Windows Active Directory
Creating a new forest

The steps mentioned in this document can be performed on Windows Server 2012 R2 and above.

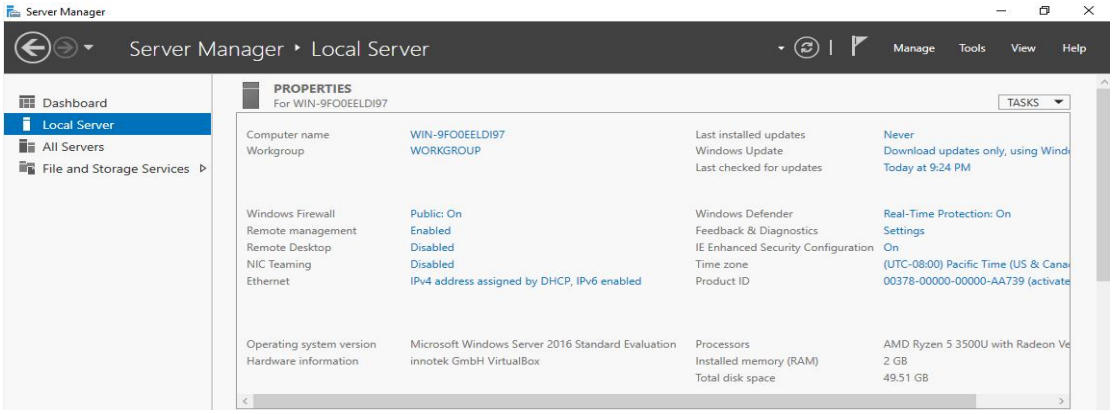
This is the first step in installing Active Directory in any organization. This step will create the first forest and first domain in an organization. Once a Forest and a Domain is created, additional domains (either child or root domain) can be created in that forest. Also additional domain controllers also can be added to the required domains.

Prerequisites :-

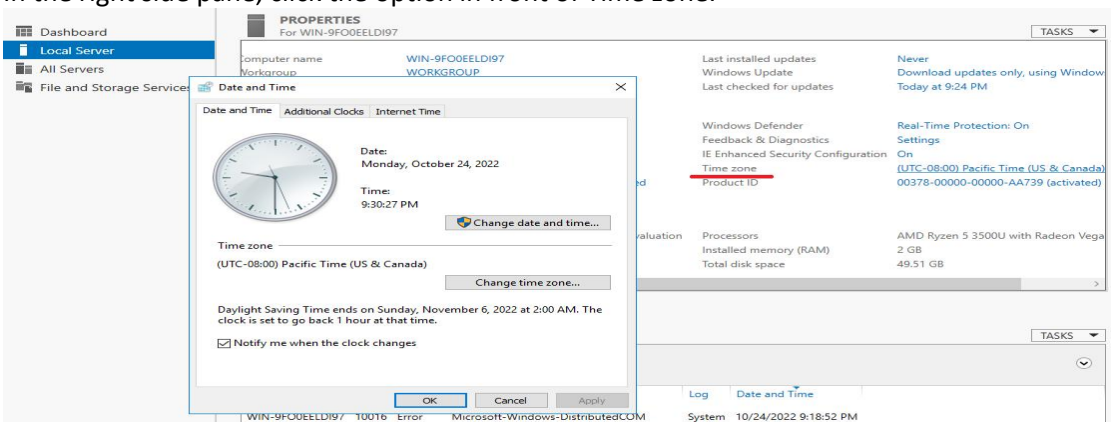
1. A Windows Server 2012 R2 or above installed either on physical server or on a virtual machine. For this document Windows Server 2016 Evaluation version is used.
2. Basic knowledge about Windows Active Directory and its terms like Forest, Domain, Domain Controller, Additional Domain Controller etc.

Steps:-

1. **Post install configuration of Windows Server.**
   A. **Set the correct time zone.**
   In the Server Manager window that opens when the server starts, click the Local Server option as shown below.

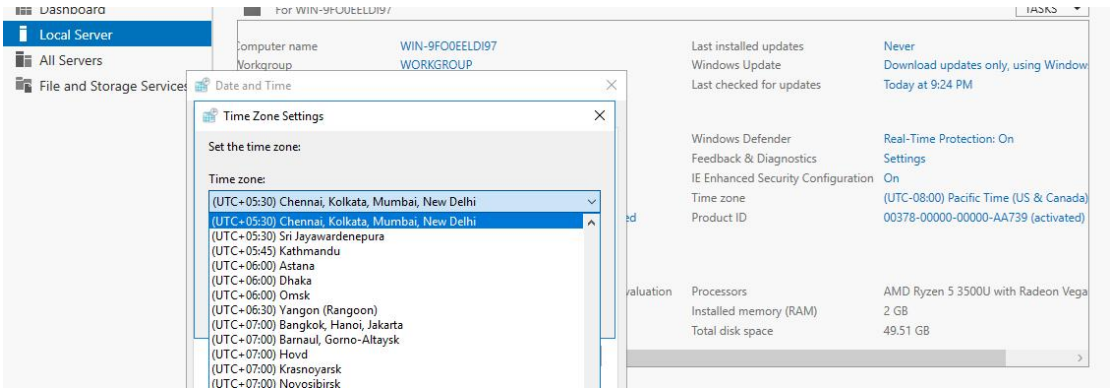


   In the right side pane, click the option in front of Time zone.



Created By:-
Sandeep Walvekar

On the new window that opens click the Change Time one button. In the new window that opens, use the drop down list to select appropriate time zone.

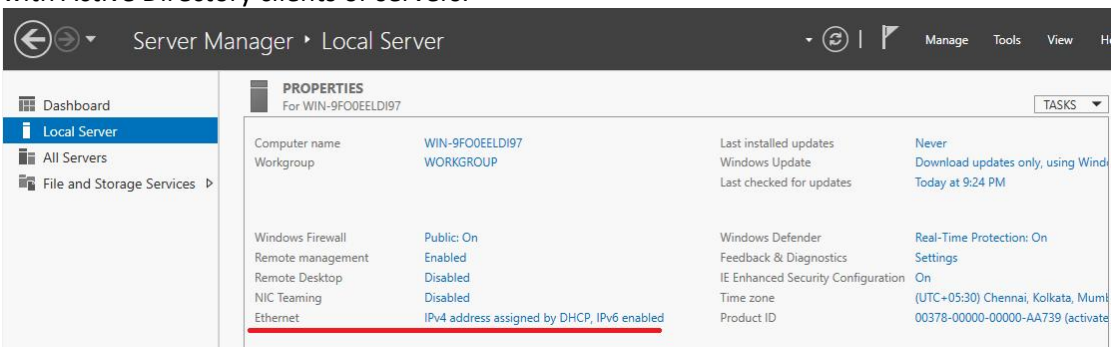


Click Ok. After you select the time zone, the time displayed will change. Make sure the time displayed is the current time displayed as per your location. Click OK to close the window.

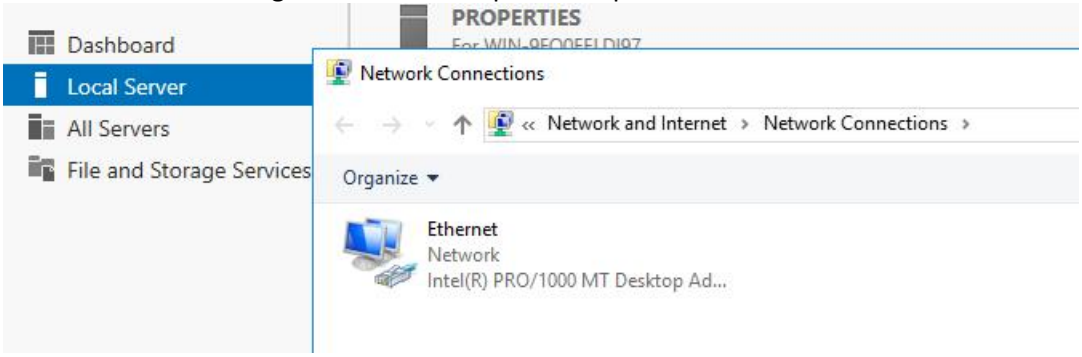
If the selected time zone is not shown in the Server Manager in front of Time zone option, click refresh button to refresh the Server Manager window.

B. **Set the IPv4 address**

To set manual IPv4 address to the server, click the option in front of Ethernet in the Server Manager Window as shown below. If multiple adapters are attached then there will be multiple entries. Select the adapter that will be used to communicate with Active Directory clients or servers.

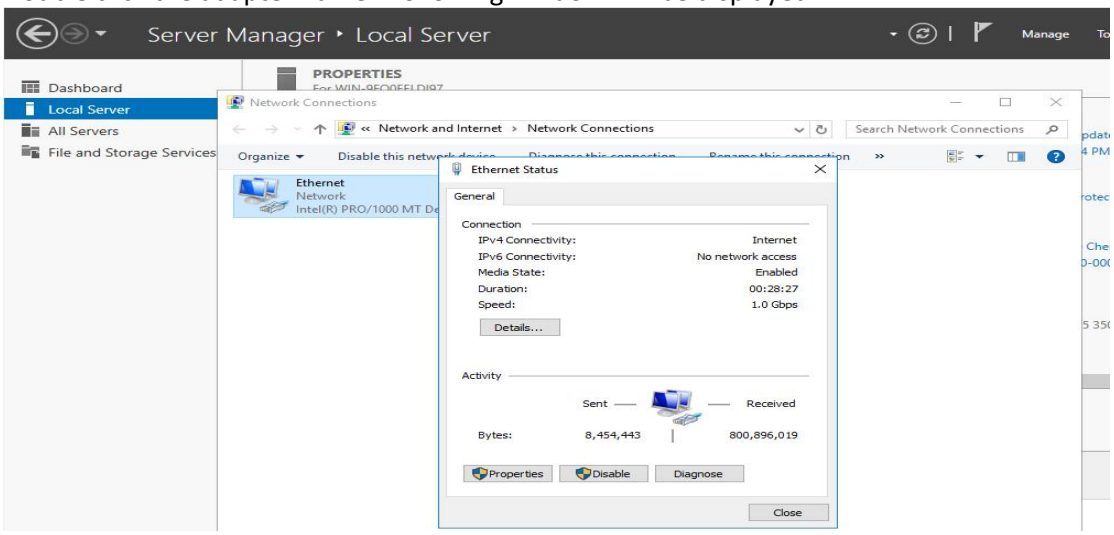


A new window showing the Ethernet adapter will open.

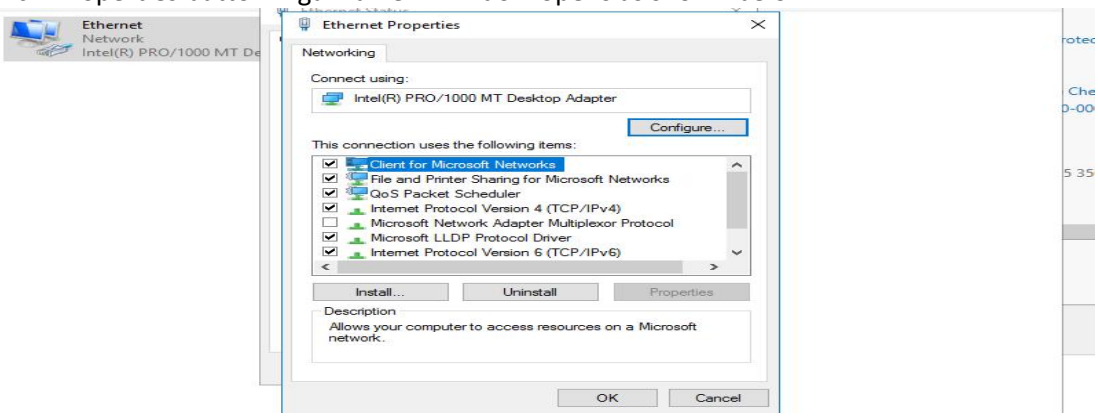


Created By:-
Sandeep Walvekar

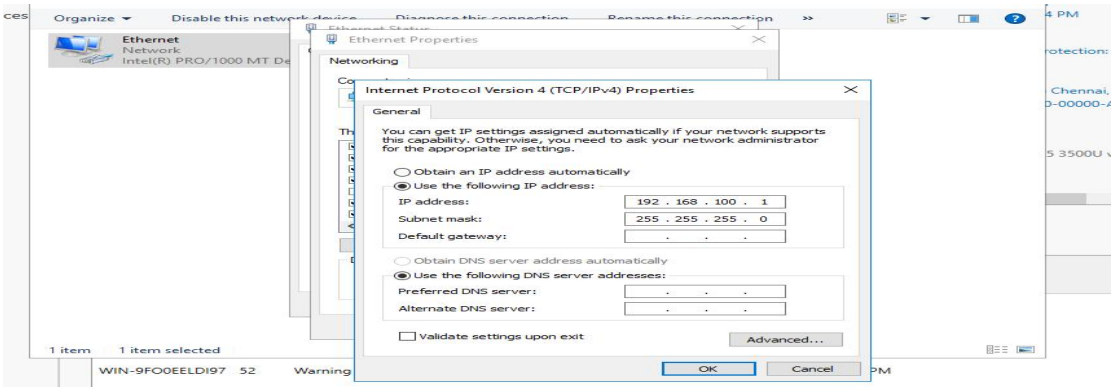
Double click the adapter name. Following window will be displayed.



Click Properties button. Again a new Window opens as shown below.



In that window double click the **Internet Protocol Version 4(TCP/IPv4)** option.
A new window is displayed. Select the Use the following IP address option. Then provide the required IP address and subnet mask.
For Lab purpose default gateway and DNS server configuration is not required. Click OK.



Then click OK on earlier windows and close all the windows opened. Do not close the Server Manager window.

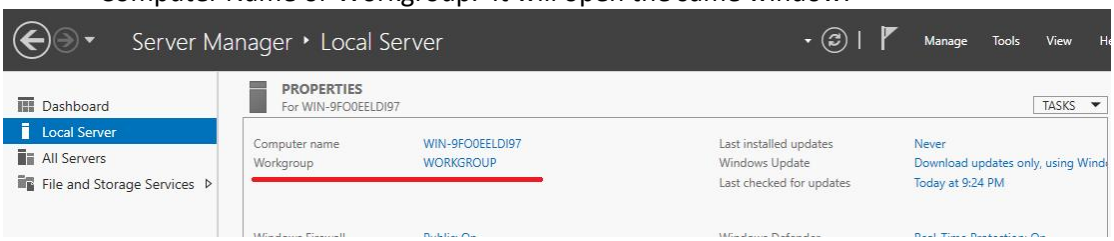
Again if the given IP address is not displayed in the Server Manager window, Click the refresh button.

Created By:-
Sandeep Walvekar

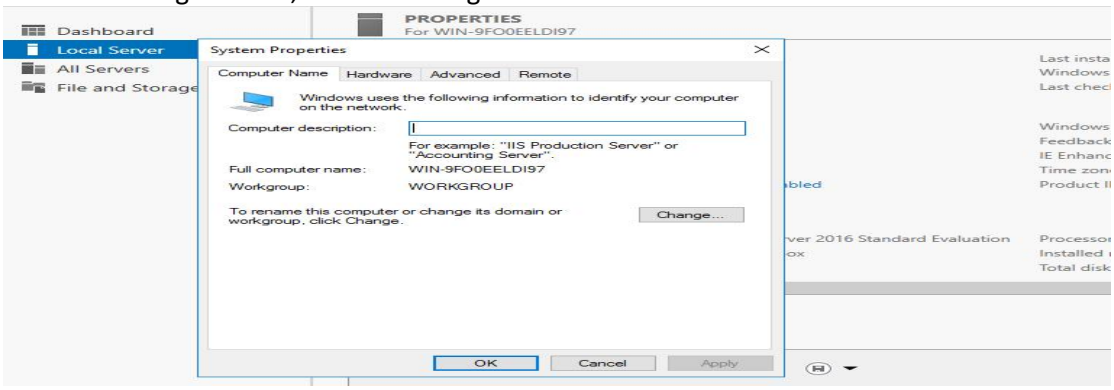
C. **Set a computer name for the server**.

After this step, you need to restart the server.

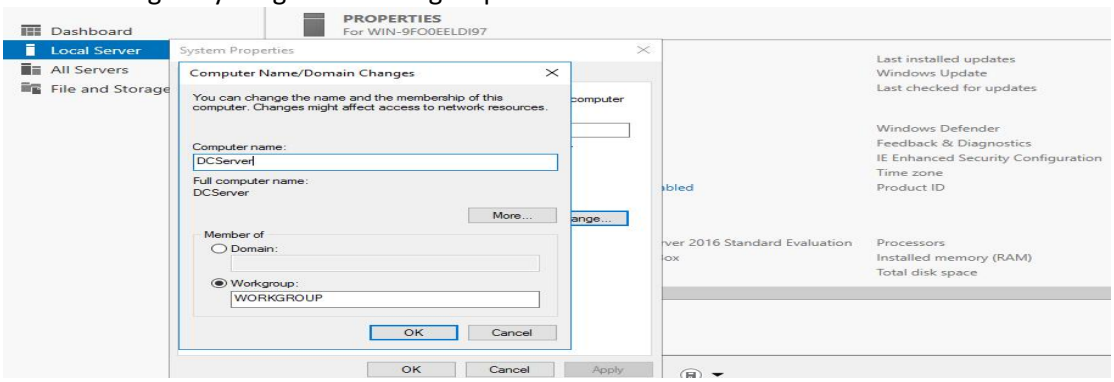
To assign a computer name to the server, in the Server Manager click any option - Computer Name or Workgroup. It will open the same window.



In the following window, click the change button.



This will open following window. In the Computer Name field specify a name for this server. Do not change anything in the workgroup field.



Click OK. It will display a restart warning. Click OK to close all earlier windows. The server restart option will be displayed. Click Restart Now and restart the server. This will bring the new computer name in effect.

Restart is necessary to successfully install Windows Active Directory.
After restart logon as Administrator and now you are ready to install your first forest and create your first Active Directory domain.

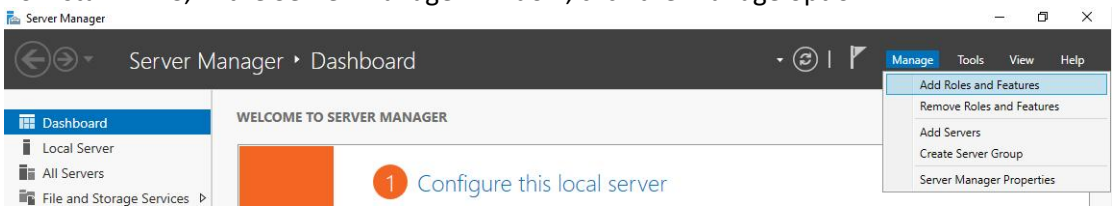
2. Install Active Directory Domain Services (ADDS)

A. Install Active Directory Domain Services (ADDS)

To create a new forest and a new domain, you need to first install the Windows Active Directory Domain Services (ADDS). This will copy all the files and create a directory structure required.
You do not require Windows Server installation media (CD/DVD/USB) for any of the steps.

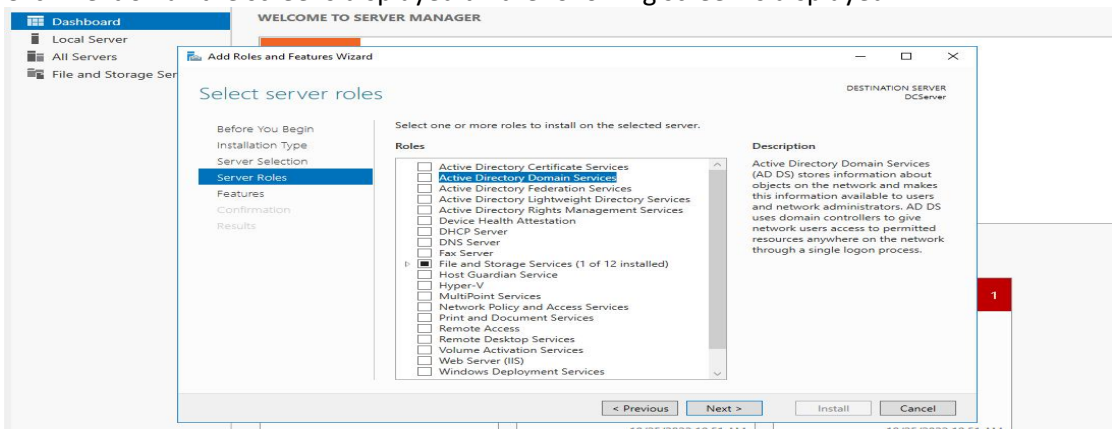
Created By:-
Sandeep Walvekar

To install ADDS, in the Server Manager window, click the Manage option.

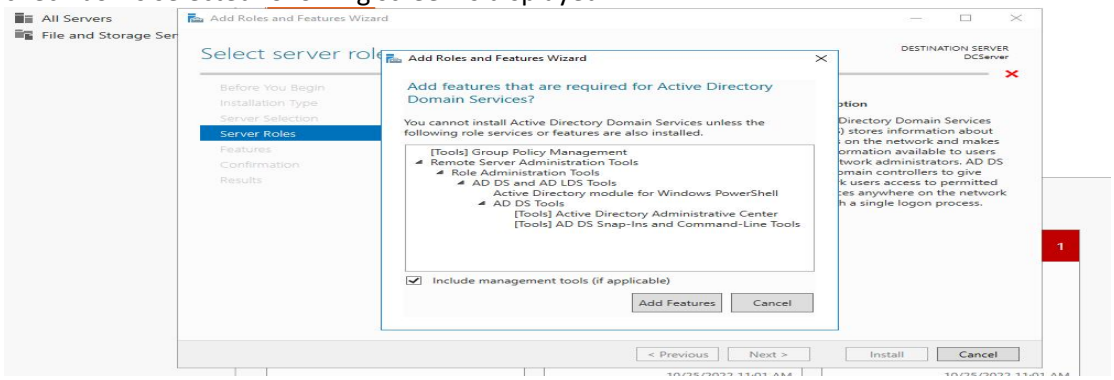


Then Click the **Add Roles and Features** option.

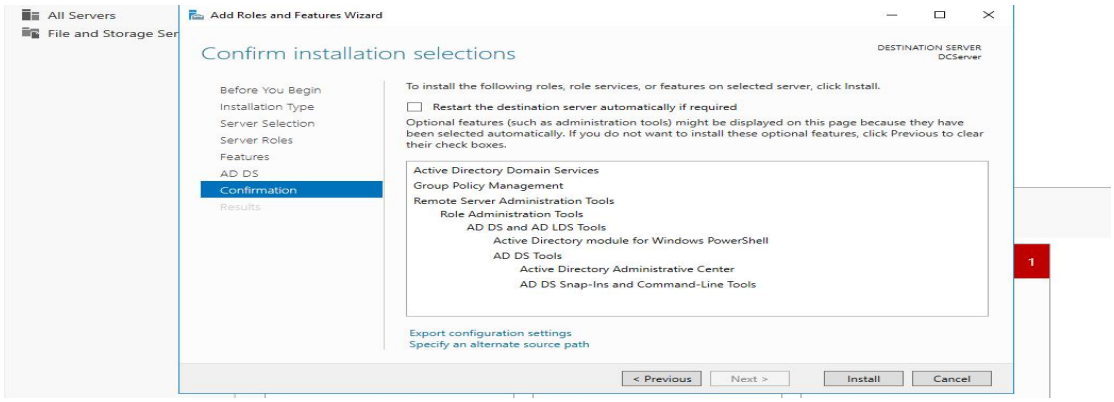
Click Next on all the screens displayed till the following screen is displayed.



In this screen, select the check box in front of **Active Directory Domain Services** role. As the check box is selected following screen is displayed.



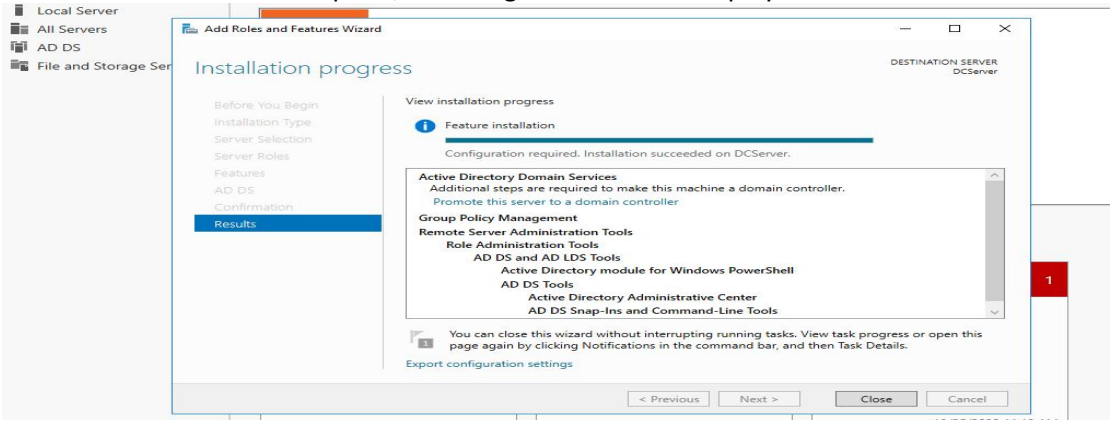
Click Add Features button.
Click Next on all screens till you get the following final screen.



Click Install button to start installing the ADDS role on the server.

Created By:-
Sandeep Walvekar

Once the installation is complete, following screen will be displayed.

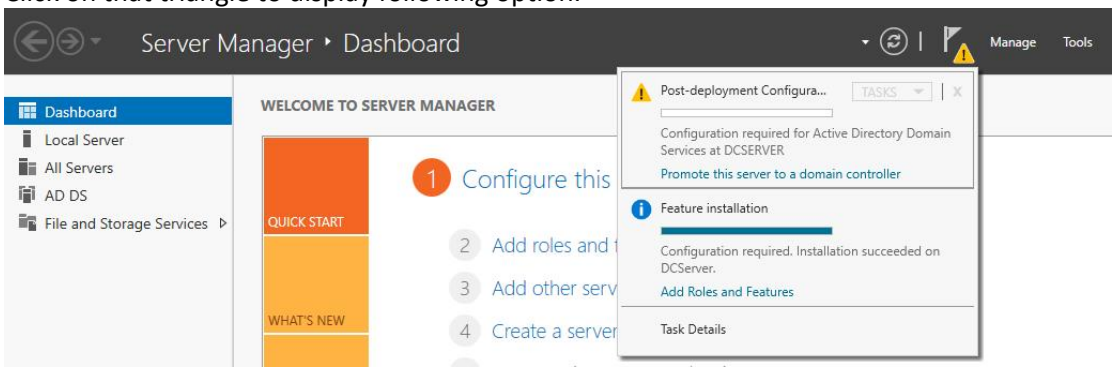


Make sure the installation succeeded without any errors. Click Close.

B. **Configure Windows Active Directory Domain Services (ADDS)**

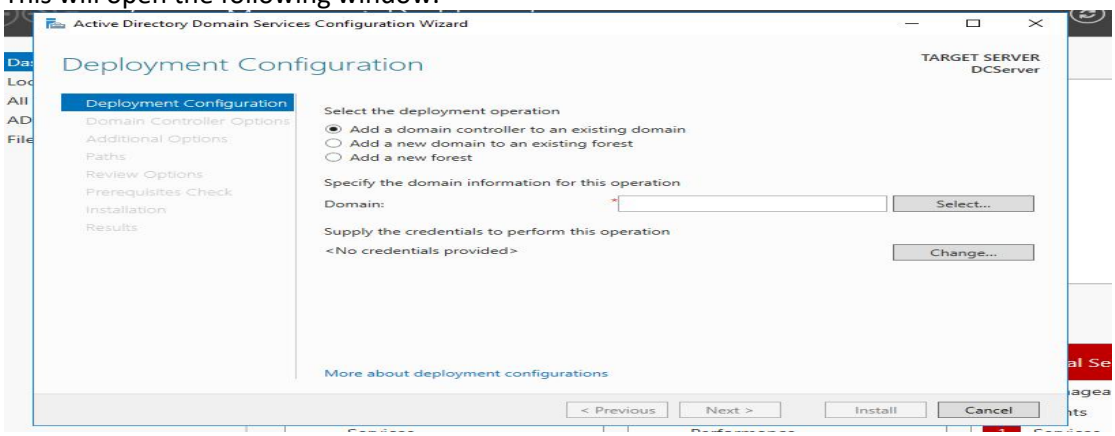
Once the ADDS service is successfully installed. The Server Manager window will display a yellow triangle near flag in right upper corner as shown below.

Click on that triangle to display following option.



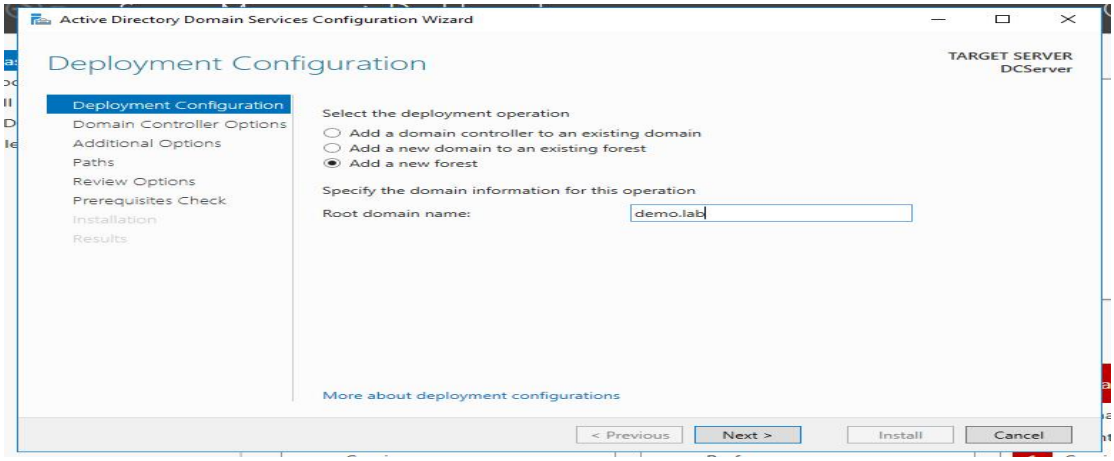
Click **Promote this server to a domain controller** option in the post-deployment configuration section.

This will open the following window.



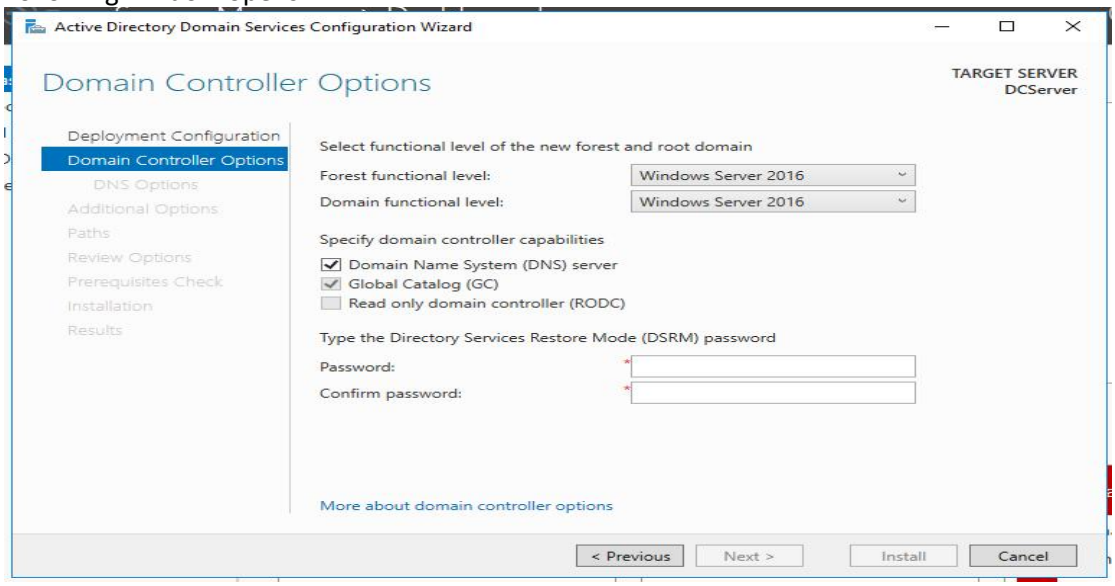
Select **Add a new forest** option and specify a Root domain name.

Created By:-
Sandeep Walvekar



This will create a new forest by the same name as provided for the Root domain. Thus a new forest and a new domain tree will be created.
Click Next.

Following window opens.



In this window you need to set the Forest Functional Level and Domain Functional Level.

The **Forest functional level** decides the Windows Server editions that can be added as domain controllers in the entire forest. If the forest functional level is set to Windows server 2016 then only Server 2016 and above server editions like 2019 and 2022 can be added as domain controllers. In other words if you want to add another domain in this forest, the server on which you install ADDS service, needs to have a Windows Server 2016/2019/2022 operating system installed. Earlier Server versions like 2012 R2 will not be allowed. An error will be displayed if you try to add this server.

The **Domain Functional level** depends on the Forest Functional Level. The Domain Functional level can be same or higher than Forest Functional level. However it can not be lower than forest functional level. The Domain functional level decides which Windows Serve editions can work as additional domain controllers within a domain.

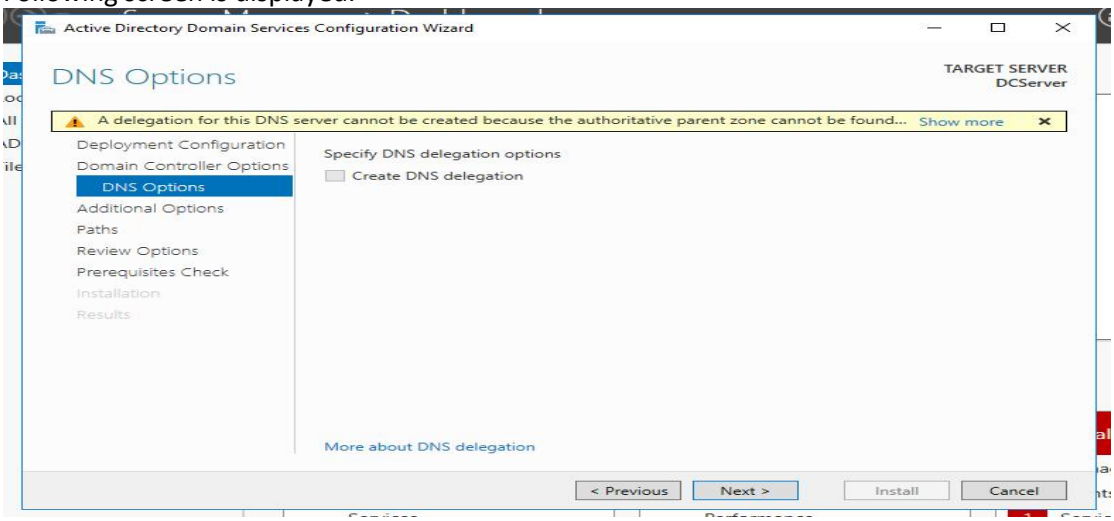
Here for this practical we keep both Forest Functional level and Domain Functional level to default. The default option displayed depends on the Windows Server OS installed on this server.

Created By:-
Sandeep Walvekar

Keep all other options as default.
Type a Directory Restore Mode Password (DSRM).
This password is required when the active directory fails. The password provided should be complex means it needs a capital letter, Special character and small characters. As we are installing active directory on this server its SAM database (the database that holds usernames and passwords) is disabled. All the usernames and their passwords will be stored in the active directory database. You always take backup of this database. Thus when this database fails no username and password is available for logon. Thus this DSRM password will allow you to logon to server and restore your active directory database from backup.

The server can be started into a DSRM mode by pressing F8 button when the server starts.

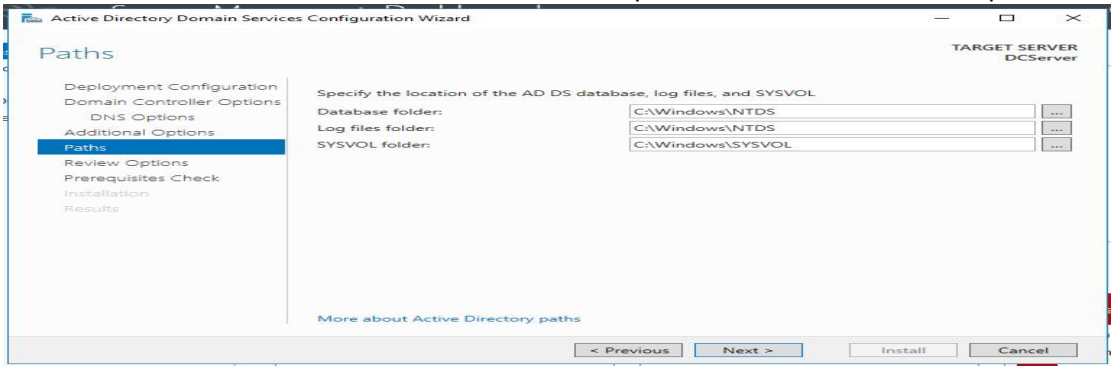
Thus keep all settings as default. Provide DSRM password. Click Next.
Following screen is displayed.



Windows active directory requires a working DNS server. However we do not have any DNS sever installed. Thus above warning screen is displayed. **Click Next**.

The following screen checks the NetBIOS domain name of the given domain name. It varifies that the domain name is not in use. The NetBIOS protocol does not support Internet naming style like demo.labs. Thus it removes the anything after . and keeps the starting name as the NetBIOS domain name. This is for the backward compatibility with older operating systems like Windows NT etc. **Click Next**.

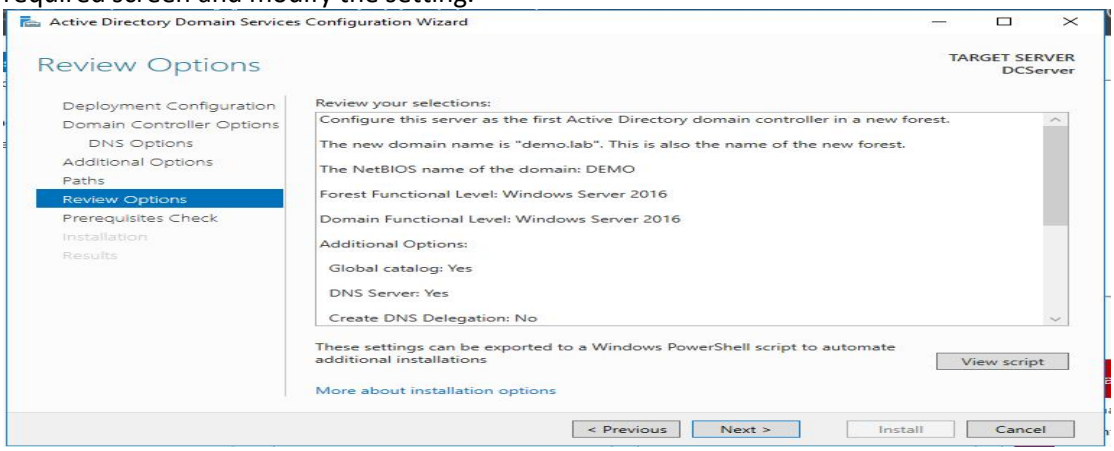
The next screen displays the directory paths where the active directory database and active directory logs will be stored. The **sysvol** folder is used to replicate data to other domain controllers and domain clients. This folder should be placed on an NTFS formatted partition.



Keep all defaults on this screen and click Next.

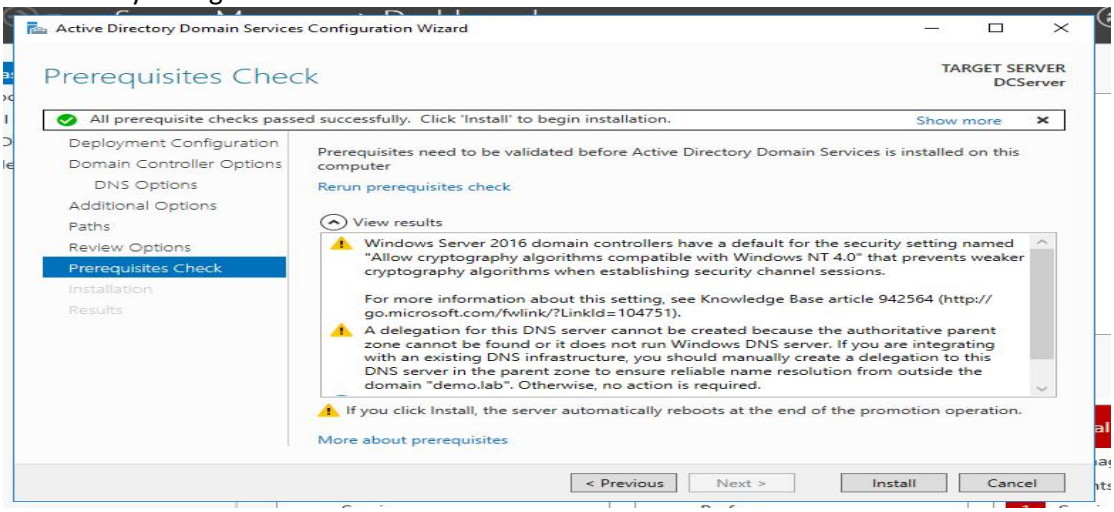
Created By:-
Sandeep Walvekar

The review screen displays all the earlier settings done. Please verify the options selected on all earlier screens. If you have selected a wrong option you can click back button to go to the required screen and modify the setting.



To finally configure the ADDS as per the settings , click Next.

The installer will verify that all the required prerequisites are met and the ADDS can be successfully configured on this server.



If there is any red coloured warning message, the Install button will be disabled. In such case read the error carefully and solve the problem.
Any warning with yellow signs can be neglected and will not create any problems for ADDS configuration.
Click Install.

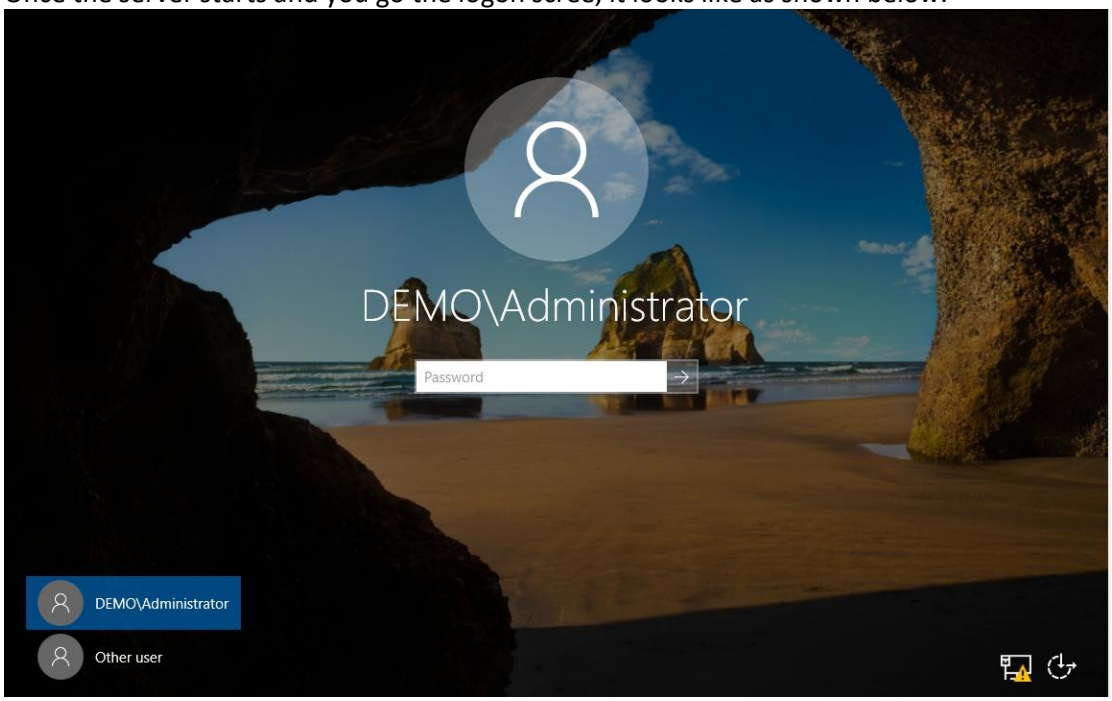
This will start configuring ADDS service. Once it finishes, following message will be displayed.

Just wait and server will automatically restart.

Created By:-
Sandeep Walvekar

It will require some time for the server to start.

Once the server starts and you go the logon scree, it looks like as shown below.



Now the Logon name is displayed as **domain-name/Administrator**.
Provide earlier administrator password to logon.
Now in the Server Manager window that opens, click Local Server option. In the workgroup option it will display your domain name.

This is how you have successfully installed the ADDS role on this server. You configured ADDS on this sever to create a new forest and a new domain. This server is now domain controller for the domain demo.lab.

Created By:-
Sandeep Walvekar