vmware

CLOUD COMPUTING

PROJECT ON ACTIVE DIRECTORY DOMAIN SERVICES

Akshay Dubey
Ayush Mittal
Ashutosh Anand
Prabhat Kumar

GLA UNIVERSITY | MATHURA

ACKNOWLEDGEMENT

We have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals and organizations. We would like to extend our sincere thanks to all of them.

We are highly indebted to **Mr. Binayak Prasad Gupta** for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.
We would like to express my special gratitude and thanks to industry persons for giving me such attention and time.
Our thanks and appreciations also go to my colleague in developing the project and people who have willingly helped us out with their abilities.

NAME: Akshay Dubey
Ayush Mittal
Ashutosh Anand
Prabhat Kumar

INDEX

PROJECT DETAILS

Active Directory Infrastructure Administration	Configure & administer a forest or a domain.
	Understanding the read-only domain controller (RODC).
Configuring Active Directory Group Policy	Create and apply Group Policy objects (GPOs).
	Configure & administer account policies.

INTRODUCTION

Cloud computing

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software.

Virtualization

In computing, virtualization refers to the act of creating a virtual version of something, including virtual computer hardware platforms, storage devices, and computer network resources.

Server

A server is a computer program or device that provides a service to another computer program and its user, also known as the client.

Client

A client is the receiving end of a service or the requestor of a service in a client/server model type of system. The client is most often located on another system or computer, which can be accessed via a network.

1. Active Directory Infrastructure Administration

Active Directory (AD)

Active Directory (AD) is a Microsoft product that consists of several services that run on Windows Server to manage permissions and access to networked resources.

The main service in Active Directory is Domain Services (AD DS), which stores directory information and handles the interaction of the user with the domain. AD DS verifies access when a user signs into a device or attempts to connect to a server over a network. AD DS controls which users have access to each resource. For example, an administrator typically has a different level of access to data than an end us.

Major features in Active Directory Domain Services

Active Directory Domain Services uses a tiered layout consisting of domains, trees and forests to coordinate networked elements.

A domain is a group of objects, such as users or devices, that share the same AD database. Domains have a domain name system (DNS) structure.

Tree

A tree is one or more domains grouped together. The tree structure uses a contiguous namespace to gather the collection of domains in a logical hierarchy. Trees can be viewed as trust relationships where a secure connection, or trust, is shared between two domains. Multiple domains can be trusted where one domain can trust a second, and

the second domain can trust a third. Because of the hierarchical nature of this setup, the first domain can implicitly trust the third domain without needing explicit trust

Forest

A forest is a group of multiple trees. A forest consists of shared catalogs, directory schemas, application information and domain configurations. The schema defines an object's class and attributes in a forest. In addition, global catalog servers provide a listing of all the objects in a forest.

RODC (read-only domain controller)

A read-only domain controller (RODC) is a server that hosts an Active Directory database's read-only partitions and responds to security authentication requests.

RODC, which was designed to be used in branch offices that cannot support their own domain controllers, can be used in a Windows Server 2008 environment or higher.

Before installing RODCs, Microsoft recommends that organizations meet some prerequisites to ensure they work properly, including having a functional AD forest level set at Windows Server 2003 or higher and at least one writeable domain controller deployed on Windows Server 2008 or higher.

2. Configuring Active Directory Group Policy

Group Policy

Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. A set of Group Policy configurations is called a **Group Policy Object (GPO).**

Account policy

A user account policy is a document which outlines the requirements for requesting and maintaining an account on computer systems or networks, typically within an organization.

Password Restrictions

The Password Restrictions section is where minimum and maximum password age (how often a password can and must be changed), minimum password length (the number of characters in a password), and password uniqueness (how frequently the same password can be used) can be configured. Password restrictions enable you to control the kinds of passwords that users choose and the frequency with which they must change them.

Maximum Password Age

The Maximum Password Age area enables you to configure the number of days a password can be used before it must be changed.

Minimum Password Age

The Minimum Password Age area enables you to configure the number of days a password must be used before it can be changed.

Minimum Password Length

The longer a password is, the more difficult it is to guess. As a result, the minimum password length restriction enables you to require that passwords must be between 0 (Permit Blank Password) and 14 characters long.

Password Uniqueness

This setting enables you to control how often the same password can be used. By allowing your domain controller to remember the passwords used, you can prevent a user from switching between two or three passwords that are easy to remember.

VMware ESXi

VMware ESXi (formerly **ESX**) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers. As a type-1 hypervisor, ESXi is not a software application that is installed on an operating system (OS); instead, it includes and integrates vital OS components, such as a kernel.

The name *ESX* originated as an abbreviation of **Elastic Sky X.**

VMware vSphere

VMware vSphere -- formerly known as VMware Infrastructure -- is the brand name for VMware's suite of server virtualization products that includes its ESXi hypervisor and vCenter management software.

vCenter

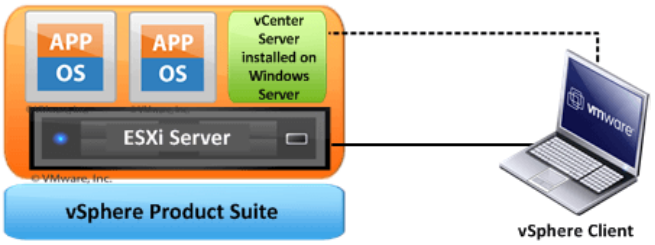
vCenter Server is the centralized management utility for VMware, and is used to manage virtual machines, multiple ESXi hosts, and all dependent components from a single centralized location

Difference between vSphere, ESXi and vCenter

- **vSphere** is a software suite that comes under data center product. vSphere is like Microsoft Office suite which has many softwares like MS Office, MS Excel, MS Access and so on. Like Microsoft Office, vSphere is also a software suite that has many software components like vCenter, ESXi, vSphere client and so on. So, the combination of all these software components is vSphere.

- **ESXi**, vSphere client and **vCenter** are components of VMware vSphere. ESXi server is the most important part of vSphere. **ESXi** is the virtualization server. It is type 1 hypervisor. All the virtual machines or Guest OS are installed on ESXi server. To install, manage and access those virtual servers which sit above of ESXi server, you will need other part of vSphere suite called vSphere client.

- **vCenter** server is another piece of vSphere suite. There are two flavors of vCenter servers. vCenter server can be installed on Windows Server or can be Linux based virtual appliance. VMware will discontinue Windows based vCenter server and release only Linux based vCenter appliance in the future. VMware vCenter server is a centralized management application that lets you manage virtual machines and ESXi hosts centrally. vSphere client again is used to access vCenter Server and ultimately manage ESXi servers.



OUR OBJECTIVE

- We are going to implement an Active Directory Infrastructure.

- Then we will manage an Active Directory forest and domain structure

  RODC essential.
  - Read-only feature
  - DNS protection:
  - Password protection
  - Administrator Role Separation

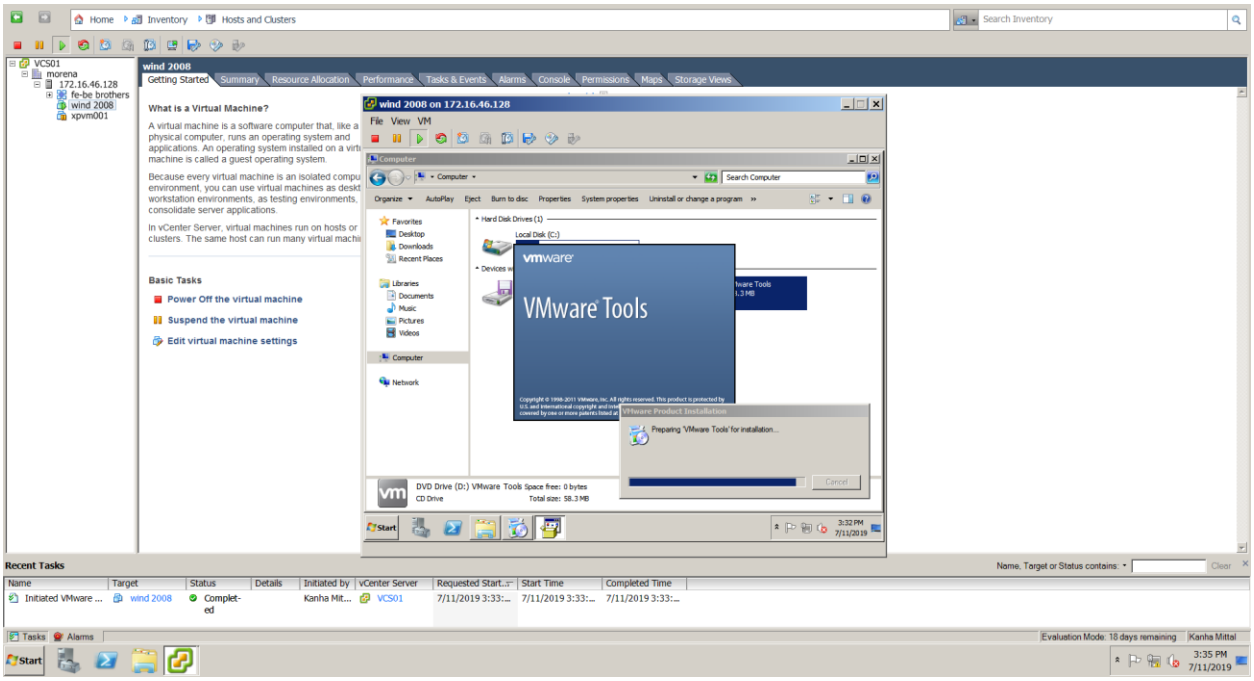
- **Group Policy** which is typically used to apply consistent security and behavior settings on groups of systems, organized into different OGs.

- Applying Password Policies and Control Panel Policies to the server side.

- The primary goals of an administration manager are to direct, control and supervise the support services of the organization to facilitate its success. The manager achieves this goal by ensuring free flow of communication and efficient use of resources throughout the organization.

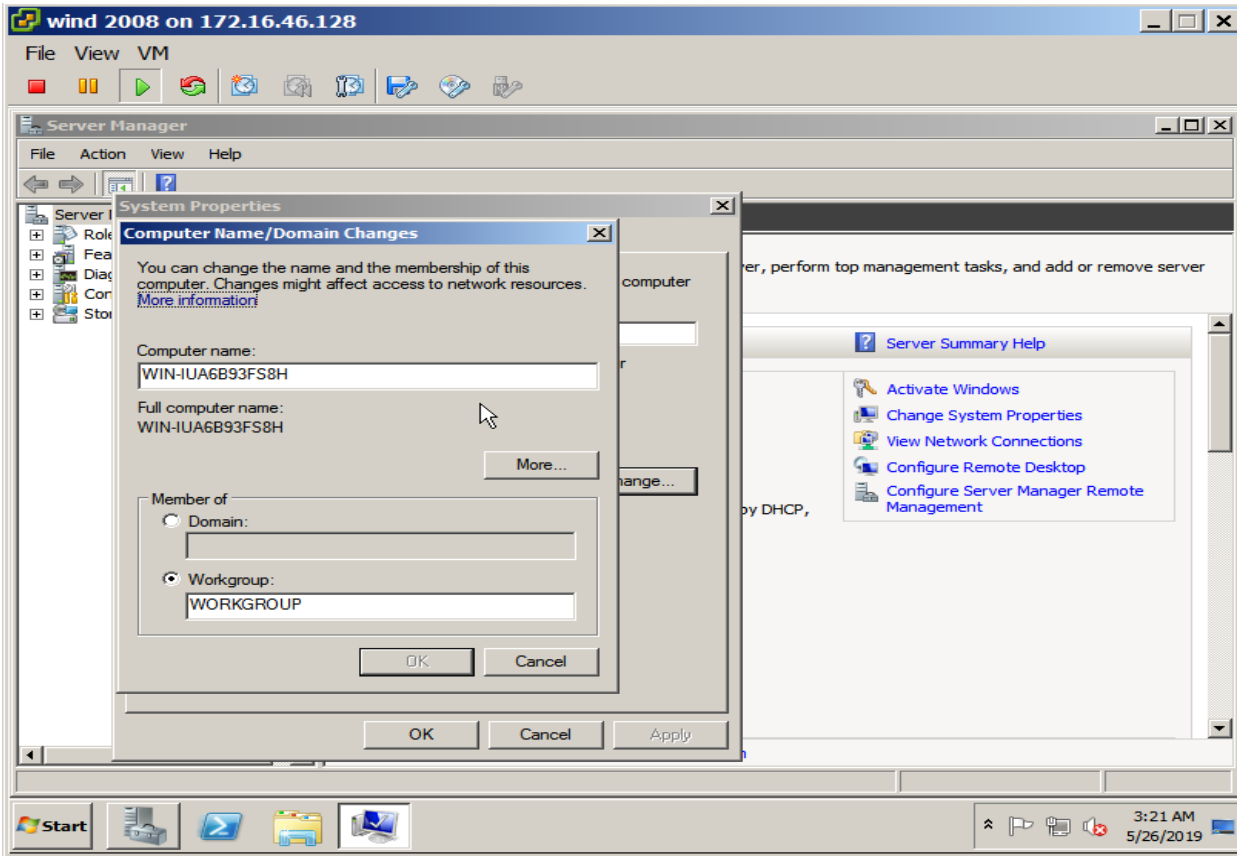
CONTENTS

1. Active Directory Infrastructure Administration

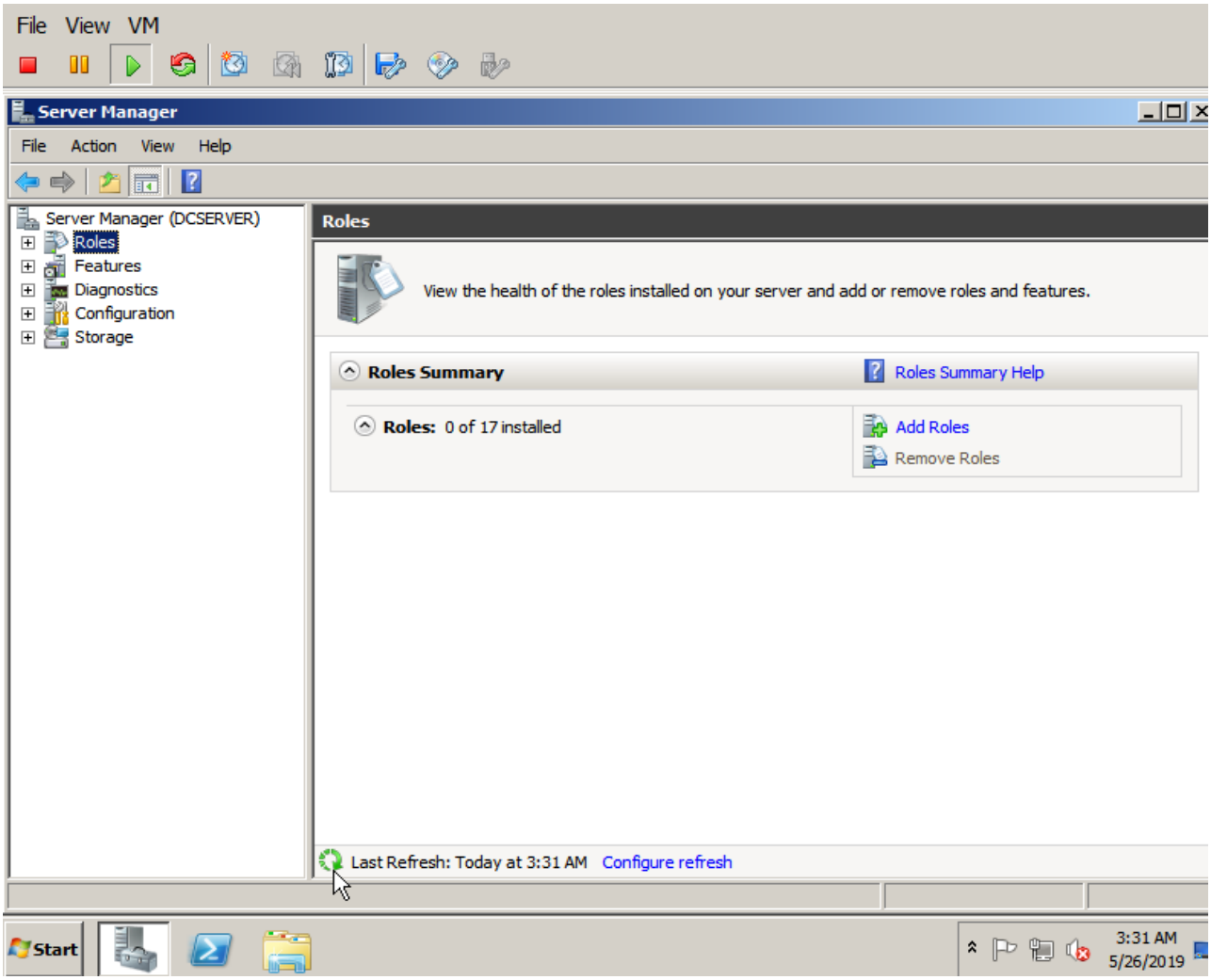


- ✓ This is the first step we have taken , we are installing the Windows Server 2008 inside the vSphere Client .

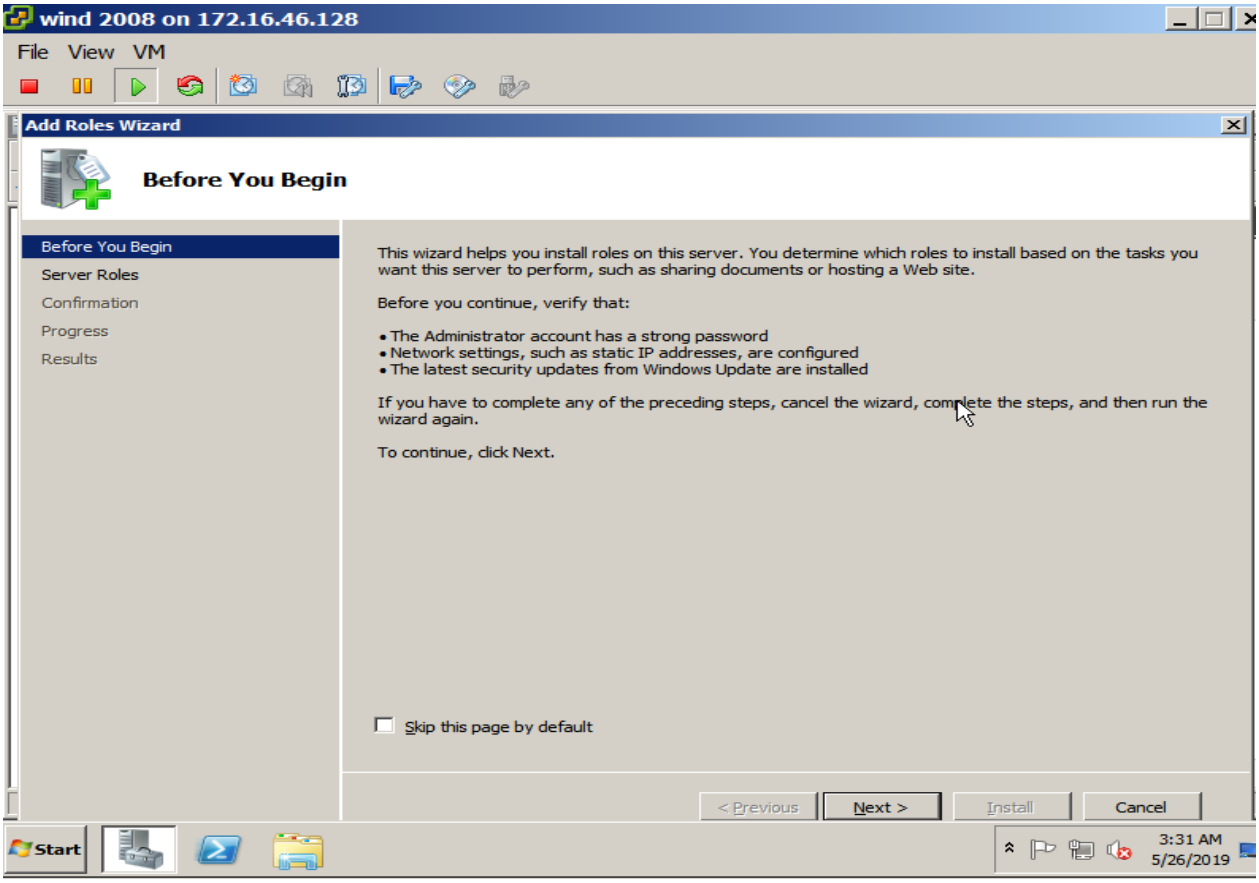
- ✓ We are installing the VMware Tools to get benefits like :
  - Low video resolution.
  - Restricted movement of the mouse etc.



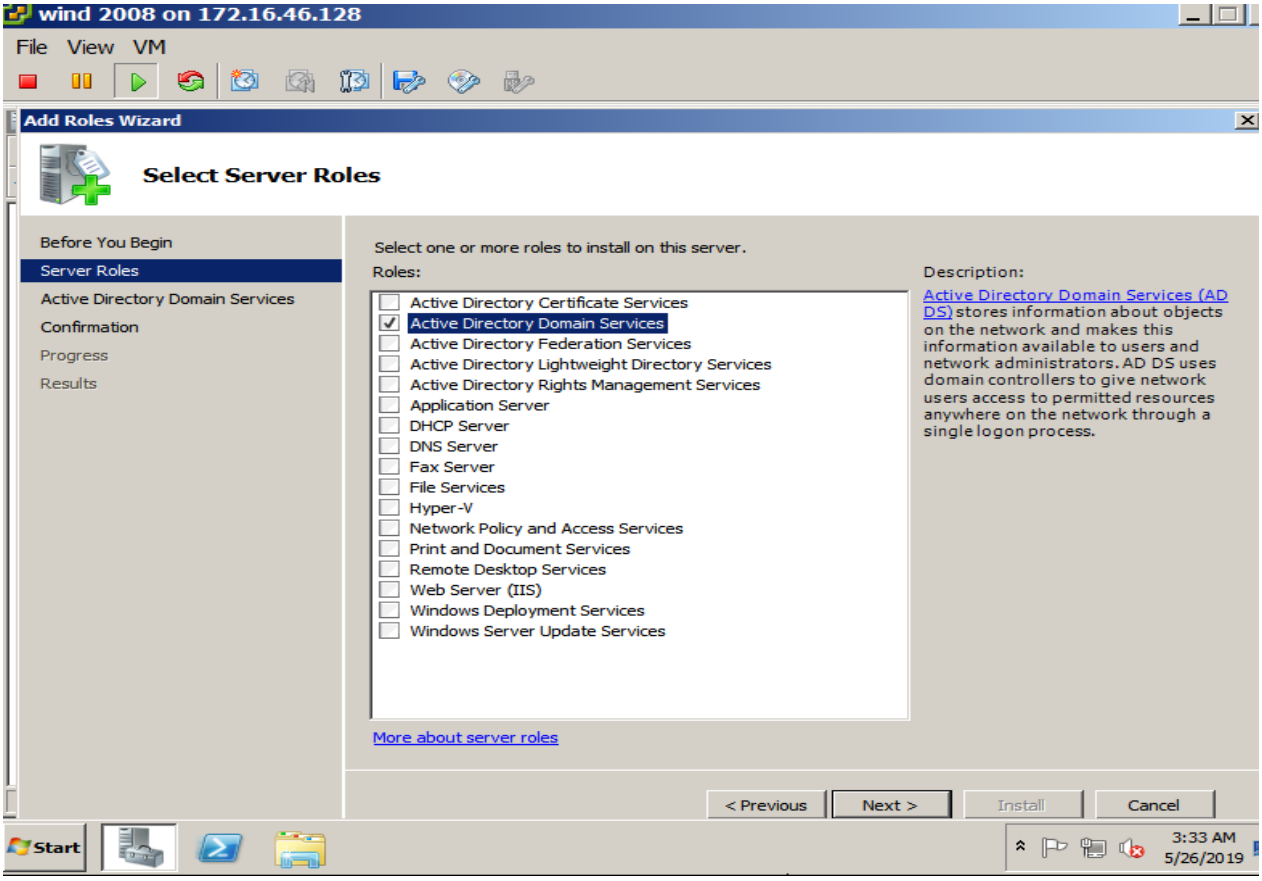
- ✓ Currently, we do not have any domain.
- ✓ So, we are making the domain first by going to Computer Name/Domain Changes.
- ✓ After entering the name click “OK” .



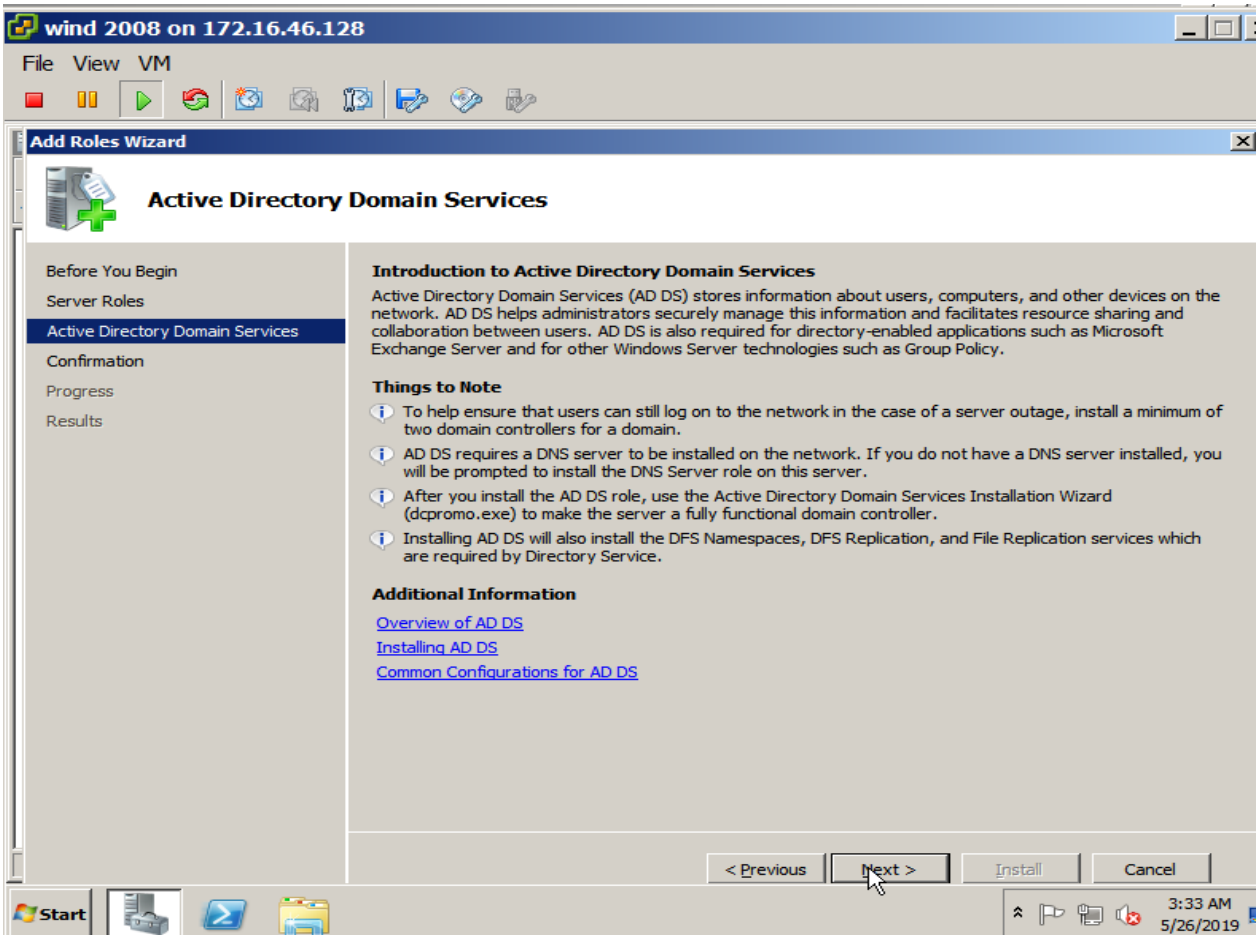
- ✓ Now, we are going to add up roles like active directory.
  .
- ✓ Click on the Roles you will get the Roles Summary .
- ✓ Currently we do not have any Roles Installed out of 17



- ✓ This is the Add Roles Wizard.
- ✓ This Wizard will pop up when you select add roles in the previous step.

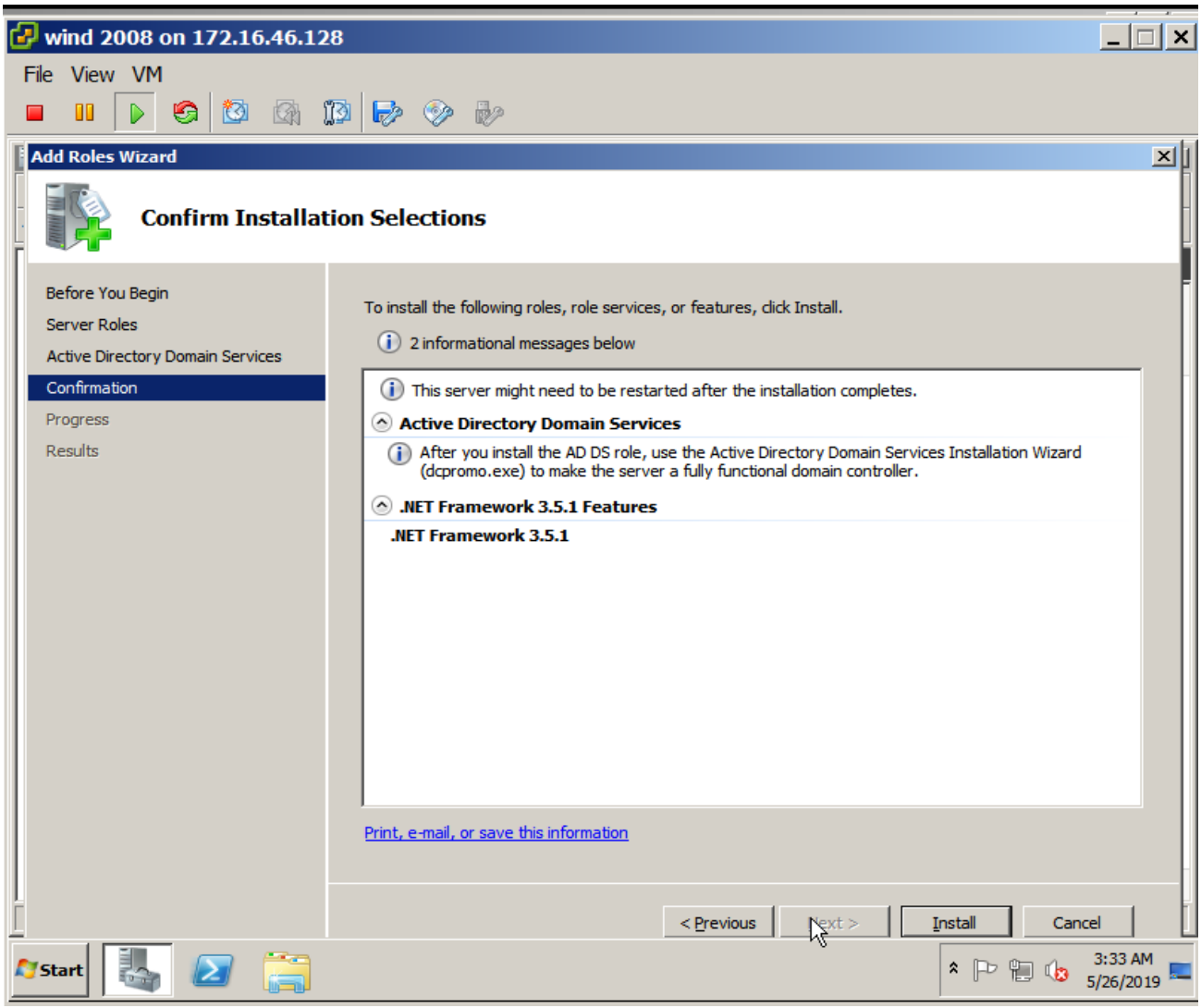


- ✓ This is the next wizard, which allows you to select roles to install on this server.
- ✓ Here, we are choosing AD Domain Services because this can stores and manages User account and Computer accounts.
- ✓ This will make DNS server automatically.



- ✓ This is the next wizard which is giving extra information for the AD Domain Services.

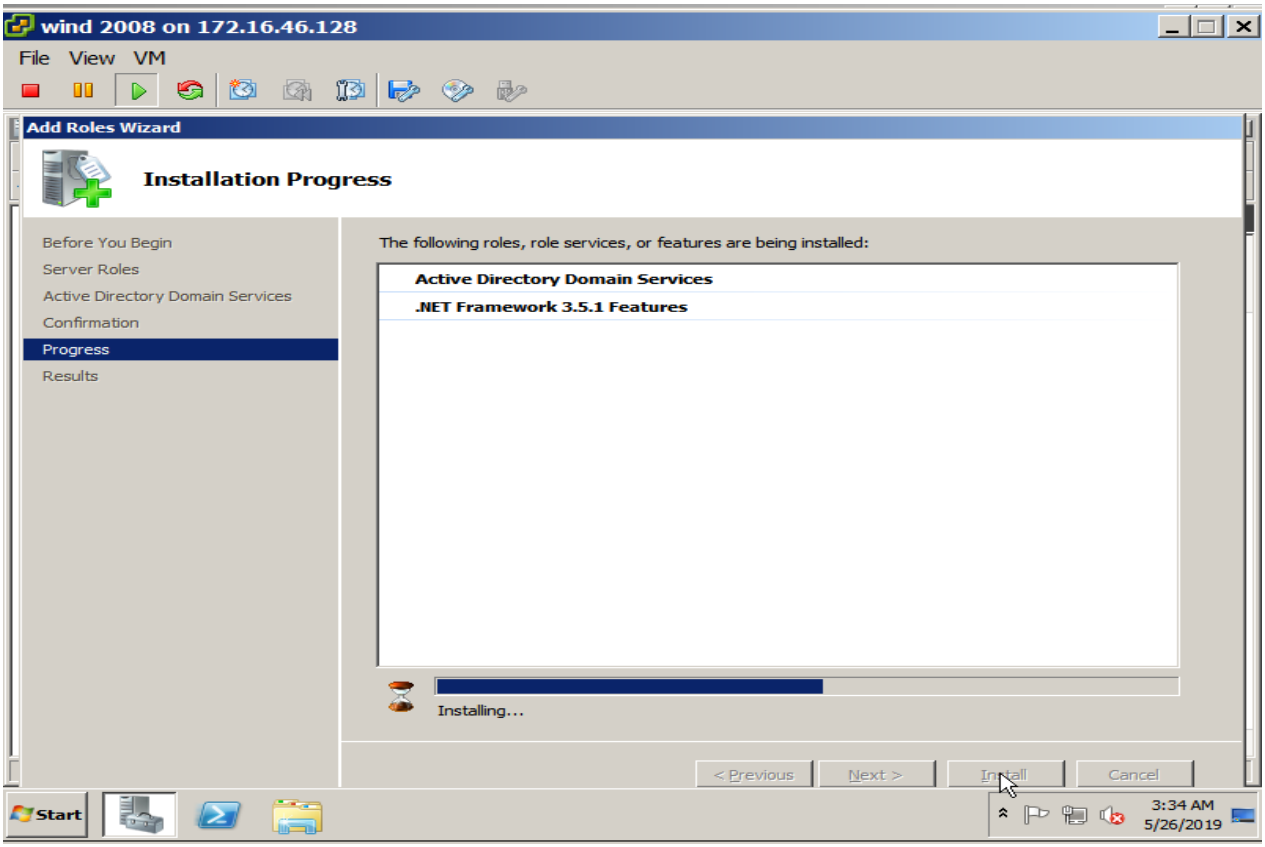
- ✓ We must have to choose “Next” option to move on.



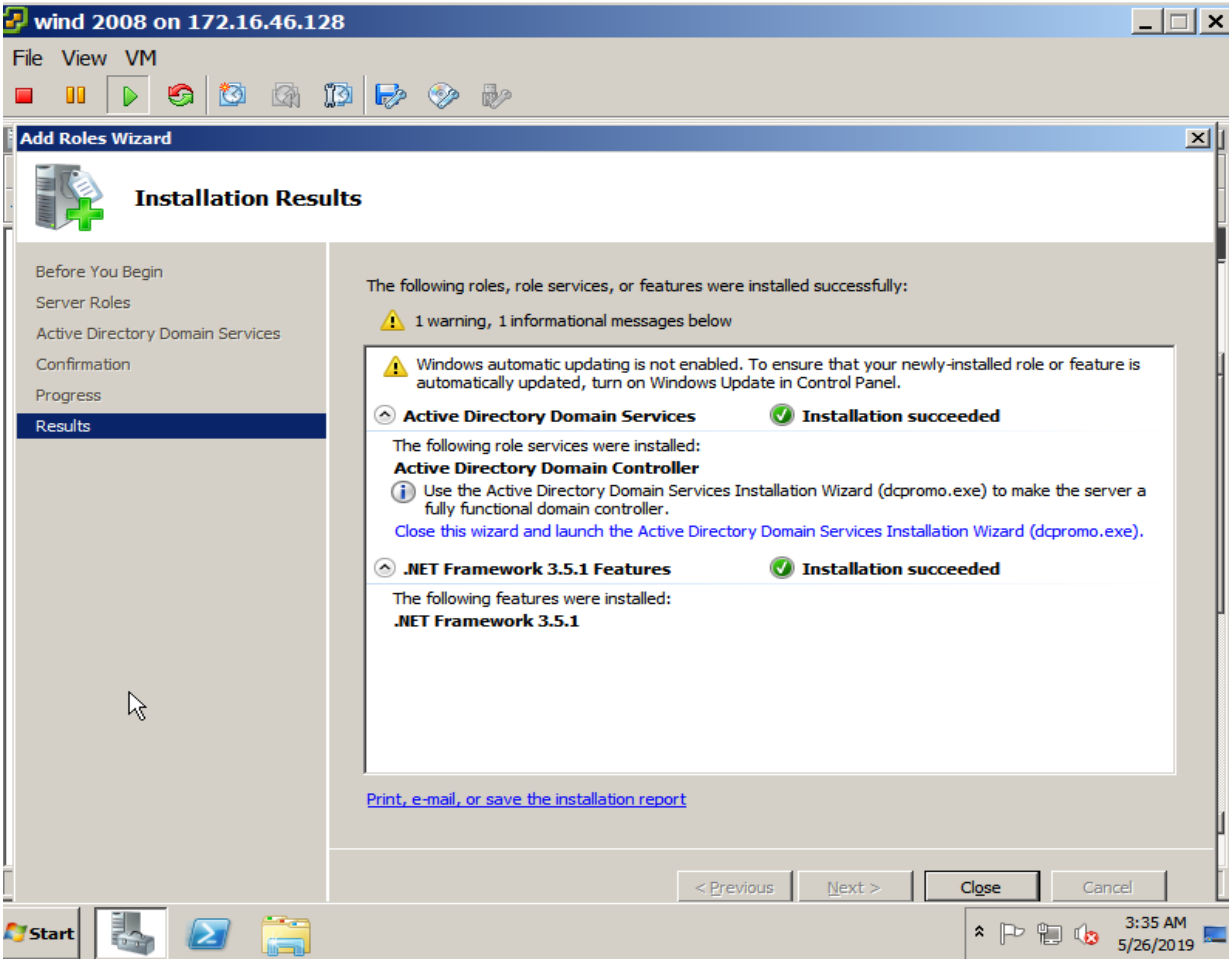
- ✓ This is the next wizard which is showing the confirmation message.
- ✓ This window also giving two informative messages:

  - The server might have to restart after installation completes &

  - After install AD DS role, use the dcpromo.exe to make the server fully functional domain.

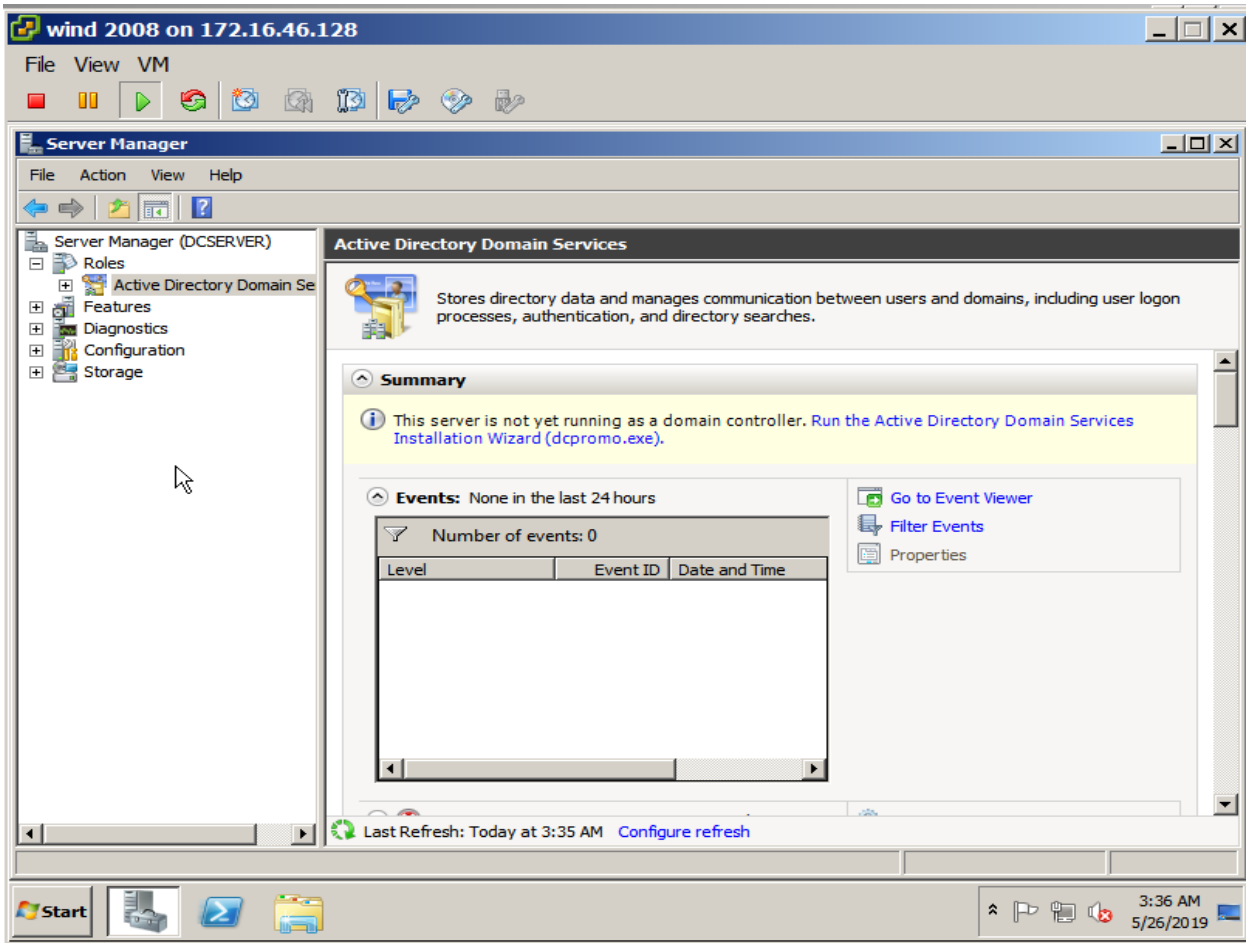


- ✓ AD DS role is installing.
- ✓ This can take atleast 2-5 minutes to install.
- ✓ You have to wait for it.



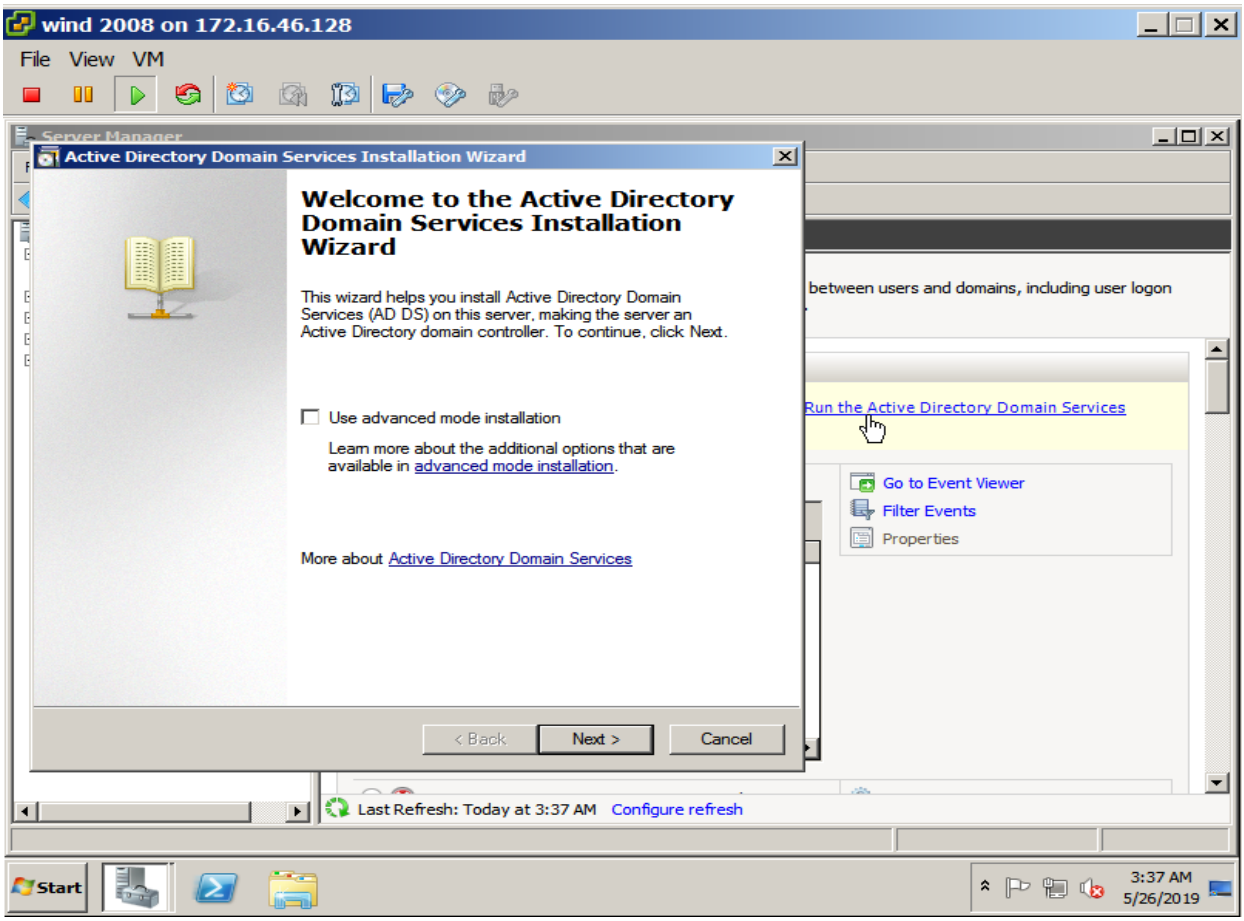
- ✓ The new wizard is pop up when AD DS role and .NET framework 3.5.1 is installed successfully.

- ✓ Further, we have to choose close step to close this window and move on further.



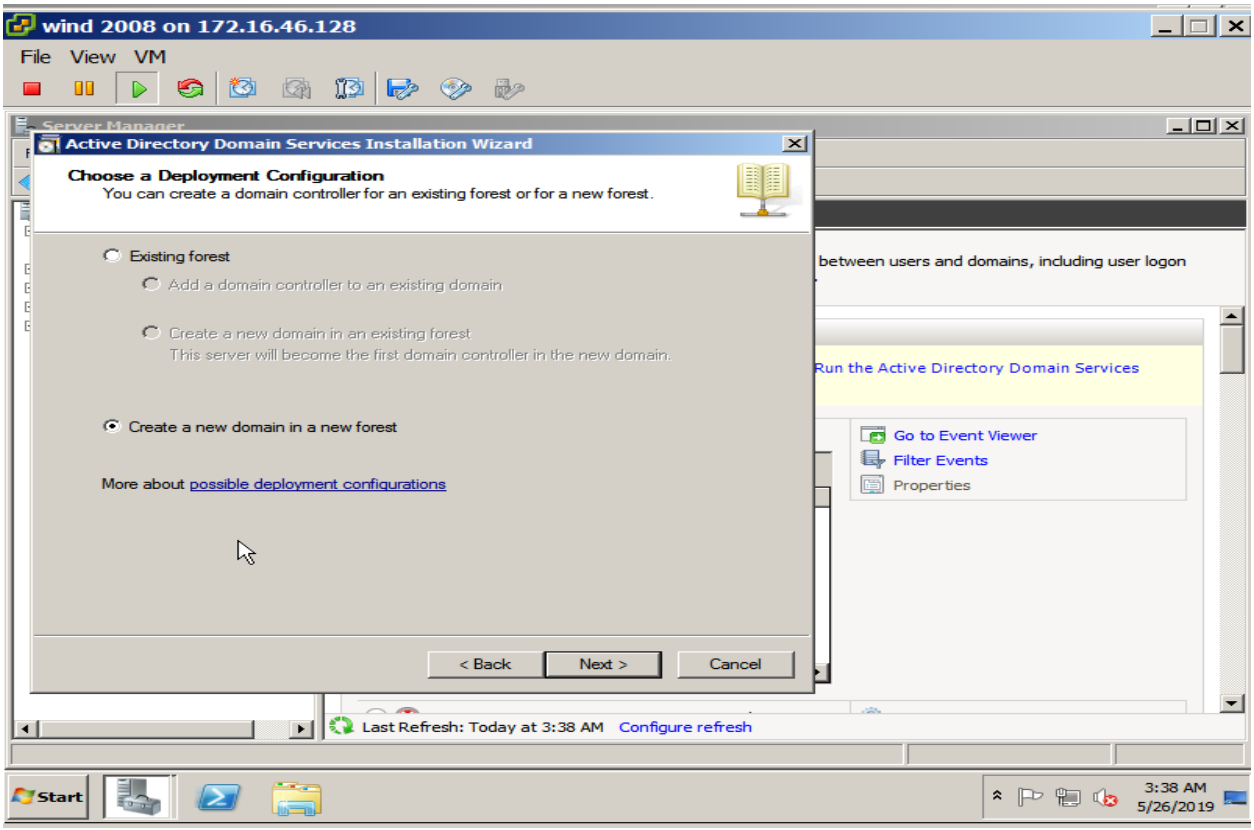
- ✓ Now after closing the installation wizard, we can see in the service manager that our AD DS showing but this server is not running as a domain controller.

- ✓ Run the dcpromo.ese to run this server.



- ✓ After the successfully running of dcpromo.exe, the new AD DS Installation Wizard comes out.

- ✓ We have to choose "Next" Button to move further.

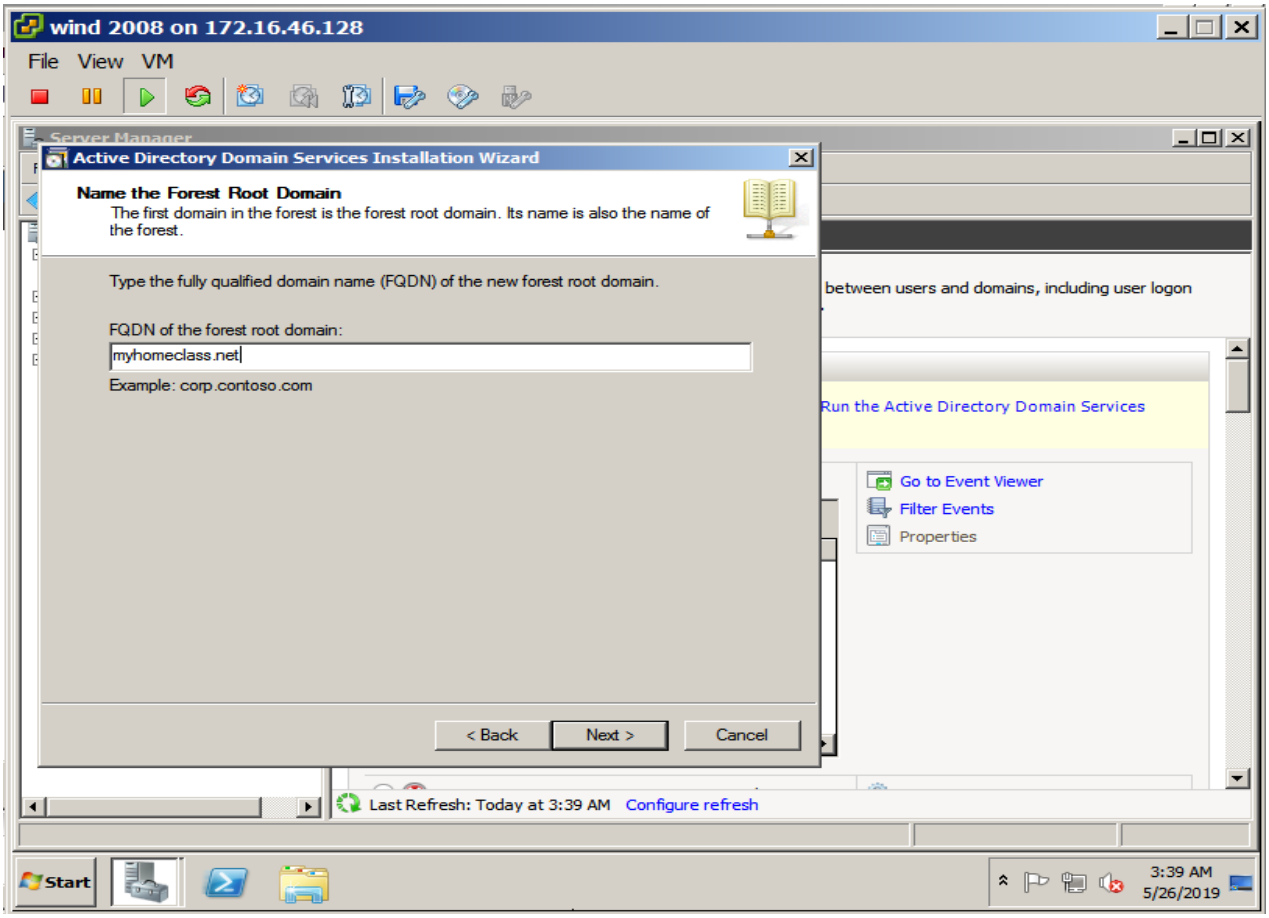


- ✓ After, choosing "Next", the new window pop out and asking to choose any of the following option.

  - Existing forest or Create a new domain in a new forest.

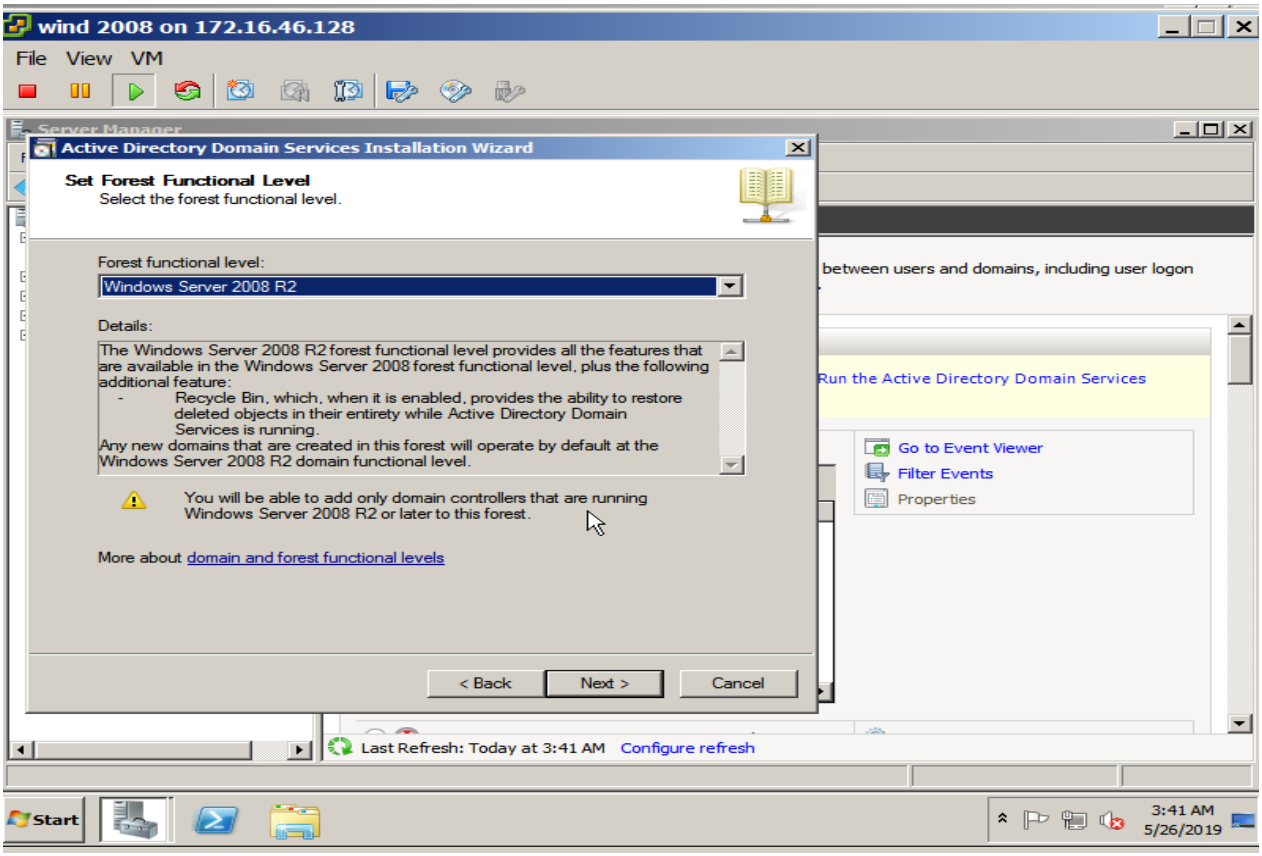
- ✓ Since we do not have any domain yet, so we will choose "Create a new domain in a new forest."

- ✓ The forest root domain contains the Enterprise Admins and Schema Admins.

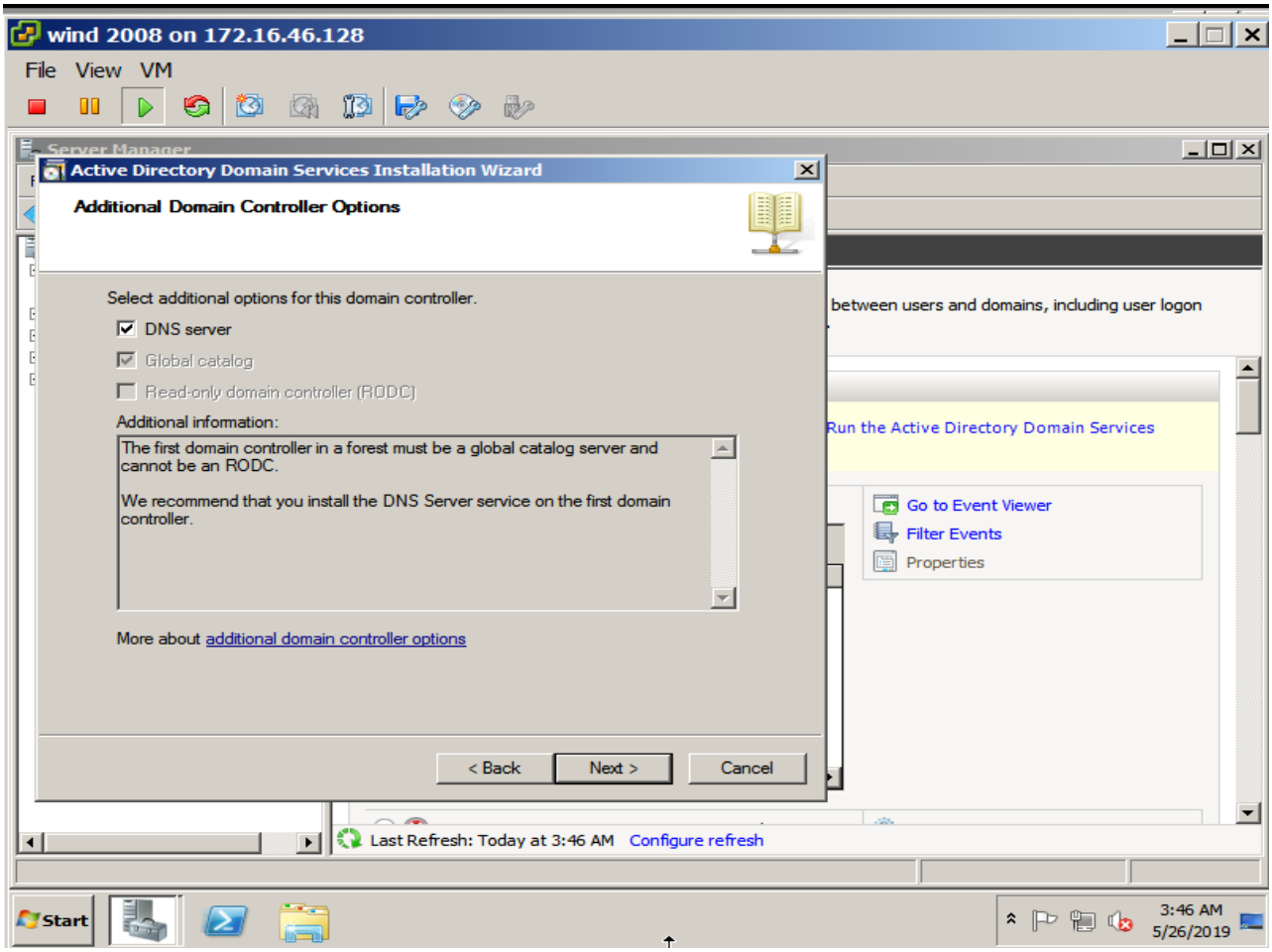


- ✓ Now, we are giving fully qualified domain name of the forest i.e. "myhomeclass.net".

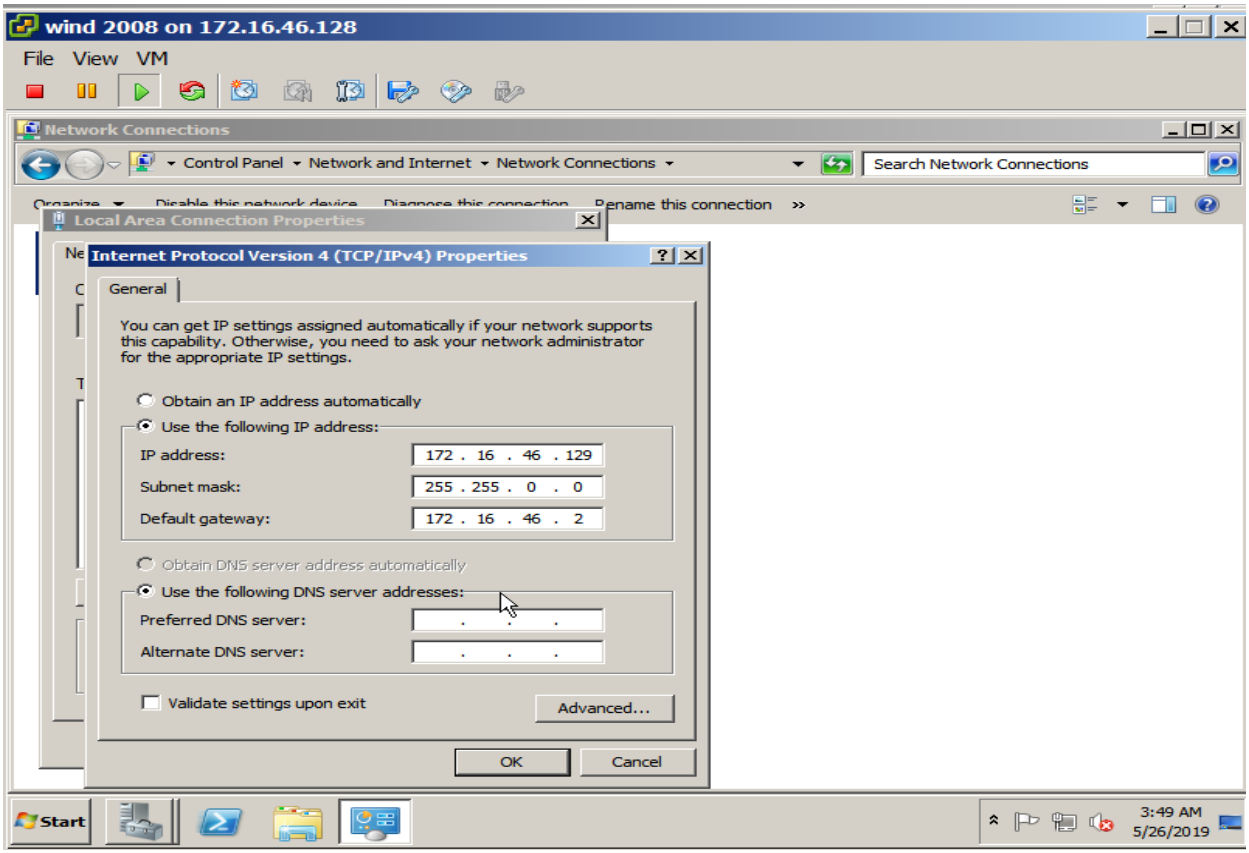
- ✓ After giving the FQRN of the forest root domain, click on "Next".



- ✓ After choosing "Next" in the previous window, we have to set the functional level in the next wizard.
- ✓ We must have to select Windows Server 2003 or more than this .
- ✓ So, we are selecting the Windows Server 2008 R2 because it provides all the features available in this server.



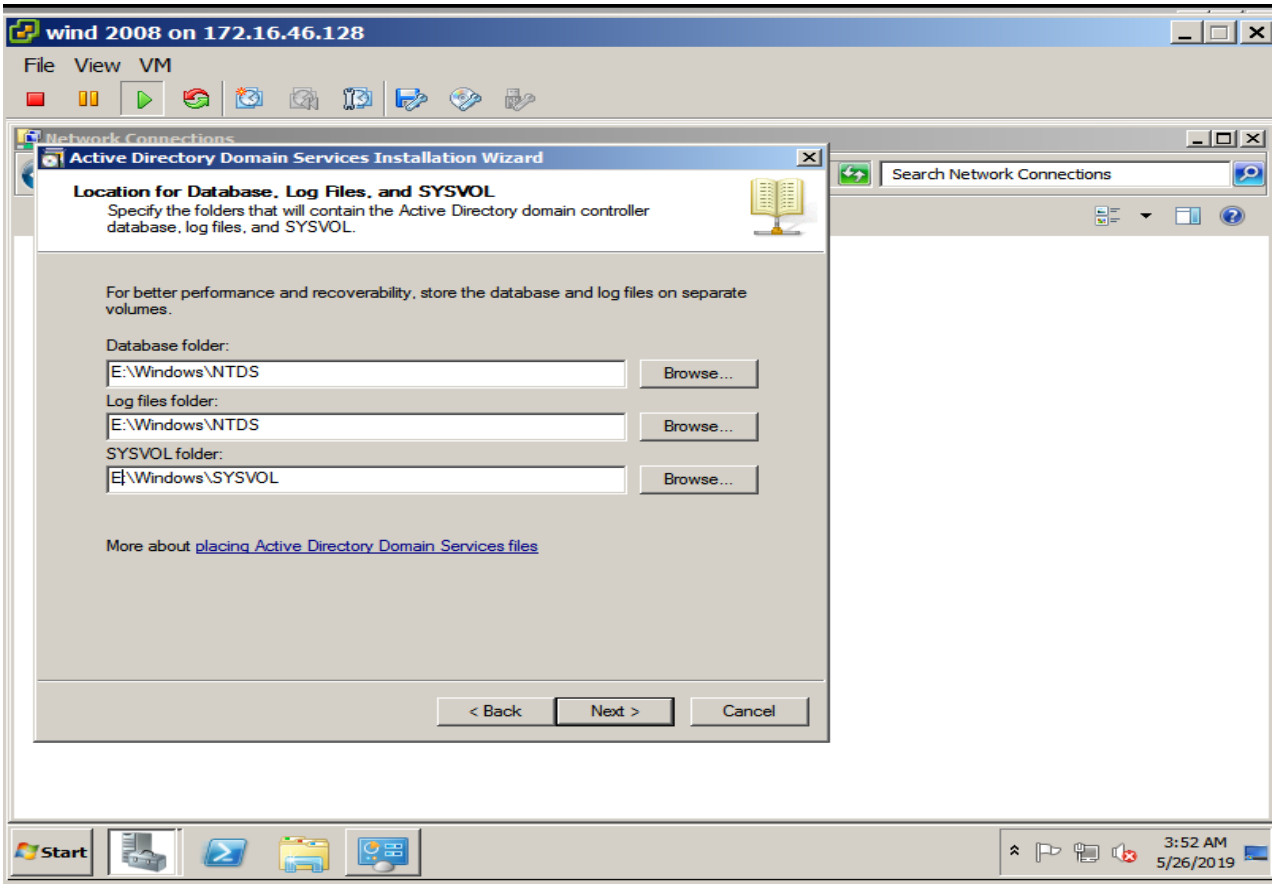
- ✓ Since, we are installing first time in this system so we must have to select DNS server service on the first domain controller because it can installed automatically.
- ✓ We cannot add RODC here.
- ✓ After selecting click on “Next”.



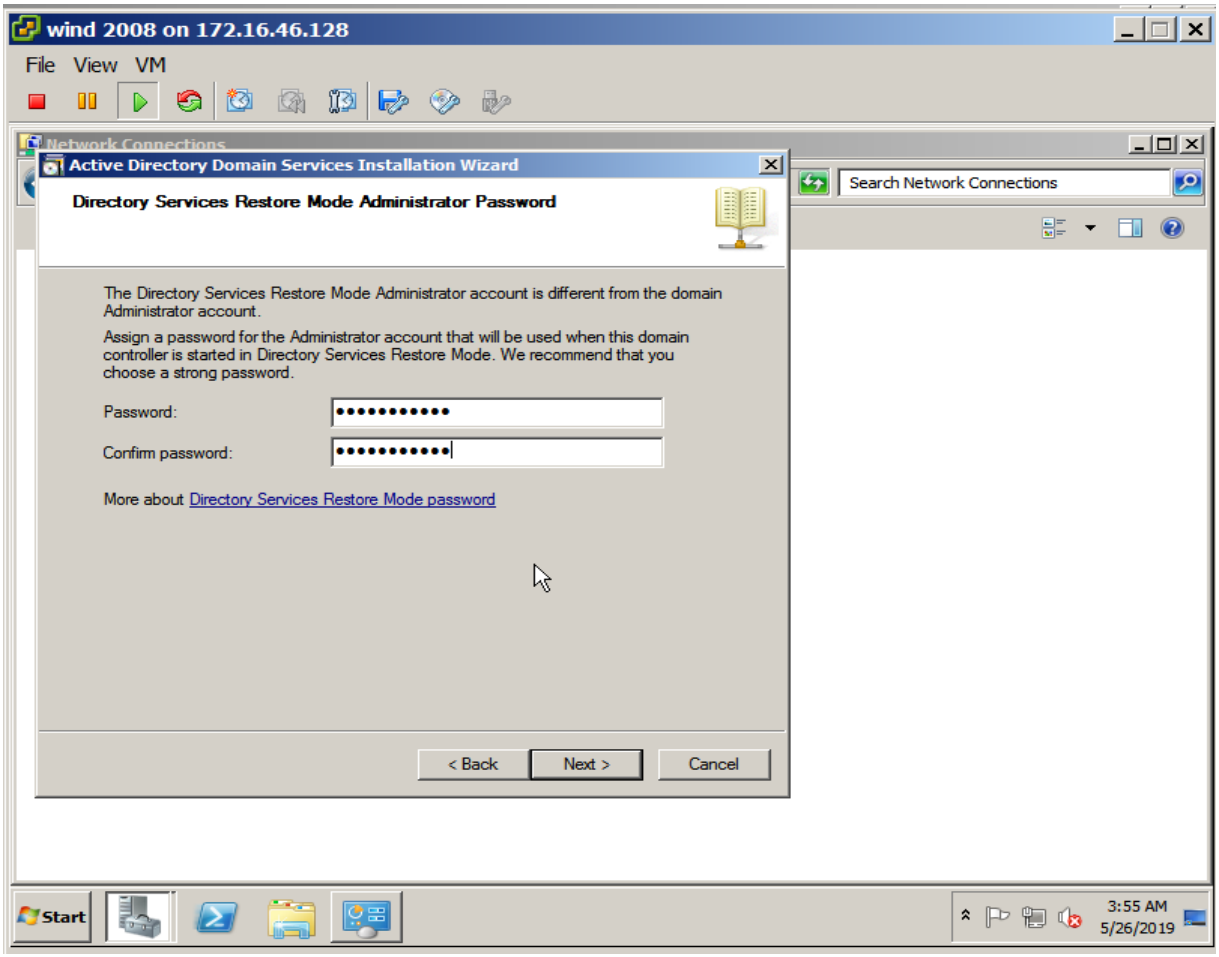
- ✓ Now, before moving further we can go to network connection of the system and make the IP from dynamic to static.

- ✓ So, we can select ipv4 and by refusing the obtain IP address automatically click on "Use the following IP address."

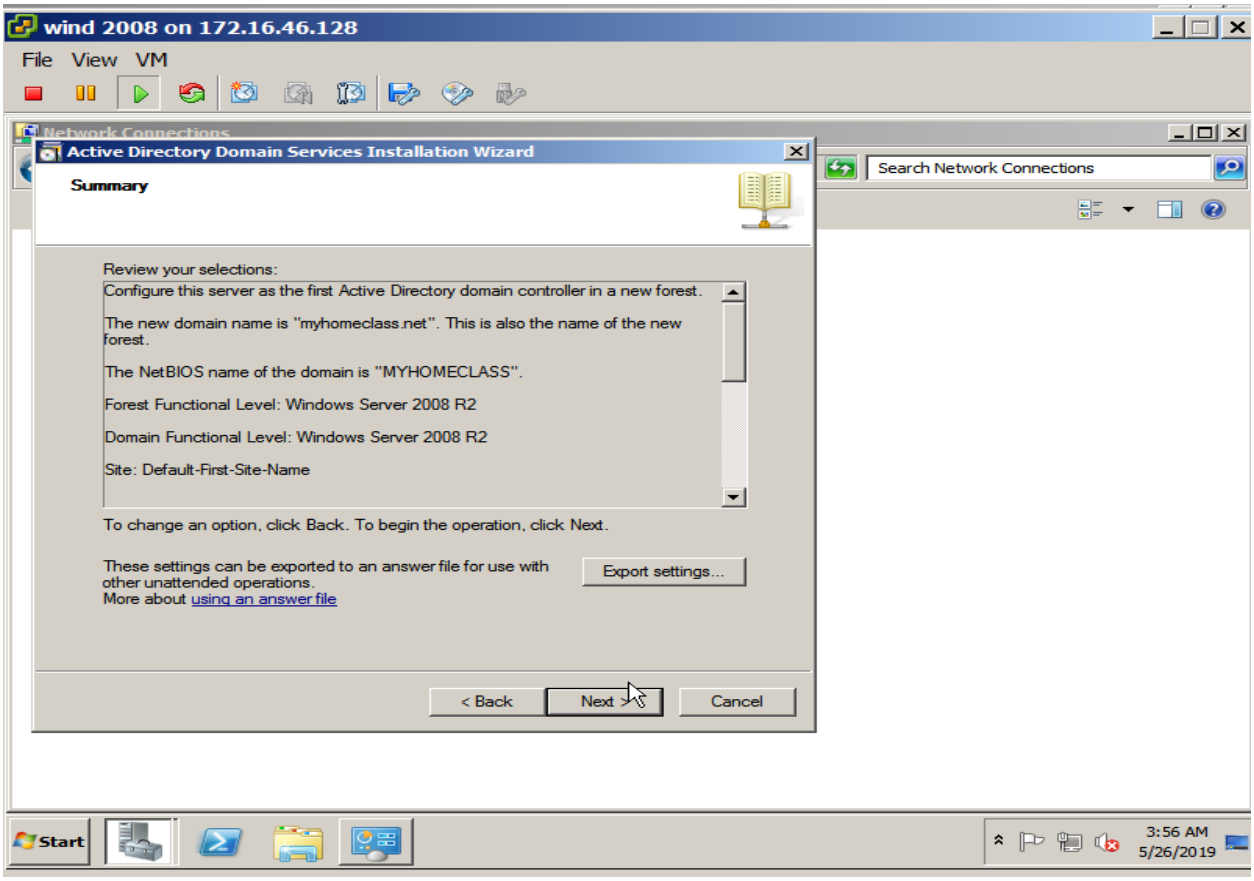
- ✓ We provide 172.16.46.129 IP address (i.e. of esxi), following Subnet Mask 255.255.255.0 and Default Gateway as 172.16.16.2 and select "OK" button.



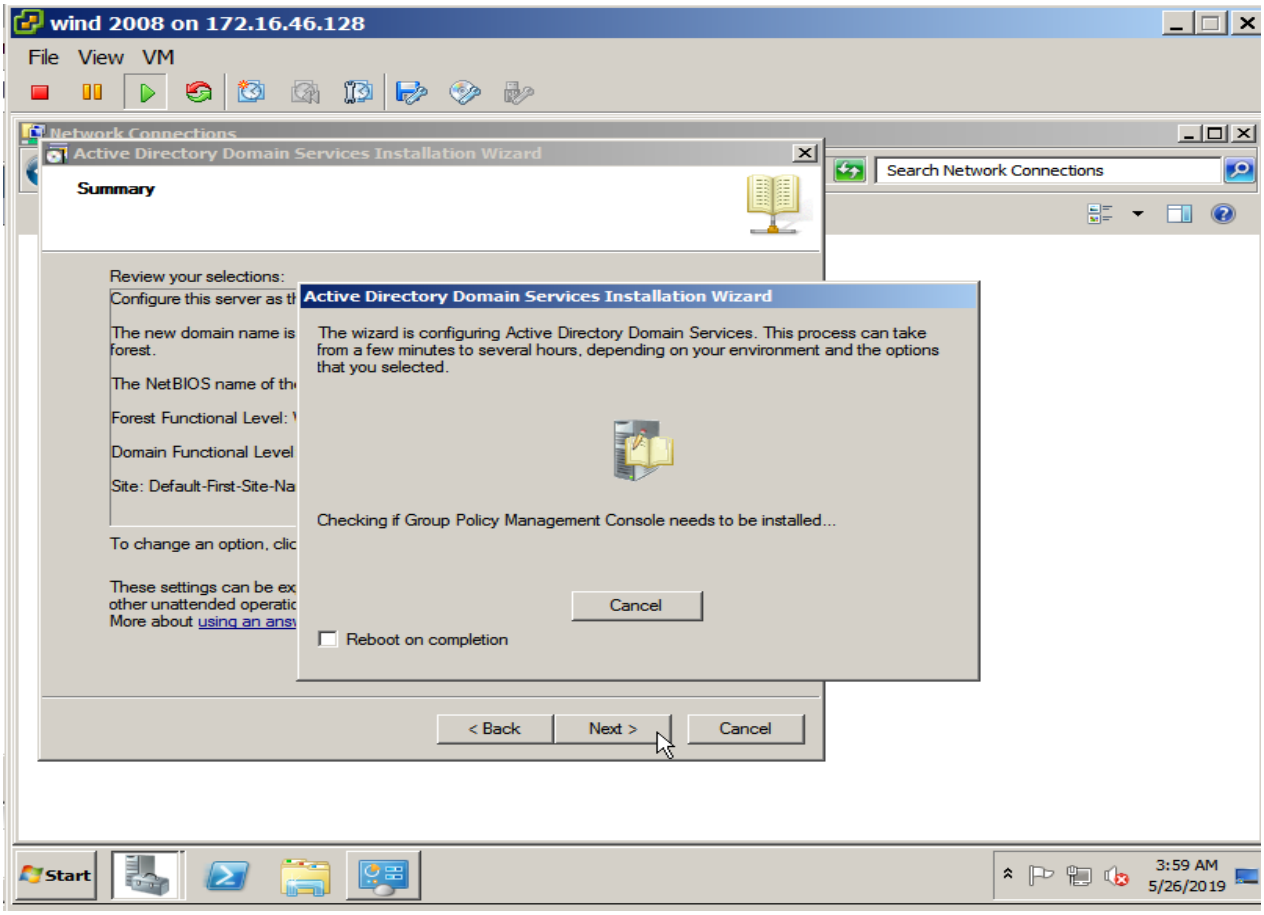
- ✓ After making the IP static, we again come to AD DS wizard and choose the locations for database, log files and SYSVOL.
- ✓ Then click on "Next" button.



- ✓ Now a new window is pop up that will ask to provide password.
- ✓ So, we will assign a strong password for login AD DS as administration account.
- ✓ Now after assigning strong password, click on “Next” button.

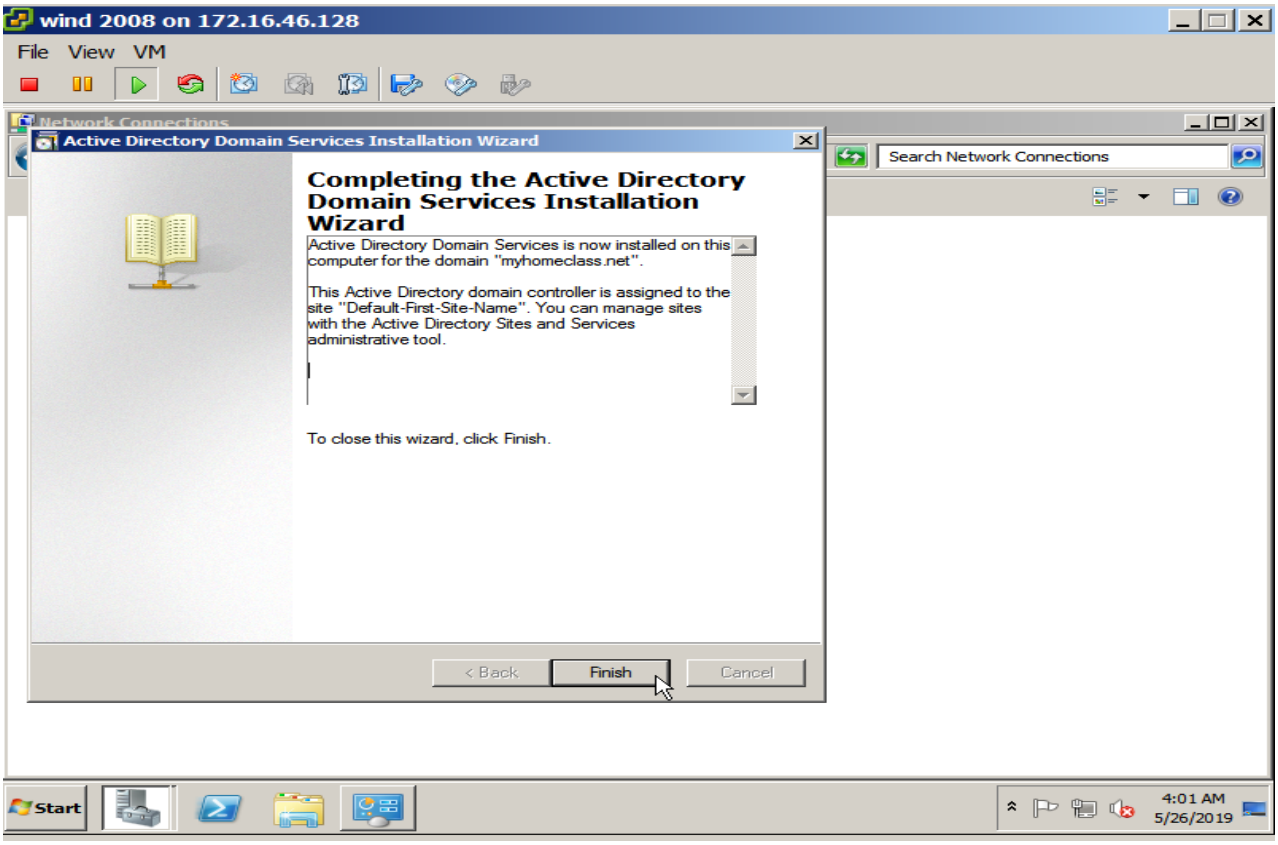


- ✓ After that , new window is pop up that will provide all the summary of our installation.
- ✓ Now we have to click “Next” button .



- ✓ After selecting "Next" button in the previous step a new box is come up .

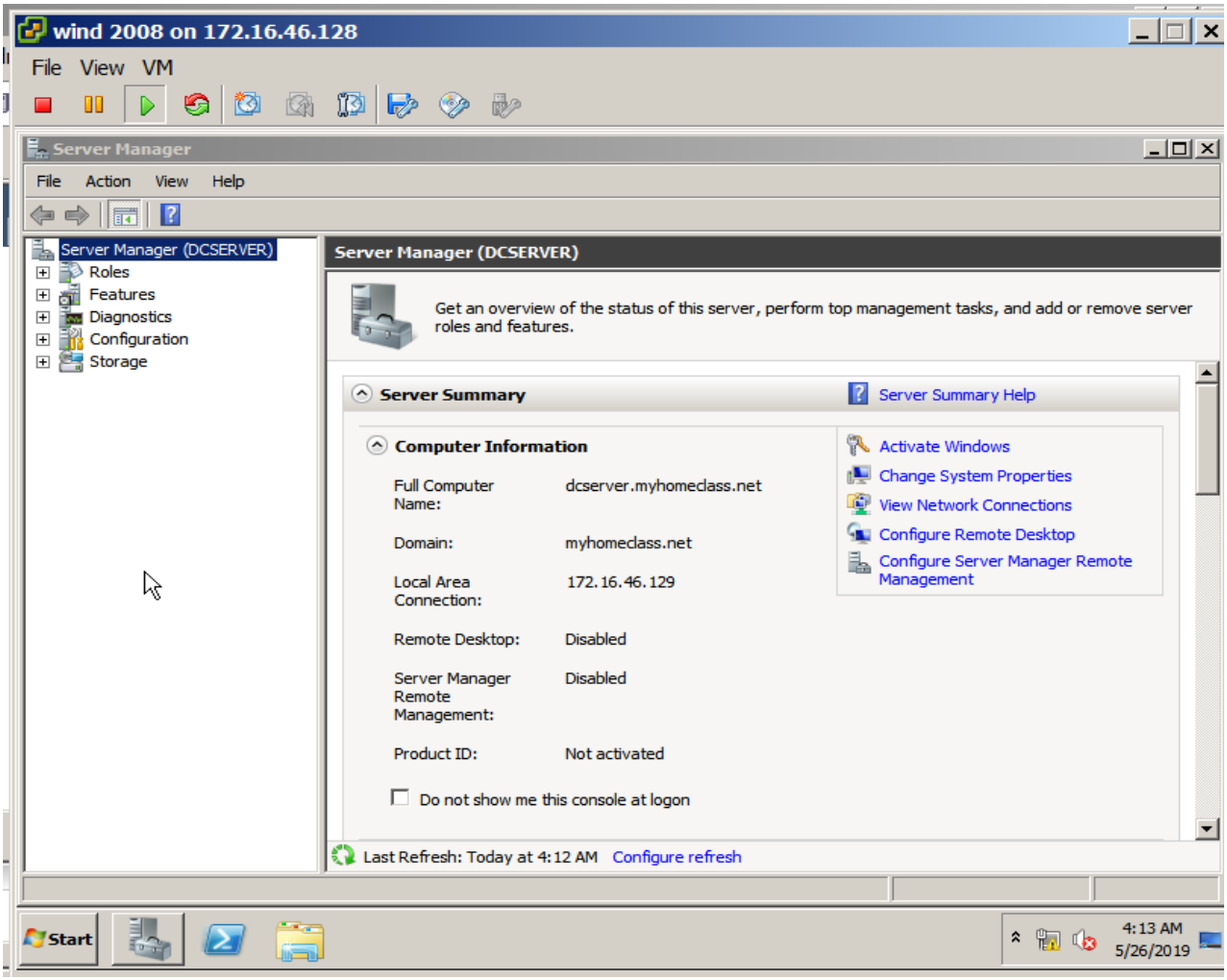
- ✓ This box is giving the message that," the wizard is configuring AD DS" so we have to wait for few minutes .



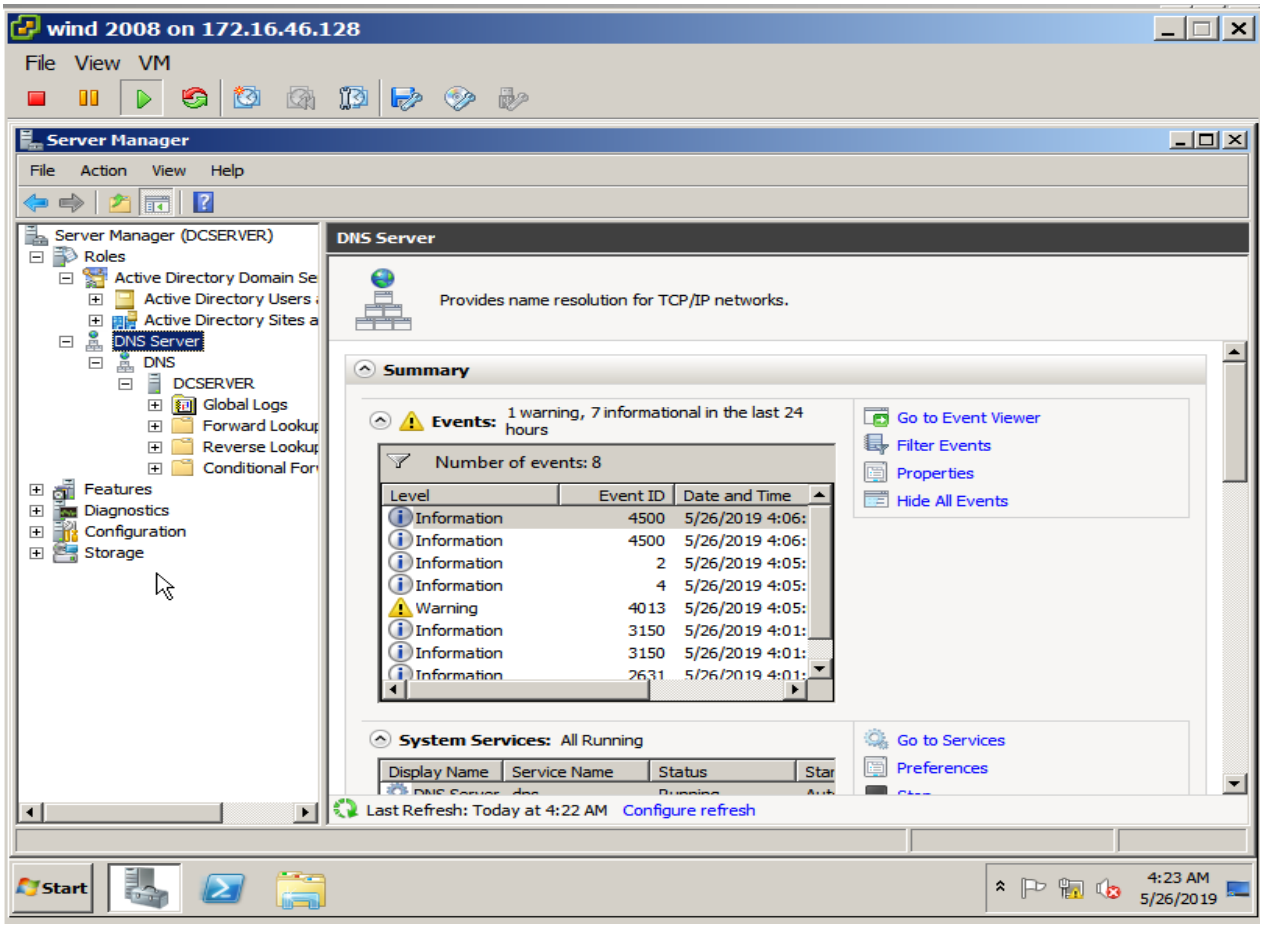
- ✓ A new window pop up that will give information that the installation of AD DS on this computer for the domain "myhomeclass.net" is done successfully .

- ✓ We must have to select "Finish" button now.

- ✓ Now, we have to reboot our Window Server 2008.
- ✓ When the reboot is done, we can see the name MYHOMECLASS/Administrator on the login window.
- ✓ We have to provide the Password and login to the Windows Server 2008.

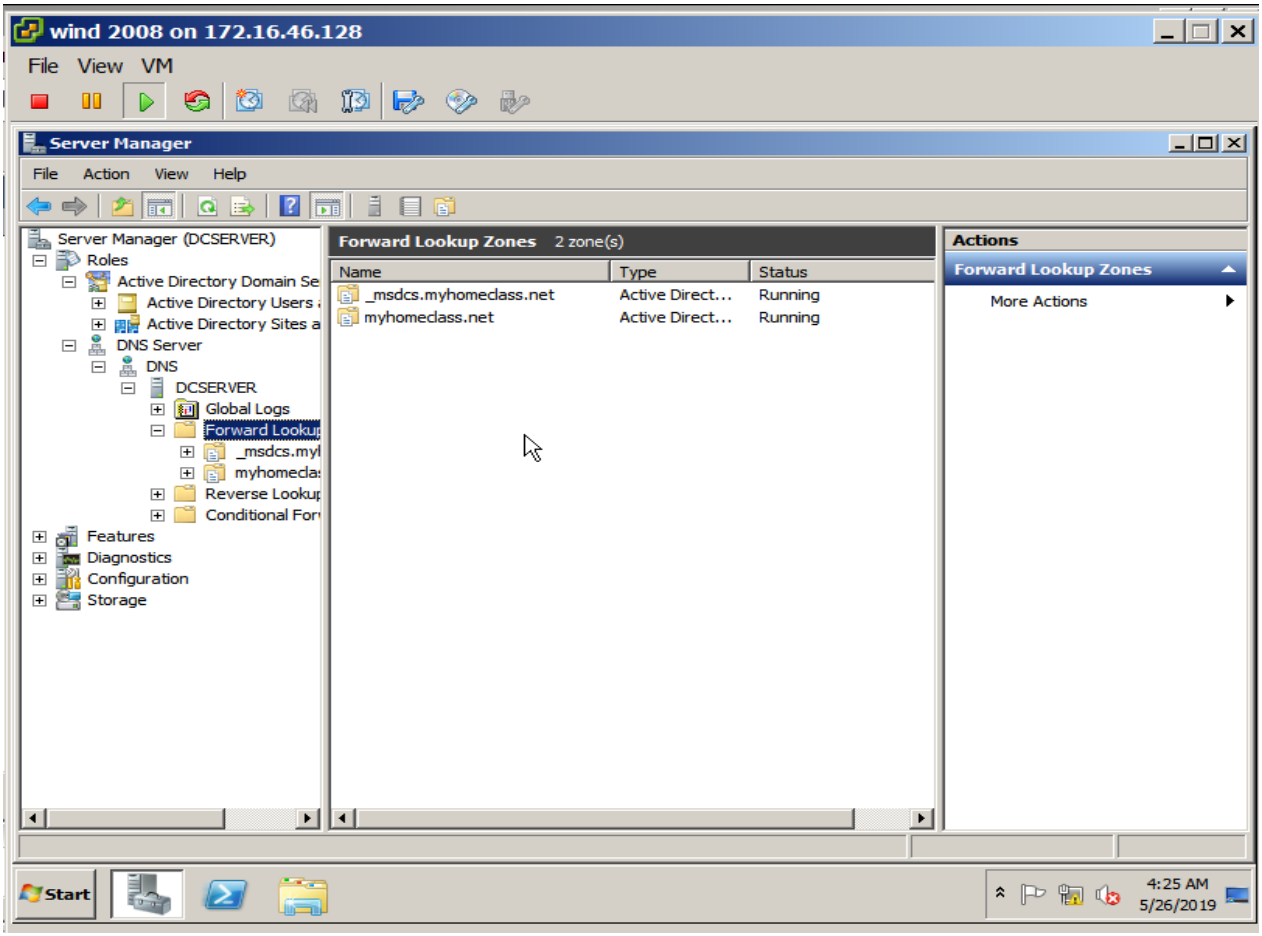


- ✓ After login, we are seeing the Server Manager of our system .
- ✓ Here, we get that our new computer name is dcserver.myhomeclass.net .
- ✓ dcserver.myhomeclass.net is because dcserver is the name of our previous Computer .



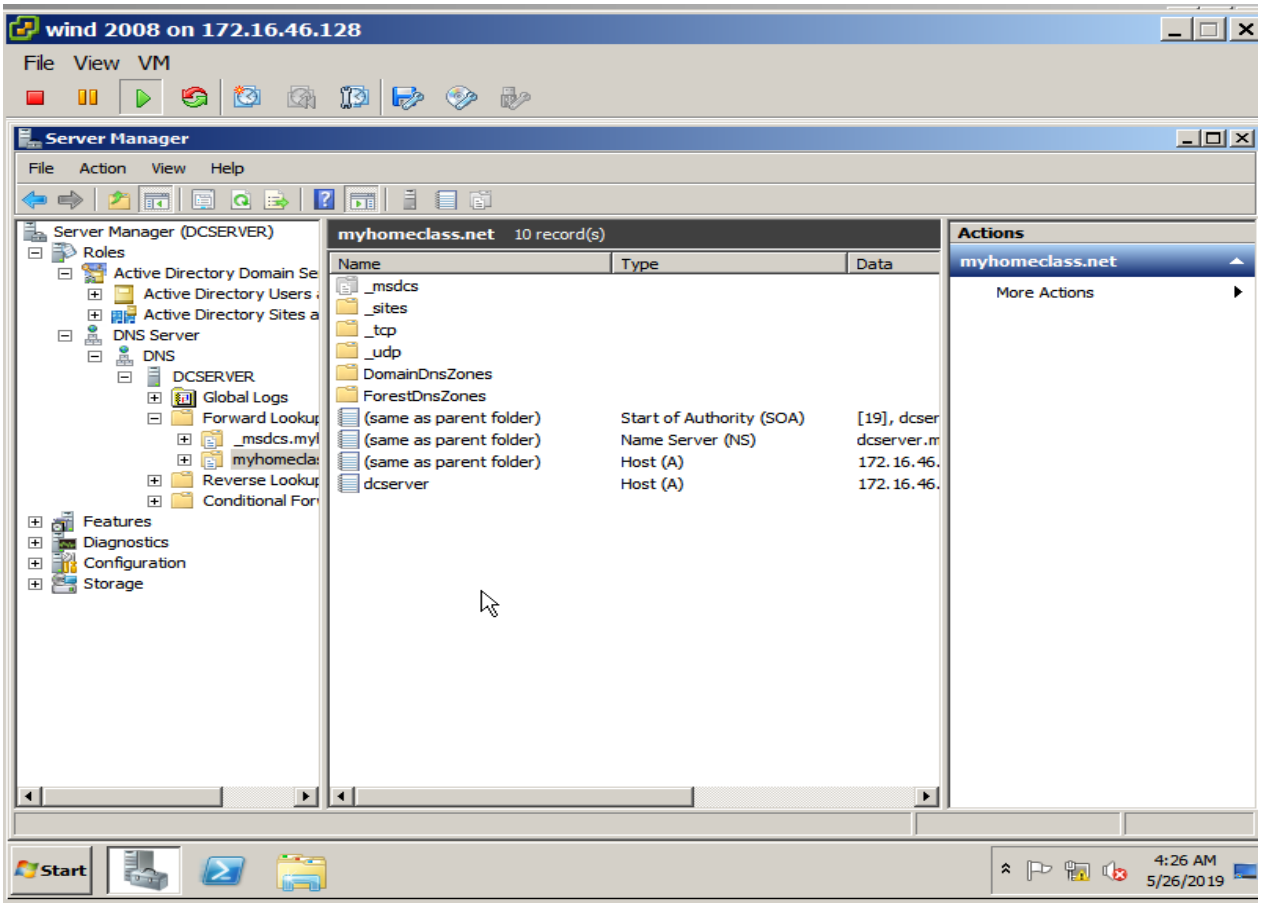
- ✓ Now, we can check our Roles that our DNS server is automatically made.

- ✓ This happens because of the setup that is given by us.



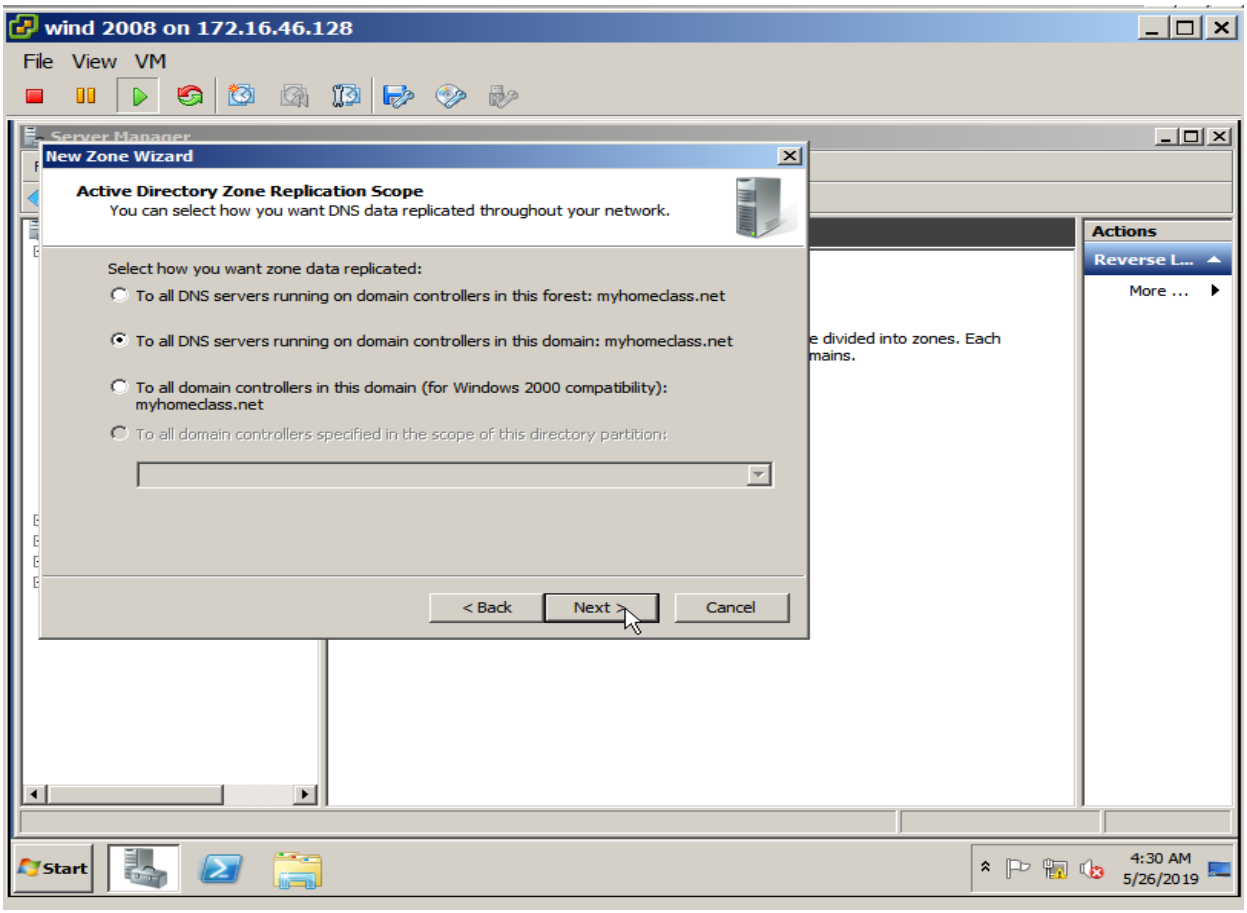
- ✓ When we opens the DCSERVER in DNS, there is an option named "Fixed Lookup Zone".

- ✓ If we double click on it, we can see Active Directory "myhomeclass.net" that is in running state.

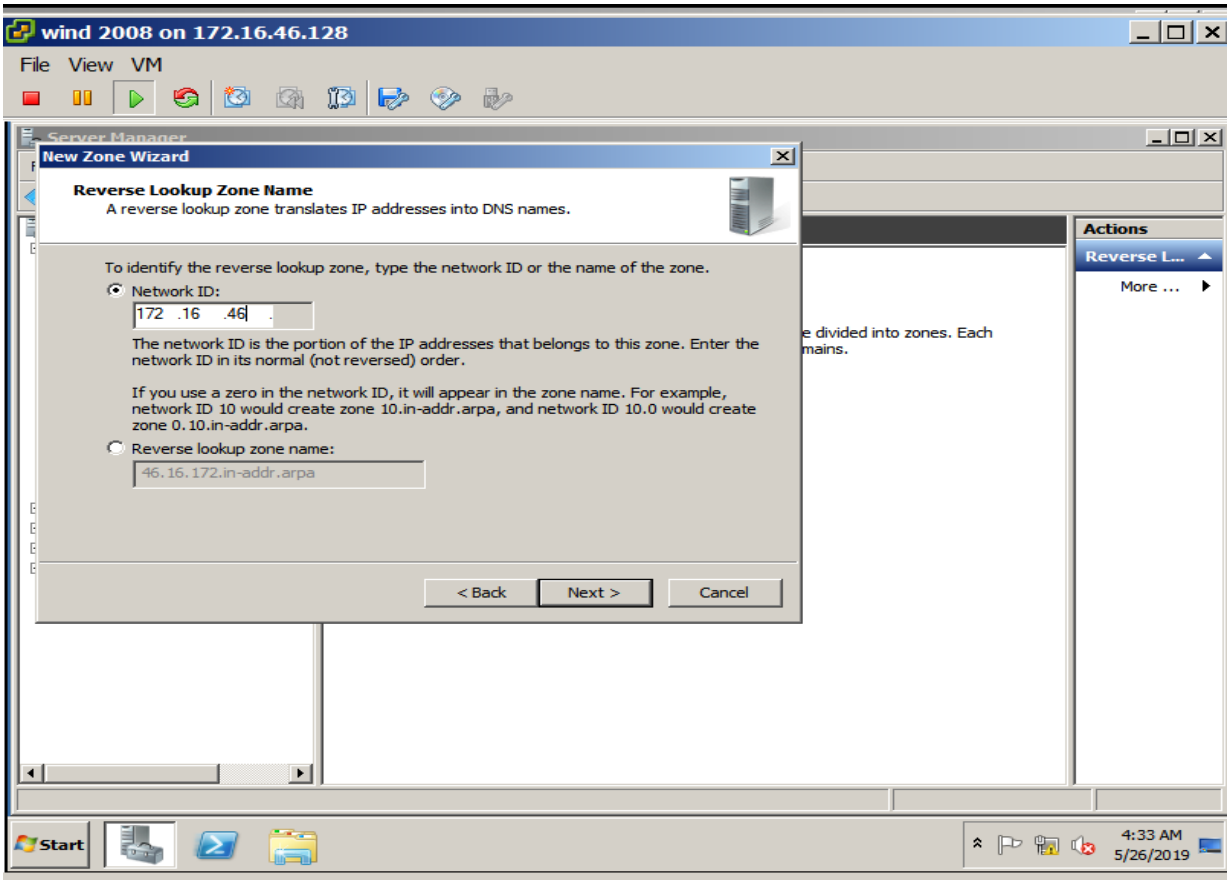


- ✓ If we open double click on the myhomeclass.net, we can see all the hosts.

- ✓ There are 10 records available.

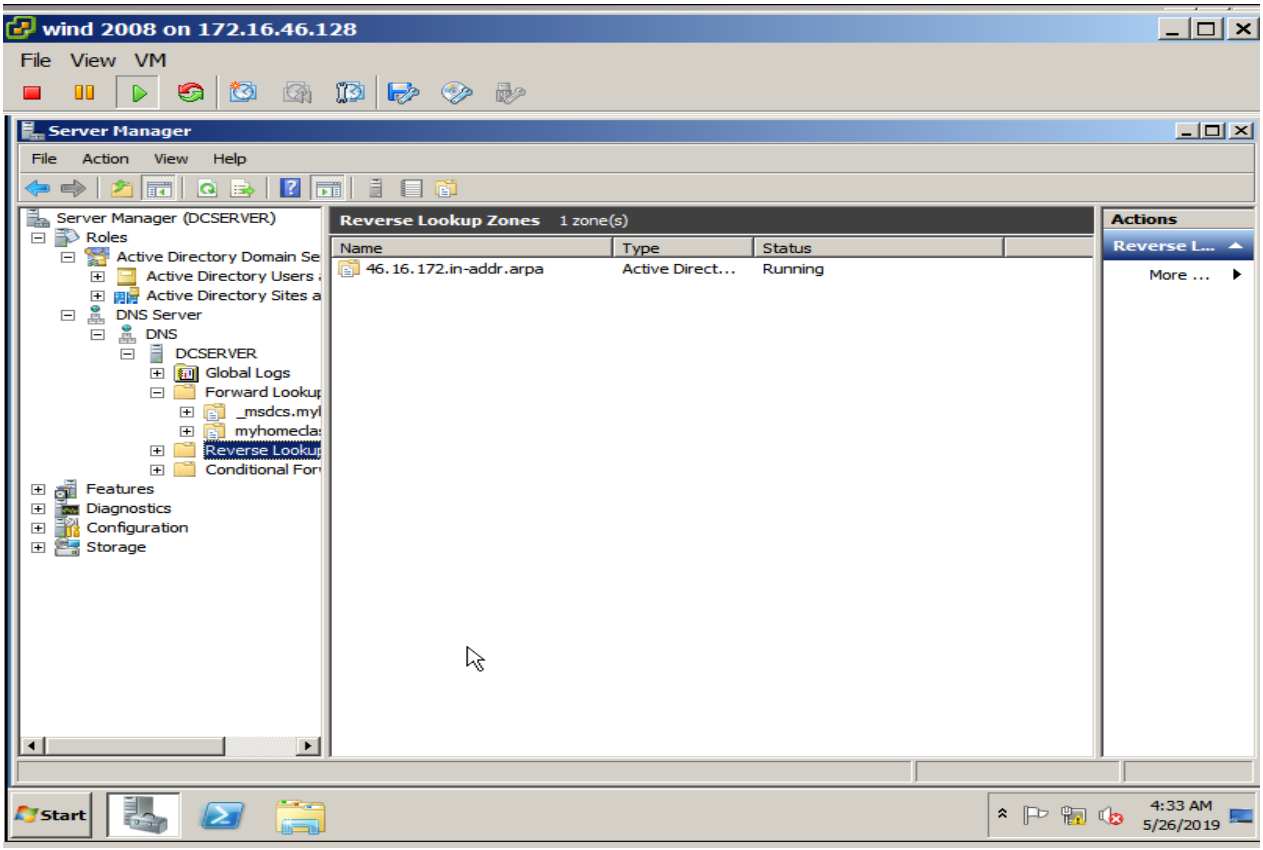


- ✓ Now, we can select how data replicated our Network in Active directory replication zone.
- ✓ Only domain controllers that reside in the Active Directory Domain in which the zone data is stored can host the zone.
- ✓ Here, we can select the "to all DNS servers running in domain controllers in the domain: "myhomeclass.net."
- ✓ After selecting this, click on "Next" button.



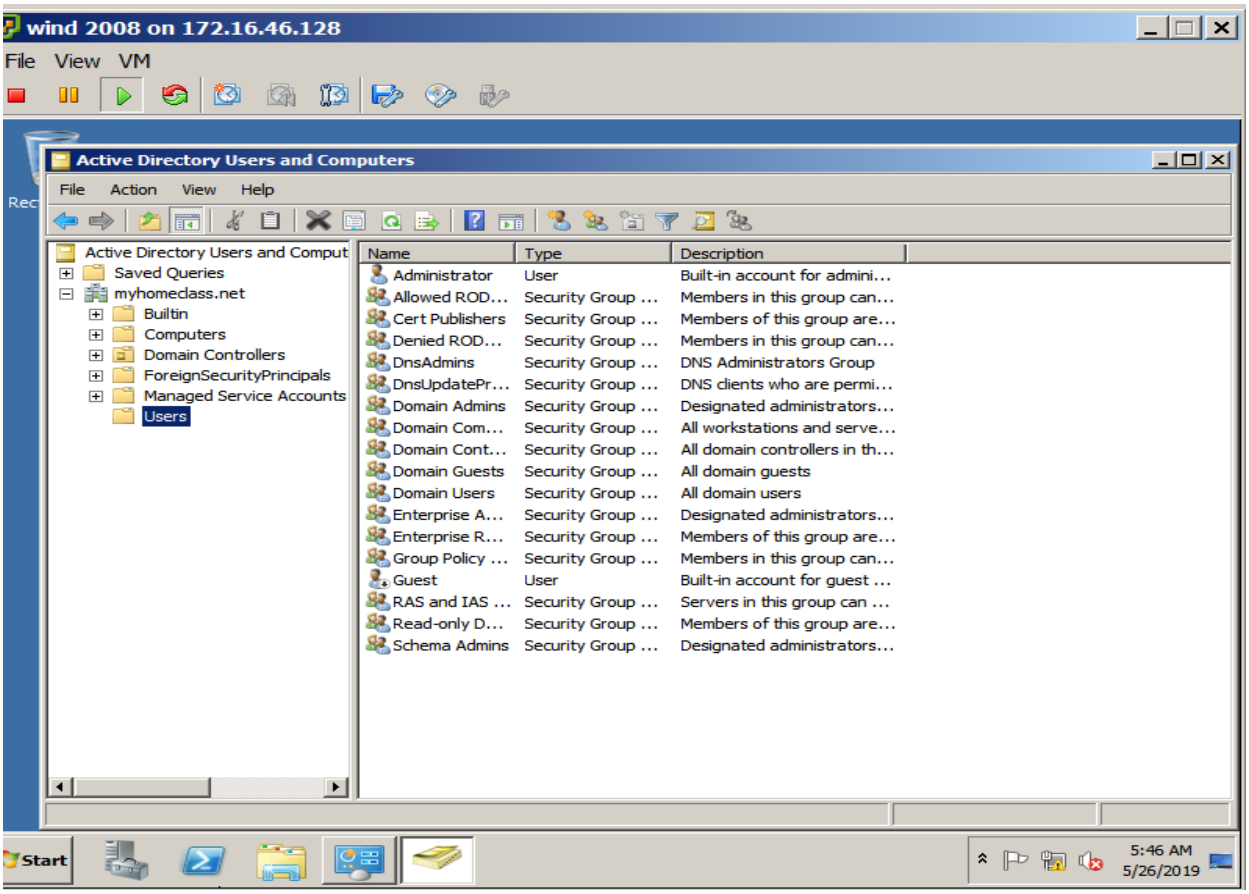
- ✓ In the next wizard, we have to select Network ID option and enter the ID 172.16.46.

- ✓ Then click on the "Next" Button.

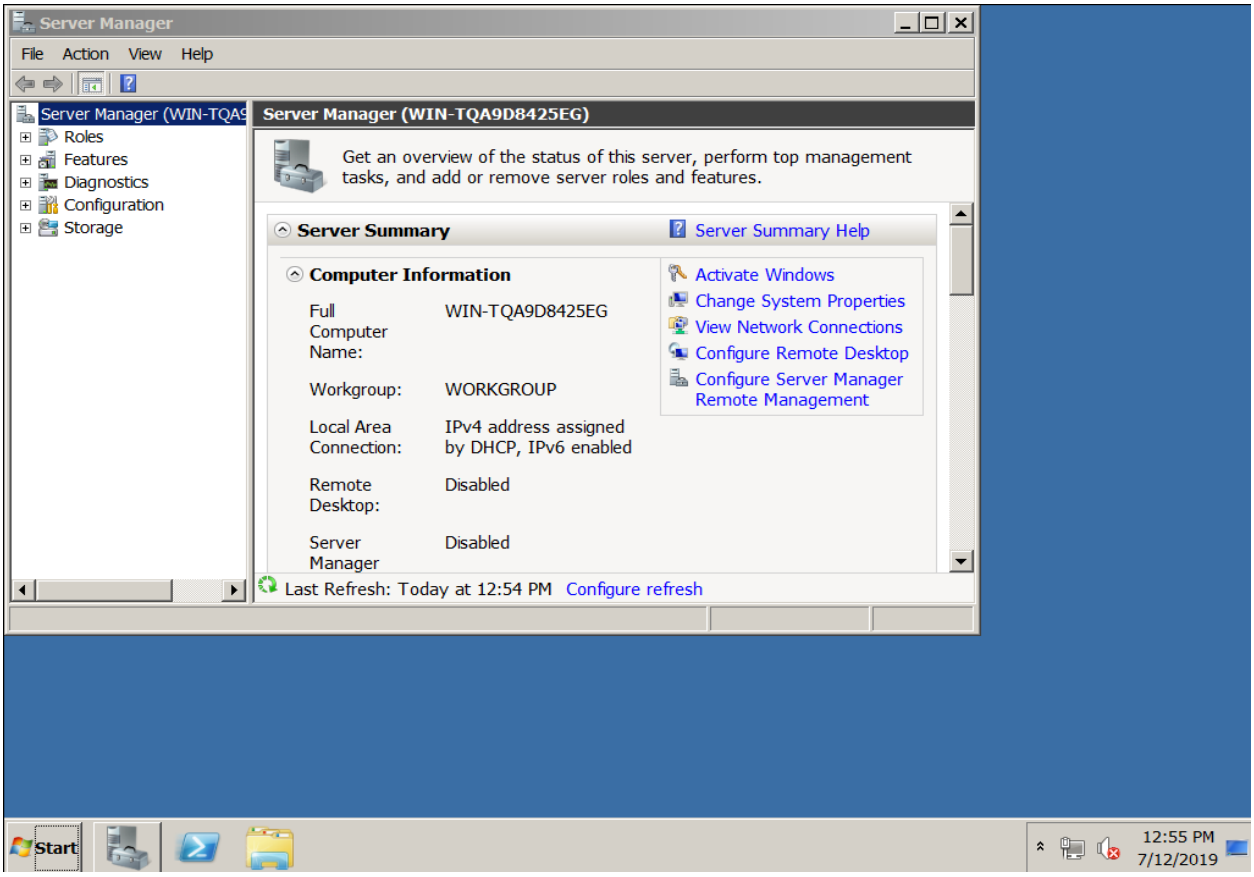


- ✓ Now, after clicking on the "Next "button in the previous step, we are able to see that our reverse lookup zone is ready and we see this in DNS server.

- ✓ Open DCSERVER -> Reverse Lookup to see our IP address.

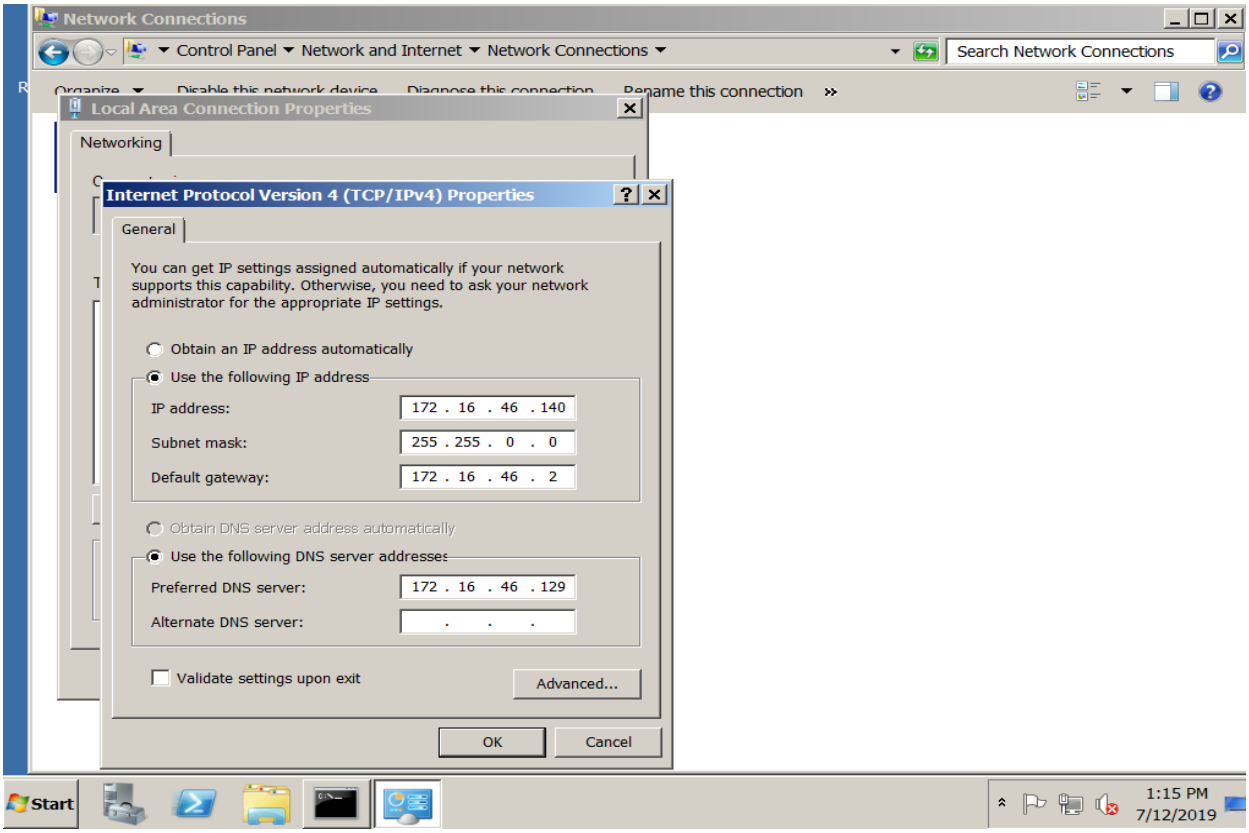


- ✓ Active Directory Users and Computer -> myhomeclass.net -> Users
- ✓ Here, we can see all the users.
- ✓ This is because we have a Read Write Domain.

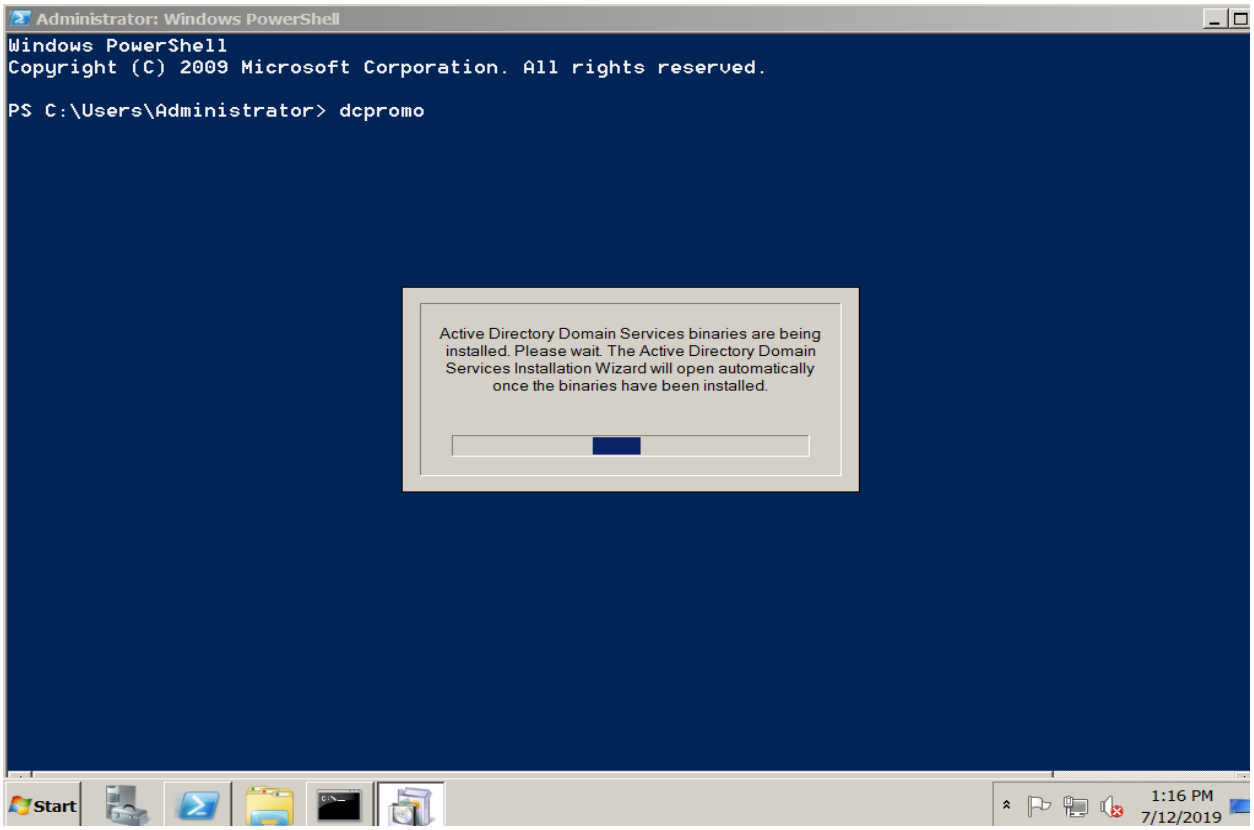


- ✓ Now, at our workstation we make a client.

- ✓ Then, we will set this client as the Domain Controller with the help of our Server.

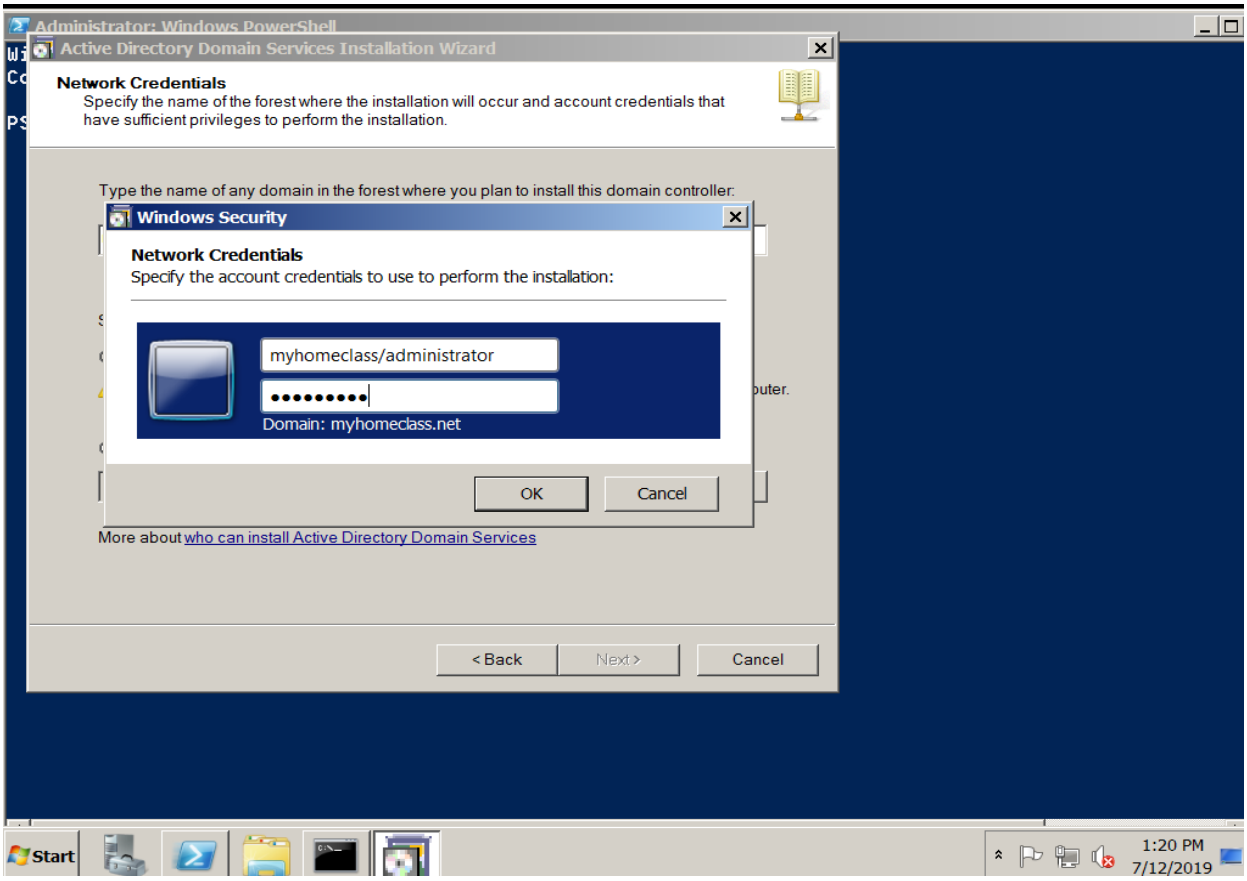


- ✓ Here, we are giving a static IP address to our client.
- ✓ Since, we have already the IP of the DNS Server so we will provide that IP to the Client so that we can remotely access to the client.
- ✓ We are setting up the IP address: 172.16.46.140 and other data and click on "OK".



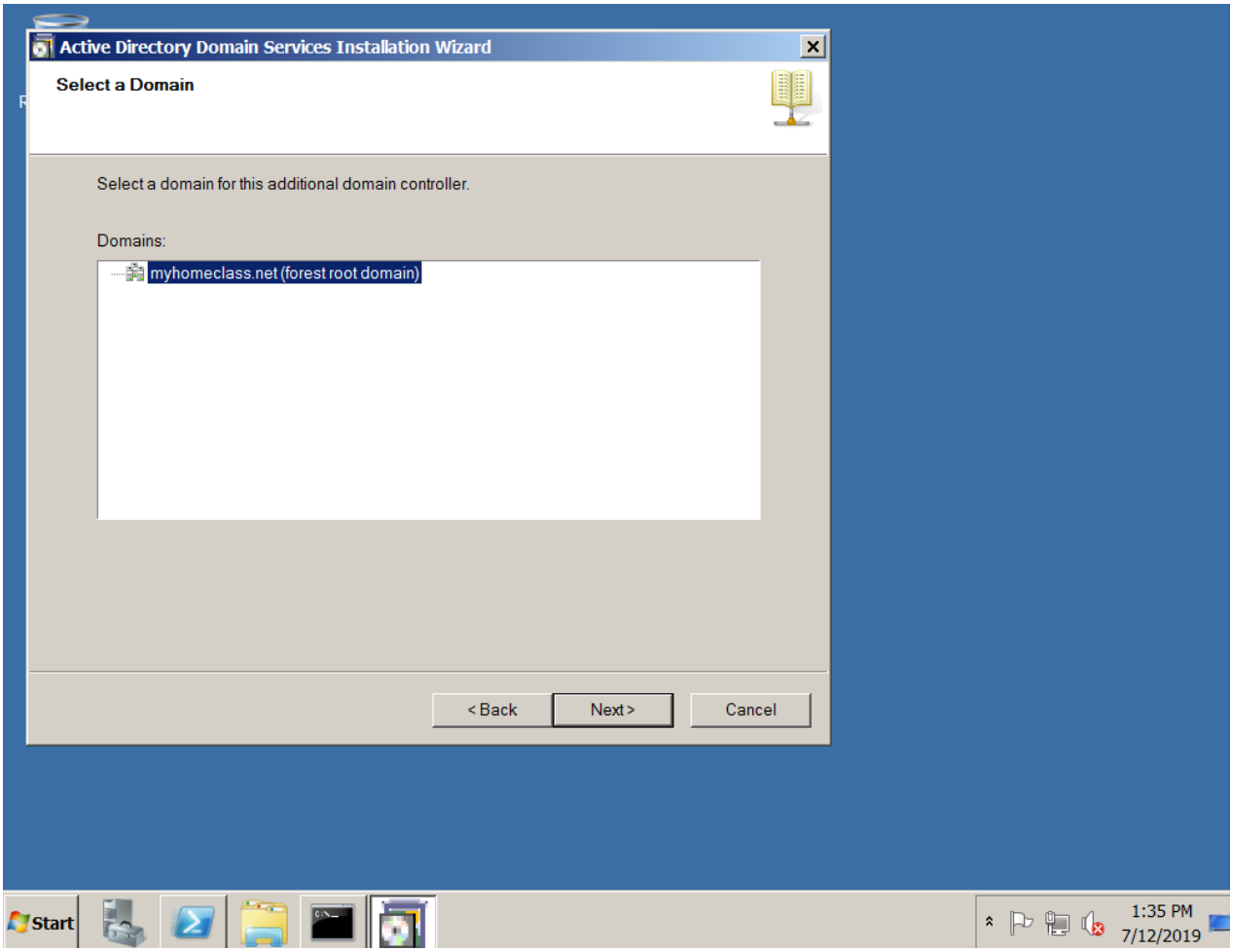
- ✓ Now, we can open Windows PowerShell and run dcpromo.

- ✓ After running dcpromo, a new box comes up that is showing that AD DS binaries are being installed. Please Wait.



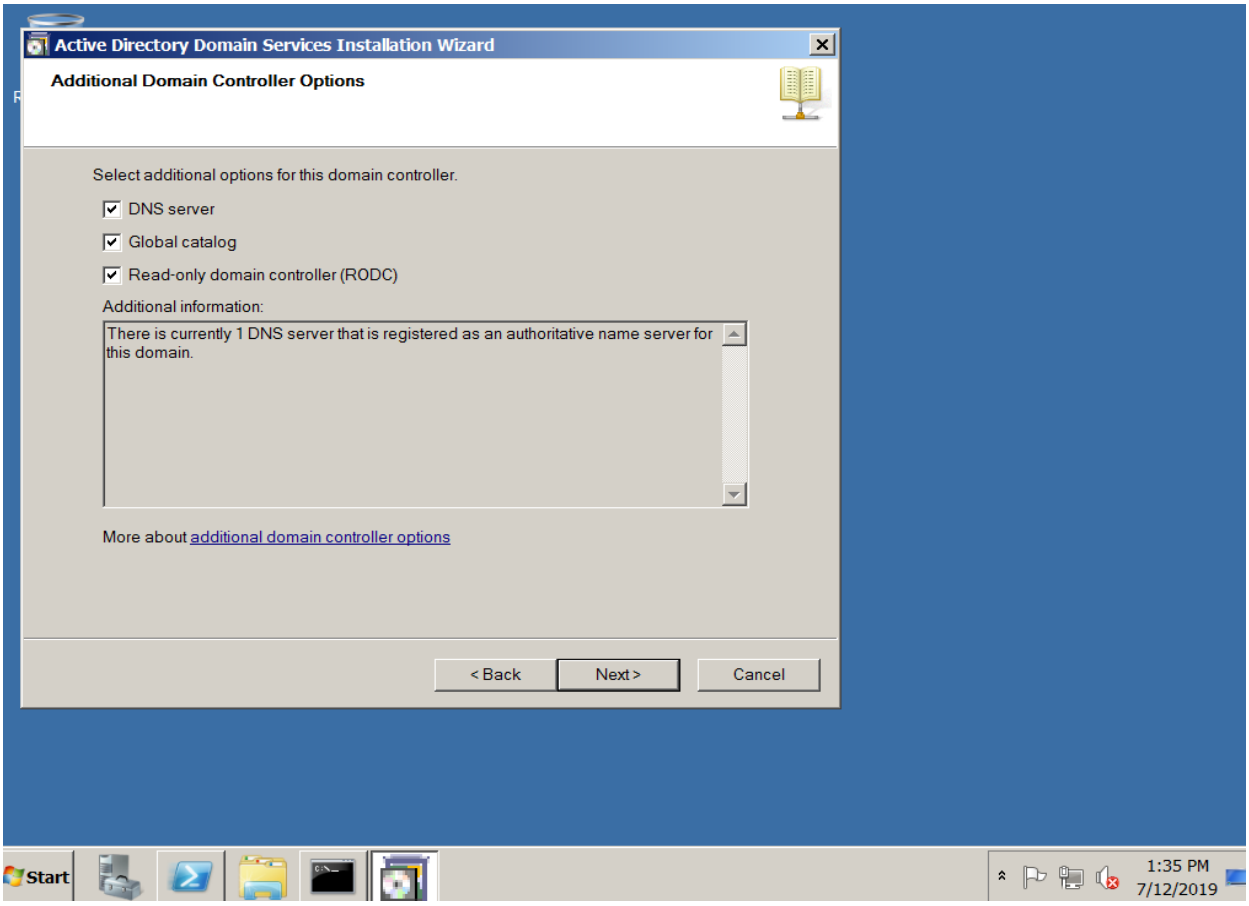
- ✓ Now, we will provide the account credentials to use to perform the installation.

- ✓ After providing the necessary credentials, click on “OK”.



- ✓ In the very next step, select the domain "myhomeclass.net (forest root domain)".

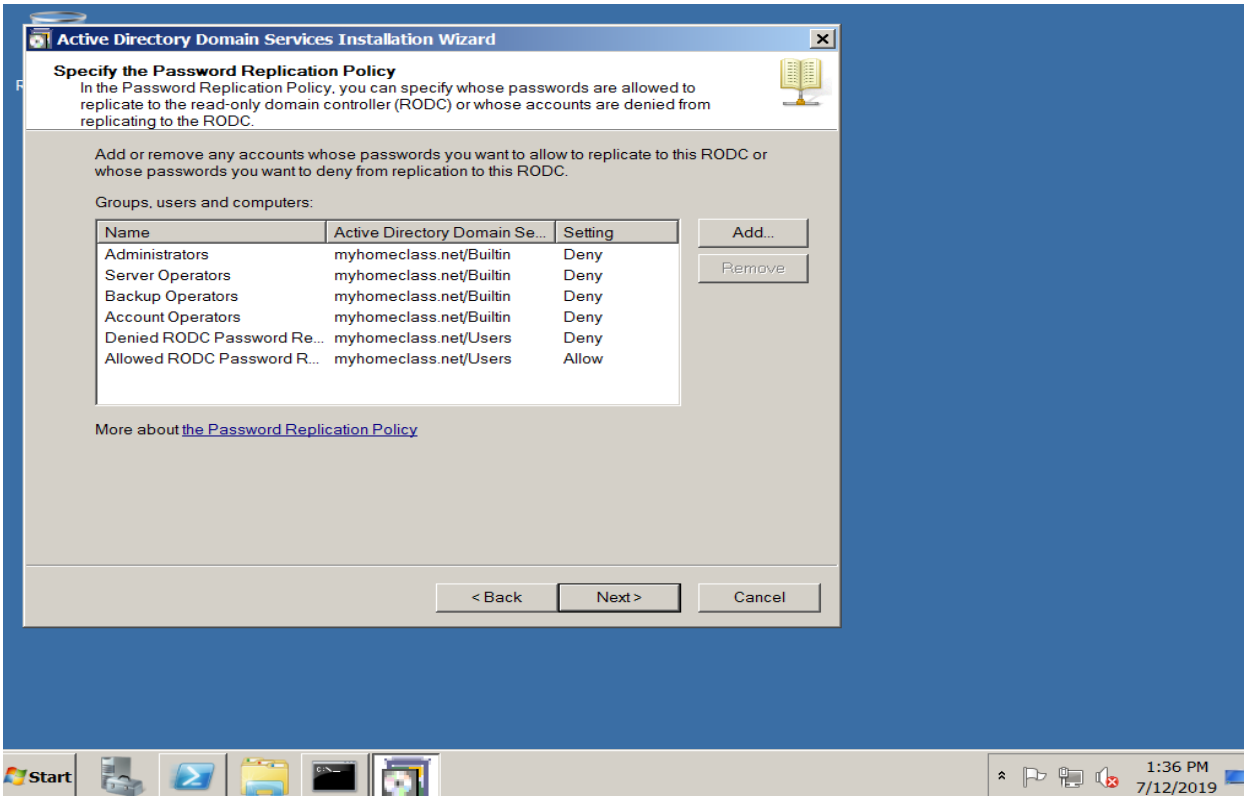
- ✓ After selecting the only domain, click on the "Next" button.



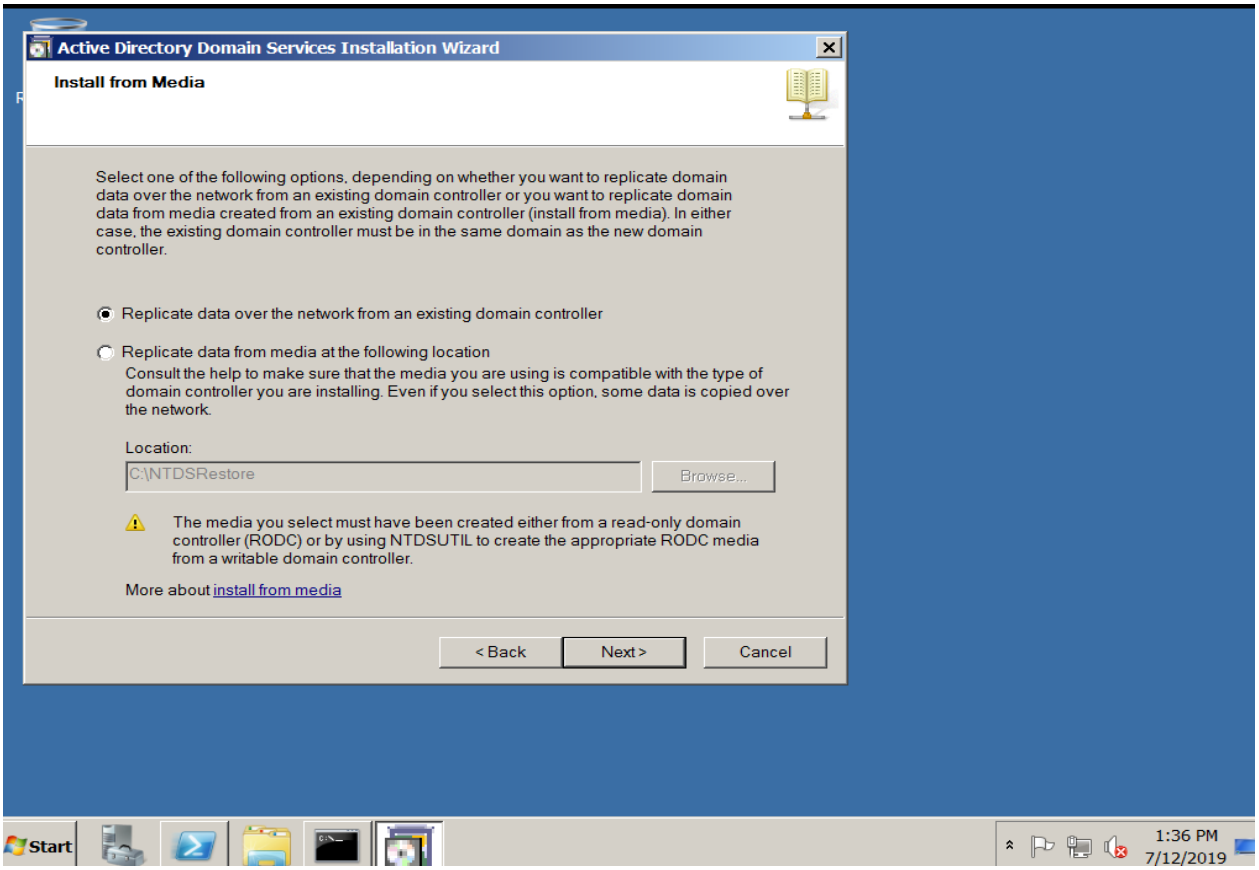
- ✓ In the AD DS Installation Wizard, we get the additional options for this domain controller.

- ✓ After selecting all the three additional options; DNS server, Global catalog and RODC.

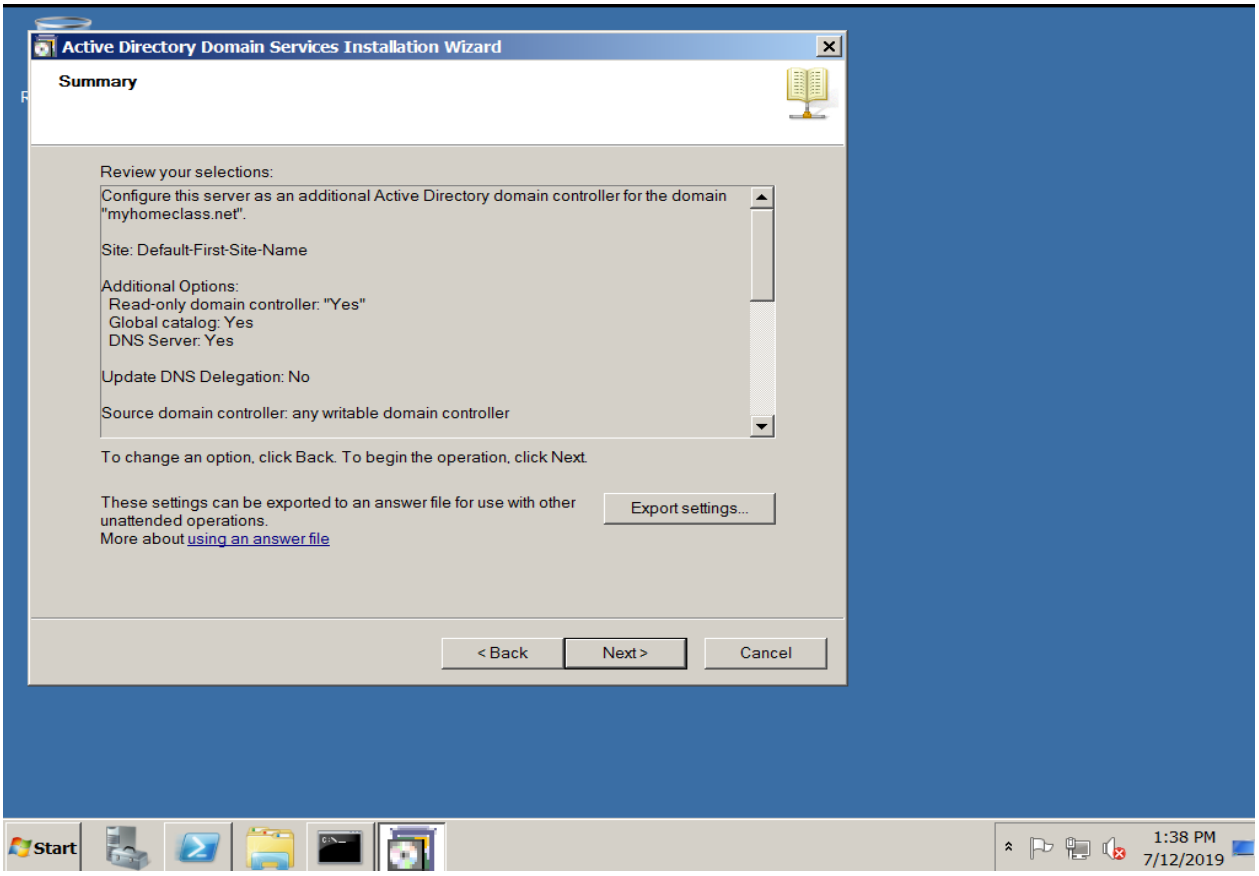
- ✓ Click the “Next” button.



- ✓ After clicking the “Next” button in the previous step, a new wizard comes up.
- ✓ This window can provide you to add or Remove any accounts whose passwords you want to allow/deny to this RODC.
- ✓ If you do not want any change click on the ”Next” button.

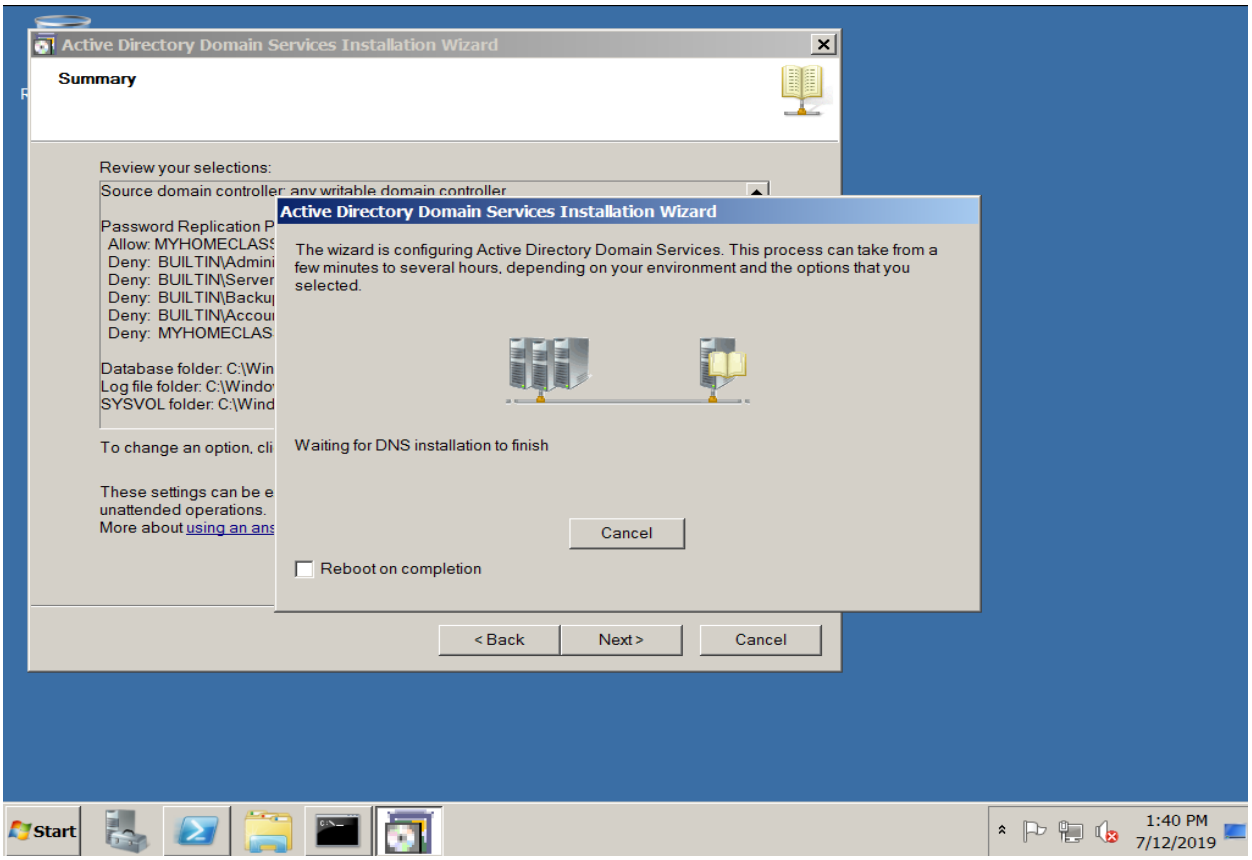


- ✓ After that the new windows comes up which let you to select either Replicate data over the network from an existing domain controller or Replicate data from media at the following location.
- ✓ We are selecting the first one.
- ✓ Location is automatically defined.
- ✓ After selecting click on the “Next” button.



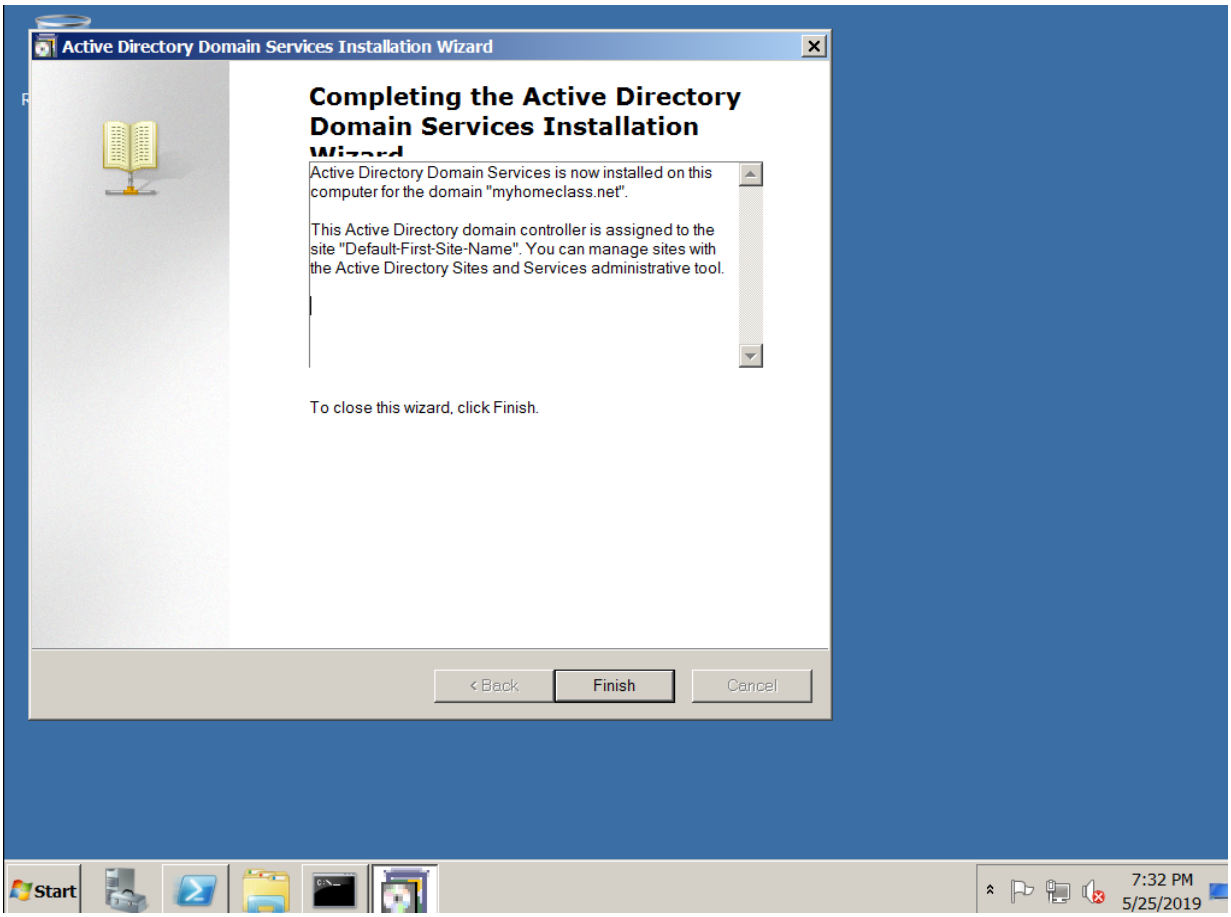
- ✓ In the next window, we get the full summary of our selections.

- ✓ We have to review it and select the “Next “option to move further.



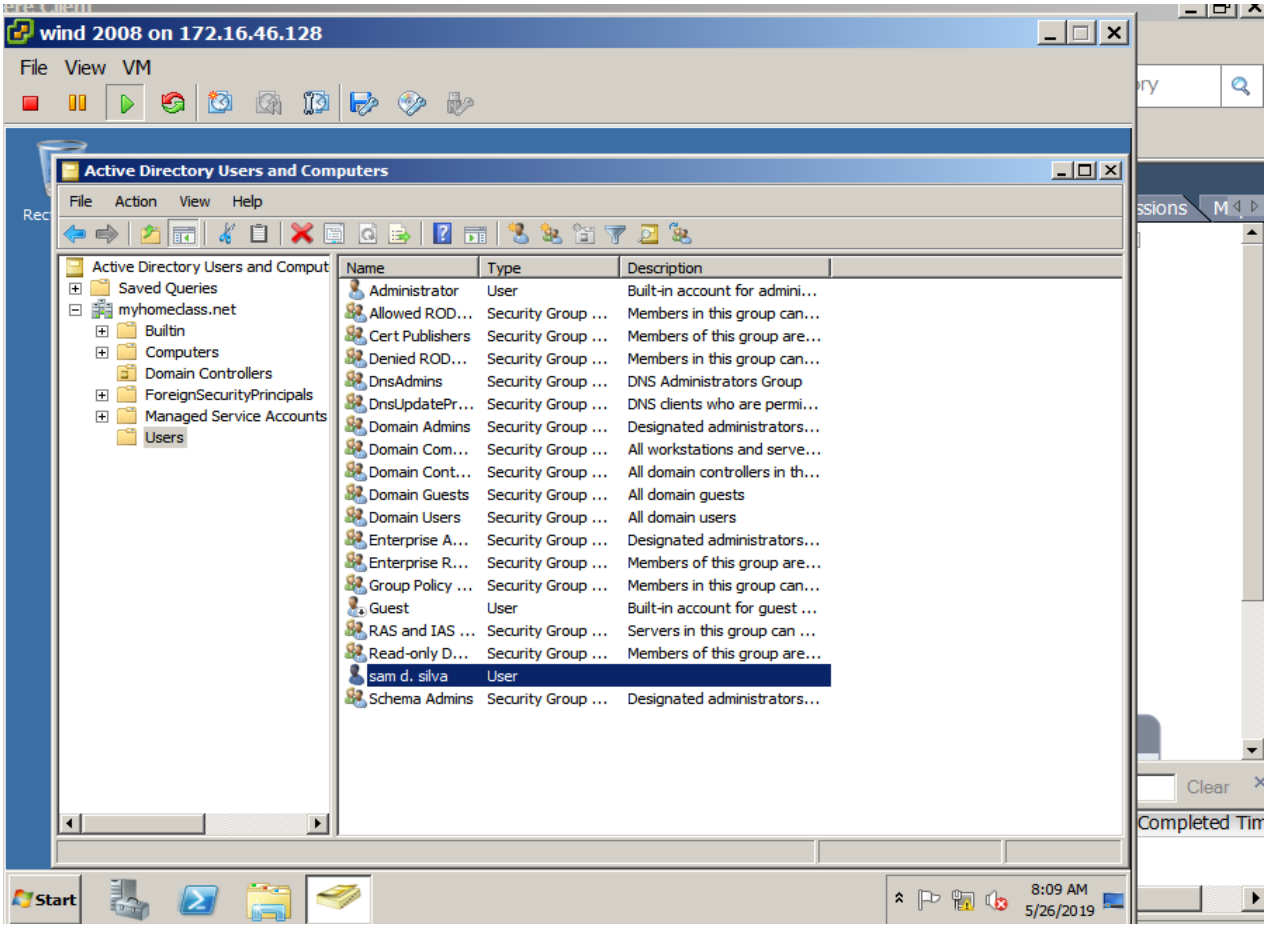
- ✓ After selecting the "Next" button in our previous step, wait for the DNS installation to be finish.

- ✓ This wizard is configuring AD DS.



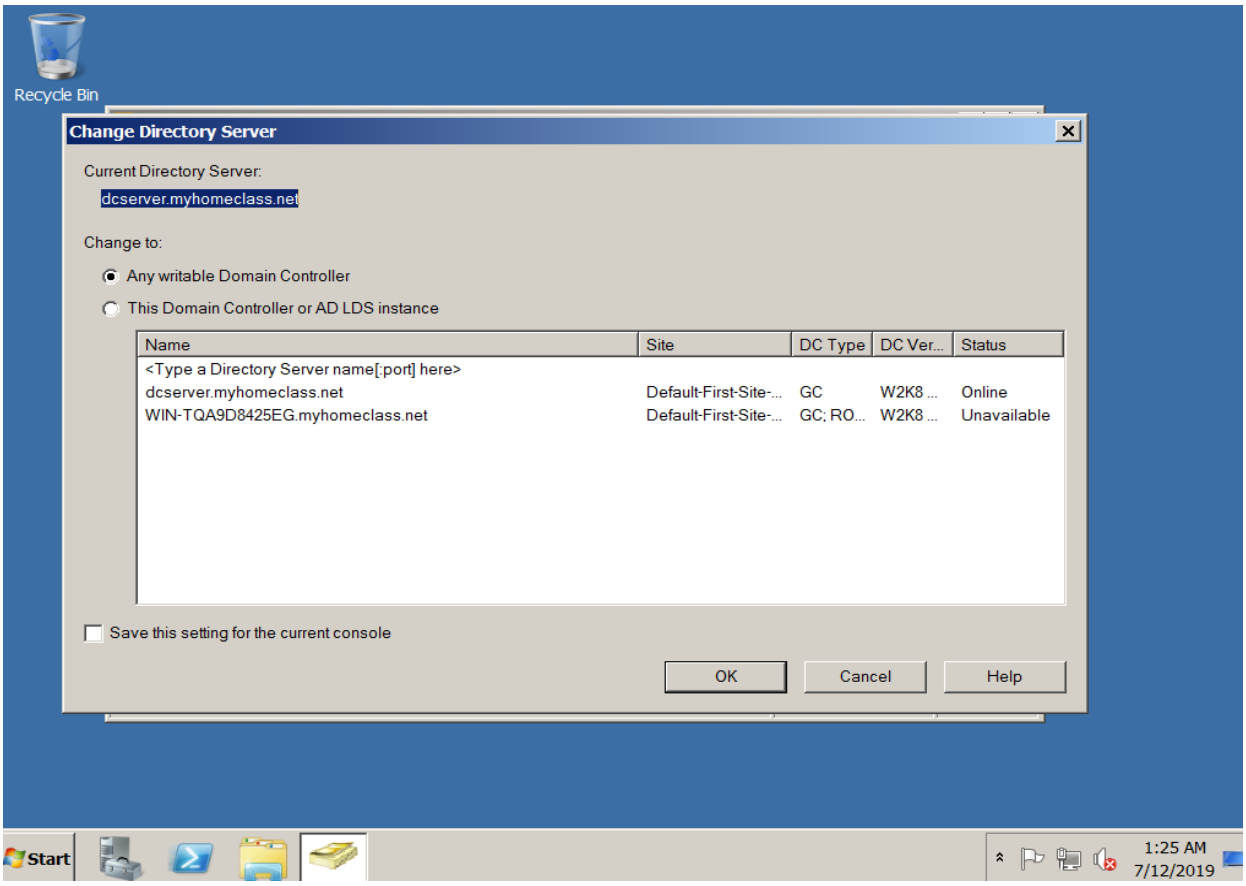
- ✓ After the successful installation , the Installation completing wizard is pop up.

- ✓ We must have to click “Finish” button now.

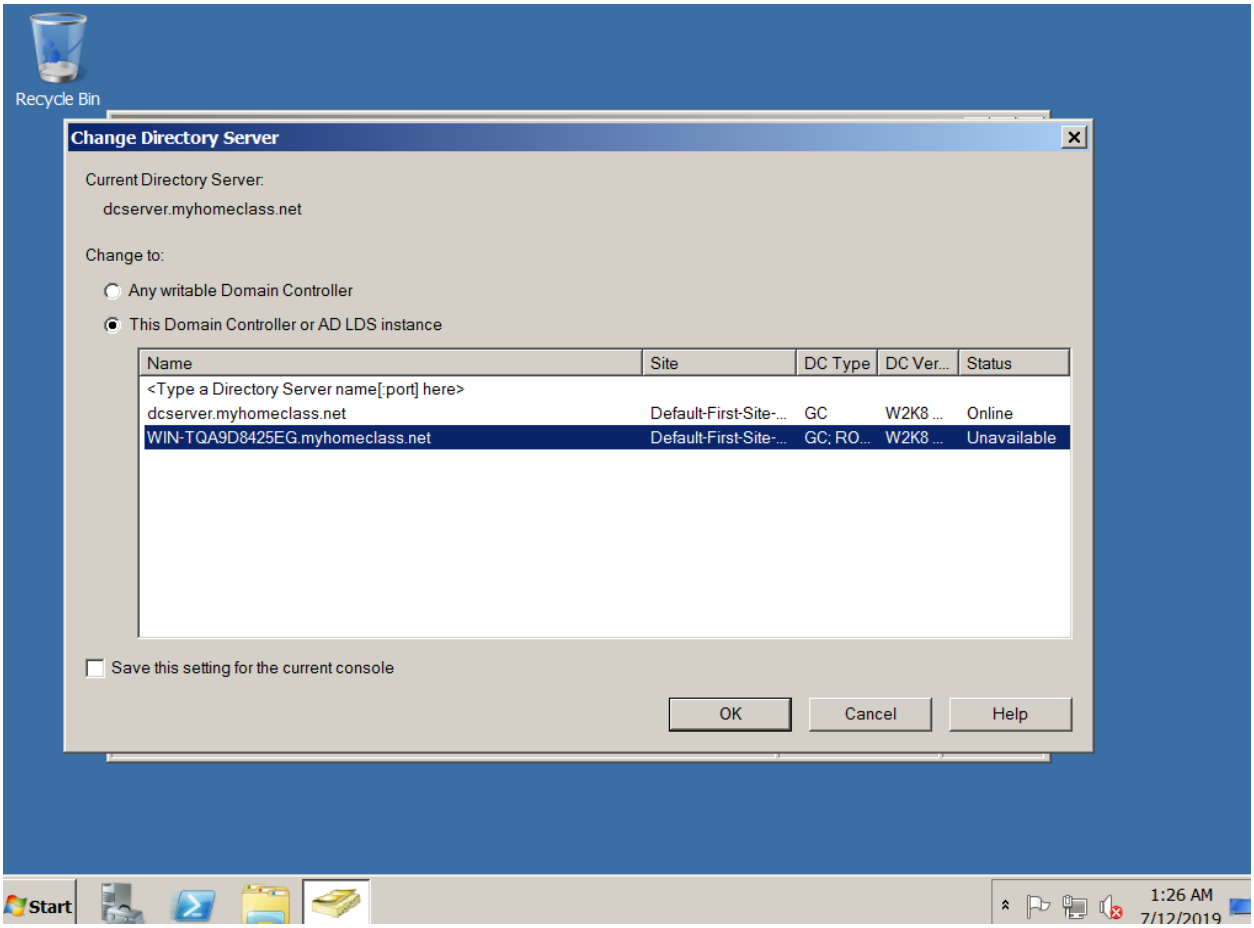


- ✓ Now, AD Users and Computers -> myhomeclass.net -> Users(Double Click)

- ✓ We are able to see all the users.

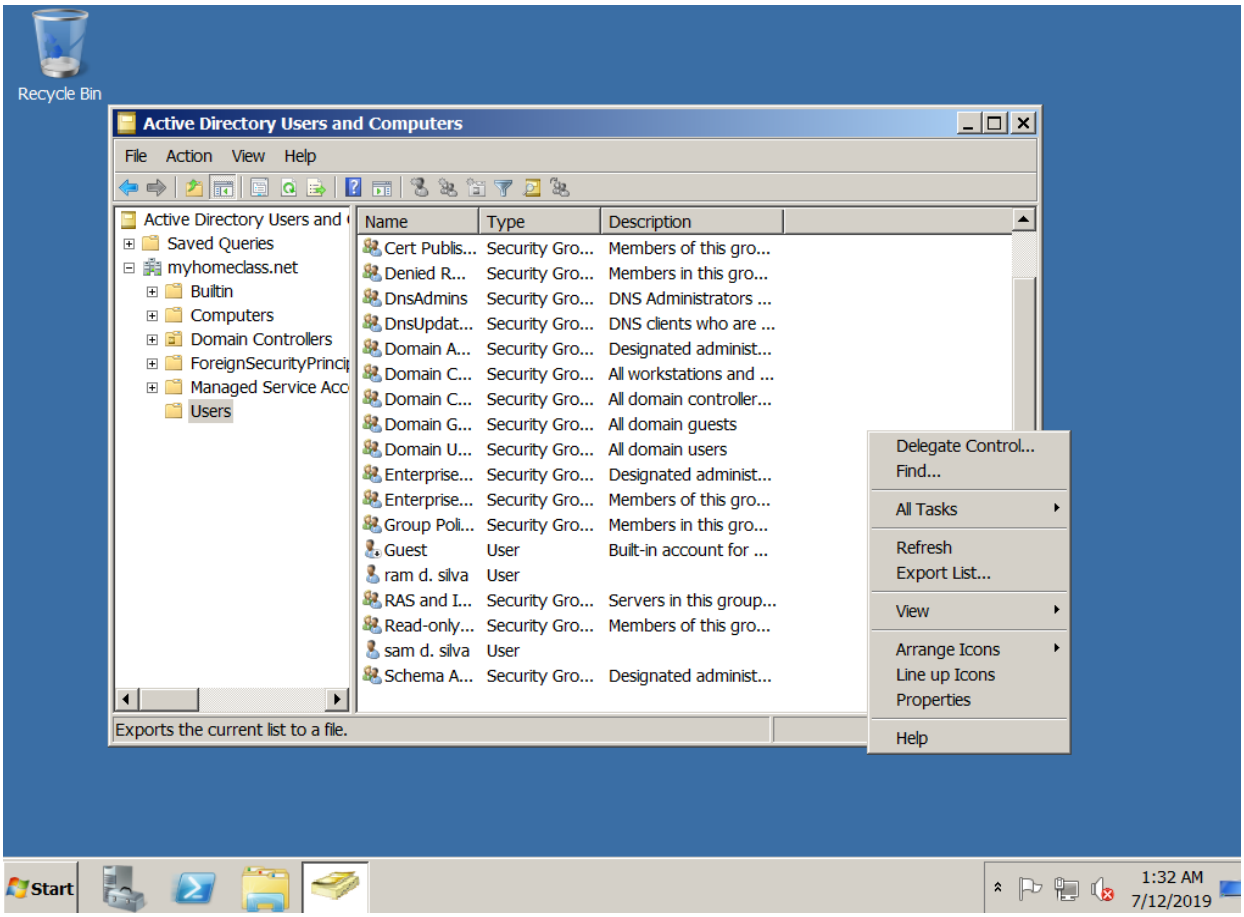


- ✓ This is our client screen.
- ✓ We can change directory server or read write or read only domain here.
- ✓ Because it contains one server of domain and one server of client.



- ✓ Now, we are choosing the second one i.e. This Domain Controller or AD LDS instance.

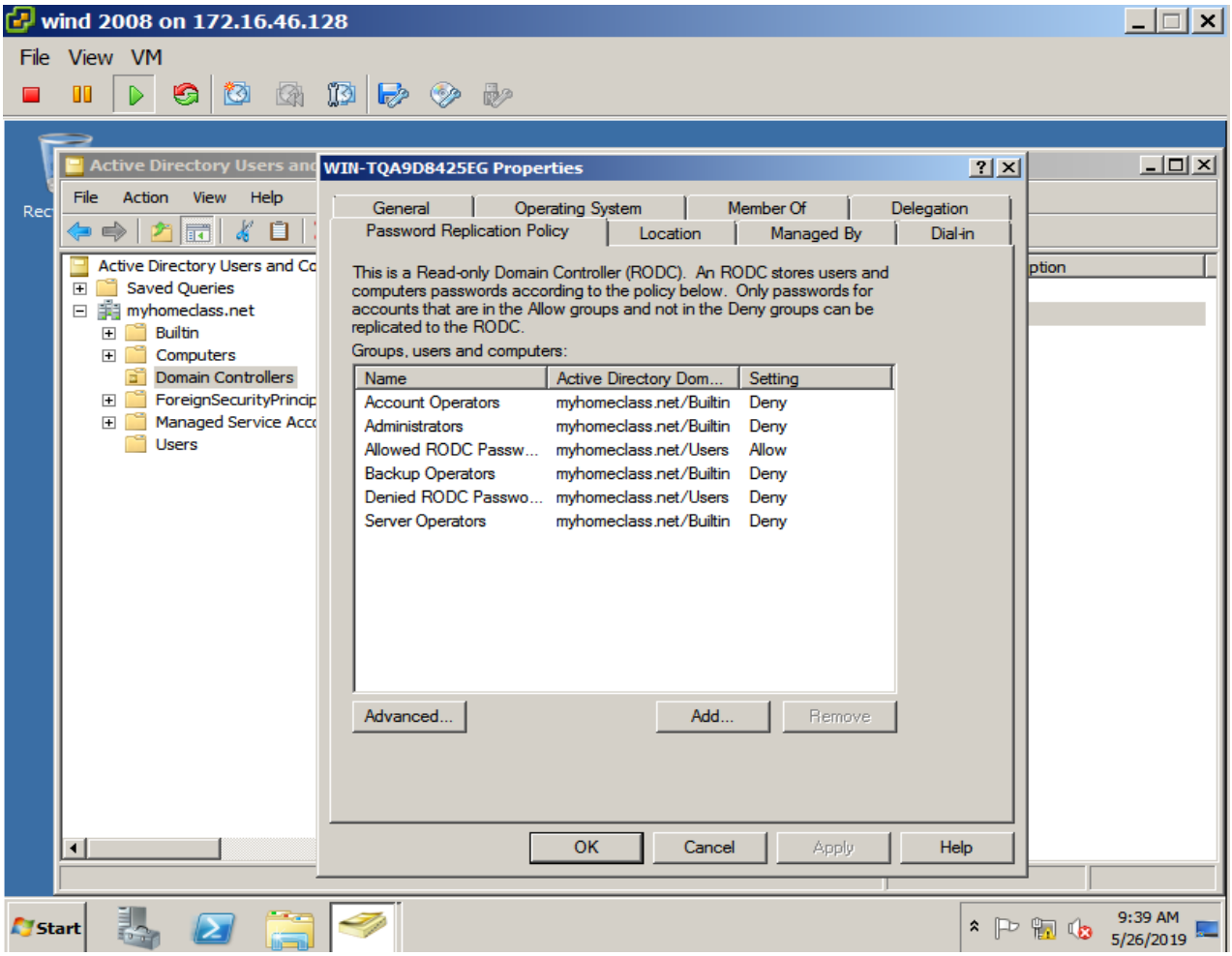
- ✓ And Click on the "Save Setting for this current console" for avoiding to changing the client in future.



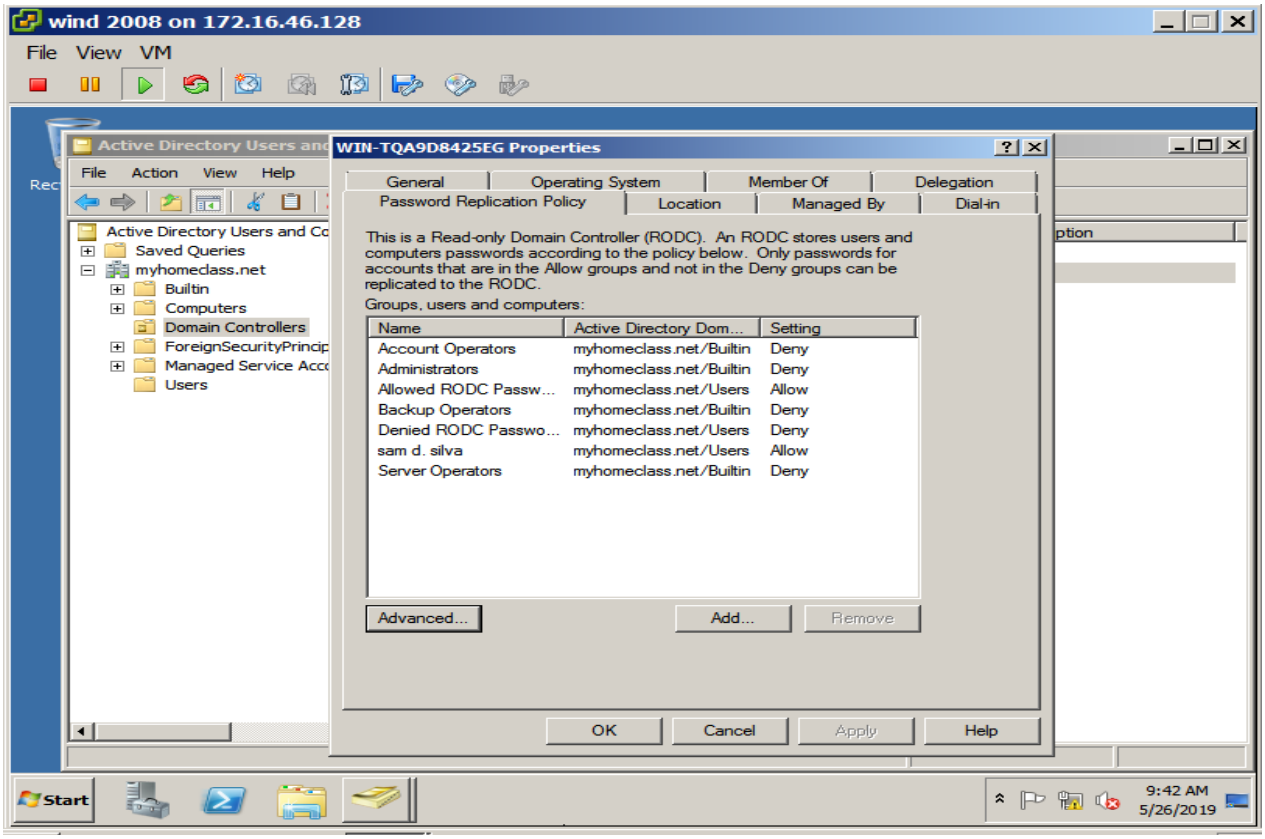
- ✓ Now, at our client side we can open AD Users and Computer and click the right button of mouse.

- ✓ After clicking, we can see that there is no new option available. This means that it is RODC.

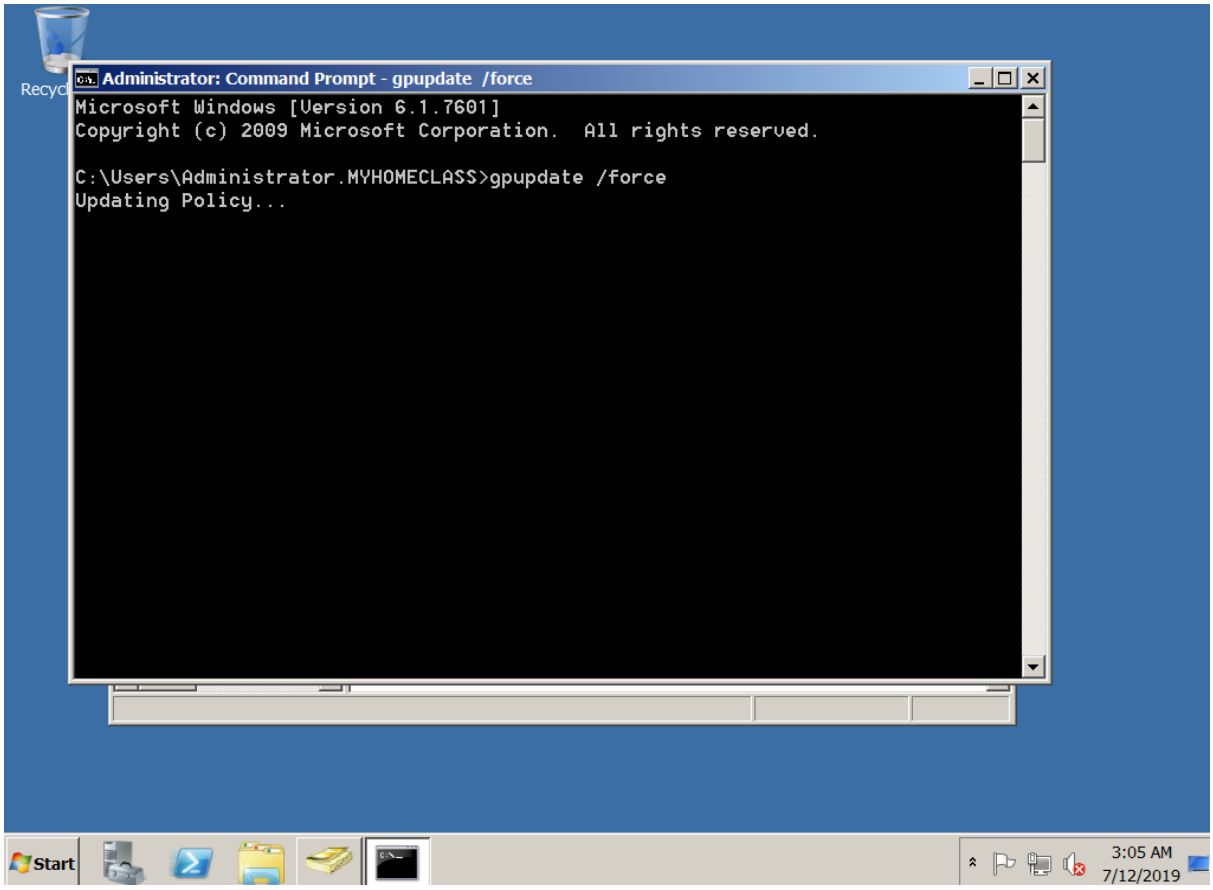
- ✓ So, this will not make any new users, you are only allowed to read.



- ✓ Now when we open Windows server AD Users and Computer -> myhomeclass.net -> Domain Controller.
- ✓ Then, the new window will open which contain different properties.
- ✓ One of them is Password Replication Properties in which different types are named.

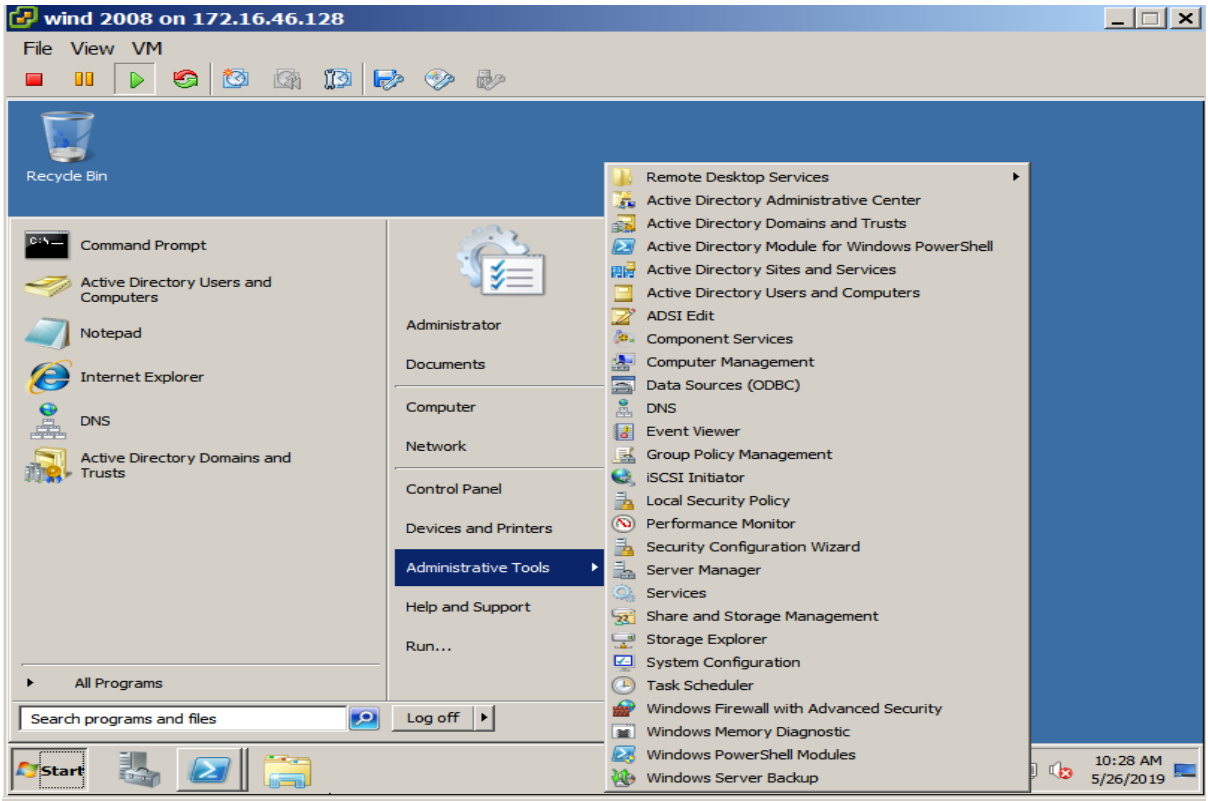


- ✓ We adds a new user having a name sam d. silva .
- ✓ With this user we are allowing the Password Replication Policy.
- ✓ This Password Replication Policy will stores the password of user and different computers according to the policy.
- ✓ We allowed our new user named sam d. silva to read all things at server side.

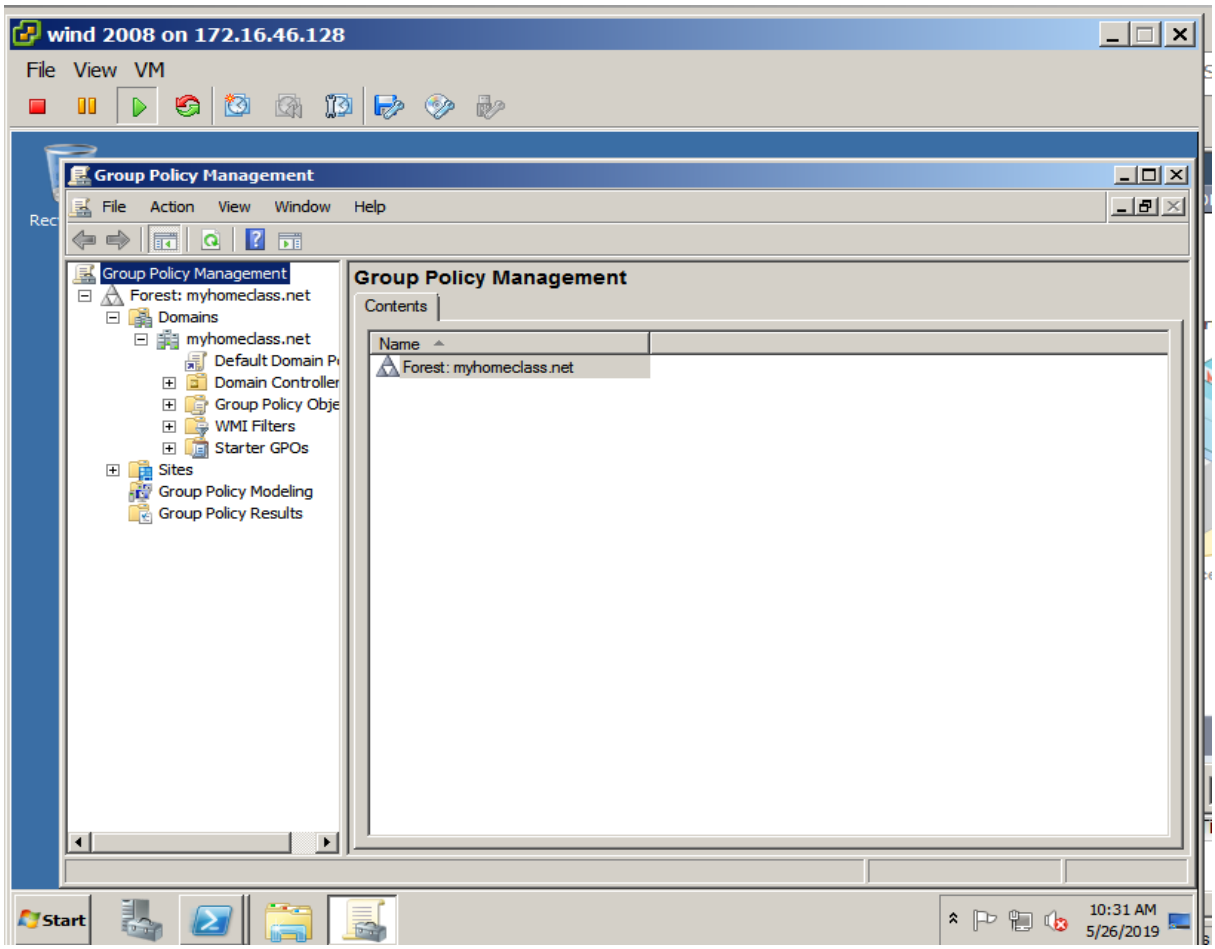


- ✓ Now we will open Command Prompt and run “gpupdate /force” .
- ✓ This Command will Reapplies all the policies and update them.
- ✓ By default, only policy settings that have changed are applied.

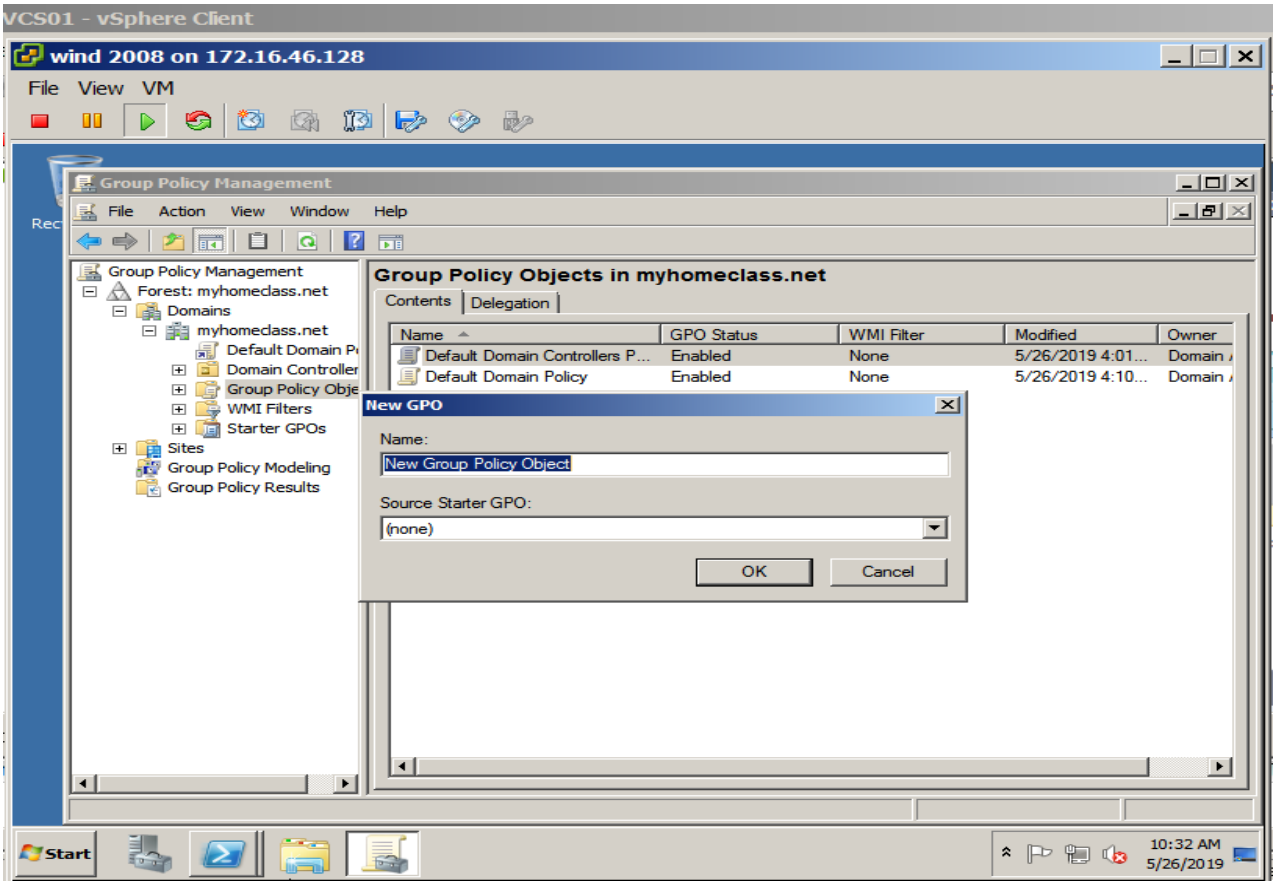
2. Configuring Active Directory Group Policy



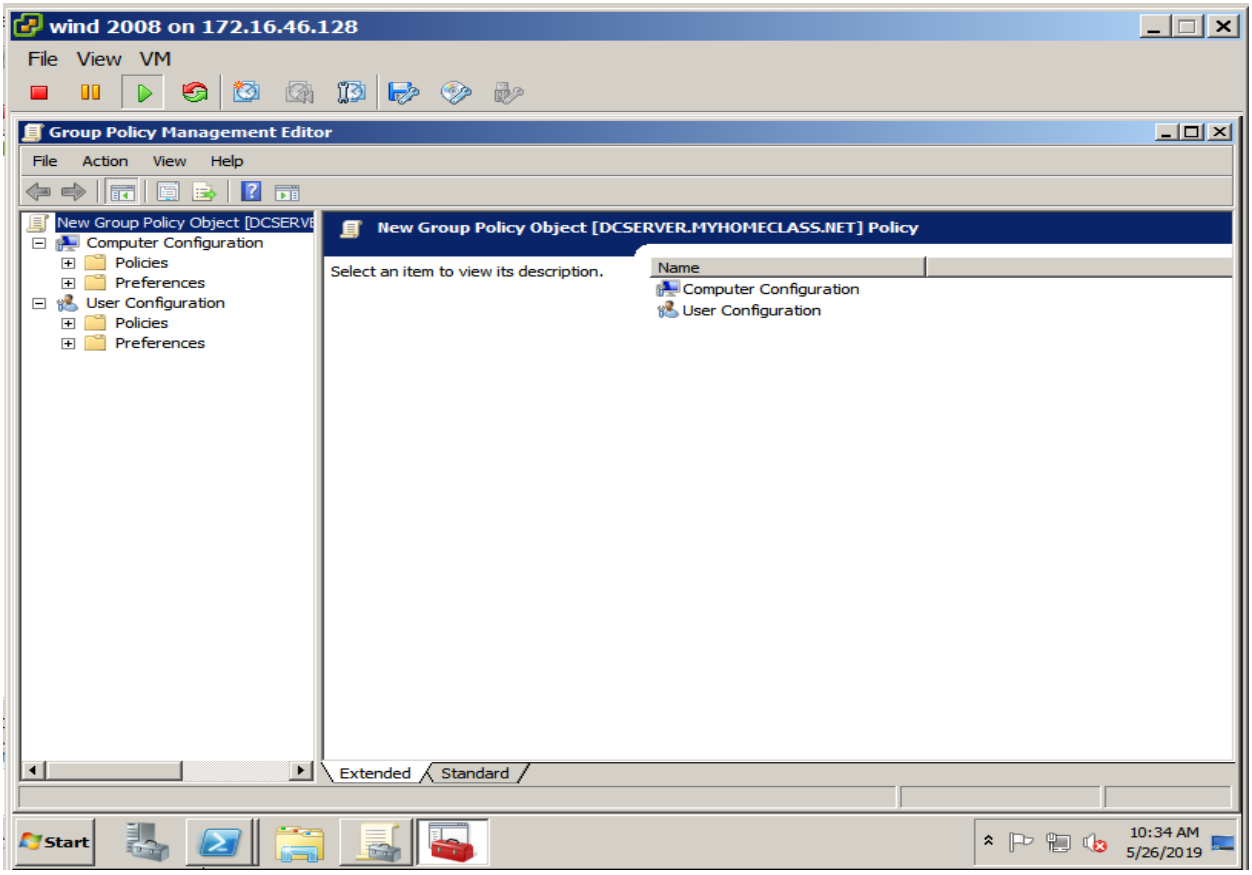
- ✓ Go To Start -> Administrative Tools.
- ✓ Here, we can check that our AD administrative Centre, AD module for PowerShell, AD sites and services and many more new options are now open.



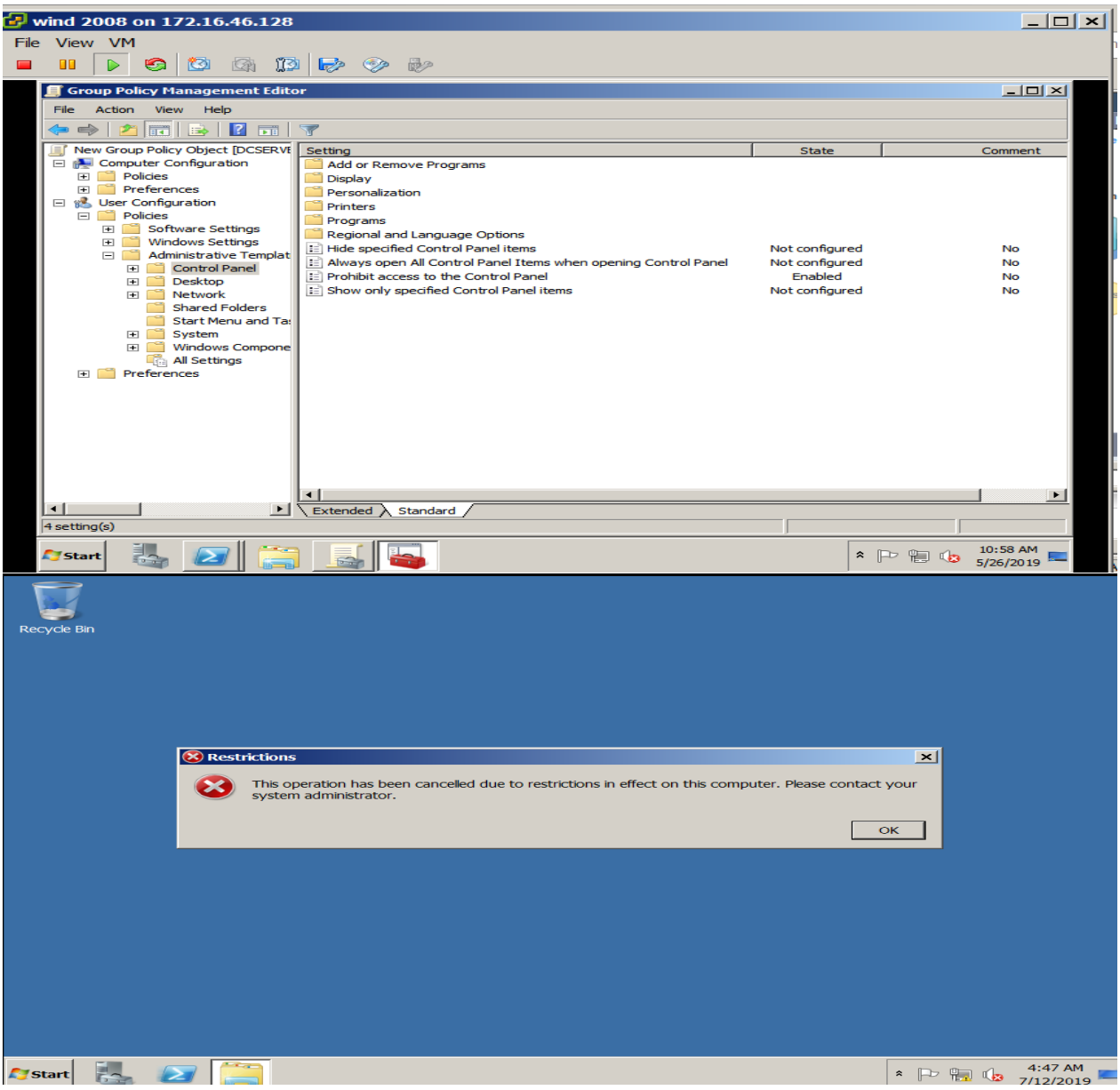
- ✓ We can Group Policy in our Group Policy Management
- ✓ Because we can make Active Directory already.
- ✓ So, we have a more new functions are open.



- ✓ Now, if we want to make a new Group Policy Objects (GPOs).
- ✓ Go To Group Policy Management ->Forest: myhomeclass.net -> Domains -> myhomeclass.net -> GPOs (Right Click).
- ✓ New window will pop out that will ask to provide name and Source Starter GPO.

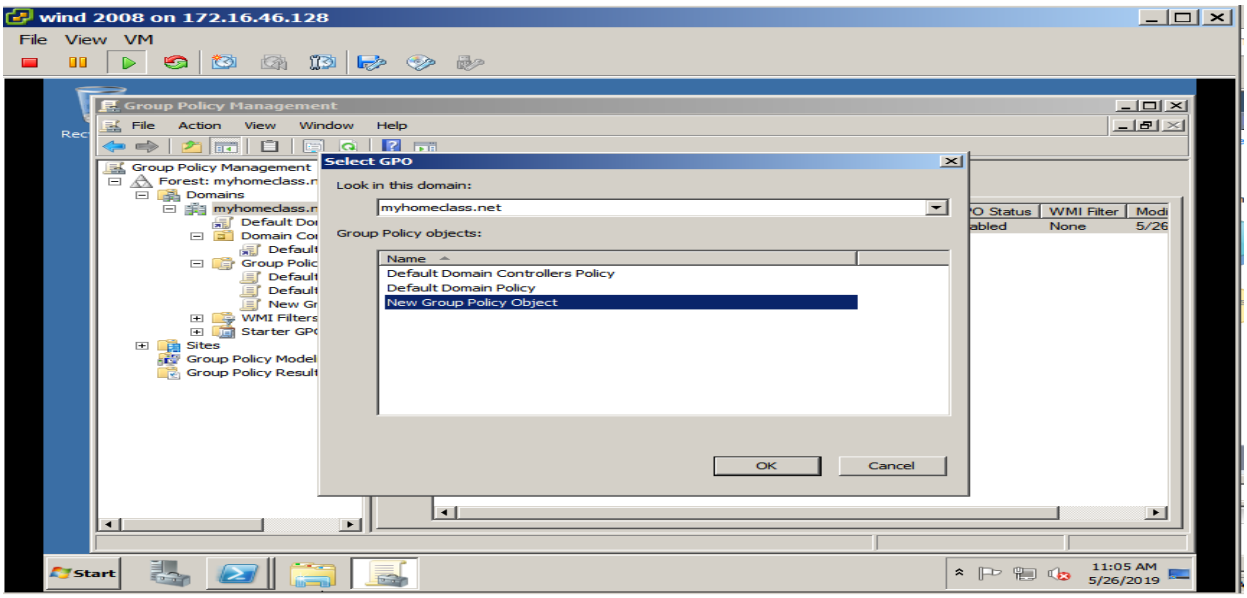


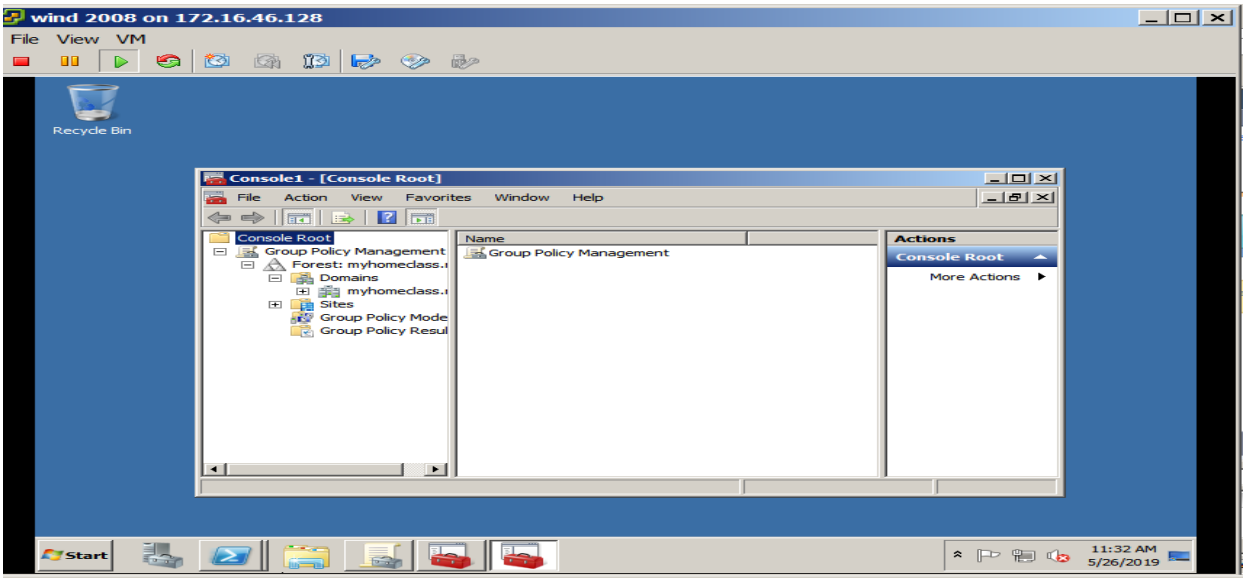
- ✓ So , now our Group Policy is ready .
- ✓ It contains Computer Configuration and User Configuration.
- ✓ In Computer Configuration we can change or handle our all computer configuration.
- ✓ In User Configuration we can handle our users.



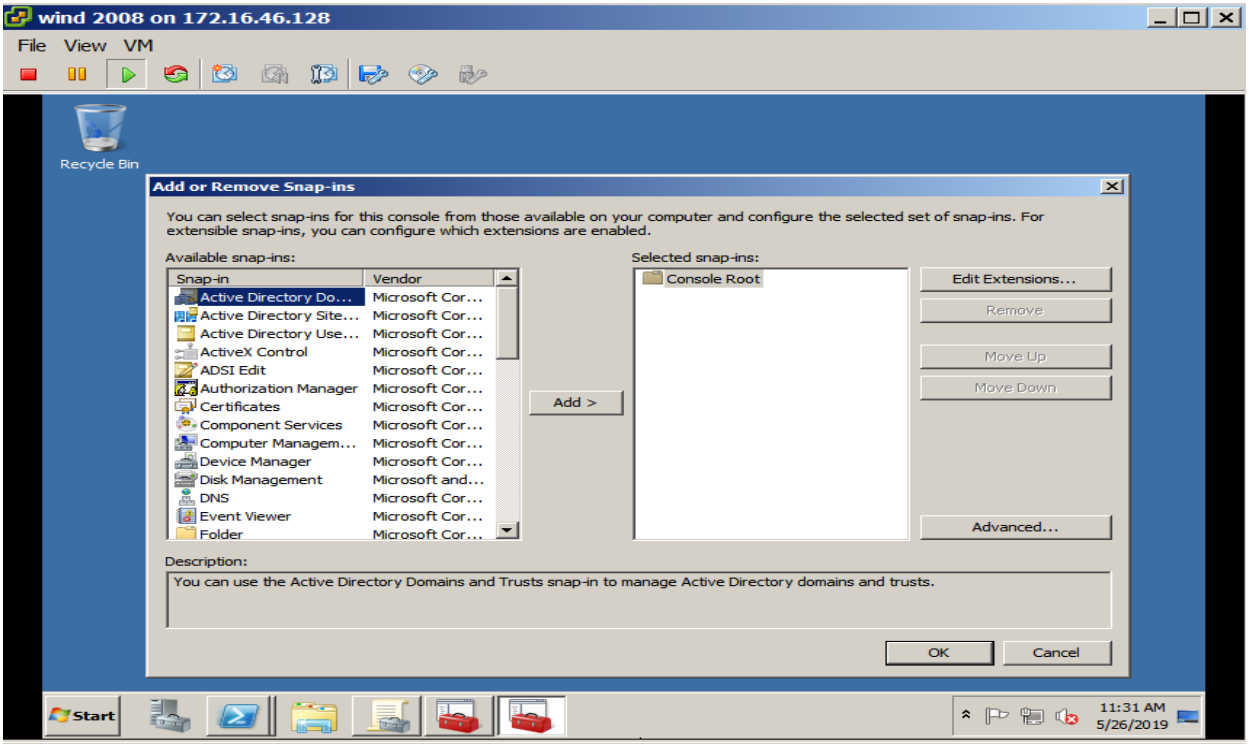
- ✓ Now , we are going to restrict our clients to do not open control panel in his system and do not make any changes on his system , if he/she wants to do anything the restricted message will show to his screen .

- ✓ At Server Configuration -> Policies -> Administrative Template -> Control Panel (Right click).

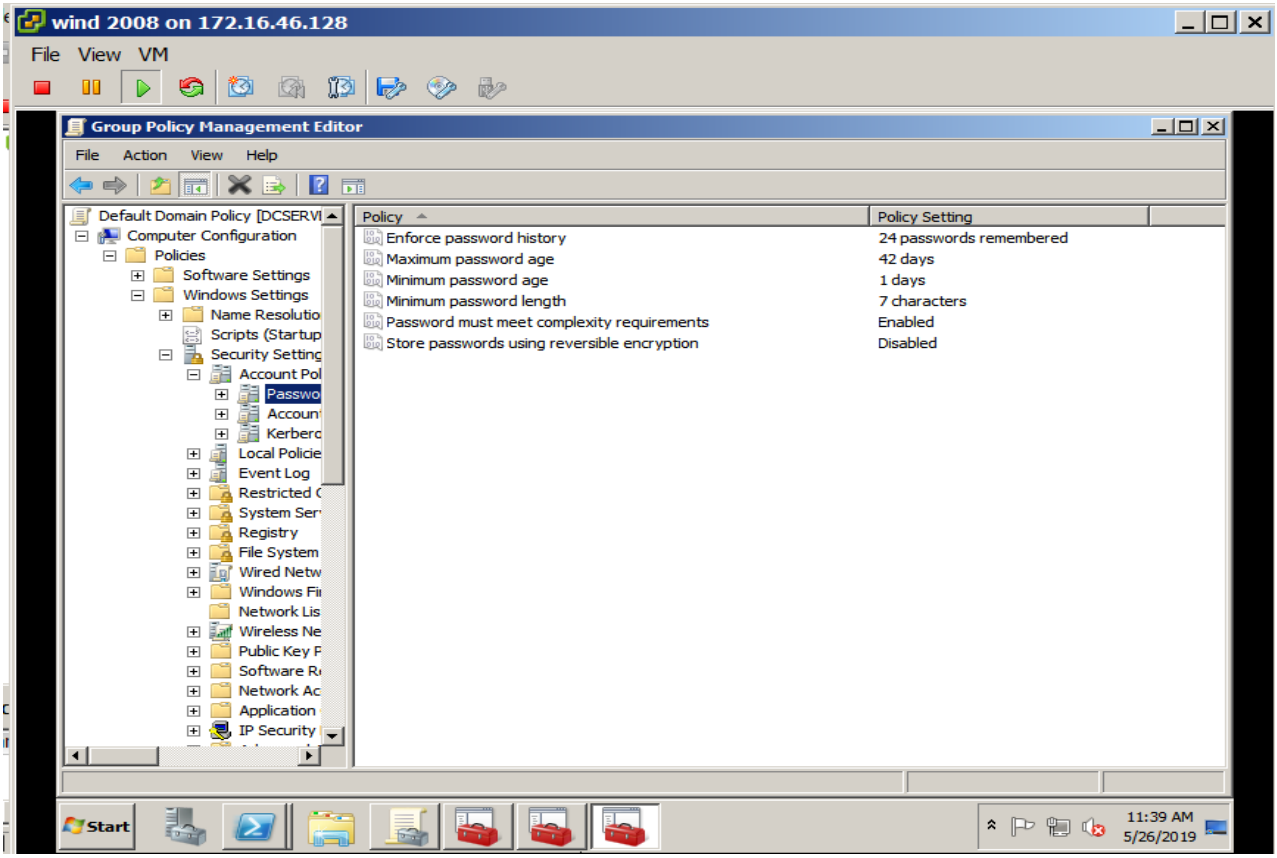




- ✓ Open Group Policy Management Console -> Click Forest -> Domain.
- ✓ Then Right click for our Domain and Select GPO.
- ✓ You will get a new window which gives you three options, you have to select the third one “View GPO” and click “OK”.
- ✓ Now, a new window comes up that will show GP Management.

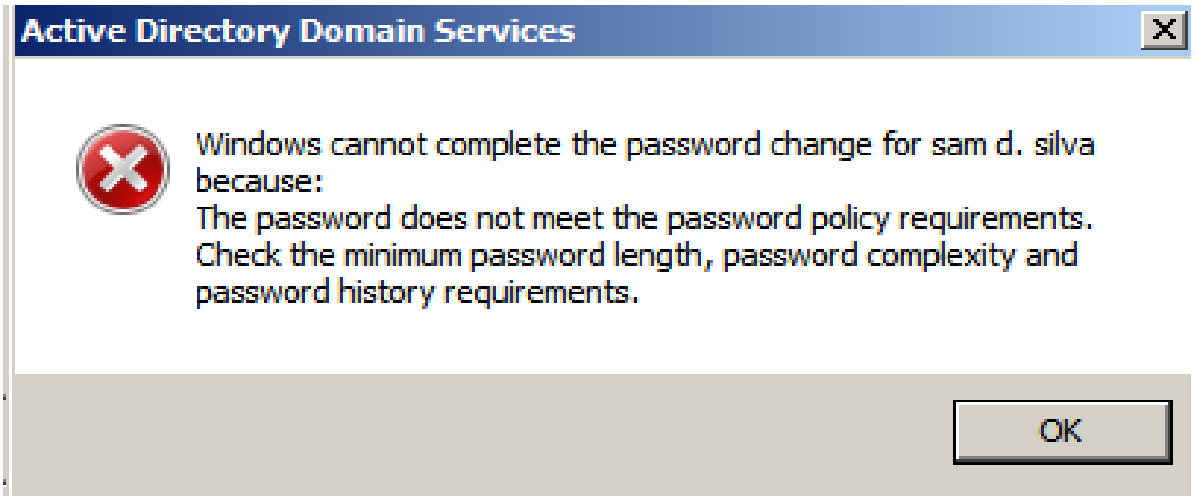


- ✓ Now we are able to add or remove the Snap-ins in the new window that will open up automatically.
- ✓ Here, you can use the ADD and Trusts snap-in to manage Active Directory Domains and Trusts.
- ✓ Click on ADD -> Console Root.



- ✓ Now, we can manage our password policies by going to Security Settings -> Account Policies -> Password.

- ✓ Here, we can see different policies to manage at the client side like Maximum Password Age, Maximum Password Length, Minimum Password Age etc.



- ✓ This Message will pop up when the User at the client side wants to change its password that does not meet the requirements policies generated by the Server Side/Administrator.

ABSTRACT

Our project **"Active Directory Domain Services"(AD DS)** provides authorization and authentication through a framework of secured, structured and hierarchical data storage for objects connected in a network such as users, computers and services.
It provides support for locating these object and working with these objects. It automatically creates DNS for the machines in the backend and assigns them in an orderly manner thereby causing no hassle for the programmer. This project also employs **"Read Only Domain Controller" (RODC)** which boasts features such as read only (AD DS) database, Unidirectional replication, Filtered attribute set configuration, Limited credential caching and Separation of administrator capabilities which makes it high-yielding.
Also in our project, we have implemented **"Active Directory Group Policies"(GPOs)** that provides centralized management and optimized & secure view over the remote users in an Active Directory Environment. It helps to view components at a domain-wide level to control various areas of the View environment. These policies can be used to affect specific users, specific desktop pools, or all client sessions users. We use these policies to set some pre-requirements for a user to complete a specific task such as creating account. For example, we can set the requirement for creating an account that the password should be alpha-numeric with some special characters and should at least have a minimum length thus enforcing security. They are used in managing group policy settings**. AD DS** are used by Network Administrators to automate common administrative tasks, such as adding users and groups and setting permissions for network resources. Independent software vendors and end-user developers can use AD DS programming to directory-enable their products and applications. Services can publish themselves in Active Directory Domain Services; clients can use Active Directory Domain Services to find services, and both can use Active Directory Domain Services to locate and work with other objects on a network. And because all locations are independently connected to the internet so various task such as file sharing is faster and easier in this topology.

REFERENCES

- Cloud Computing — geeksforgeeks.org
- AD DS — tutorialspoint.com
- GPOs — wikipedia.org
- Virtualization Concept — javatpoint.com
- RODC — w3schools.in
- VMware Products — my.vmware.com
- Windows Server 2008 R2 — microsoft.com