials:" (empty), "Last name:" (empty), "Full name:" with "yashika", "User logon name:" with "yashika" and a dropdown menu showing "@ignite.local", and "User logon name (pre-Windows 2000):" with "IGNITE\" and "yashika". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

New Object - User

Create in: ignite.local/Tech

First name: yashika Initials:

Last name:

Full name: yashika

User logon name: yashika @ignite.local

User logon name (pre-Windows 2000): IGNITE\ yashika

< Back Next > Cancel

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

New Object - User

Create in: ignite.local/Tech

Password:

Confirm password:

☐ User must change password at next logon

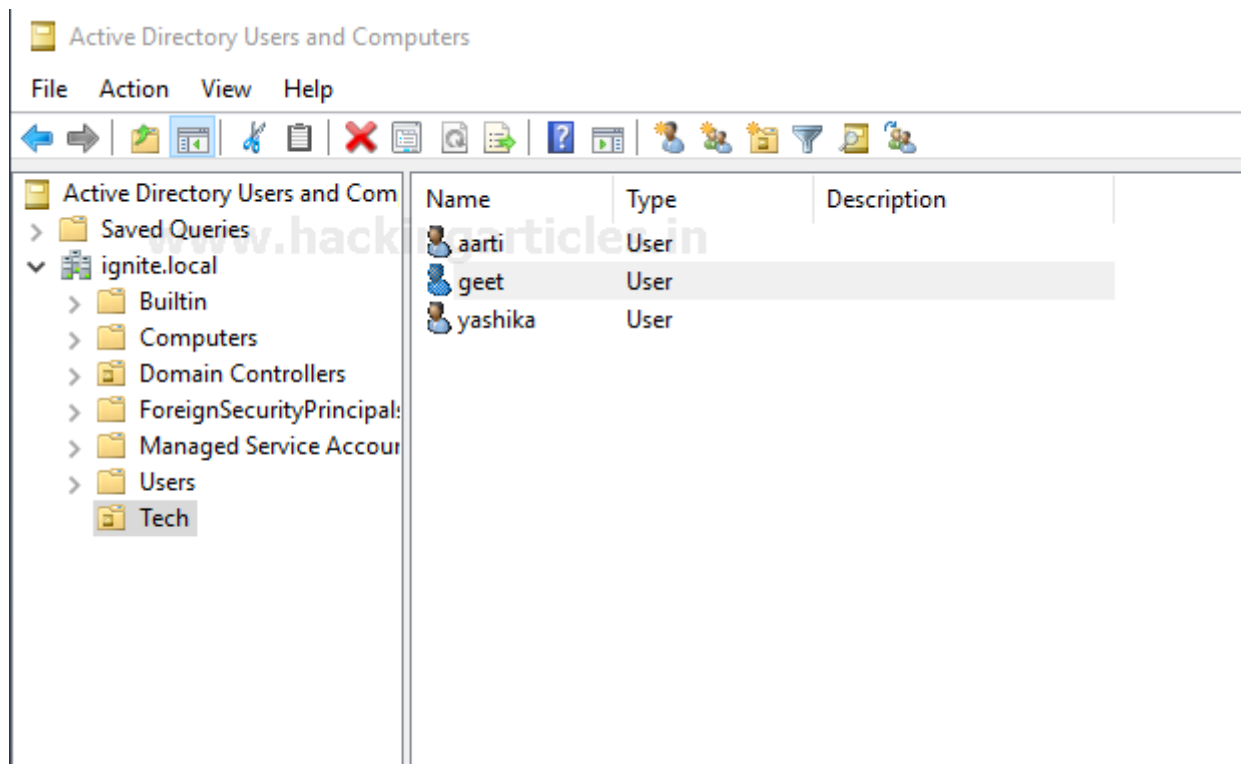
☐ User cannot change password

☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

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.

Internet Protocol Version 4 (TCP/IPv4) Properties ✕

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 1 . 104

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 105

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

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

System

Control Panel > System and Security > System

Search Control Panel


Control Panel Home

- Device Manager
- Remote settings
- System protection
- Advanced system settings

View basic information about your computer


Windows edition

Windows 10 Pro
© 2019 Microsoft Corporation. All rights reserved.



System

Manufacturer:	VMware
Processor:	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz 3.60 GHz
Installed memory (RAM):	2.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display



VMware support

Website: [Online support](#)

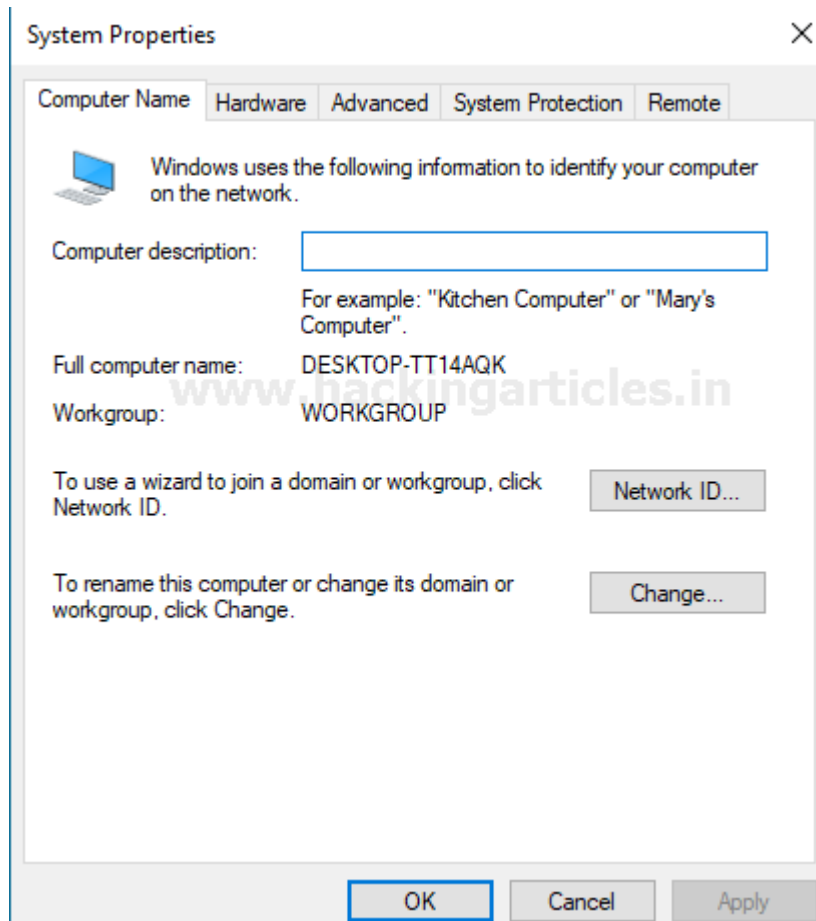
Computer name, domain, and workgroup settings

Computer name:	DESKTOP-TT14AQK	Change settings
Full computer name:	DESKTOP-TT14AQK	
Computer description:		
Workgroup:	WORKGROUP	

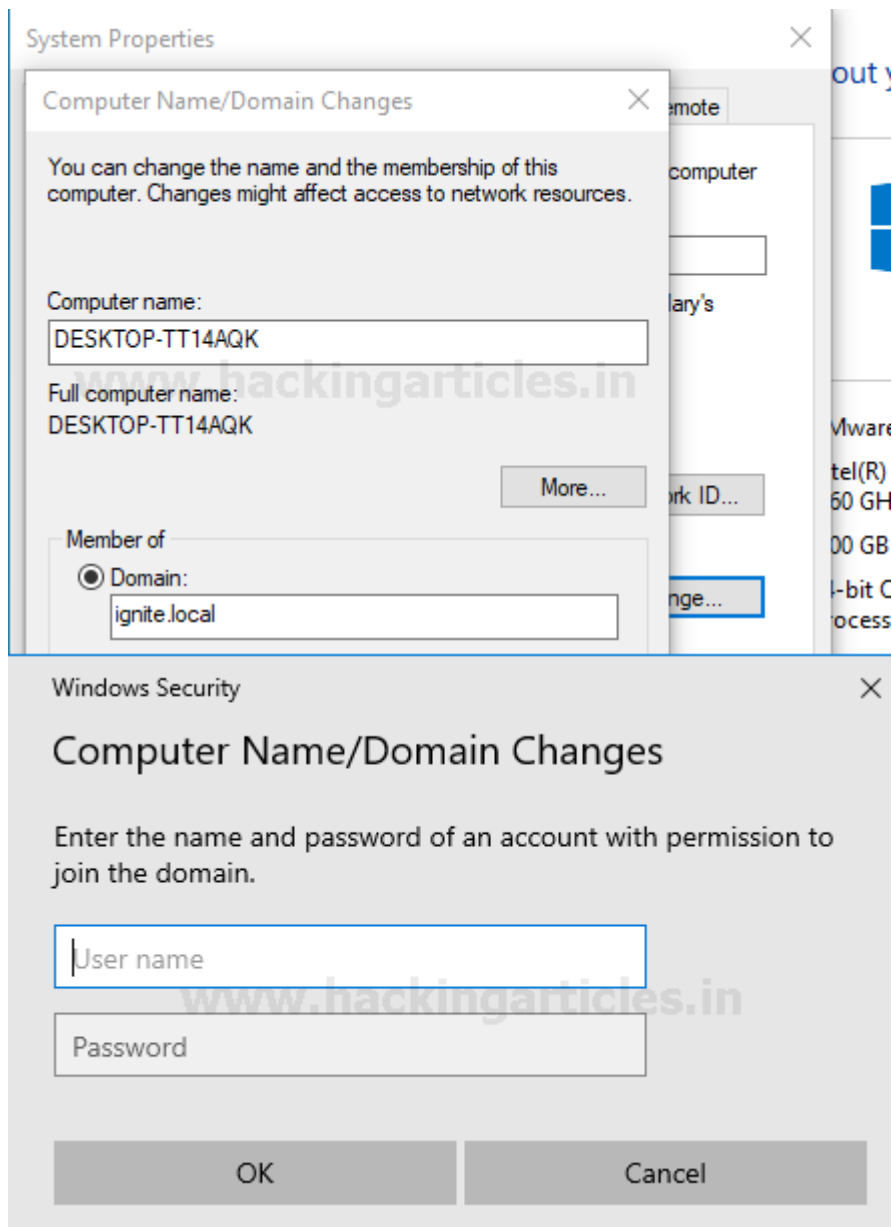
See also

Windows activation

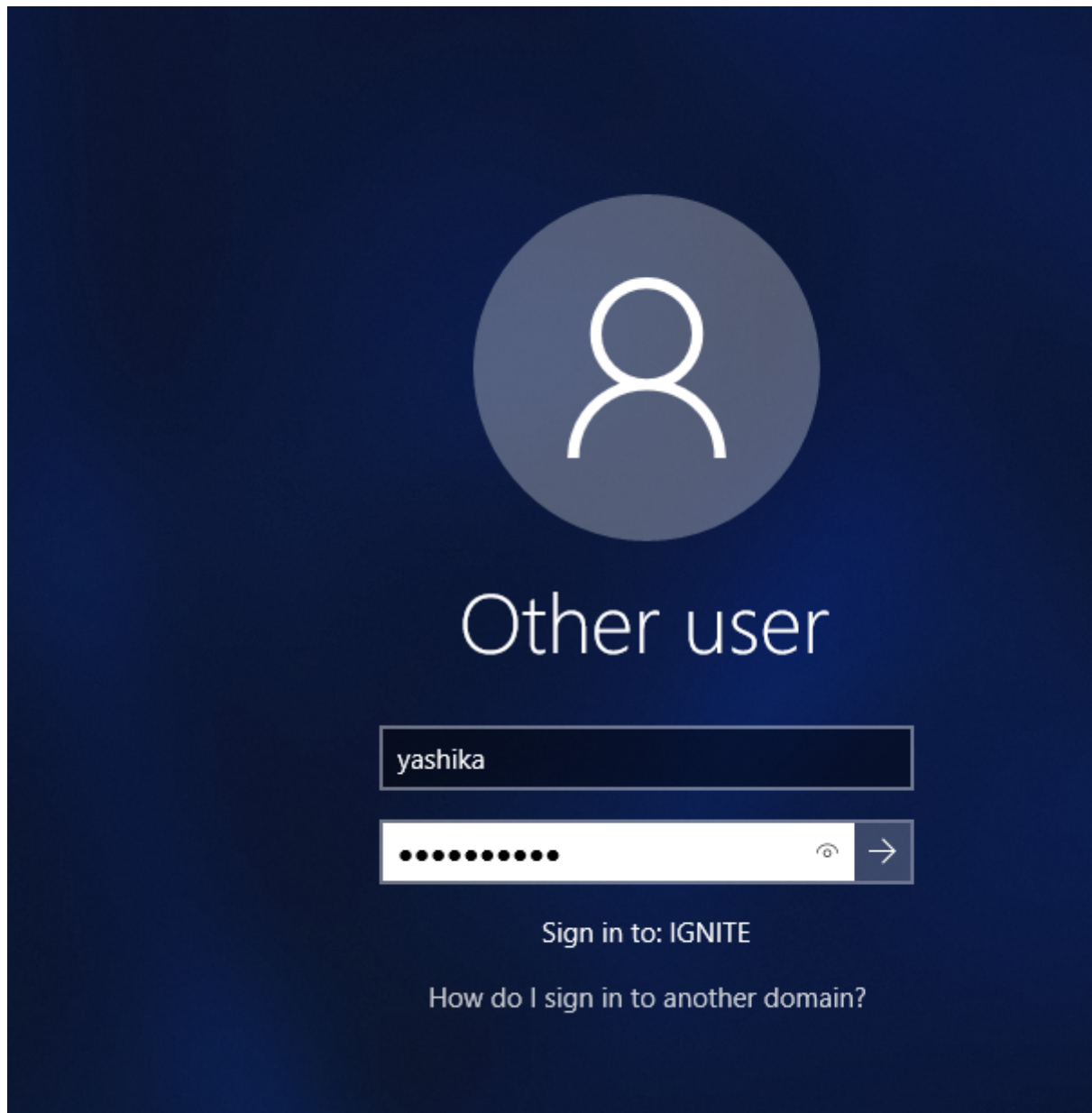
Now click on the change option to join the domain.



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 Pentesting Lab is setup and ready to use. Happy Pentesting!

Author: Jeenali Kothari is a Digital Forensics enthusiast and enjoys technical content writing. You can reach her on [Here](#)