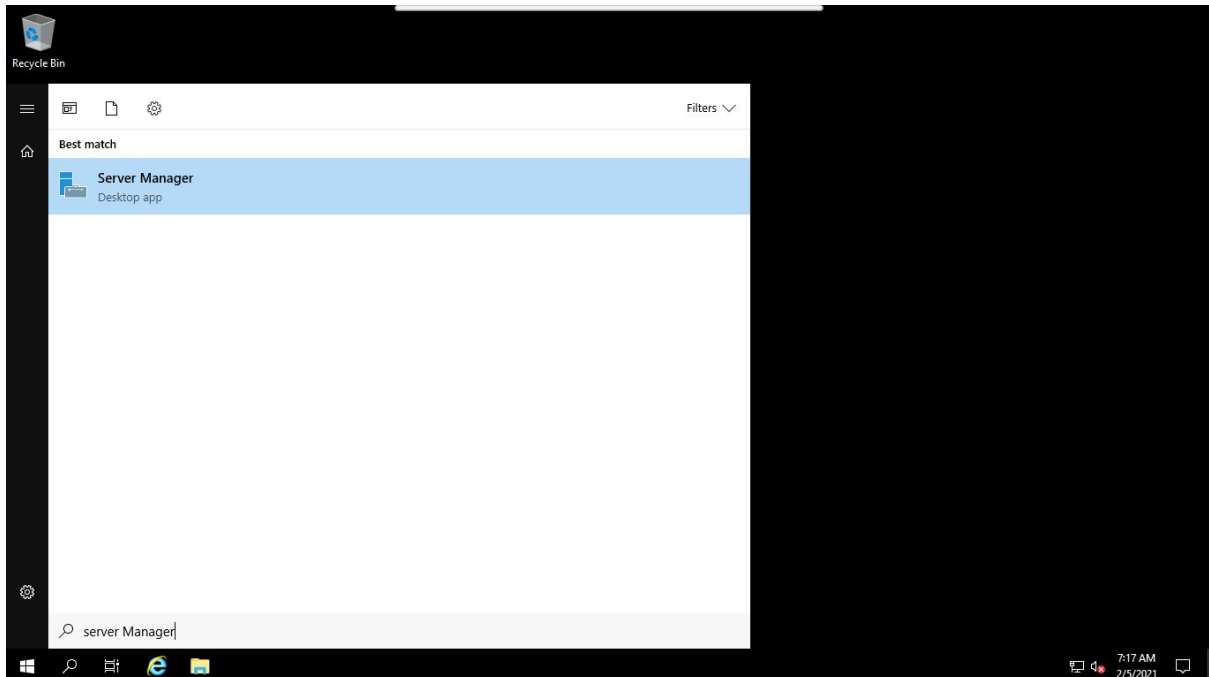
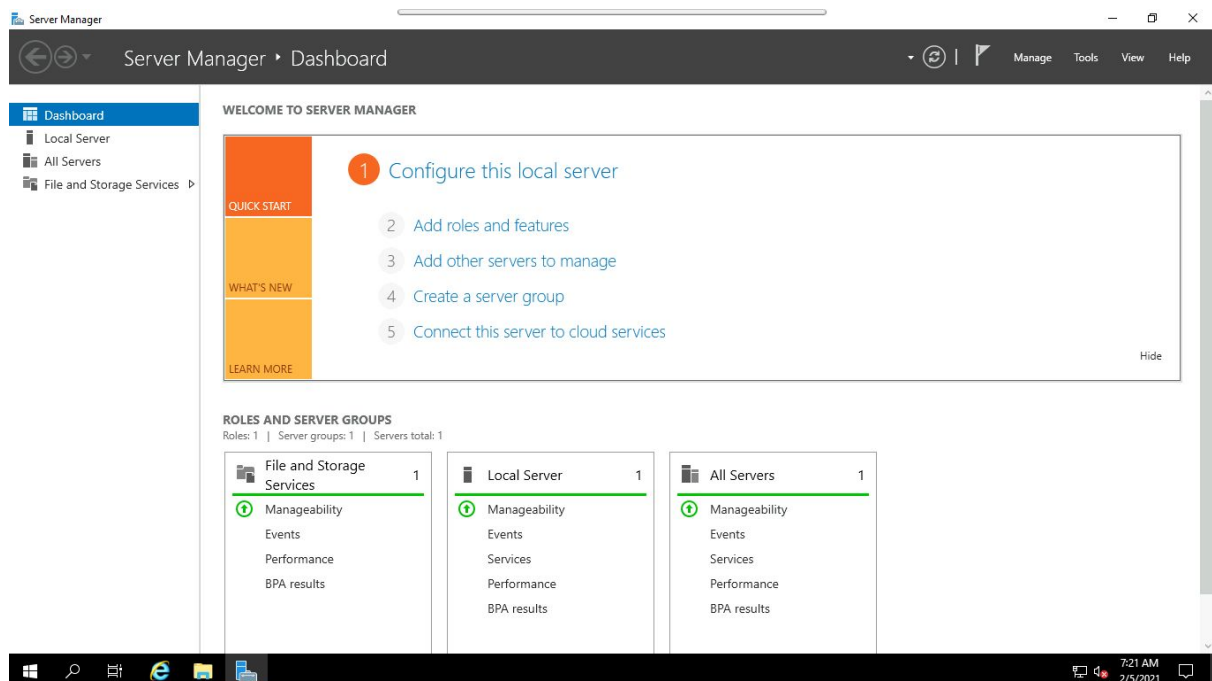


Step-1 Open Server Manager

Click on **Start** and type **Server Manager** to search for the application.



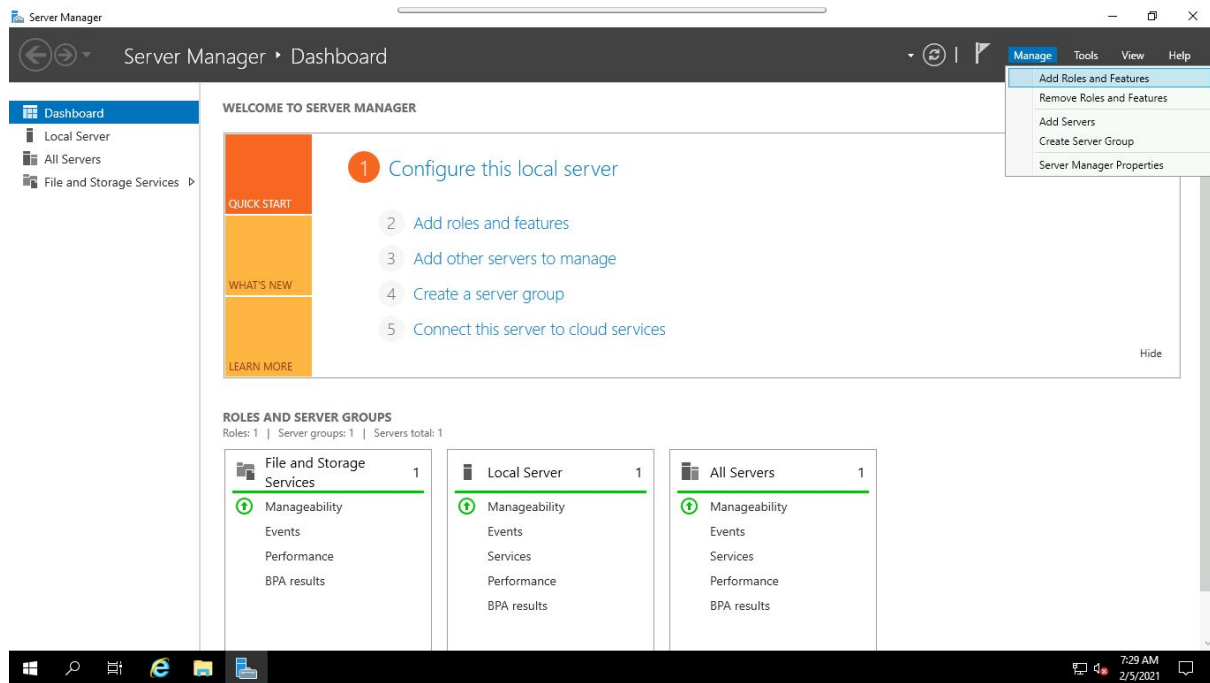
Once it is open as illustrated by the figure below,



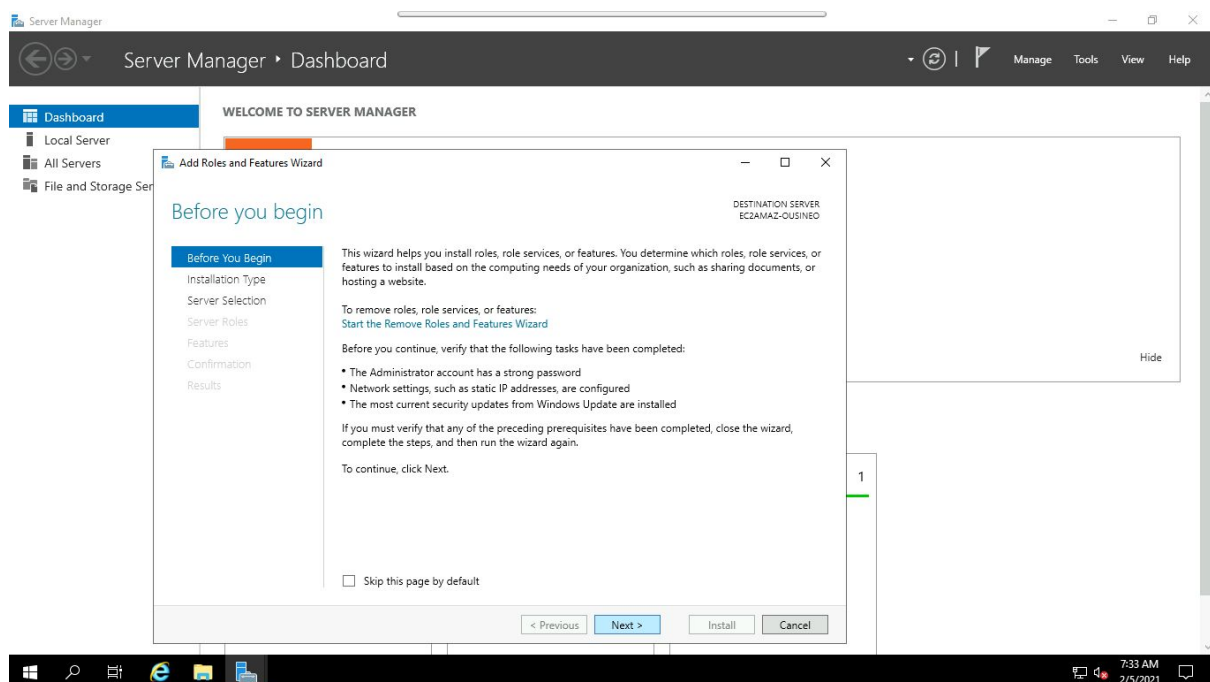
Let us now proceed on the next step for installing Active Directory Domain Services.

Step-2 Add Roles and Features

Click on Manage on the **Server Manager** window and choose **Add Roles and Features**. This will open the **Add Roles and Features Wizard**, which lands you to the part where you will install **Active Directory Domain Services**.

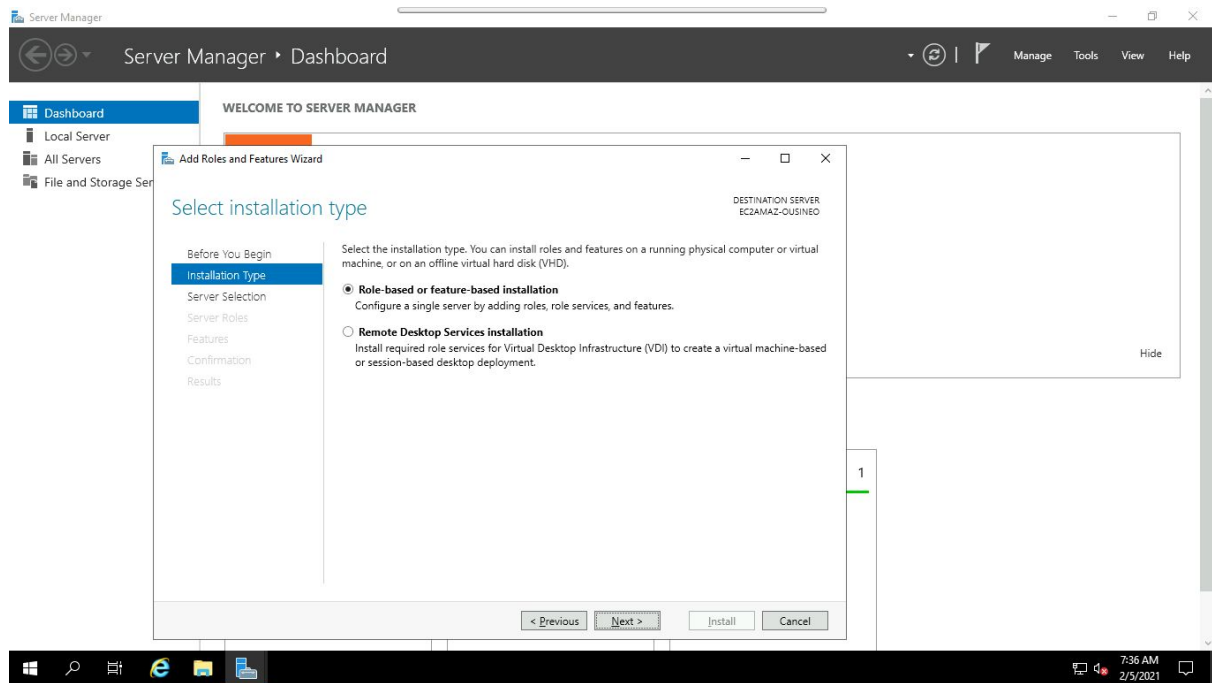


Click on Next



Step-3 Installation Type

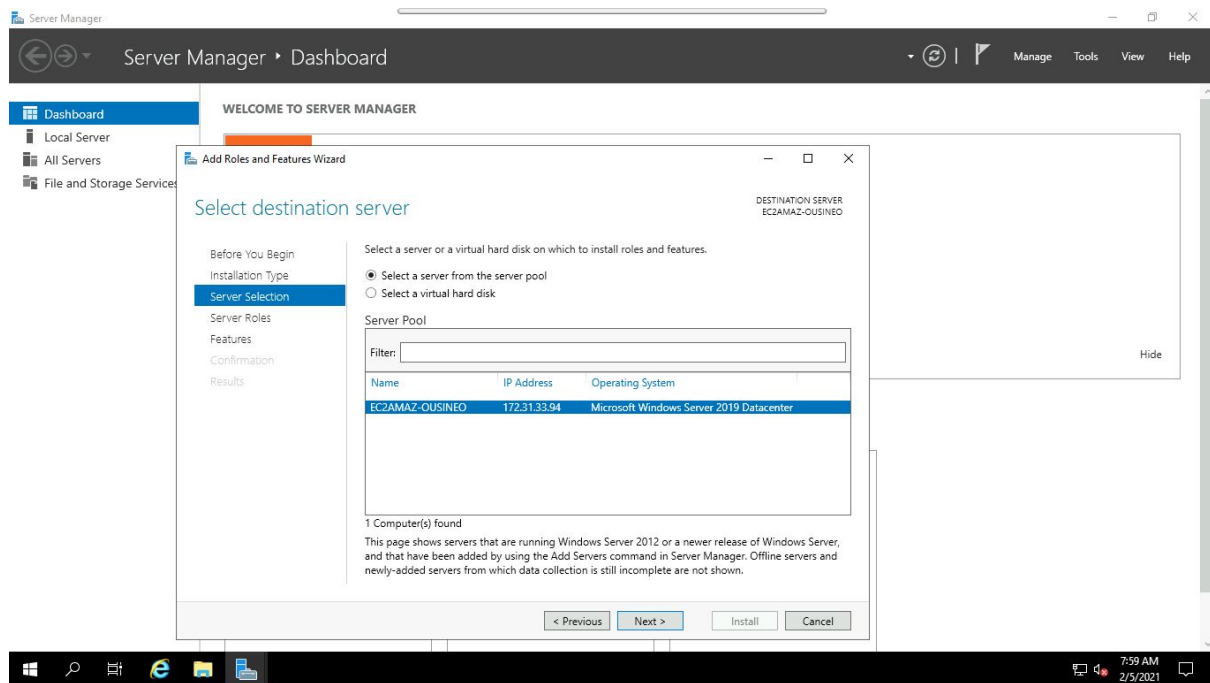
Into the **Installation Type** leave **Role-based or feature-based installation** radio button selected by default and click on **next**



Step-4 Server Selection

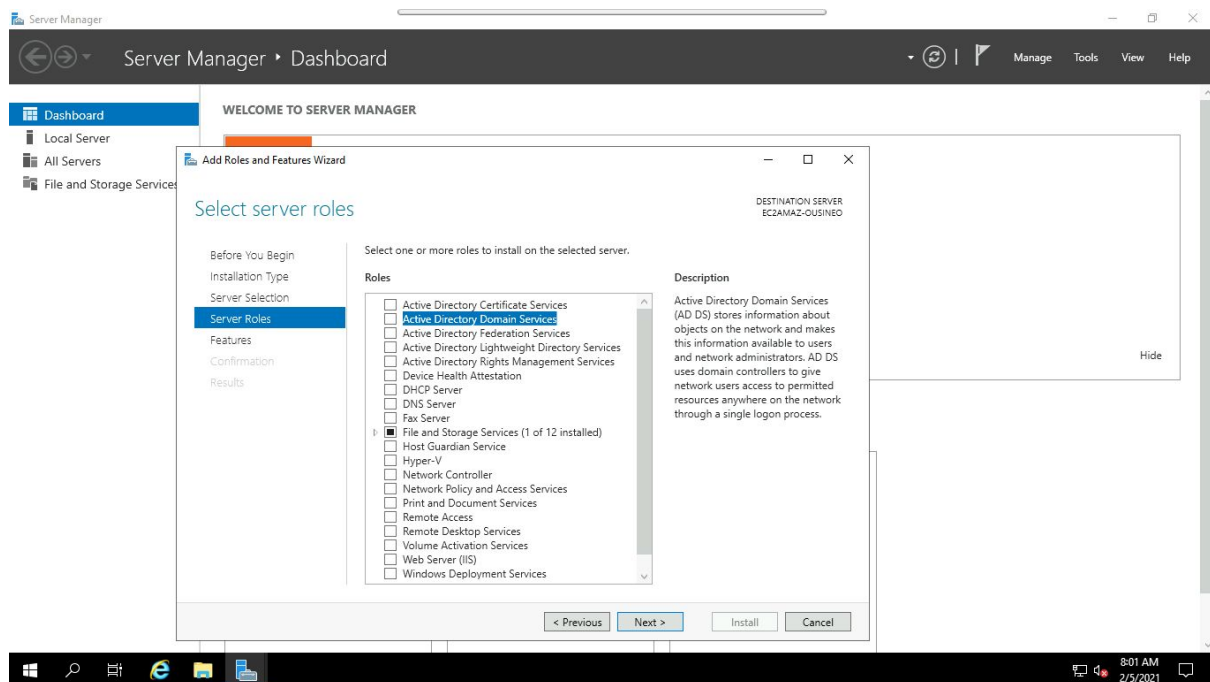
In this stage which is named **Select destination server** select the server that you need to install **Active Directory Domain Servers** and click **next**.

Here I'm proceeding with my **local server**.



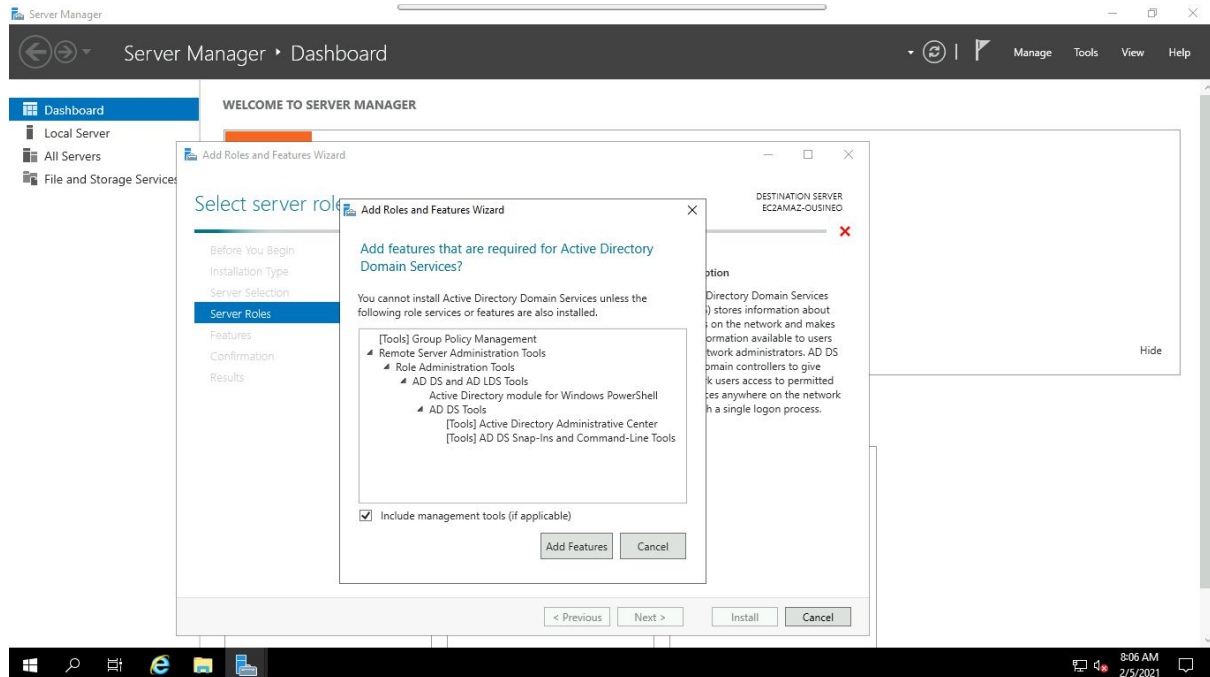
Step-5 Server Roles

Here you have many options, but you need to choose **Active Directory Domain Services** which are un-checked by default.



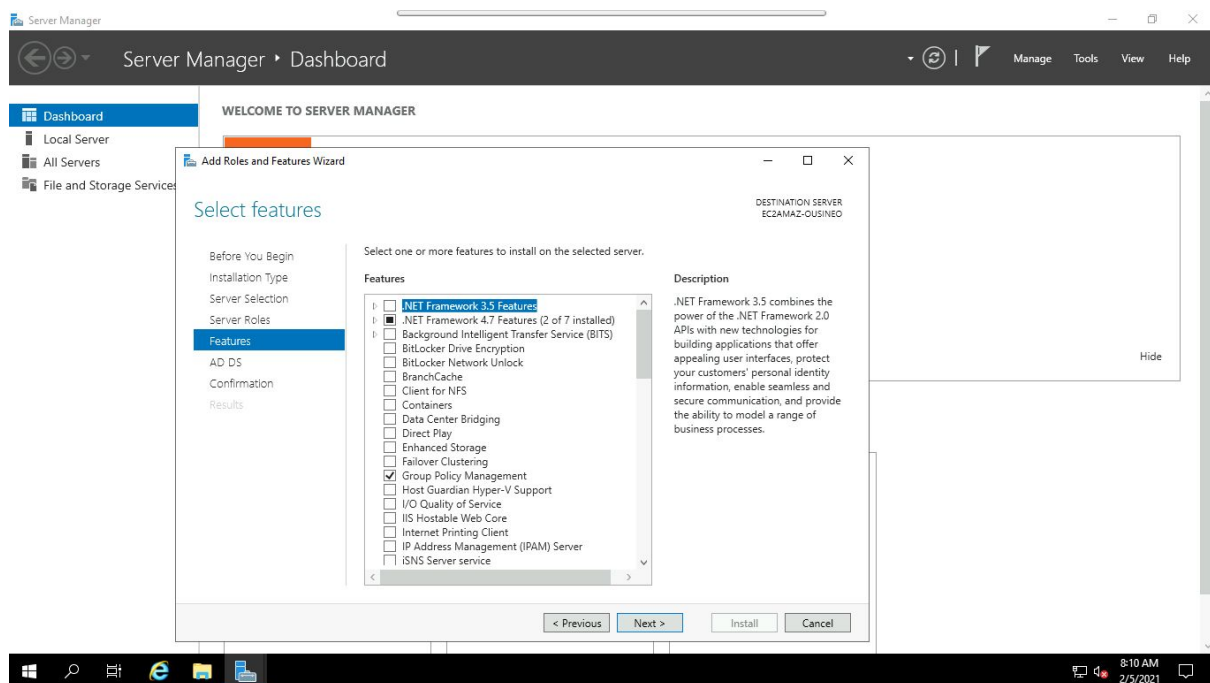
Step-6 Add Features for Server Roles

When you checked on **Active Directory Domain Servers** immediately a new part came up. On this just click on **Add Features** button and hit **Next**



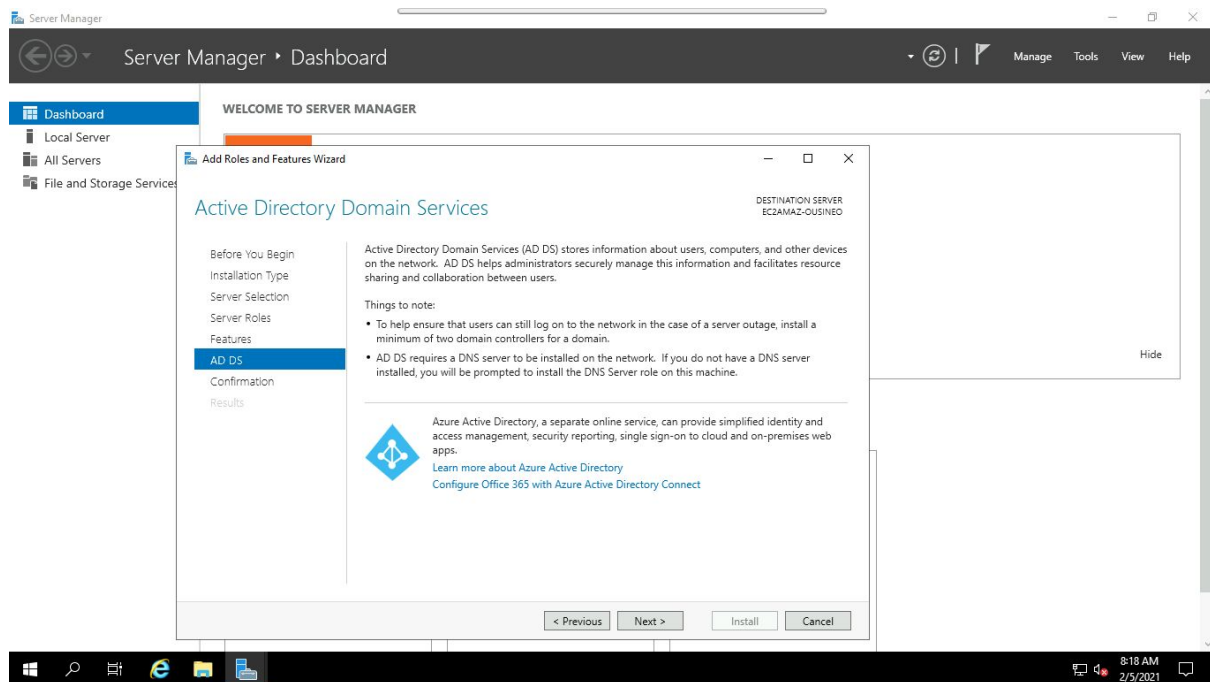
Step-7 Select Features

After **Add Features for Server Roles** you will be on the **Select Features** page and just hit **Next** to lead you to installations of **AD DS**.



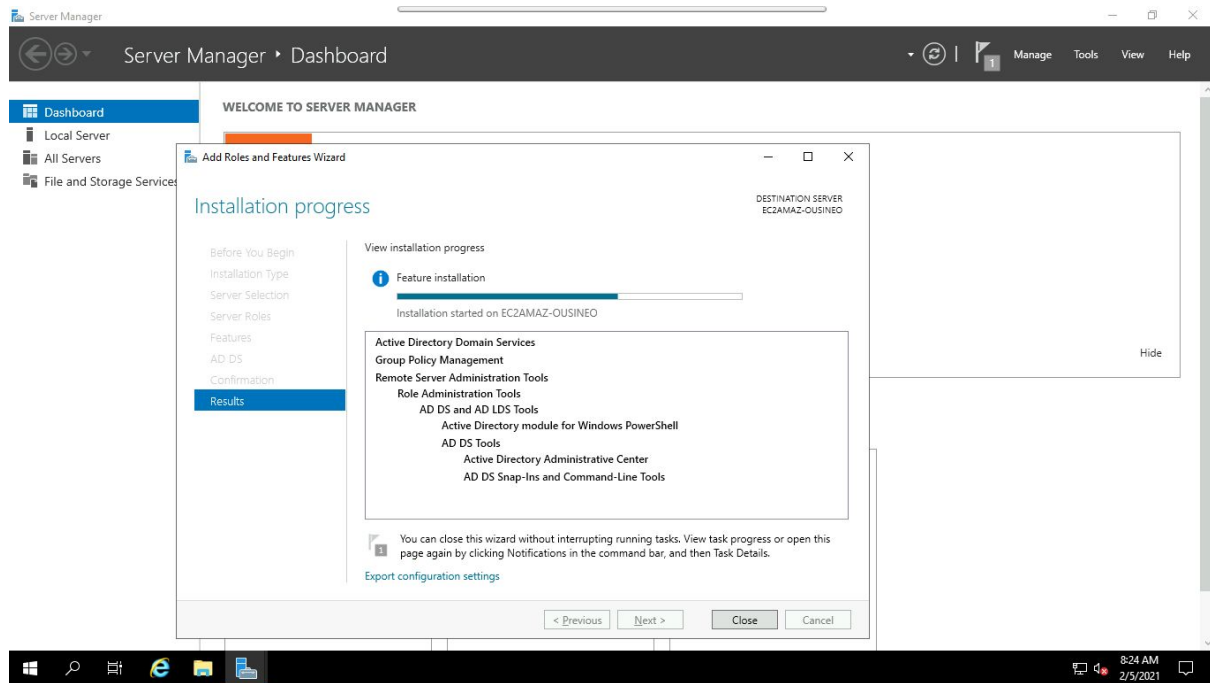
Step-8 Active Directory Domain Servers

As shown below, you will be landed on the next page which is named **Active Directory Domain Services**. Here click on **Next**.



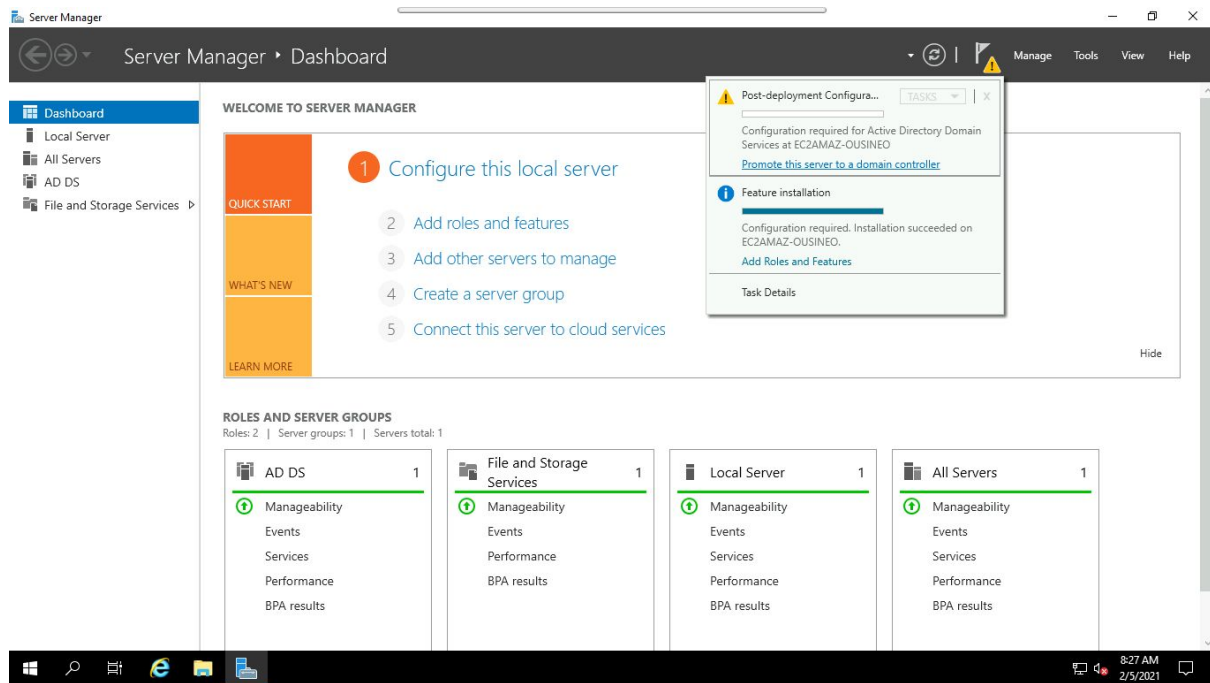
Step-9 Confirmation

The next page is just about the confirmation of what you need to install before actually installing them. If you are sure about what you have chosen then only click on **Install**. Here you can optionally choose the option that restarts the server whenever required.



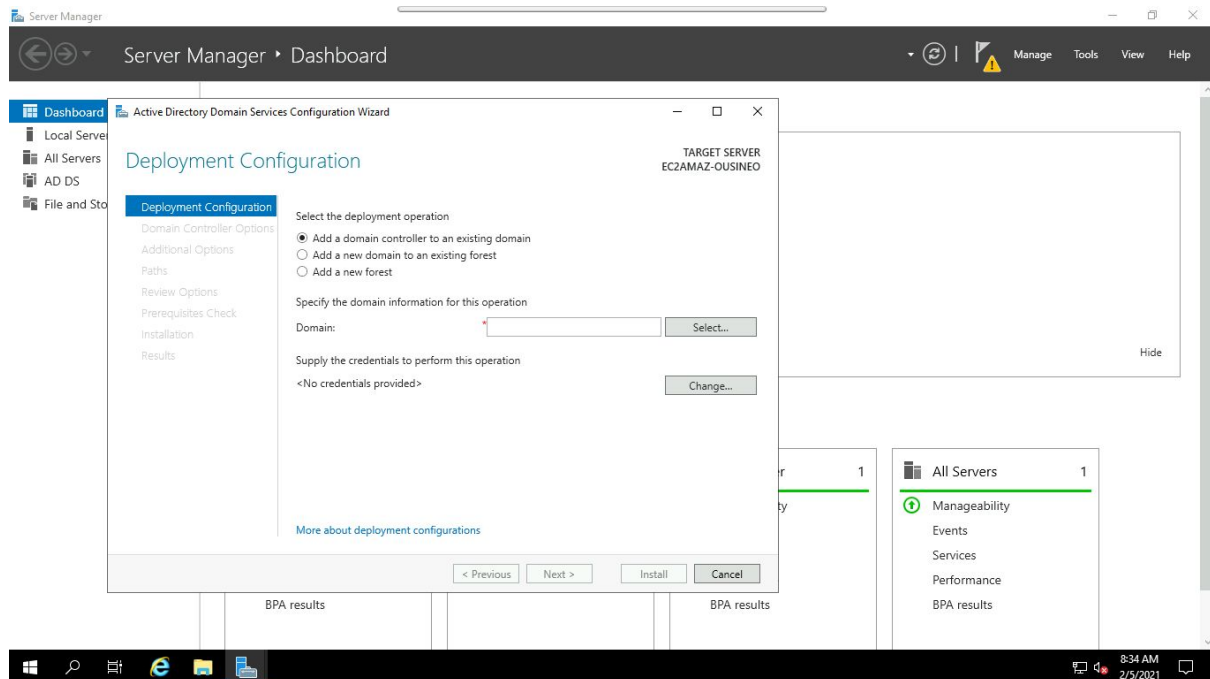
Step-10 Promote to Domain Controller

After you have finished installing **Active Directory Domain Services**, the last step is to **Promote it to a Domain Controller**. Go over to Server Manager where you notice a flag with yellow exclamation mark beside the **Manage** tab and click on it and choose **Promote this server to a Domain controller**.

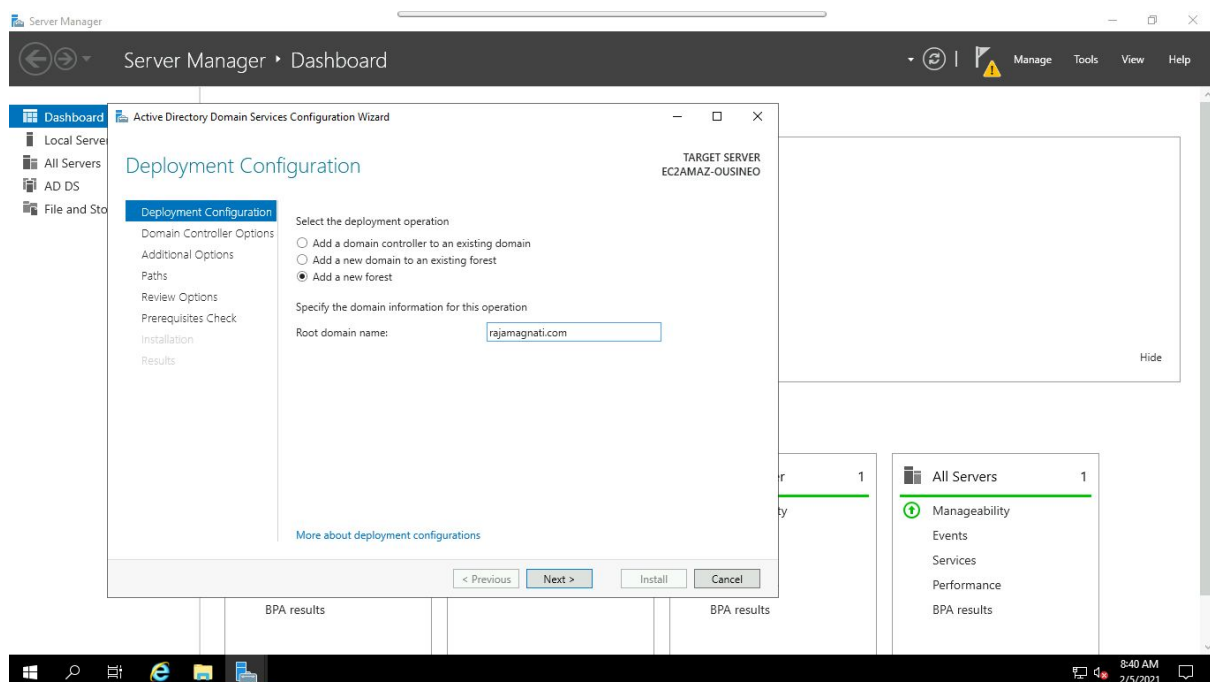


Step-11 Add a new Forest

After clicking on **Promote this server to a Domain controller** a new window titled **Active Directory Domain Services Configuration Wizard** as shown below. By default it checked on **Add a domain controller to an existing domain**.

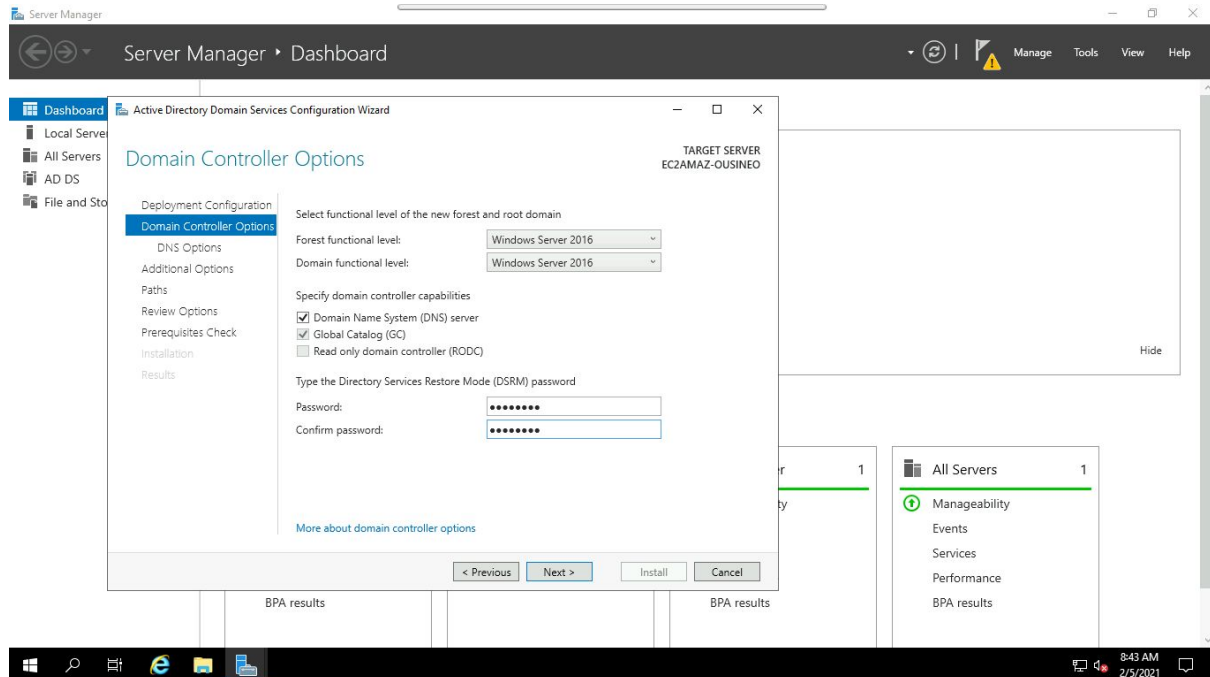


But we are going to change it to **Add a new Forest** and add your organization's root domain name. Click on **Next** after picking the choice.



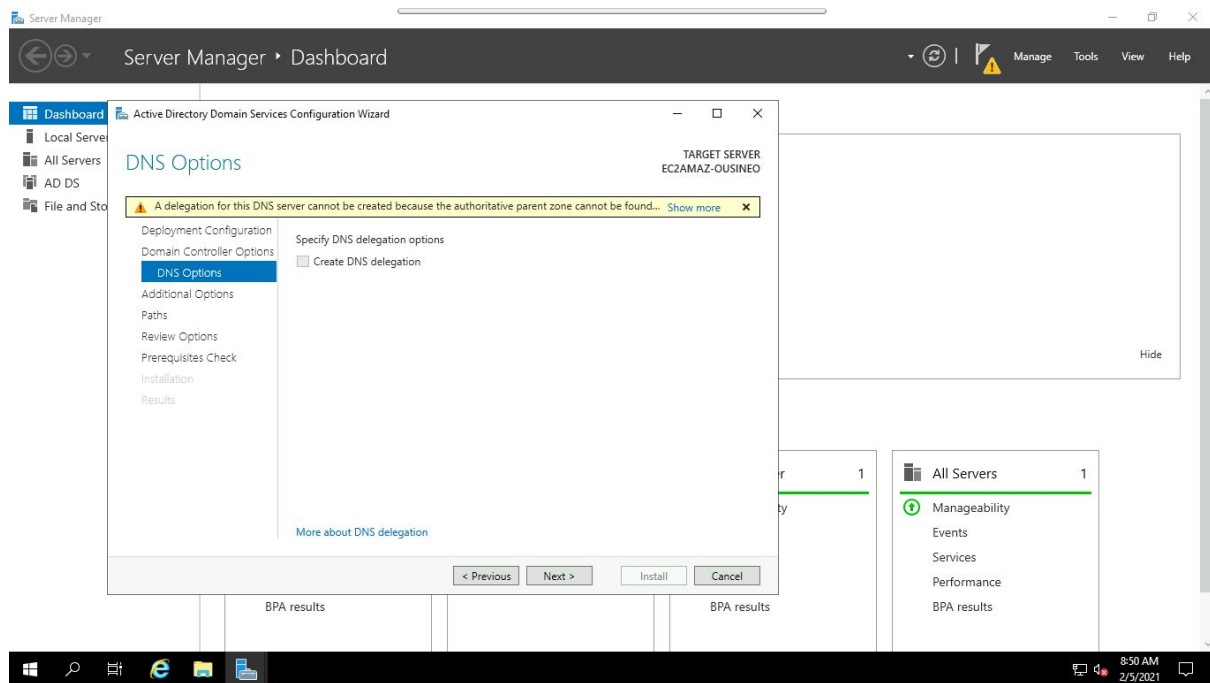
Step-12 Domain Controller Options

In this step leave the check boxes as default and input your desired password and then click **Next**.



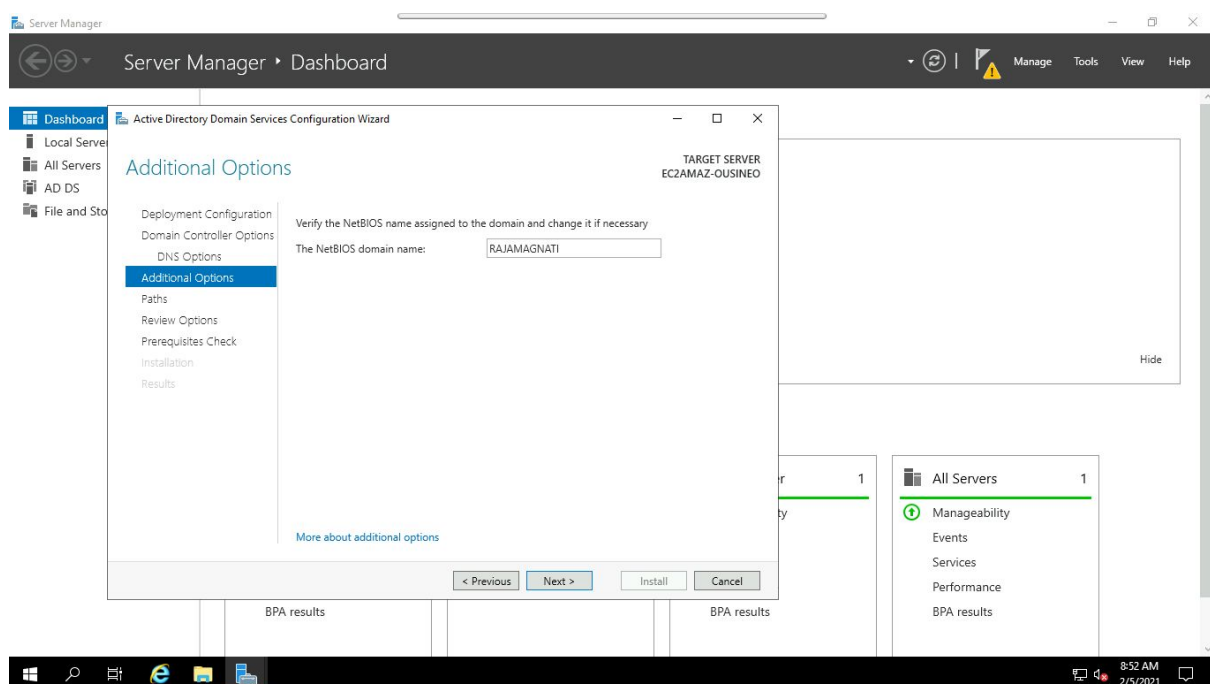
Step-13 DNS Options

On the next page of DNS Options you will probably see an error on the top with the words **“A delegation for this DNS server cannot be created because the authoritative parent zone name server cannot be found”**. Ignore it and click on **Next**.



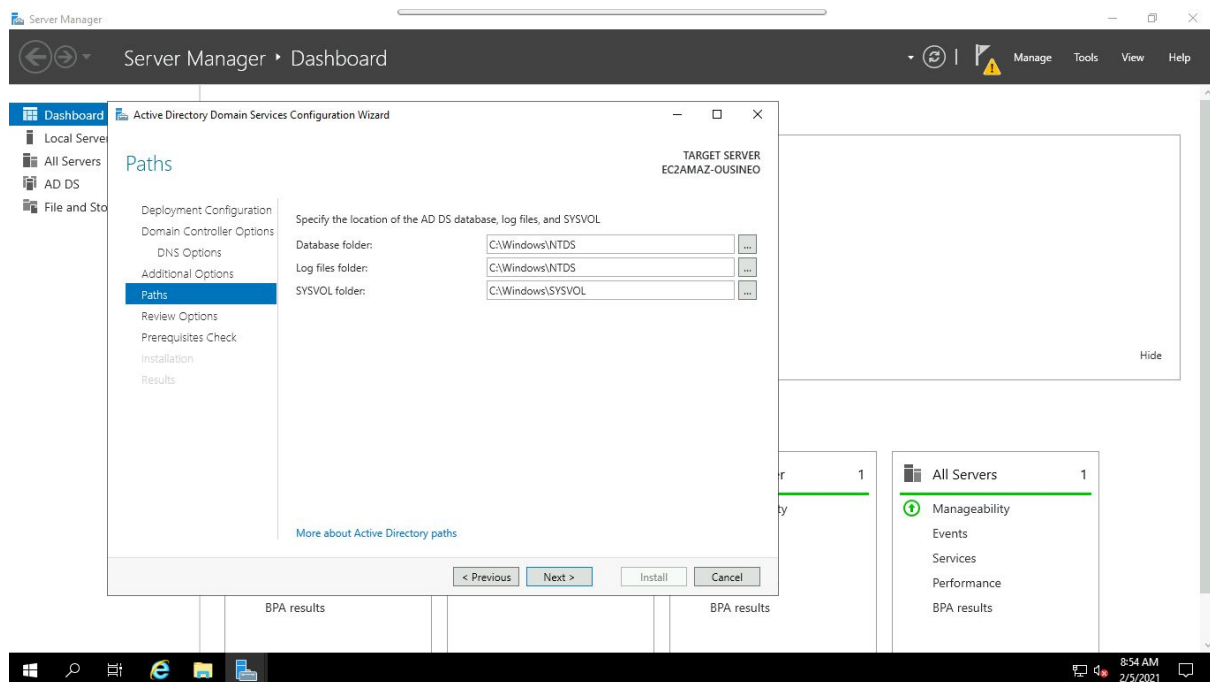
Step-14 NetBIOS domain name

Here leave the **NetBIOS domain name** as default or you can change but not longer than 15 characters. Click **Next**.



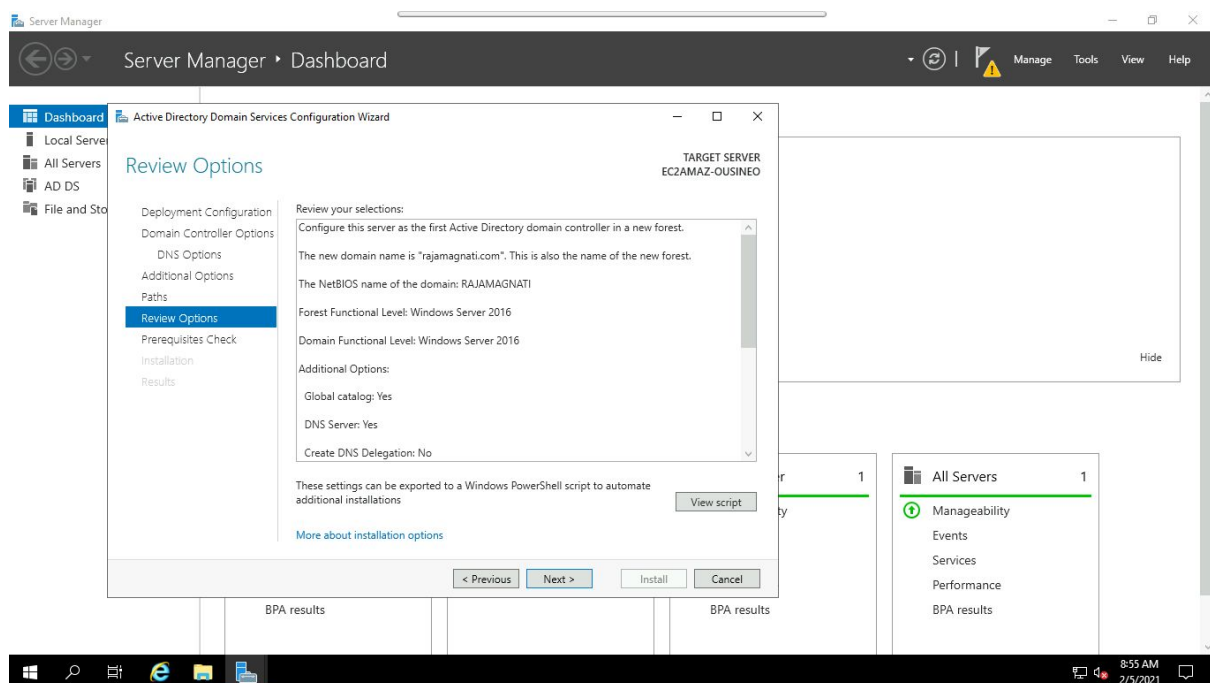
Step-15 Paths

Leave everything as default and click **Next**.



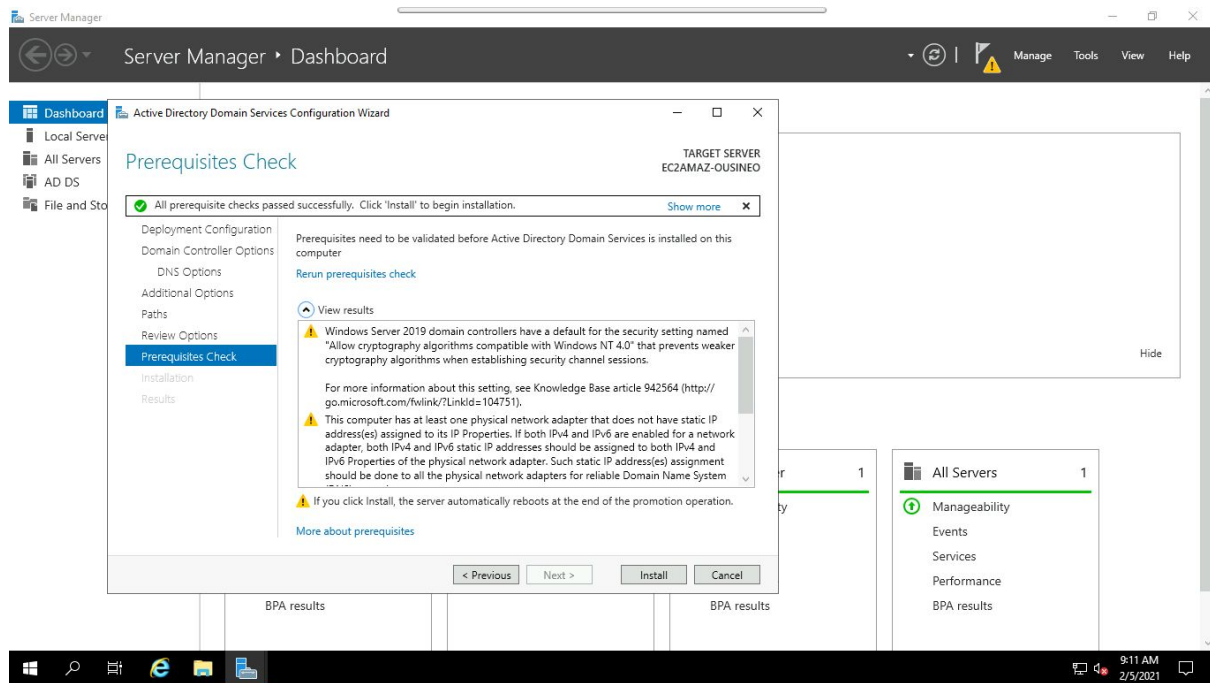
Step-16 Review Selections

In this step the server allows us to review what you have done so far. If we are good at the selections we have done. Hit **Next**.



Step-17 Prerequisites Check

In this step prerequisites will be validated before Active Directory Domain Services is installed. If you get any errors here, please take a look at it and fix anything from the previous steps. If all okay then click **Install**.



After this server will reboot and you can then log into the Domain with the credentials you set in **step-12**

Step-18 Check if the AD DS port is open or not

Execute command **netstat** on cmd

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1697]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netstat

Active Connections

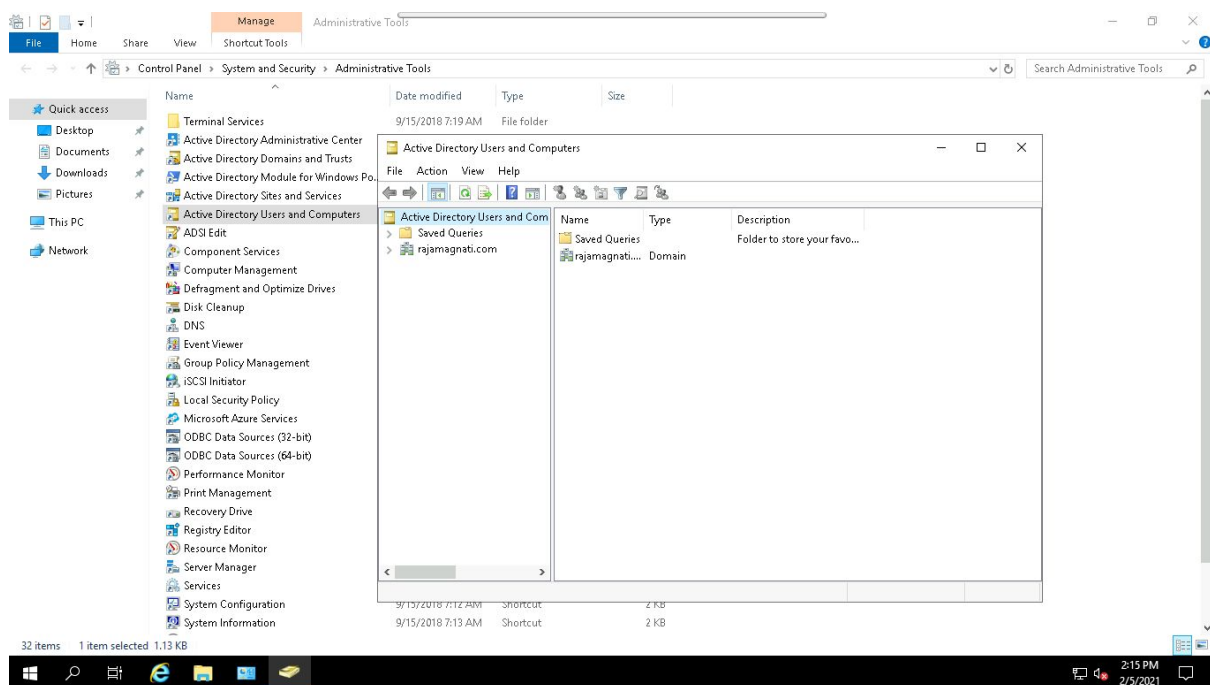
Proto Local Address           Foreign Address         State
TCP    172.31.33.94:3389       112.79.119.104:34286    ESTABLISHED
TCP    172.31.33.94:49726     instance-data:http     TIME_WAIT
TCP    172.31.33.94:49752     13.67.34.108:https     ESTABLISHED
TCP    [::]:389               EC2AMAZ-OUSINEO:49679  ESTABLISHED
TCP    [::]:389               EC2AMAZ-OUSINEO:49680  ESTABLISHED
TCP    [::]:389               EC2AMAZ-OUSINEO:49684  ESTABLISHED
TCP    [::]:389               EC2AMAZ-OUSINEO:49693  ESTABLISHED
TCP    [::]:3268              EC2AMAZ-OUSINEO:49701  ESTABLISHED
TCP    [::]:49689             EC2AMAZ-OUSINEO:ldap   ESTABLISHED
TCP    [::]:49688             EC2AMAZ-OUSINEO:ldap   ESTABLISHED
TCP    [::]:49684             EC2AMAZ-OUSINEO:ldap   ESTABLISHED
TCP    [::]:49693             EC2AMAZ-OUSINEO:ldap   ESTABLISHED
TCP    [::]:49701             EC2AMAZ-OUSINEO:msft-gc ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:389 EC2AMAZ-OUSINEO:49685  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:389 EC2AMAZ-OUSINEO:49696  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:389 EC2AMAZ-OUSINEO:49707  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49687 EC2AMAZ-OUSINEO:49703  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49667 EC2AMAZ-OUSINEO:49710  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49667 EC2AMAZ-OUSINEO:49736  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49667 EC2AMAZ-OUSINEO:49738  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49685 EC2AMAZ-OUSINEO:ldap   ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49696 EC2AMAZ-OUSINEO:ldap   ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49703 EC2AMAZ-OUSINEO:49667  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49707 EC2AMAZ-OUSINEO:ldap   ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49710 EC2AMAZ-OUSINEO:49667  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49732 EC2AMAZ-OUSINEO:epmap  TIME_WAIT
TCP    [fe80::49b3:674e:7b21:7c10%4]:49735 EC2AMAZ-OUSINEO:epmap  TIME_WAIT
TCP    [fe80::49b3:674e:7b21:7c10%4]:49736 EC2AMAZ-OUSINEO:49667  ESTABLISHED
TCP    [fe80::49b3:674e:7b21:7c10%4]:49737 EC2AMAZ-OUSINEO:epmap  TIME_WAIT
TCP    [fe80::49b3:674e:7b21:7c10%4]:49738 EC2AMAZ-OUSINEO:49667  ESTABLISHED

C:\Users\Administrator>
```

Step-19 Ensuring Domain exist or not

Follow **Control Panel\System and Security\Administrative Tools** and hit on **Active Directory Users and Computers**

Here our domain existing named **rajamagnati.com**

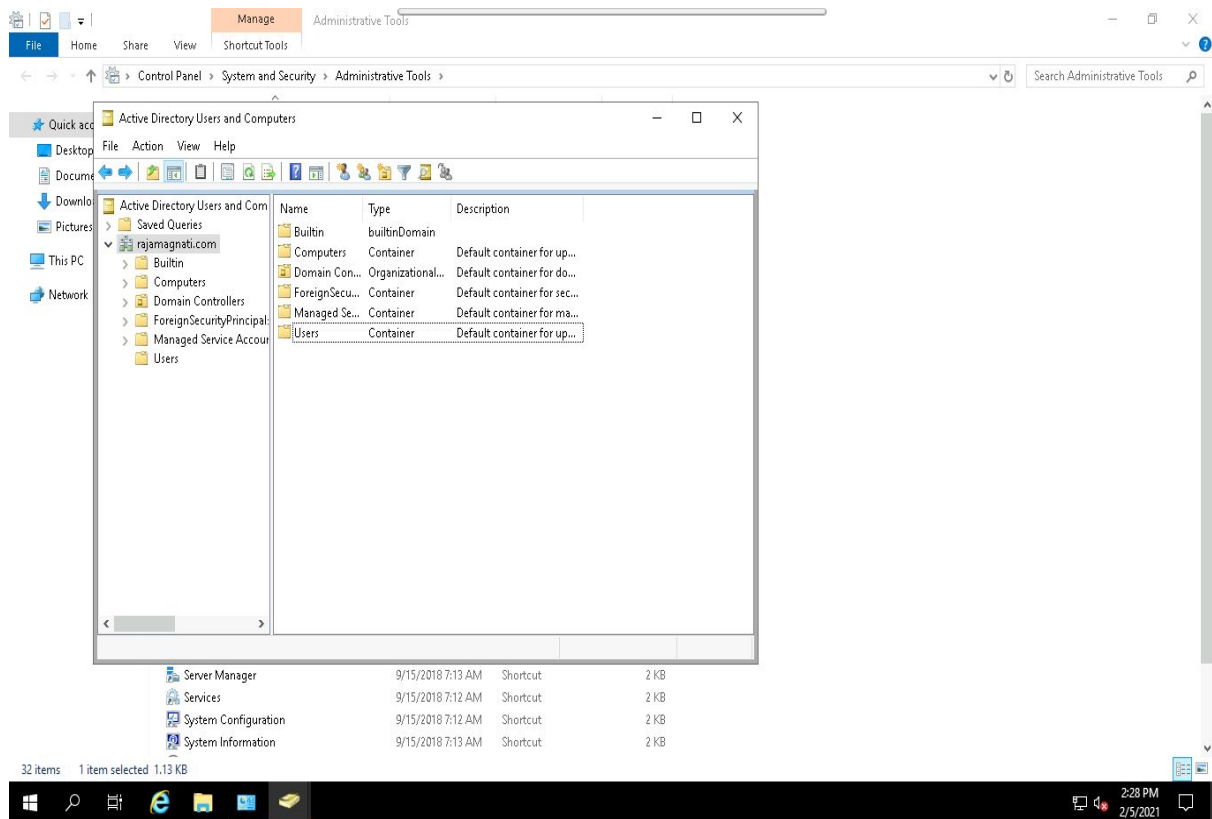


Step-20 Check list of Directories available

In domain **rajamagnati.com**

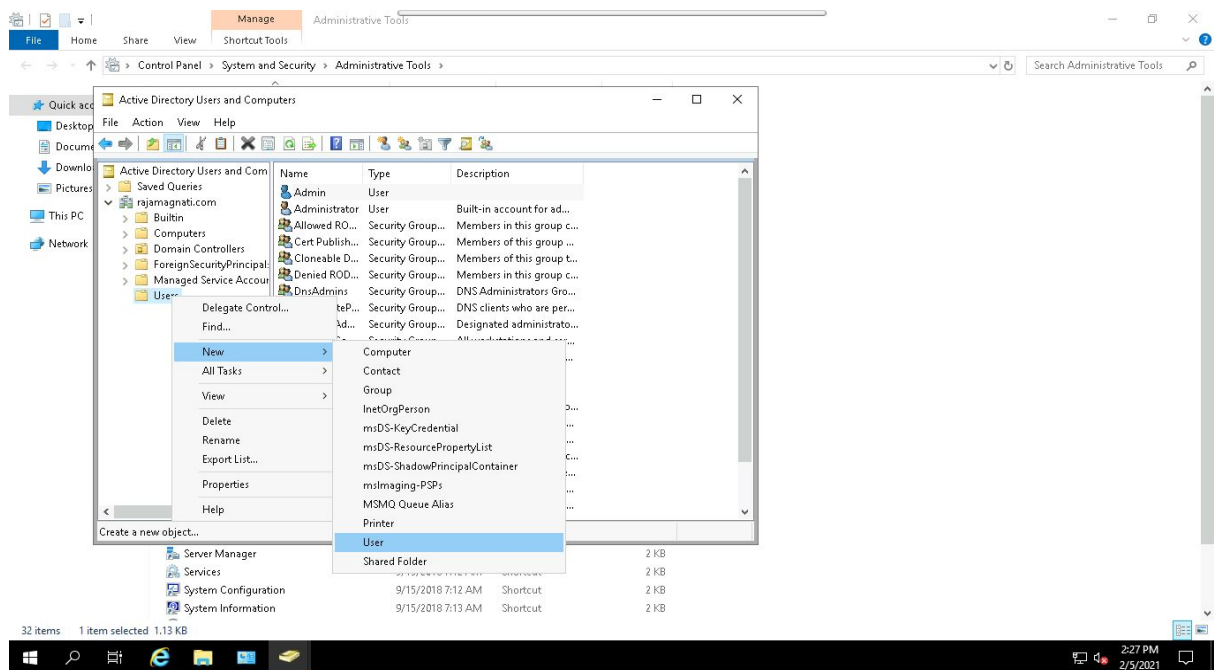
These directories are the location where all information is stored.

Example:- **User Directory** Where user related information is stored and from where user information is retrieved.



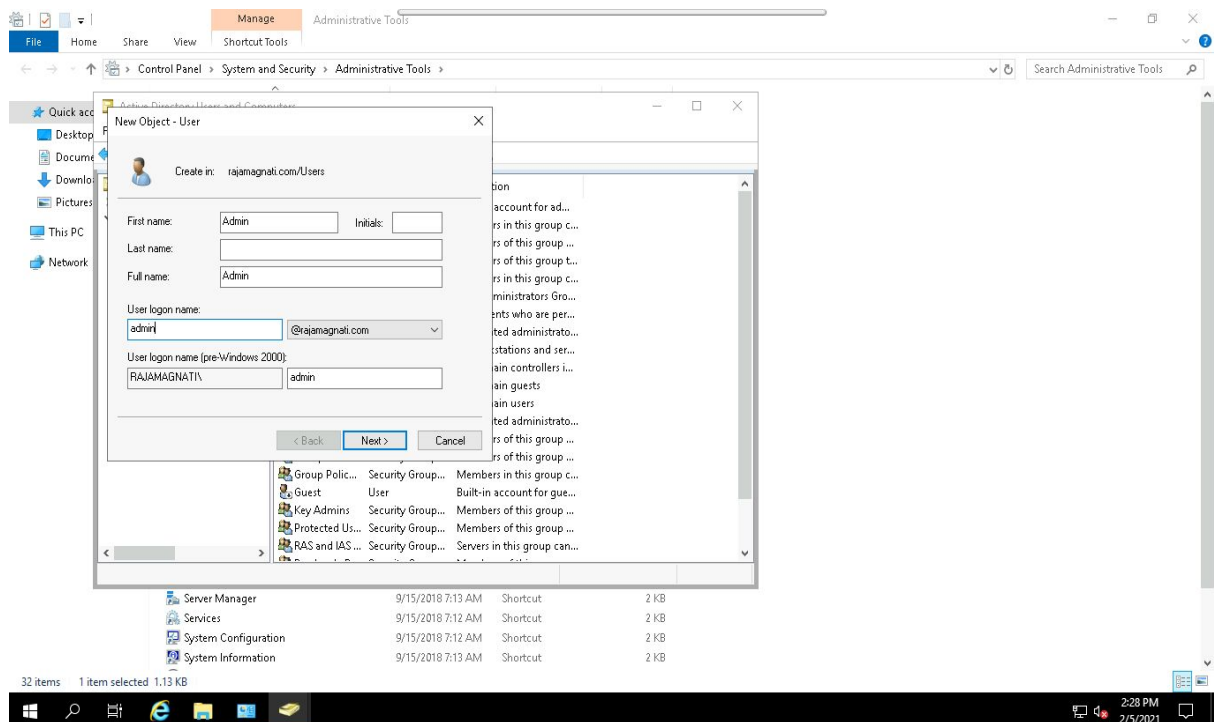
Step-21 Let's create a user

This user will be used to access jenkins. Click on **User** and use the click right button, then select **New** followed by **User**.



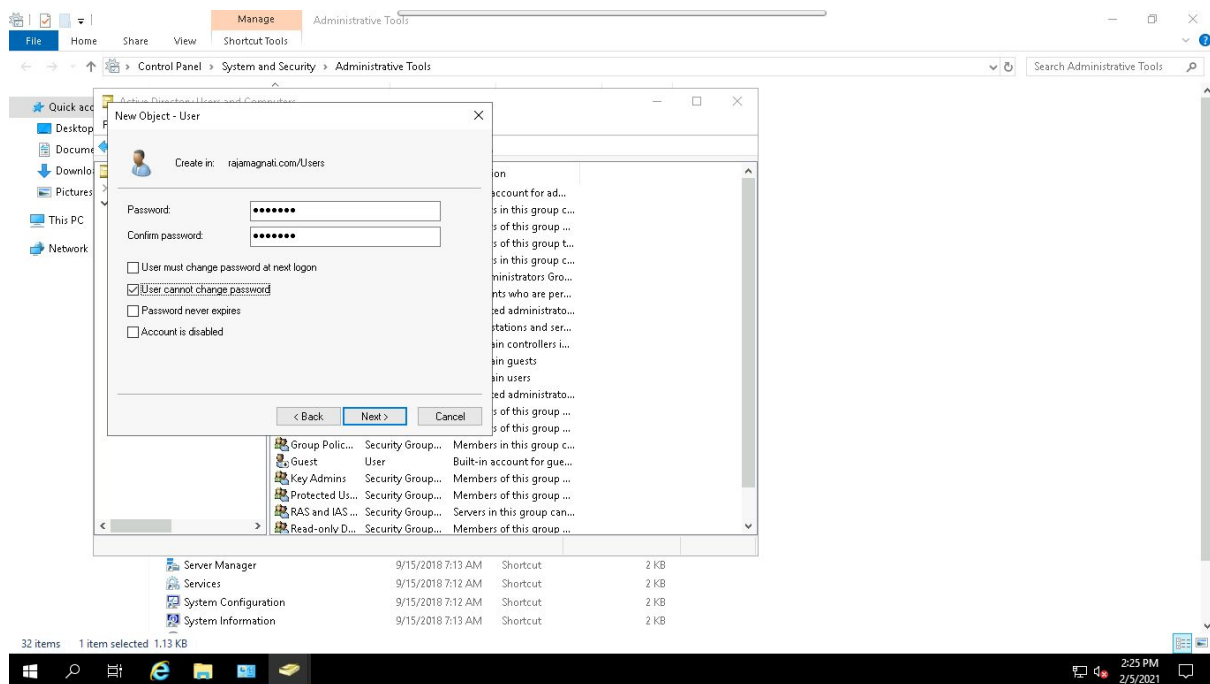
Step-22 Add details of user

This user will be used to access jenkins. Add First Name and login Name for user

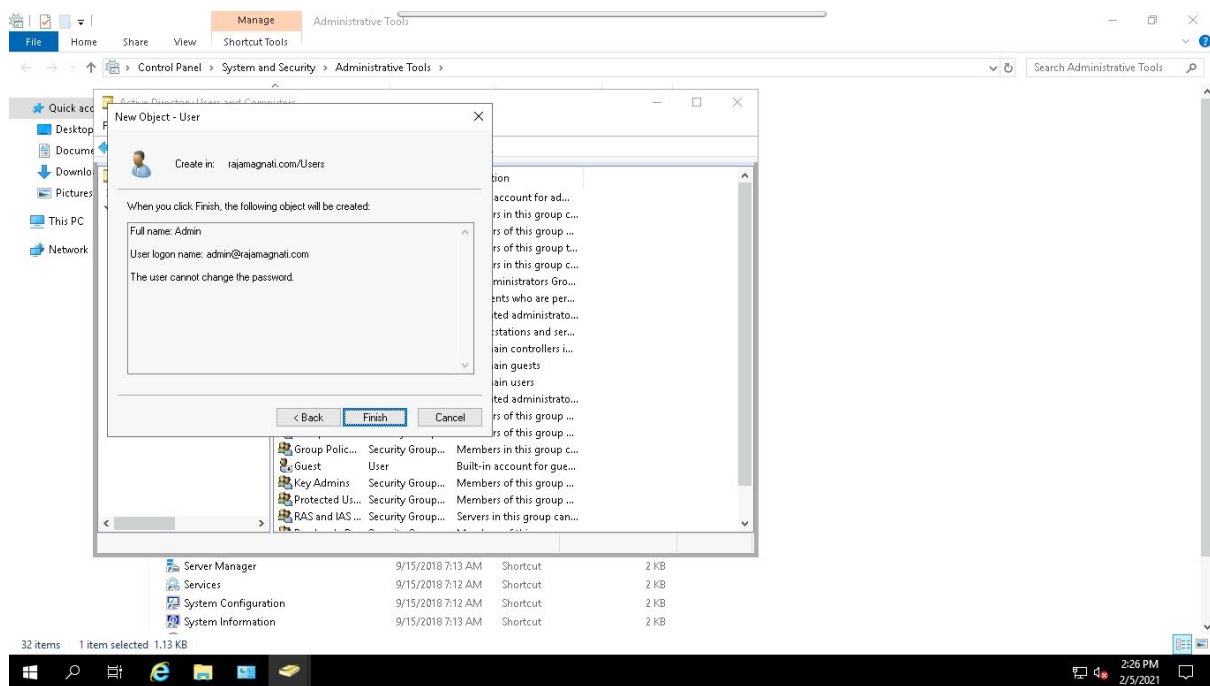


Step-23 Add Password for user

This password will be used for authentication. It must contain one small letter, one uppercase and one special character.



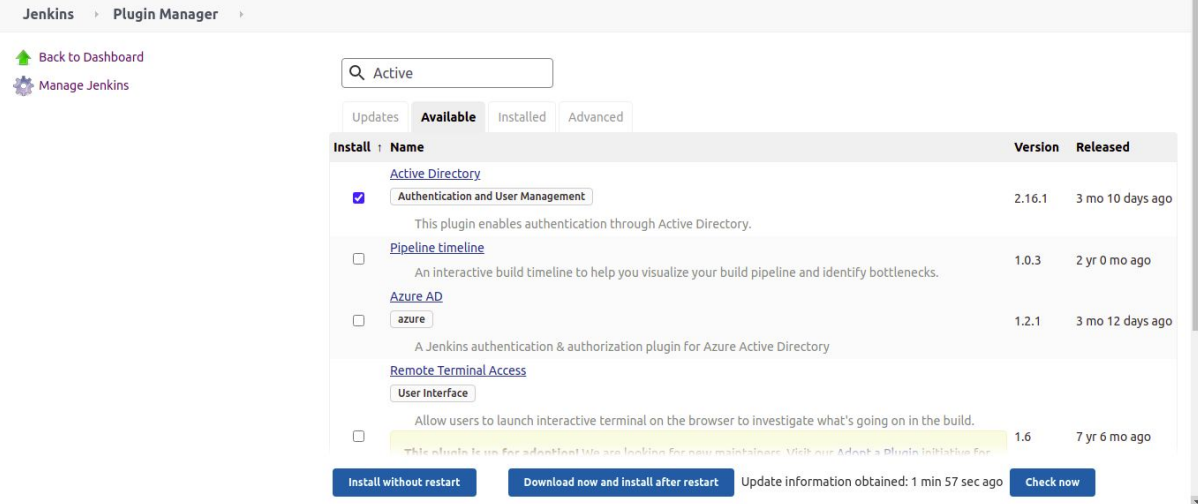
then select **Next**



Click on **Finish** and you have set up your first user.

Step-23 Install Plugin Active Directory

Select **Manage Jenkins** on the left panel in Jenkins. Then select **Manage Plugins**. Here we are installing plugin **Active Directory** in **Available** section it is necessary which will allow Jenkins to use **LDAP protocol** and hence you will be able to authenticate using Jenkins.



The screenshot shows the Jenkins Plugin Manager interface. The left sidebar has links for 'Back to Dashboard' and 'Manage Jenkins'. The main area has a search bar with 'Active' entered. Below the search bar are tabs for 'Updates', 'Available', 'Installed', and 'Advanced'. The 'Available' tab is active, showing a table of plugins. The 'Active Directory' plugin is selected with a checkbox. Below the table are buttons for 'Install without restart', 'Download now and install after restart', and 'Check now'.

Install	Name	Version	Released
<input checked="" type="checkbox"/>	Active Directory Authentication and User Management This plugin enables authentication through Active Directory.	2.16.1	3 mo 10 days ago
<input type="checkbox"/>	Pipeline timeline An interactive build timeline to help you visualize your build pipeline and identify bottlenecks.	1.0.3	2 yr 0 mo ago
<input type="checkbox"/>	Azure AD azure A Jenkins authentication & authorization plugin for Azure Active Directory	1.2.1	3 mo 12 days ago
<input type="checkbox"/>	Remote Terminal Access User Interface Allow users to launch interactive terminal on the browser to investigate what's going on in the build. <small>This plugin is in use for advertisement. We are looking for new maintainers. Visit our Adopt a Plugin Initiative for more information.</small>	1.6	7 yr 6 mo ago

Buttons: [Install without restart](#) [Download now and install after restart](#) [Check now](#)

Update information obtained: 1 min 57 sec ago

Step-24 Let's setup our security realms for Jenkins to use AD.

Select **Manage Jenkins** on the left panel in Jenkins. In **Security** sections. Select **Configure Global Security**.

Here we have various options to select the database which in our case is **Active Directory**.

Domain Name must be actual domain which we have used in **Active Directory**.

In the **Domain Controller** we need to specify where our **AD DS** is listening. It should be **IP Address** of Instance where **AD DS** is installed in our case is **52.66.120.158** and port must be **3268**.

The screenshot shows the 'Configure Global Security' page in Jenkins. The 'Authentication' section is active, and the 'Security Realm' is set to 'Active Directory'. The 'Domains' section contains the following fields:

- Domain Name: rajamagnati.com
- Domain controller: 52.66.120.158:3268
- Site: (empty)
- Bind DN: (empty)
- Bind Password: (empty)
- TLS Configuration: (Insecure) Trust all Certificates

At the bottom of the 'Domains' section, there is a warning message: "Leaving blank 'Bind DN' means that any operation performed will use anonymous binding. Keep in mind that this is not recommended as some servers do not allow it by default." Below this message are two buttons: 'Test Domain' and 'Delete Domain'. At the bottom of the page, there are 'Save' and 'Apply' buttons.

Step-25 Login to Jenkins using AD DS credentials

In earlier Step-22 and Step-23 we have created a user named **admin** and **Password**. We are using these user credentials to log into the system.



Welcome to Jenkins!

☐ Keep me signed in

Step-26 Successful authentication

Now using admin credentials we have accessed jenkins.

