

Active Directory Pentesting: Lab Setup

March 9, 2021 By Raj Chandel

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.

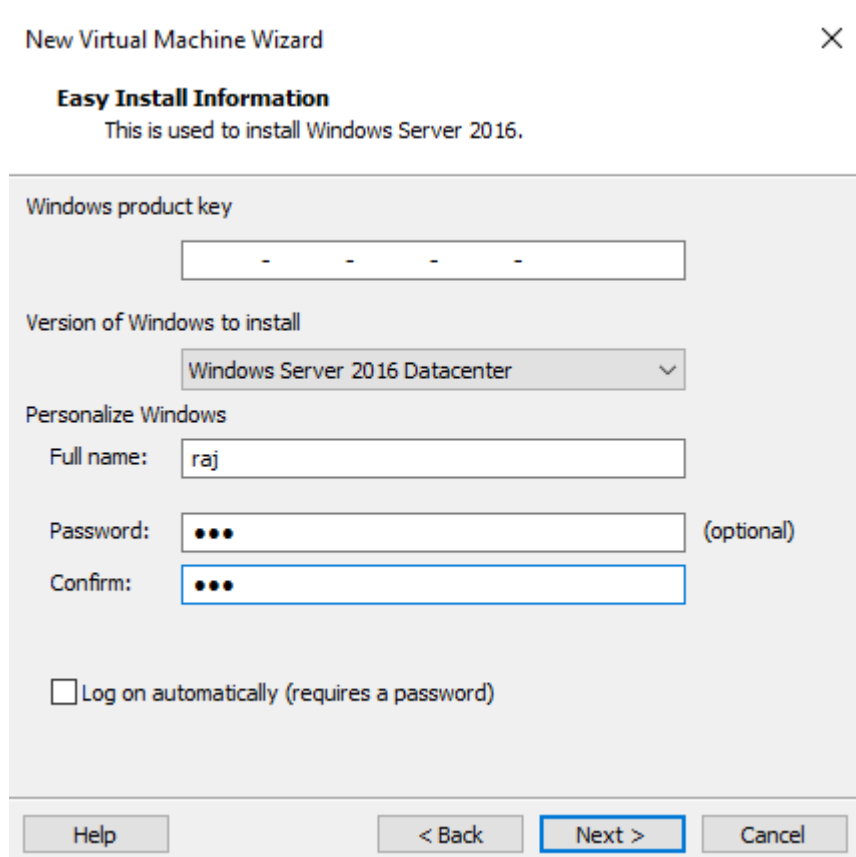
Lab Requirements

- Virtual Machine (VMware Work Station/Player)
- Windows Server 2016
- Windows 10 Pro Operating System (Client)

Configuring Windows Server 2016

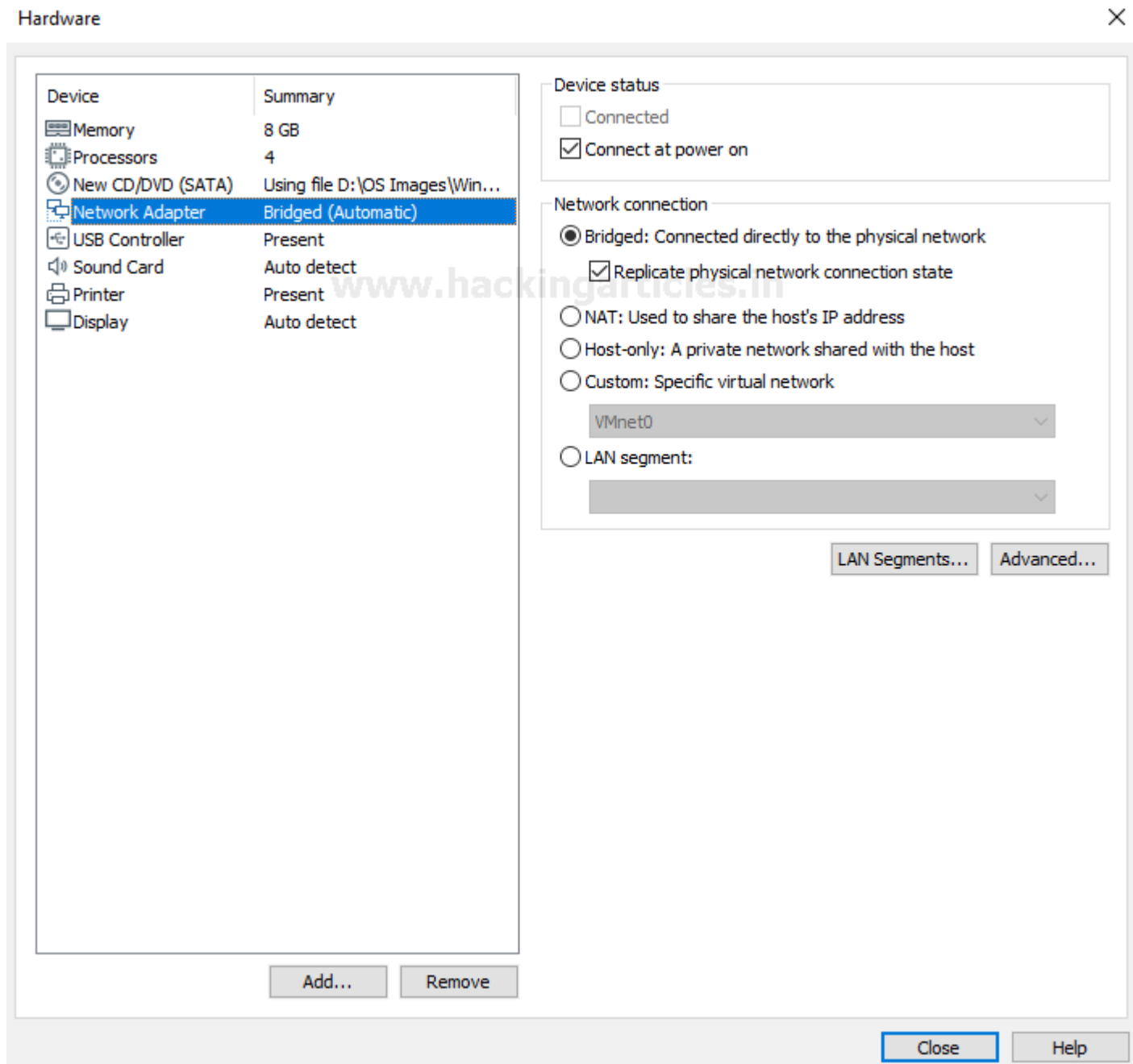
Power on your VMware, and let's begin with the installation by creating a new Virtual machine from the File option. Here you will personalise your Windows system by providing it with your username and the password

that you want to set. Then click on Next to proceed.

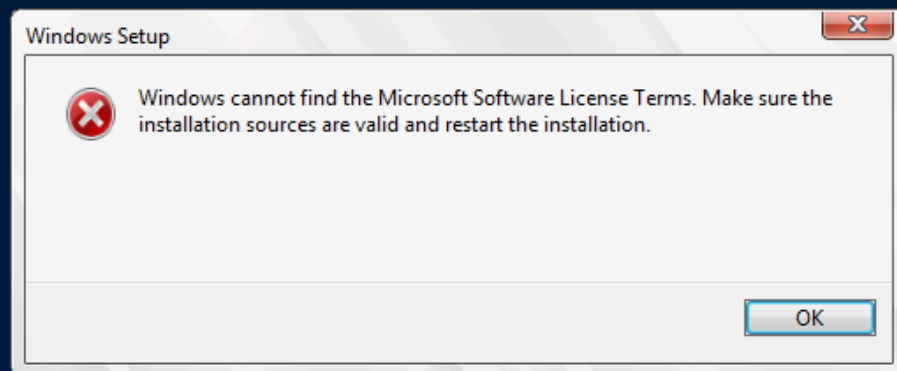


The screenshot shows the 'New Virtual Machine Wizard' window, specifically the 'Easy Install Information' step. The window has a title bar with a close button (X). Below the title bar, the text 'Easy Install Information' is displayed, followed by 'This is used to install Windows Server 2016.' The main content area contains several fields: 'Windows product key' with a text box containing four dashes; 'Version of Windows to install' with a dropdown menu showing 'Windows Server 2016 Datacenter'; 'Personalize Windows' section with 'Full name:' followed by a text box containing 'raj'; 'Password:' followed by a text box with three dots and '(optional)'; 'Confirm:' followed by a text box with three dots; and a checkbox labeled 'Log on automatically (requires a password)'. At the bottom, there are four buttons: 'Help', '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

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.

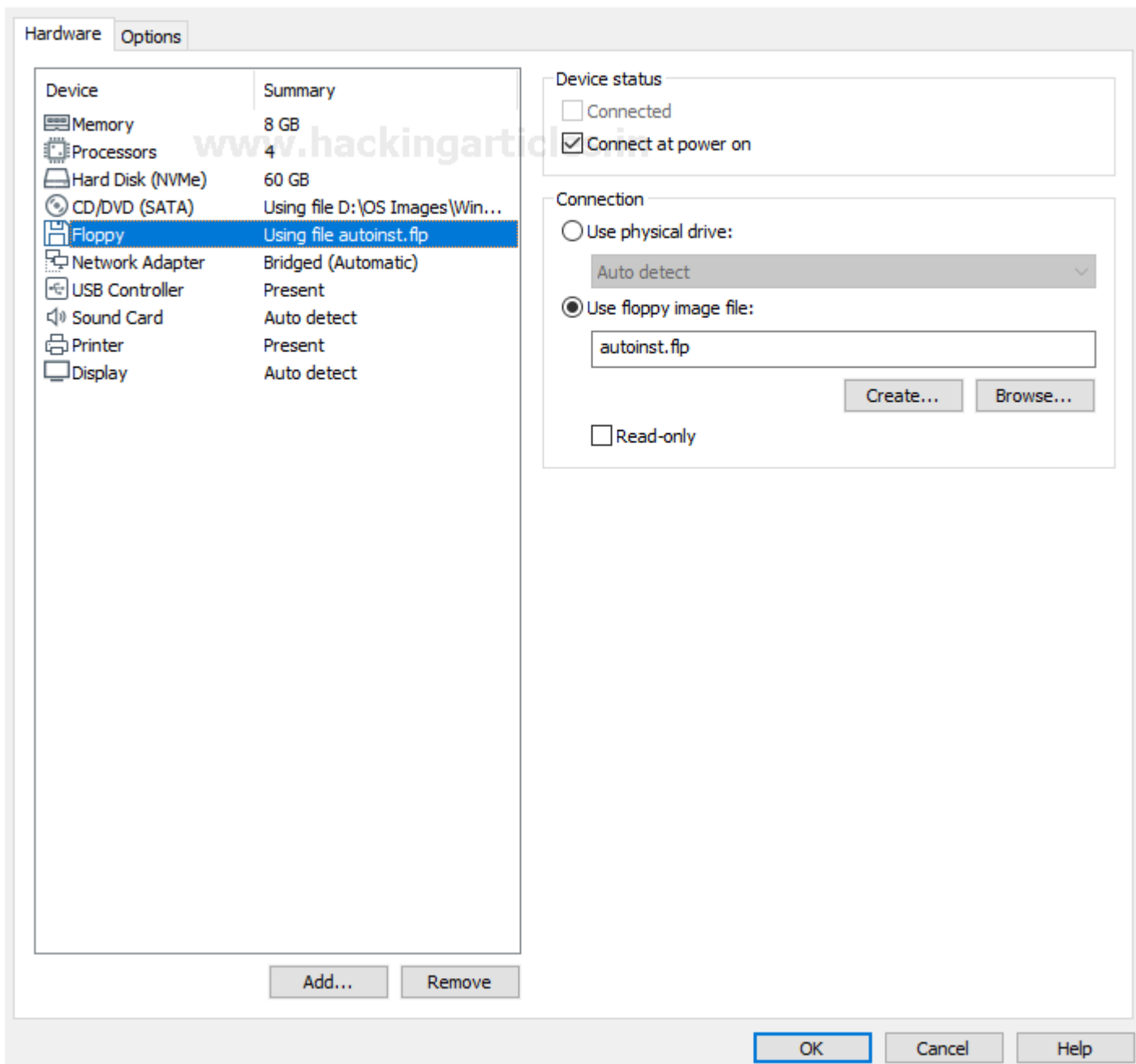


Here you see that the setup did not proceed, therefore let's go back and fix this error from occurring.

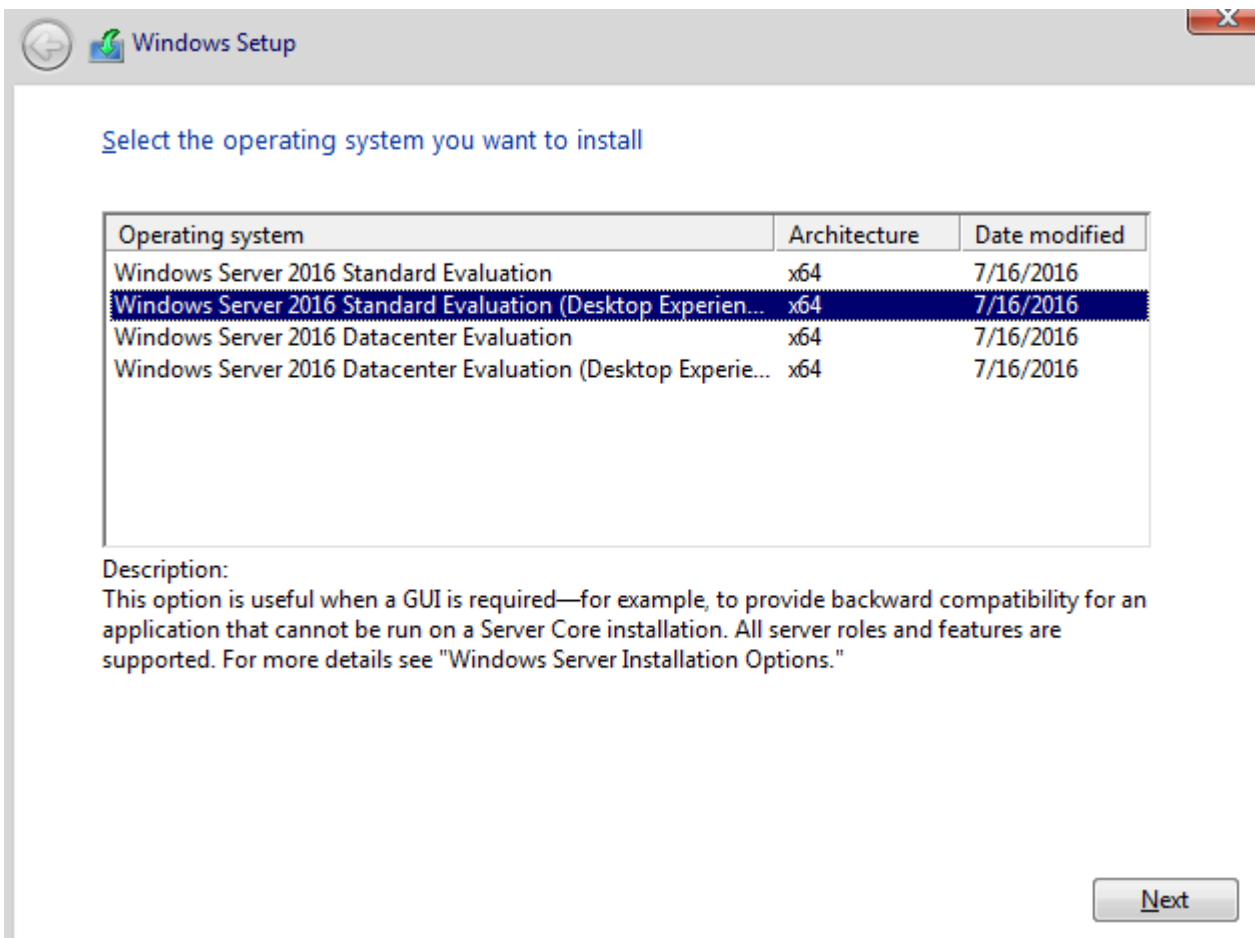


Setup is starting

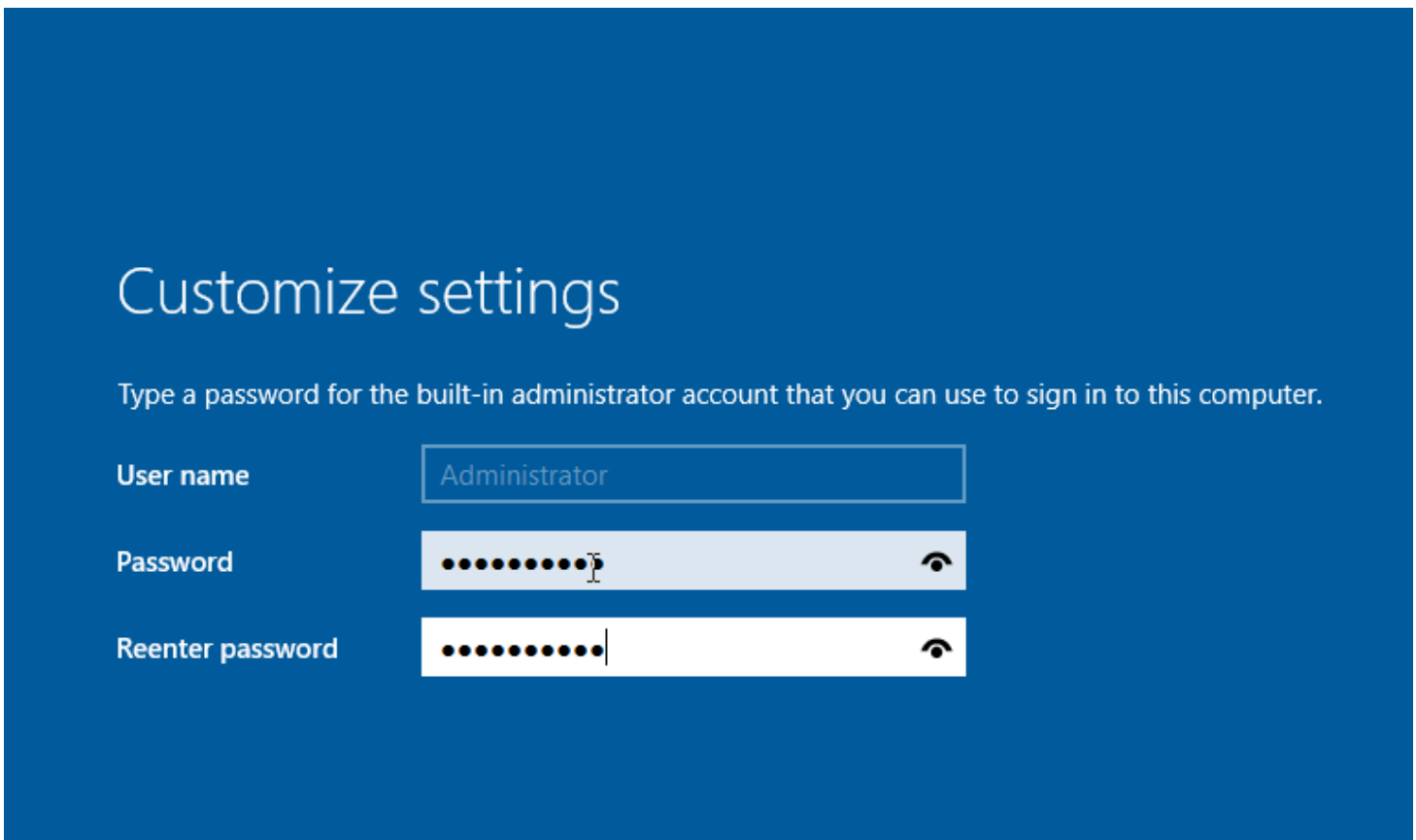
We will go back to Virtual Machine settings and click on Floppy, there under the connection option and choose the Use floppy image file option to make it work like a charm and proceed.



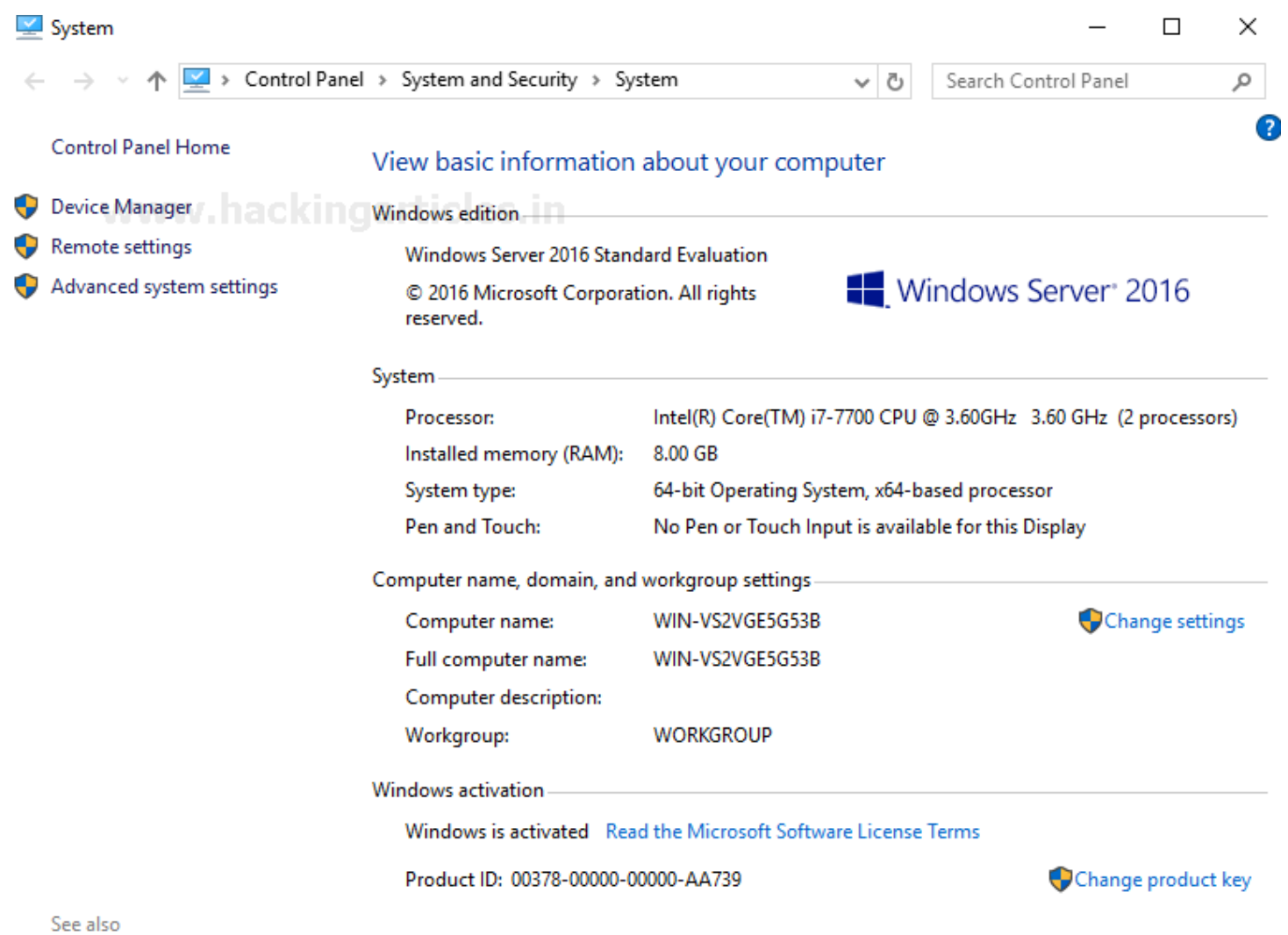
Now you will select the operating system to install from the four options given below. Here we use Standard Edition with the GUI to have a better user-interface. The Desktop Edition provides much better features as compared to the server-core as it has very limited functions. Click on next to proceed.



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.



The screenshot shows the Windows Server 2016 'System' control panel window. The title bar reads 'System'. The breadcrumb navigation shows 'Control Panel > System and Security > System'. A search bar on the right says 'Search Control Panel'. On the left, there are links for 'Control Panel Home', 'Device Manager', 'Remote settings', and 'Advanced system settings'. The main content area is titled 'View basic information about your computer'. It includes a 'Windows edition' section showing 'Windows Server 2016 Standard Evaluation' and '© 2016 Microsoft Corporation. All rights reserved.' with the Windows logo and 'Windows Server® 2016'. Below this is a 'System' section with details: Processor (Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz), Installed memory (RAM) (8.00 GB), System type (64-bit Operating System, x64-based processor), and Pen and Touch (No Pen or Touch Input is available for this Display). The 'Computer name, domain, and workgroup settings' section shows Computer name (WIN-VS2VGE5G53B), Full computer name (WIN-VS2VGE5G53B), Computer description, and Workgroup (WORKGROUP), with a 'Change settings' link. The 'Windows activation' section shows 'Windows is activated' with a link to 'Read the Microsoft Software License Terms' and Product ID (00378-00000-00000-AA739) with a 'Change product key' link. A 'See also' link is at the bottom left.

System

Control Panel > System and Security > System

Search Control Panel

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 [Change settings](#)

Full computer name: WIN-VS2VGE5G53B

Computer description:

Workgroup: WORKGROUP

Windows activation

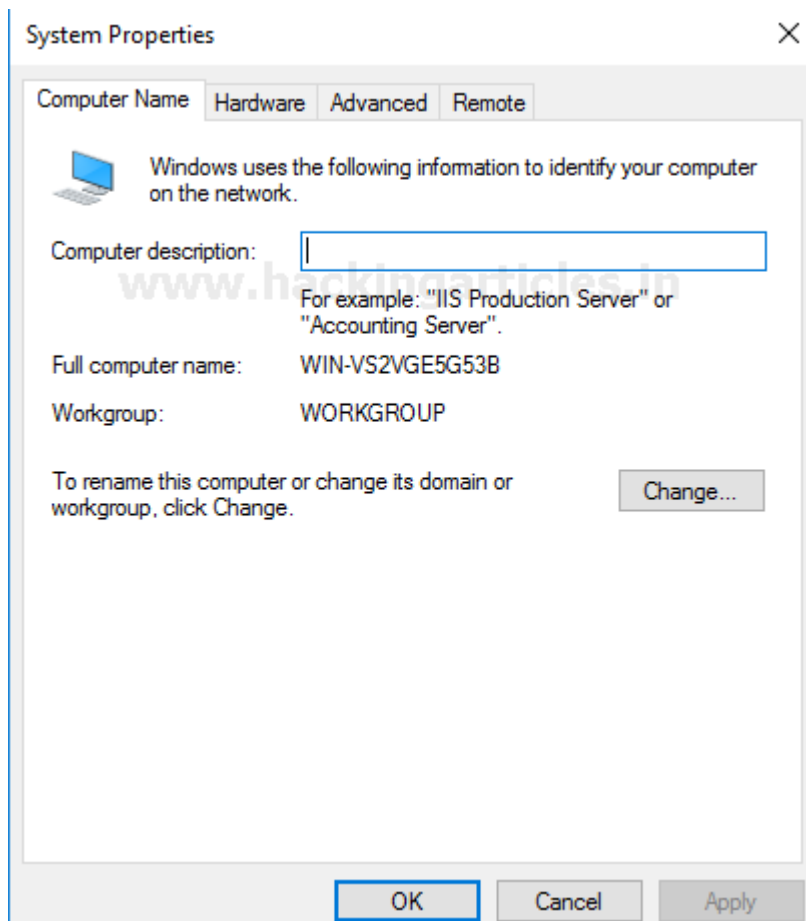
Windows is activated [Read the Microsoft Software License Terms](#)

Product ID: 00378-00000-00000-AA739 [Change product key](#)

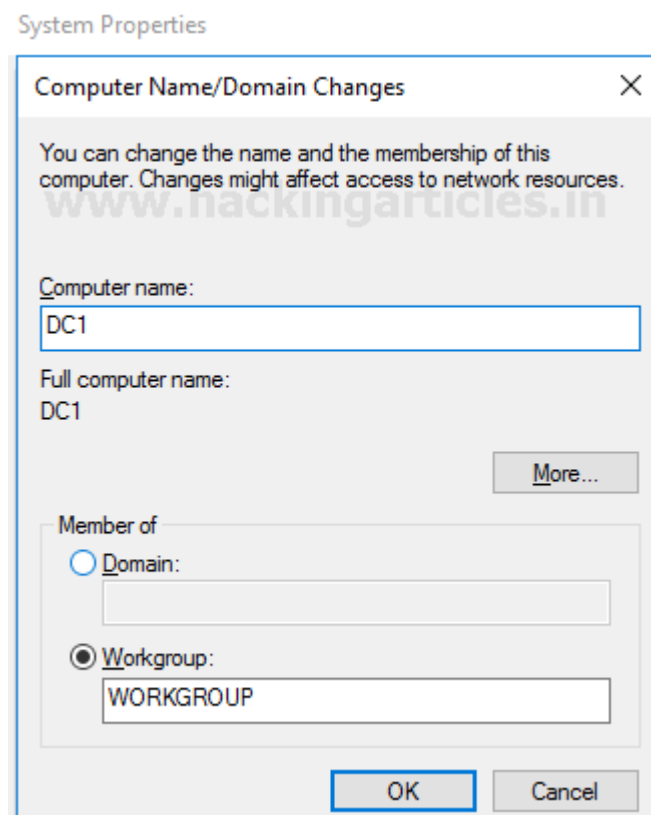
See also

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'.

Server Manager

Server Manager ▸ Dashboard

Manage Tools View Hel

Dashboard

- Local Server
- All Servers
- File and Storage Services ▸

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

Hide

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

File and Storage Services	1
Local Server	1

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

Before you begin

DESTINATION SERVER
DC1

Before You Begin

[Installation Type](#)[Server Selection](#)[Server Roles](#)[Features](#)[Confirmation](#)[Results](#)

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

☒ Skip this page by default

< Previous

Next >

Install

Cancel

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

Select installation type

DESTINATION SERVER
DC1

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**

Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel

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

Select installation type

DESTINATION SERVER
DC1

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**

Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel

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.

Select server roles

DESTINATION SERVER
DC1

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☒ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☒ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ MultiPoint Services
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous

Next >

Install

Cancel

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.

Select server roles

DESTINATION SERVER
DC1

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☒ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☒ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ MultiPoint Services
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

< Previous

Next >

Install

Cancel

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

Confirm installation selections

DESTINATION SERVER
DC1

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

To install the following roles, role services, or features on selected server, click Install.

☐ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Domain Services

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

Active Directory module for Windows PowerShell

AD DS Tools

Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools

[Export configuration settings](#)[Specify an alternate source path](#)

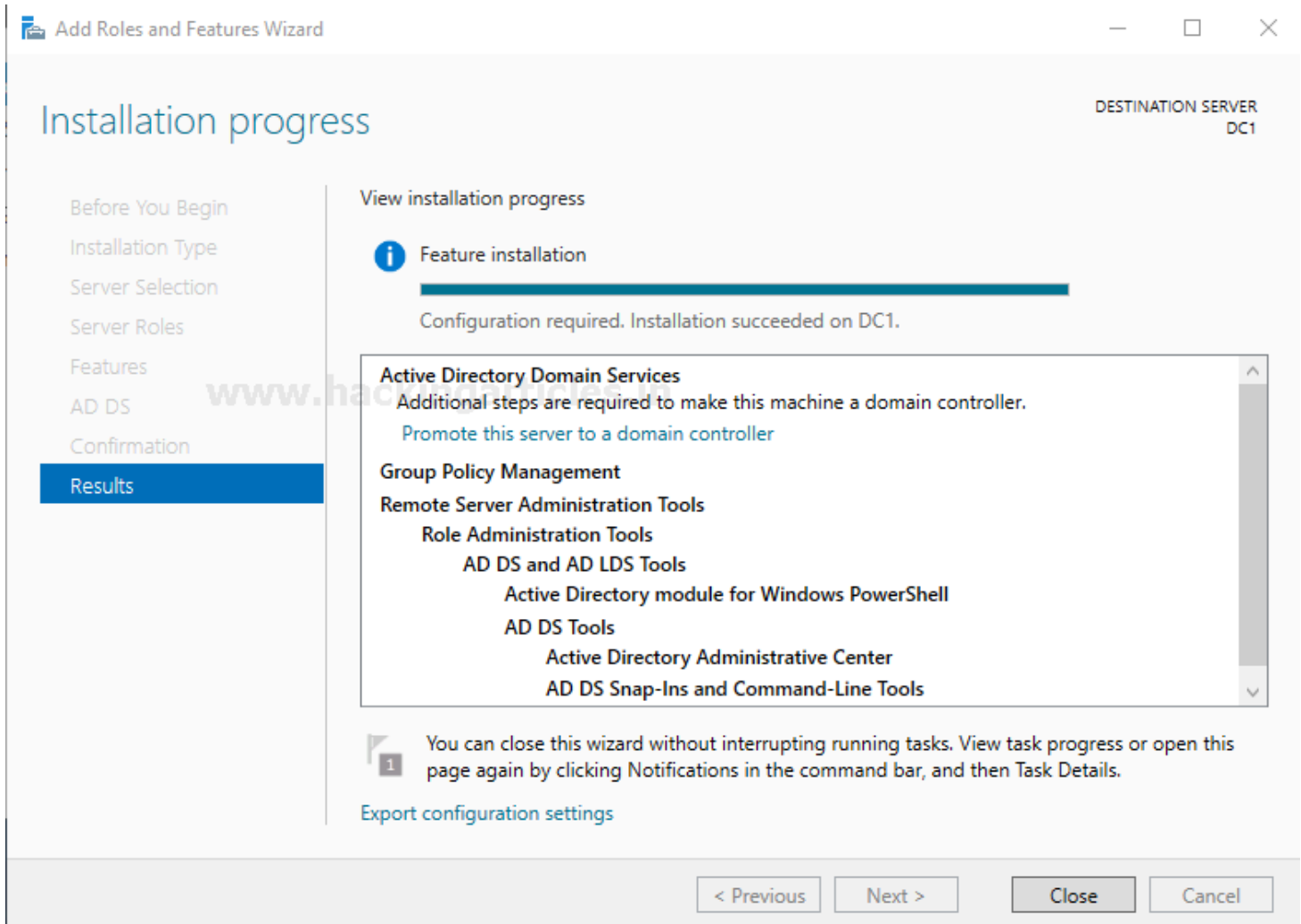
< Previous

Next >

Install

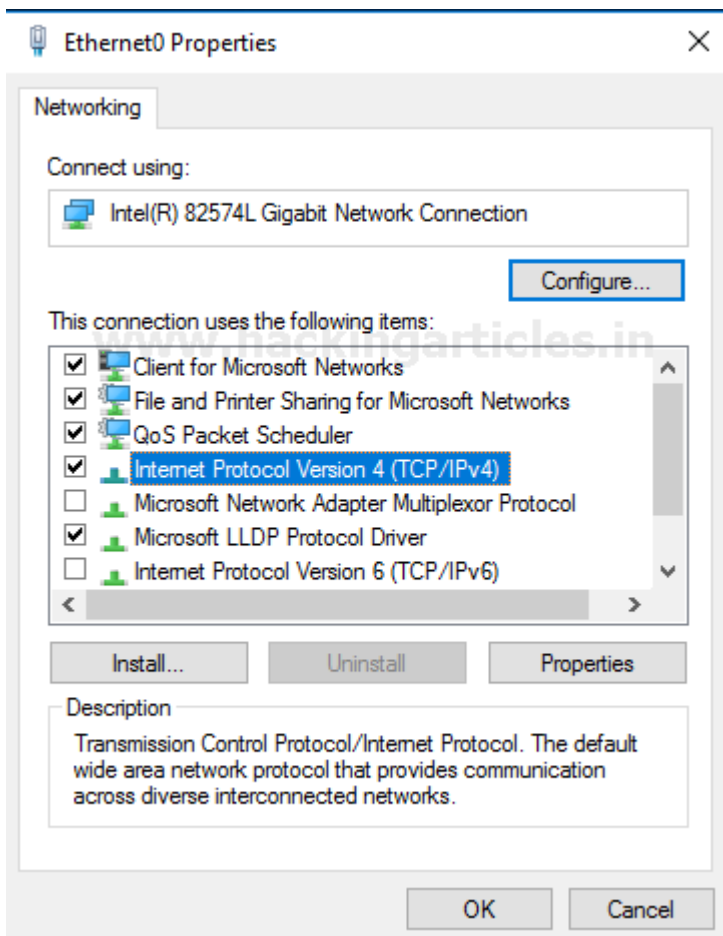
Cancel

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.

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 . 105

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

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.

The screenshot shows the Windows Server Manager interface. The top navigation bar includes 'Server Manager' and 'Dashboard'. A left-hand menu lists 'Dashboard', 'Local Server', 'All Servers', 'AD DS', and 'File and Storage Services'. The main content area displays a 'Post-deployment Configuration' task with a yellow warning icon. The task description states: 'Configuration required for Active Directory Domain Services at DC1'. Below this, there is a link to 'Promote this server to a domain controller'. A secondary section titled 'Feature installation' shows a progress bar and the message 'Configuration required. Installation succeeded on DC1.', with a link to 'Add Roles and Features'. A 'Task Details' button is at the bottom of the task card. In the background, a 'QUICK LINKS' section is partially visible, showing a step '5 Connect this server to cloud services'. At the bottom, the 'ROLES AND SERVER GROUPS' section shows 'AD DS' and 'File and Storage Services' with a count of 1 for each.

Server Manager Dashboard

Post-deployment Configuration

Configuration required for Active Directory Domain Services at DC1

[Promote this server to a domain controller](#)

Feature installation

Configuration required. Installation succeeded on DC1.

[Add Roles and Features](#)

Task Details

QUICK LINKS

5 Connect this server to cloud services

ROLES AND SERVER GROUPS

Roles: 2 | Server groups: 1 | Servers total: 1

Role	Count
AD DS	1
File and Storage Services	1

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.

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.

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

TARGET SERVER
DC1

DNS Options

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

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.

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

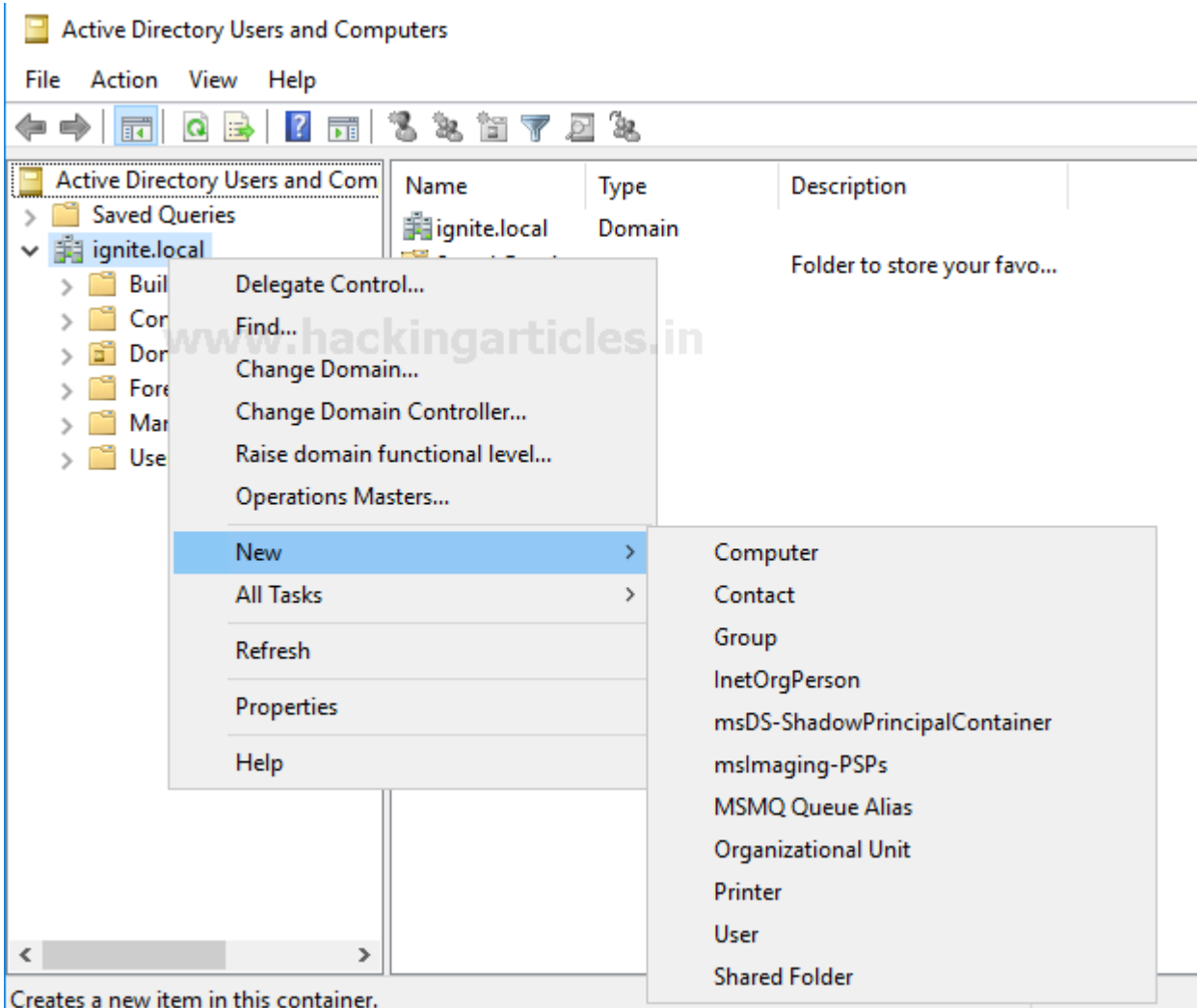
Next >

Install

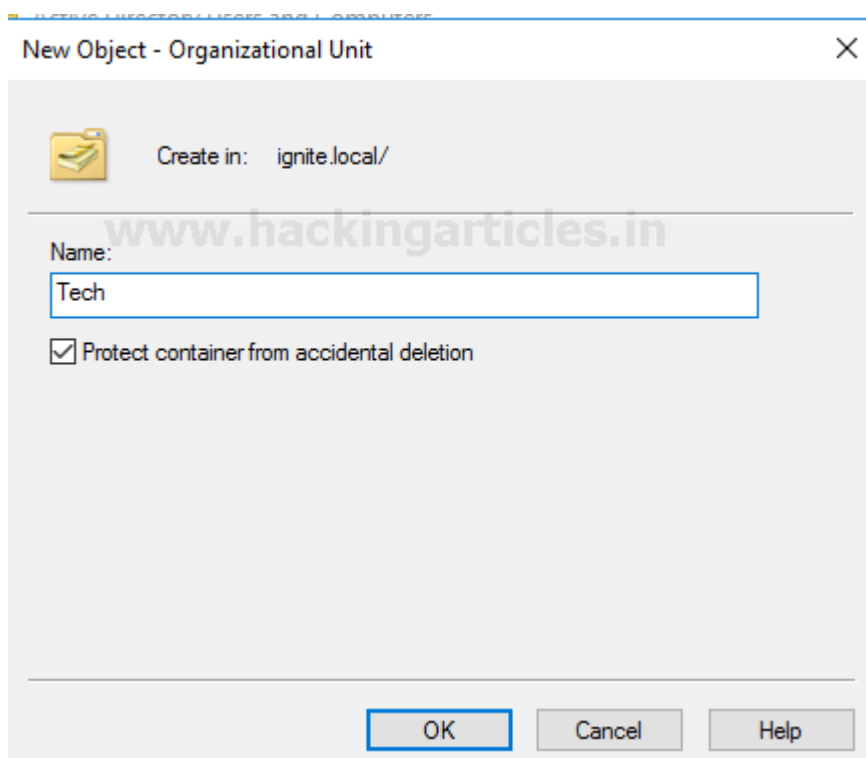
Cancel

Create OU and user

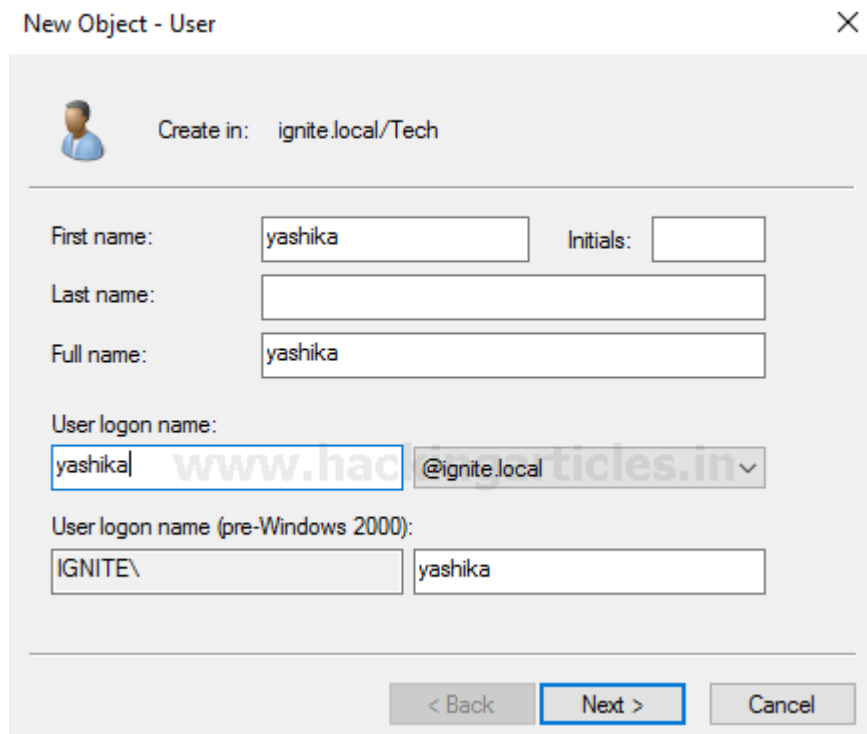
Now let us proceed to create users in our Active Directory by clicking on **Tools/Active Directory Users and Computers**. It will open a new window; click on the domain name you have created and then click on **New/Organisational Unit**.



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



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



New Object - User

Create in: ignite.local/Tech

First name: yashika Initials:

Last name:

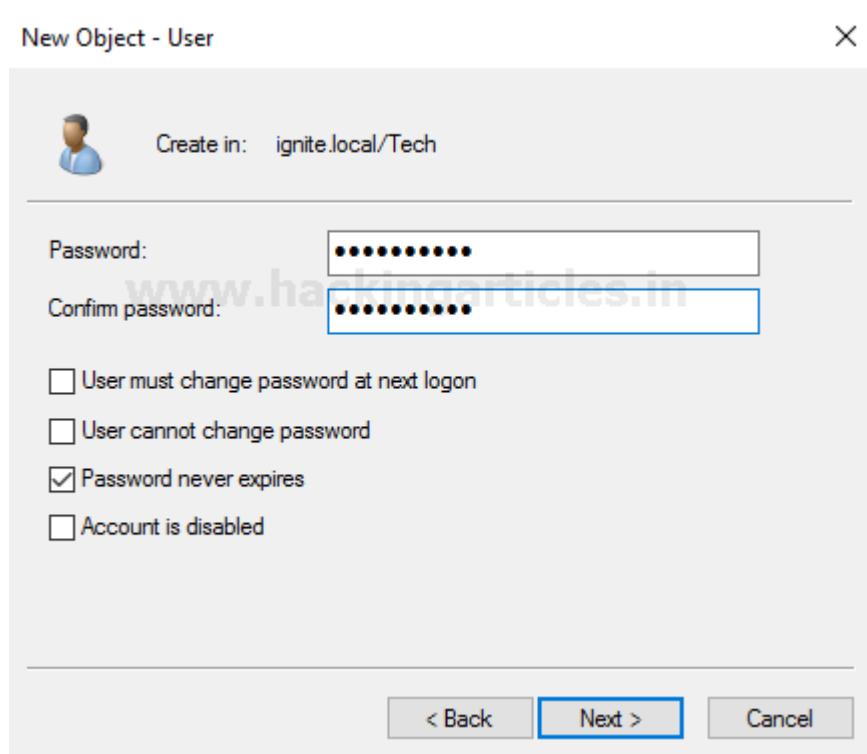
Full name: yashika

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

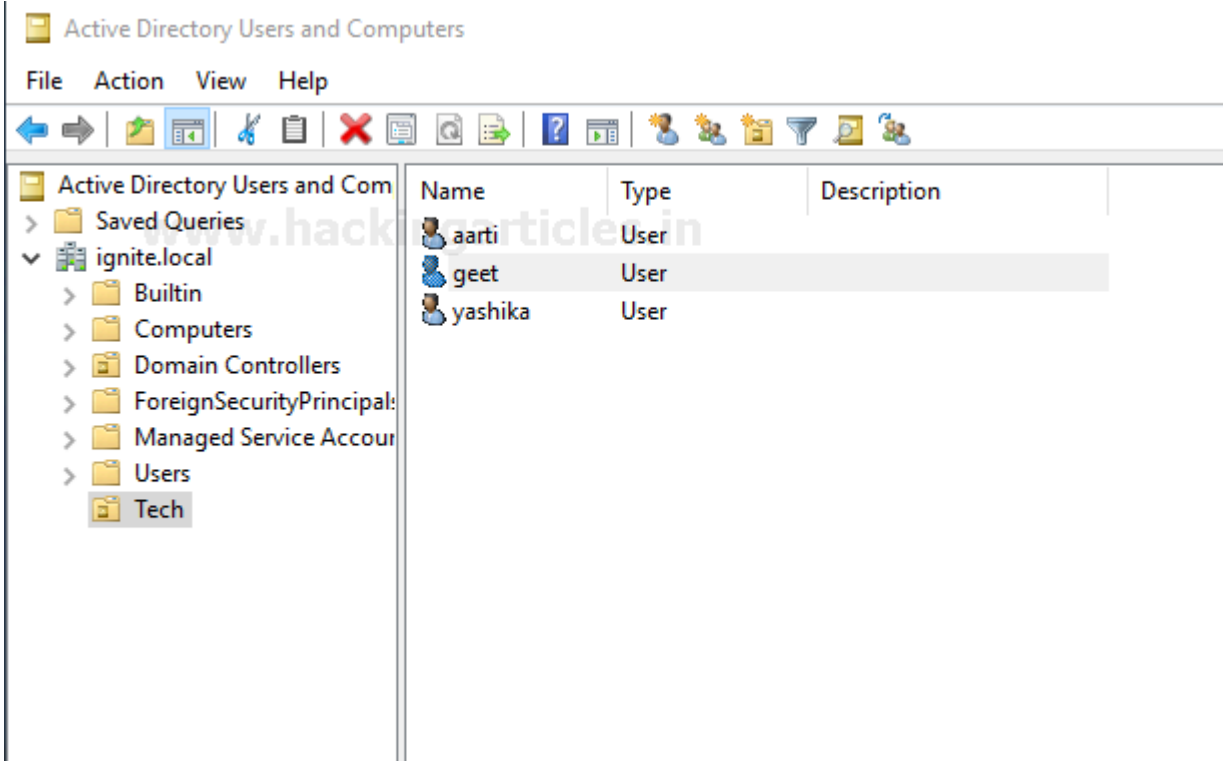
☐ User cannot change password

☒ Password never expires

☐ Account is disabled

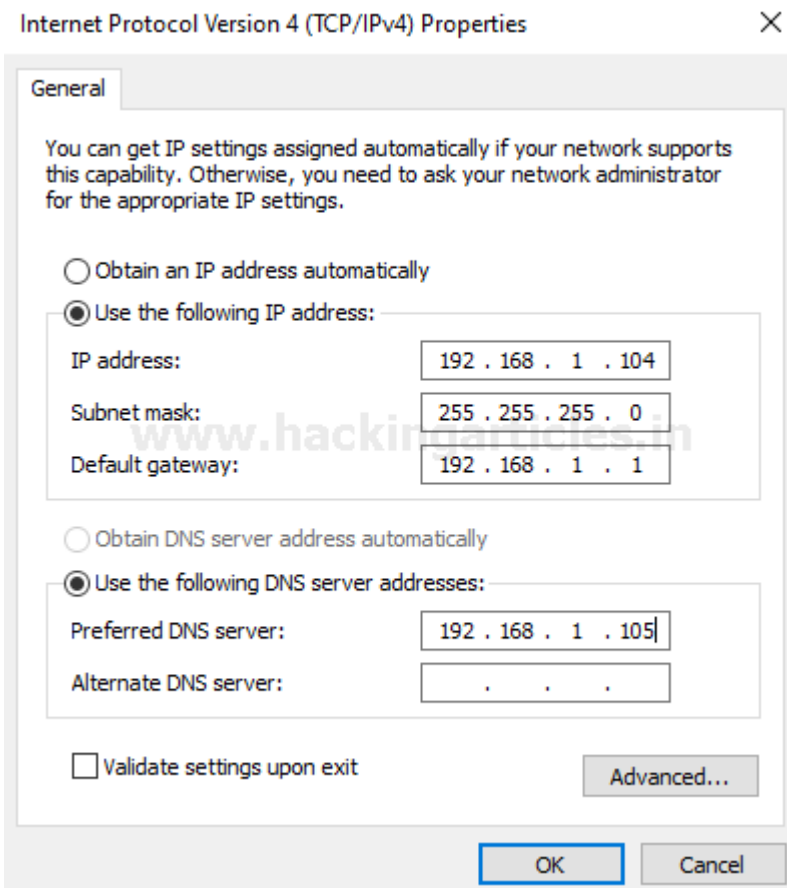
< Back Next > Cancel

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.



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

The screenshot shows the Windows 10 'System' window in the Control Panel. The title bar reads 'System'. The breadcrumb navigation shows 'Control Panel > System and Security > System'. On the left, there's a sidebar with 'Control Panel Home' and links to 'Device Manager', 'Remote settings', 'System protection', and 'Advanced system settings'. The main content area is titled 'View basic information about your computer'. It displays 'Windows edition' as 'Windows 10 Pro' with copyright information. Below this, the 'System' section lists hardware details: Manufacturer (VMware), Processor (Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz), Installed memory (RAM) (2.00 GB), System type (64-bit Operating System, x64-based processor), and Pen and Touch (No Pen or Touch Input is available for this Display). To the right of these details is the VMware logo. Further down, the 'VMware support' section provides a link to 'Online support'. The 'Computer name, domain, and workgroup settings' section shows the computer name as 'DESKTOP-TT14AQK', full computer name as 'DESKTOP-TT14AQK', computer description, and workgroup as 'WORKGROUP'. A 'Change settings' link is available next to the computer name. At the bottom, there are links for 'See also' and 'Windows activation'.

System

Control Panel > System and Security > System

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

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

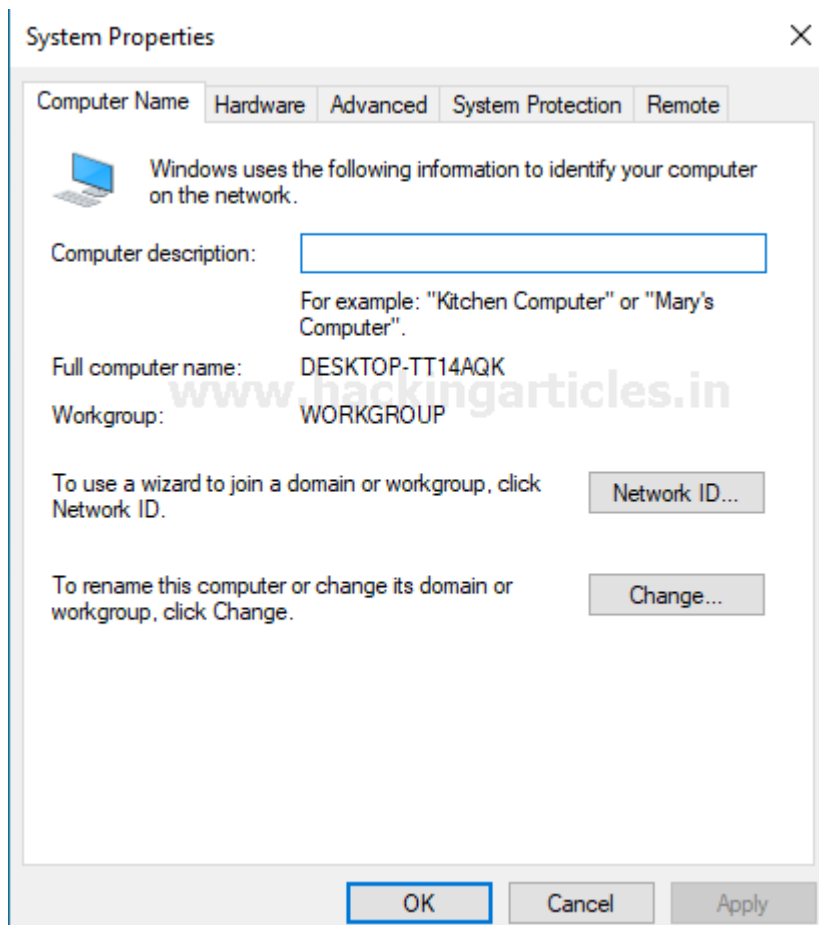
Computer description:

Workgroup: WORKGROUP

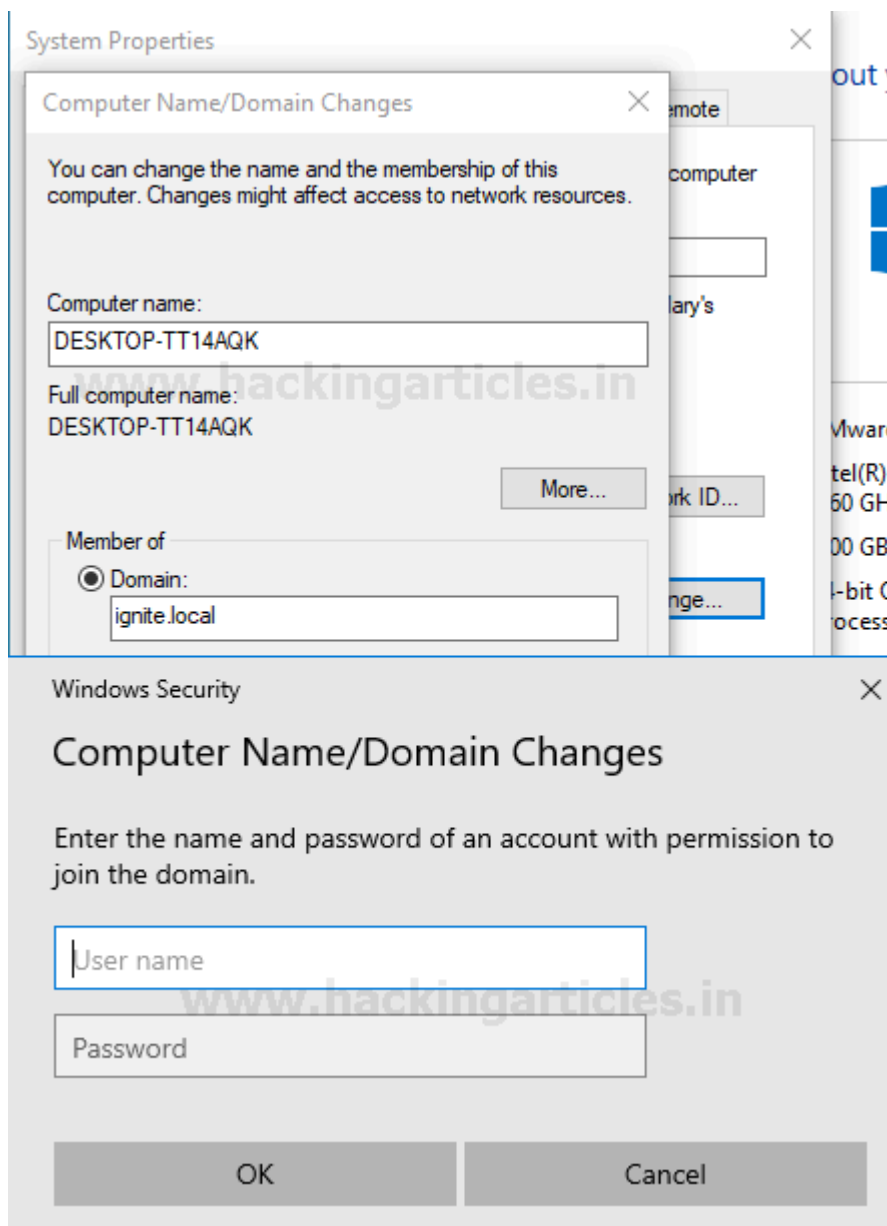
See also

Windows activation

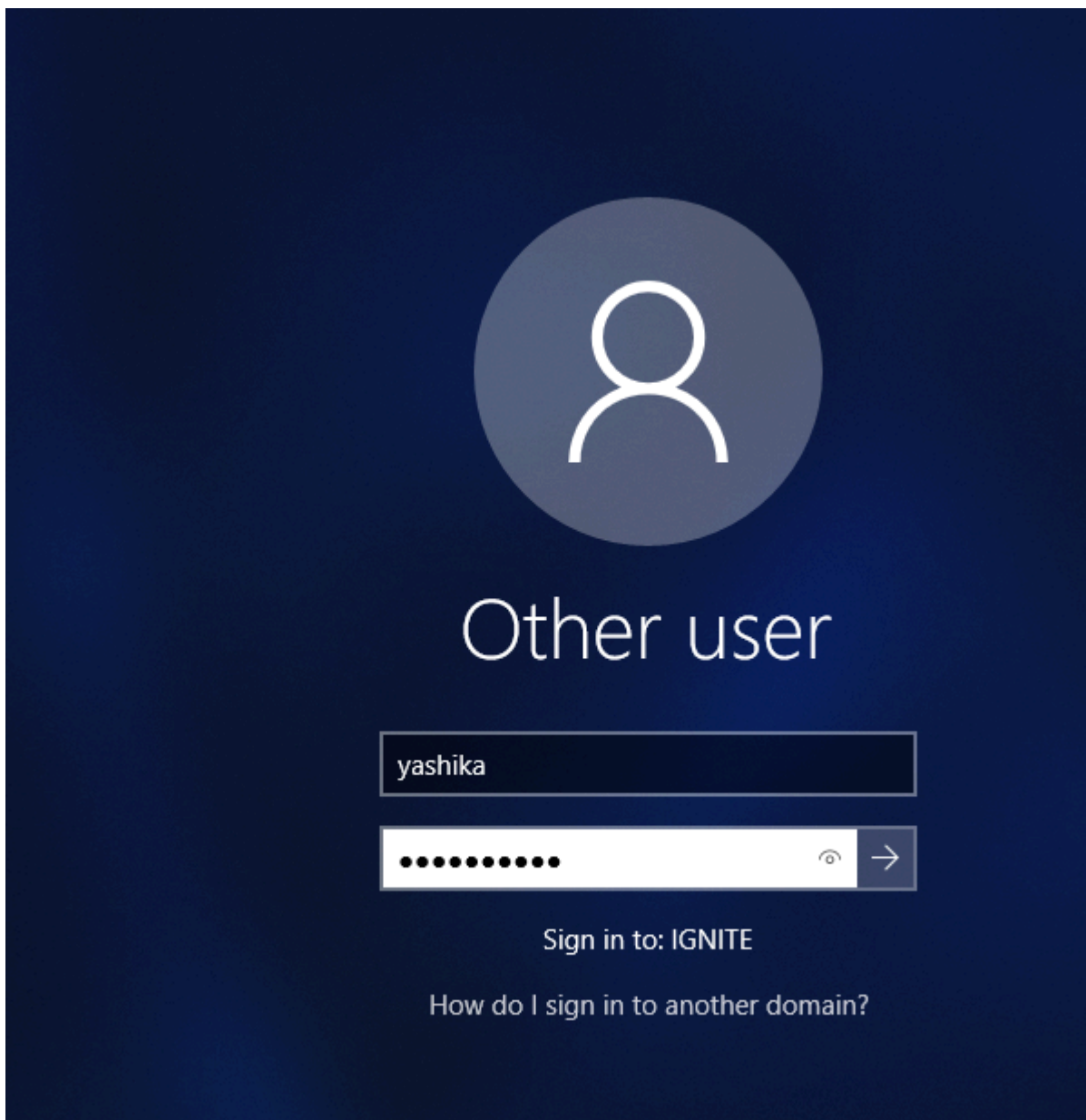
Now click on the change option to join the domain.



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>
```