

Network Operating System (NOS)

Microsoft Windows Server 2008 R2

CONTENTS

Part 1: System Requirements

Part 2: Setup and Installation

Part 3: Roles (adding Roles such as Active Directory, DNS, DHCP)

Part 4: Account Management (Users and groups)

Part 5: Sharing and Permissions

Part 6: Resources

As part of the learning process the instructor had the class utilize both a virtual environment with VMware Work Station and real world equipment in the form of switches, hubs and general PC equipment to run Windows Server 2008 R2 as a small closed network and also as part of a Trust between domains as well as roaming profiles. Personally experimenting briefly with connecting a Linux (Ubuntu) based machine as well as an older Apple Mac G4.

Compiled by Darren Boudreau – NSCC Burr ridge - December 2012

Note: Various internet sources were used to compile this document as a useful means to hopefully painlessly setup and run a basic Windows Server 2008 R2 setup and networked installation and also as a means to show what had been taught in class.

Part 1. a. System Requirements

Processor

- Minimum: 1 GHz (x86 processor) or 1.4 GHz (x64 processor)
- Recommended: 2 GHz or faster

Note: An Intel Itanium 2 processor is required for Windows Server 2008 for Itanium-Based Systems.

Memory

- Minimum: 512 MB RAM
- Recommended: 2 GB RAM or greater
- Maximum (32-bit systems): 4 GB (Standard) or 64 GB (Enterprise and Datacenter)
- Maximum (64-bit systems): 32 GB (Standard) or 1 TB (Enterprise and Datacenter) or 2 TB (Itanium-Based Systems)

Available Disk Space

- Minimum: 10 GB
- Recommended: 40 GB or greater

Note: Computers with more than 16 GB of RAM will require more disk space for paging, hibernation, and dump files.

Drive

DVD-ROM drive

Display and Peripherals

- Super VGA (800 x 600) or higher-resolution monitor
- Keyboard
- Microsoft Mouse or compatible pointing device

Part 1. b. Lab Test System

OS: Windows Server 2008 R2 Enterprise Service Pack 1

Type: Generic PC

Mother Board: MSI K9AGM2 (MS-7327 (v1.x))

Processor: AMD Athlon 64 3500+ 2.19GHz

RAM: 4 GB

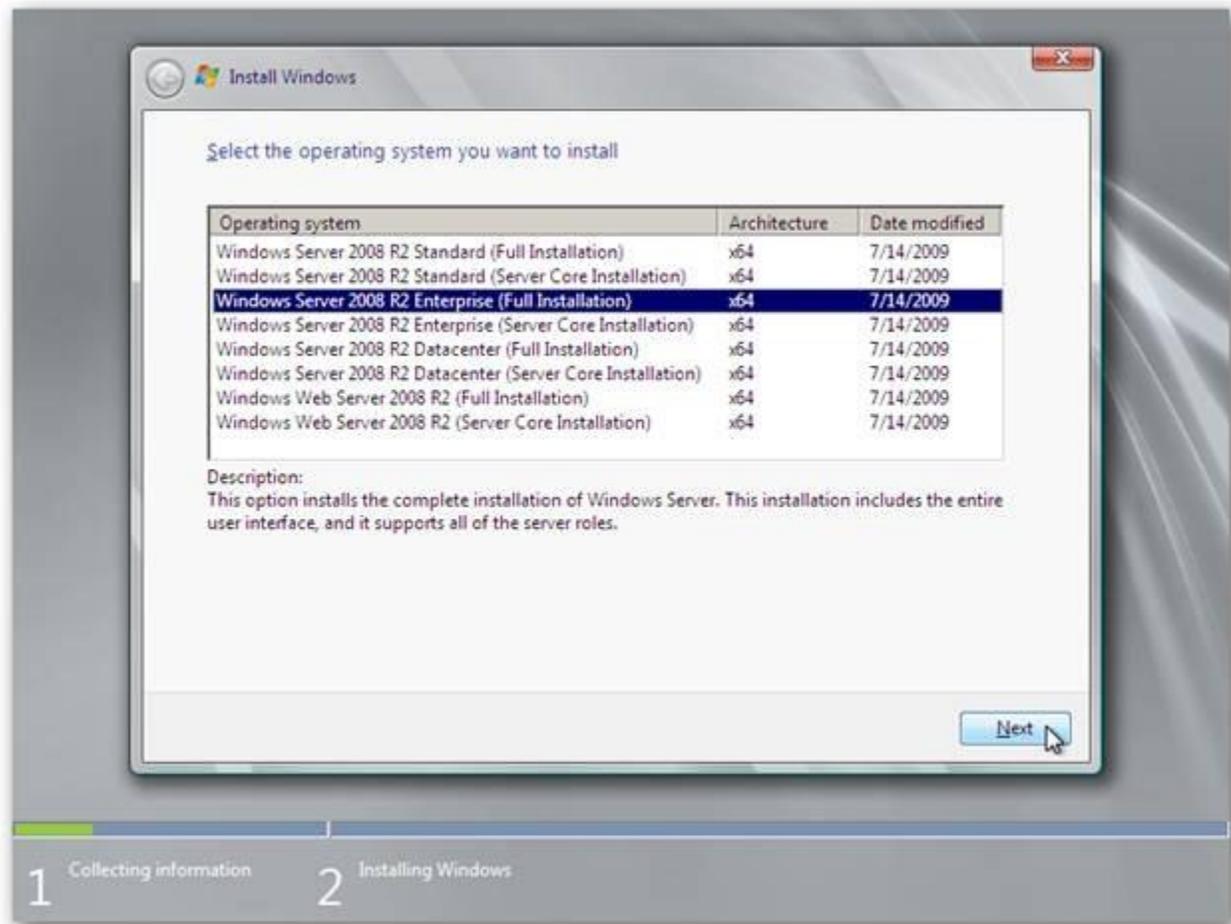
GPU: NVIDIA GeForce 8500 GT

HDD: 80 SATA and 160 SATA

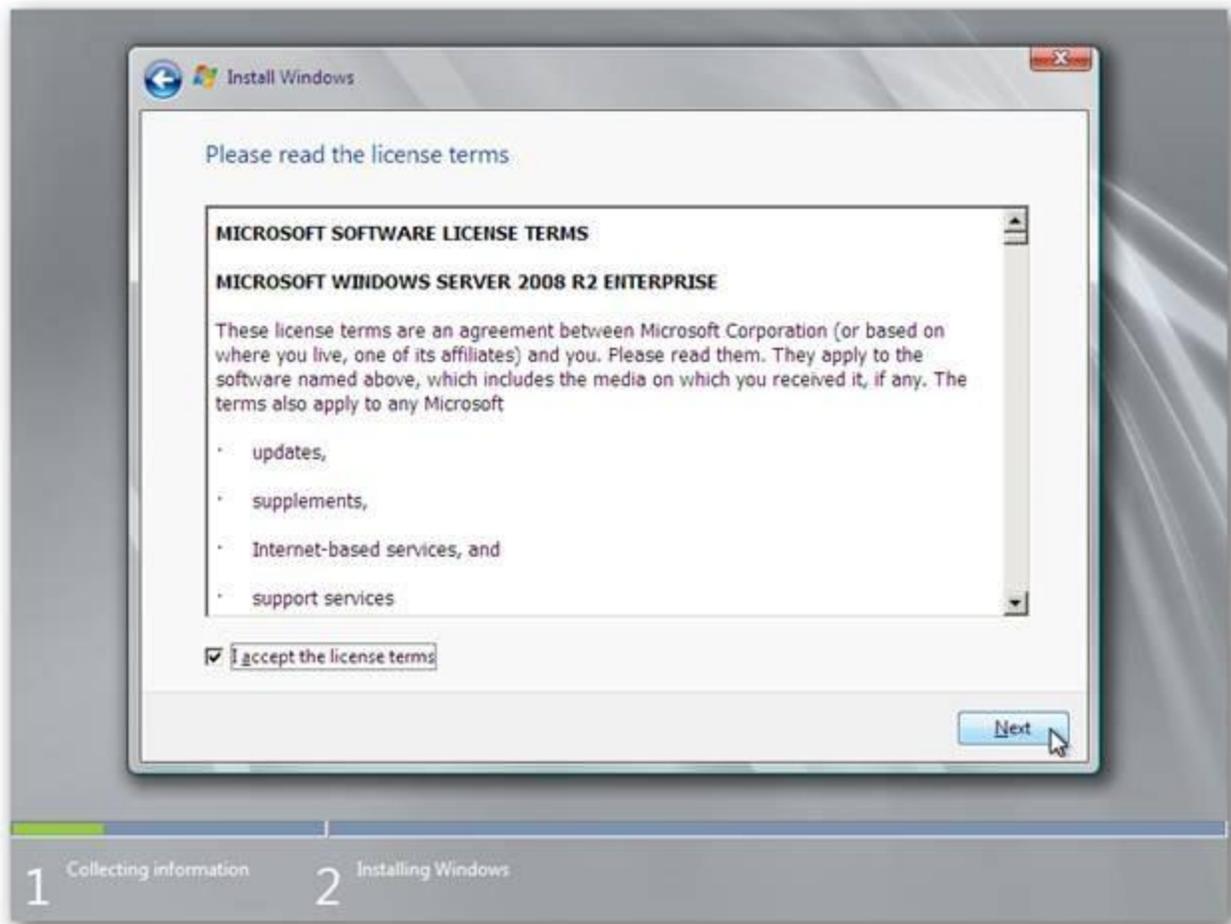
Part 2. Setup and Installation

A Basic Install

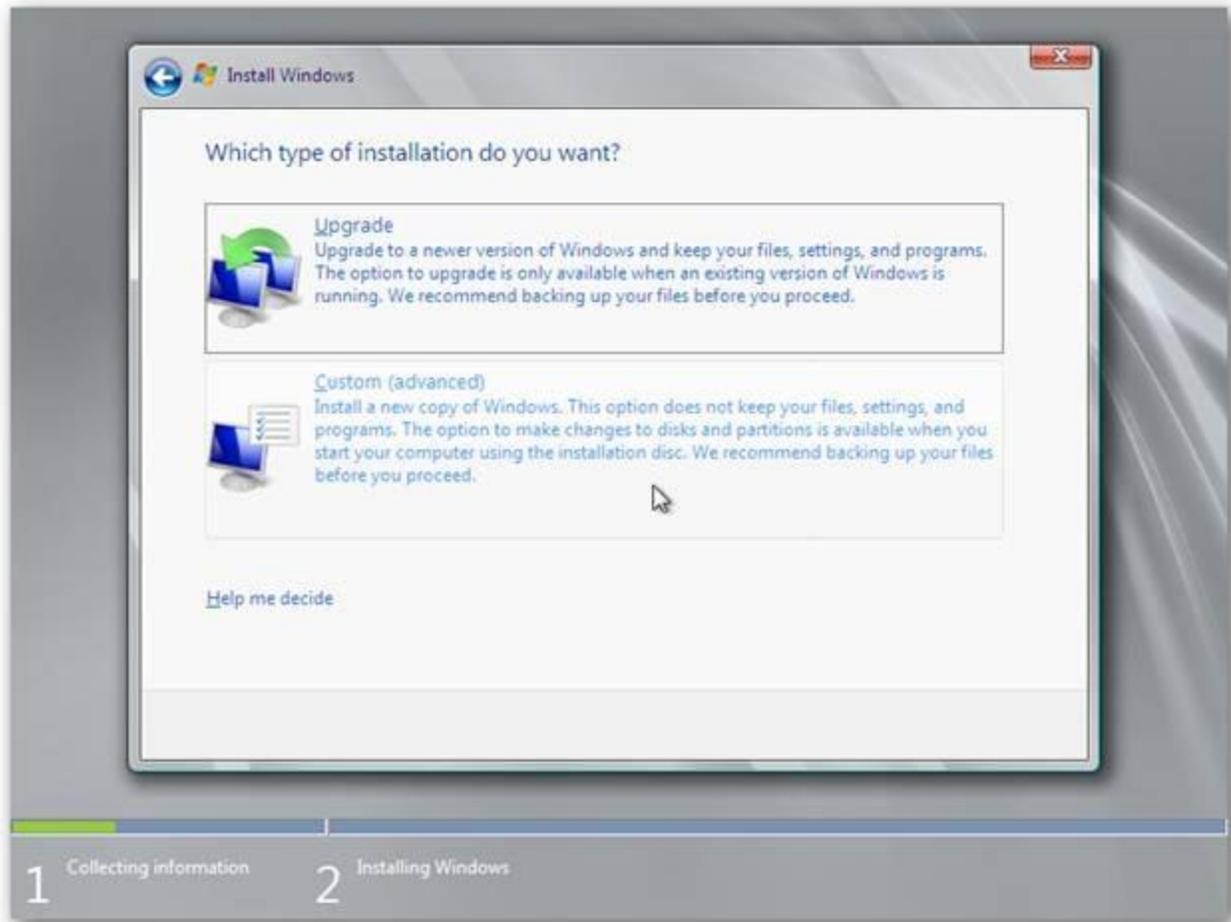
After booting up from your install disk, you will arrive at a language and preferences screen. Once you have chosen those options, you get to the Operating System Selection page. Depending on your license and the purpose of your server, there are a variety of options to choose from. For our purpose today, we are going to choose the *Enterprise (Full Installation)* version.



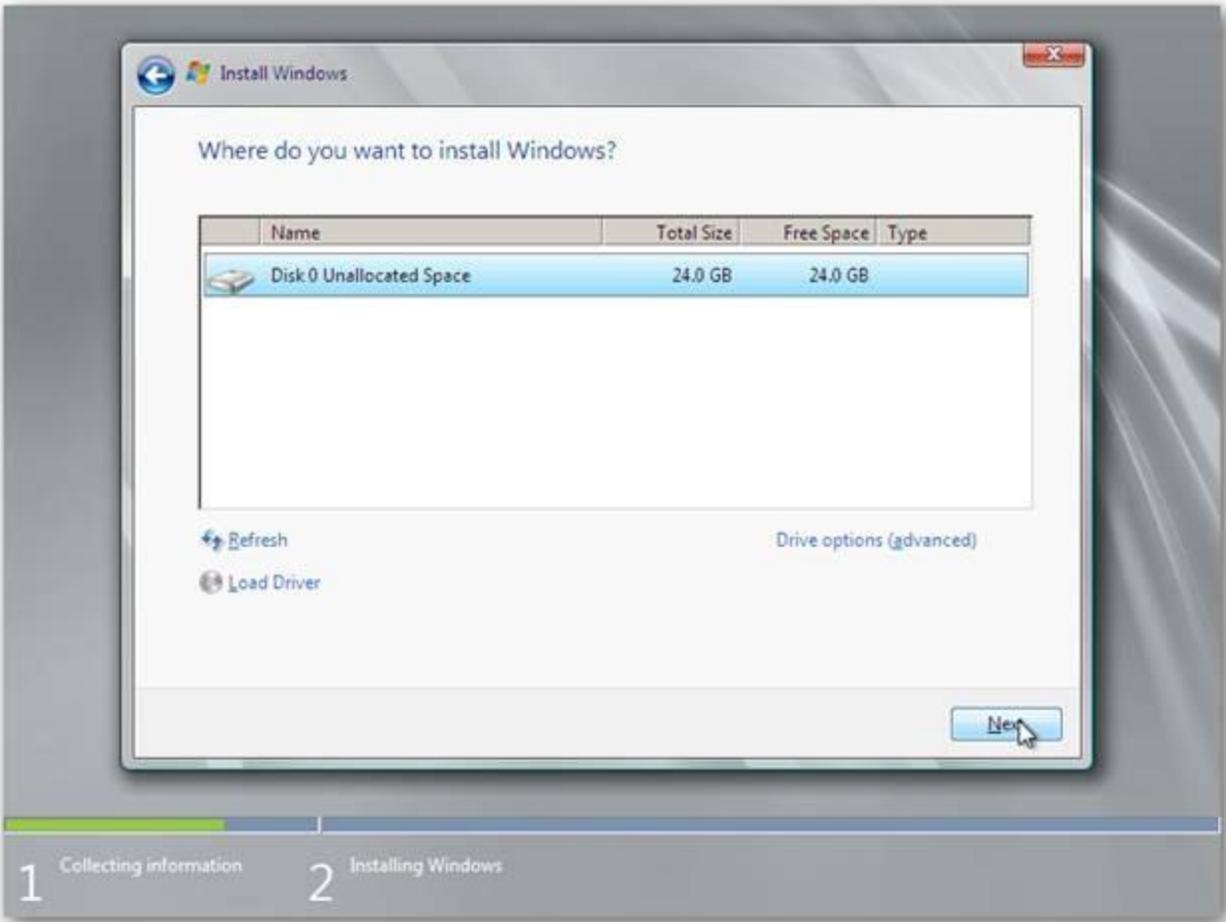
We get to read the standard End User License Agreement.



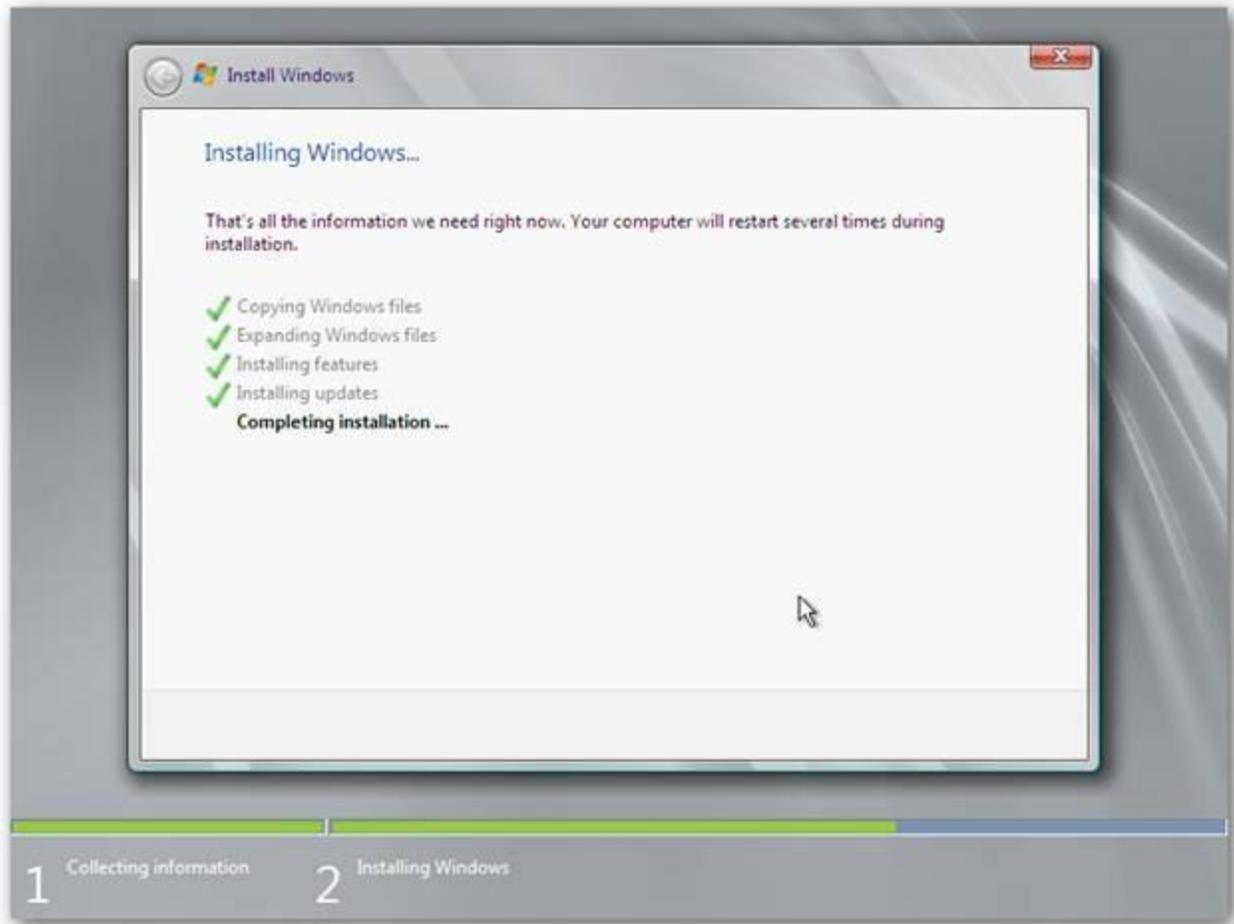
Since we're doing a base install and not an upgrade, so we choose the *Custom (advanced)* option.



We've got a blank 24 GB disk, so we're just going to install it there. If you want to create a partition out of the available drive space or reformat a drive, then choose Drive options (advanced).



Windows will take a little while with your install, and reboot a few times.



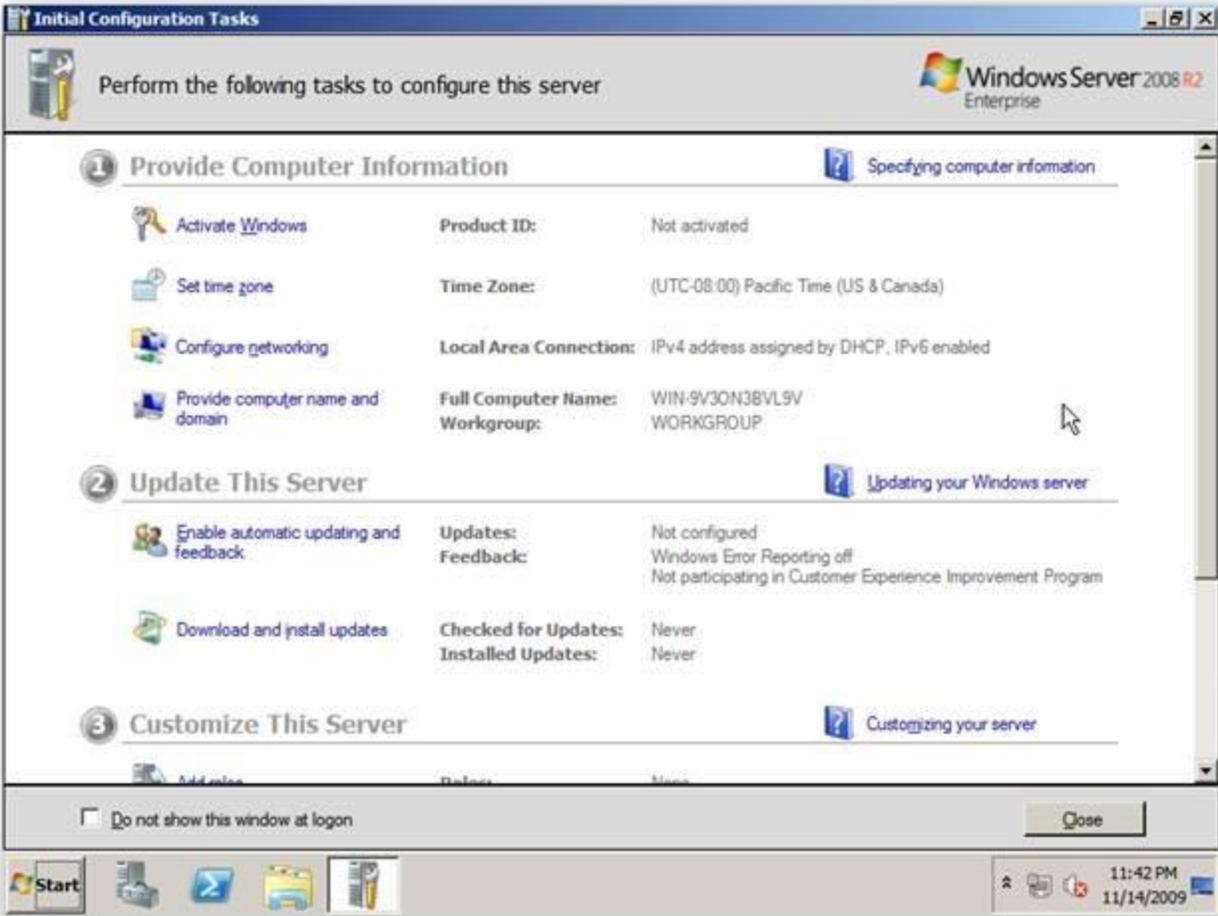
Once the install is finished, we're prompted to change our password before logging in.



Windows requires that you have a strong password, seven characters long with at least three of the four following: uppercase letter, lowercase letter, numeral, or symbol. You'll want to make sure you write it down somewhere for now, because if you forget it later, the entire install will have to be re-done.



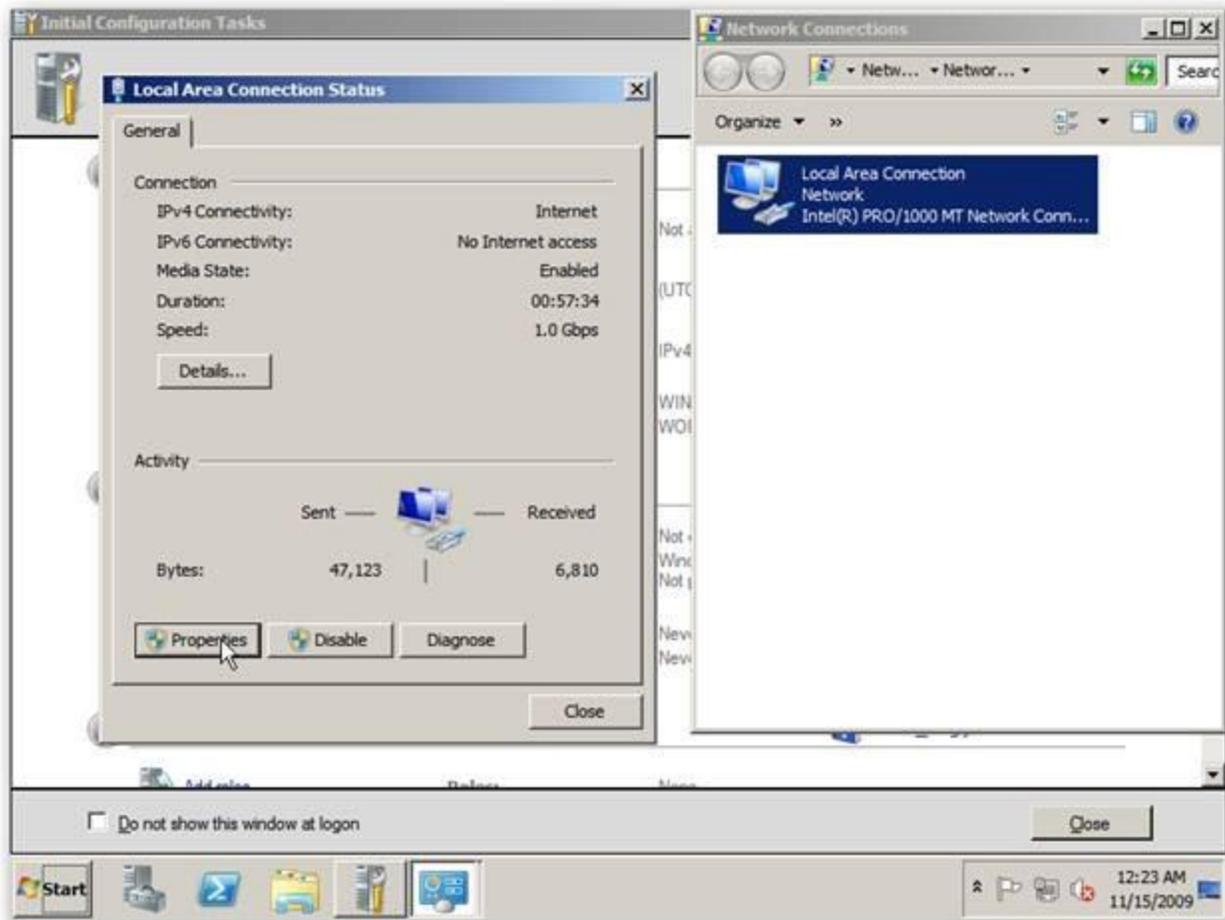
The Initial Configuration Tasks window pops up as soon as you logon. You could also type in *Oobe.exe* in the Command Prompt to arrive here.



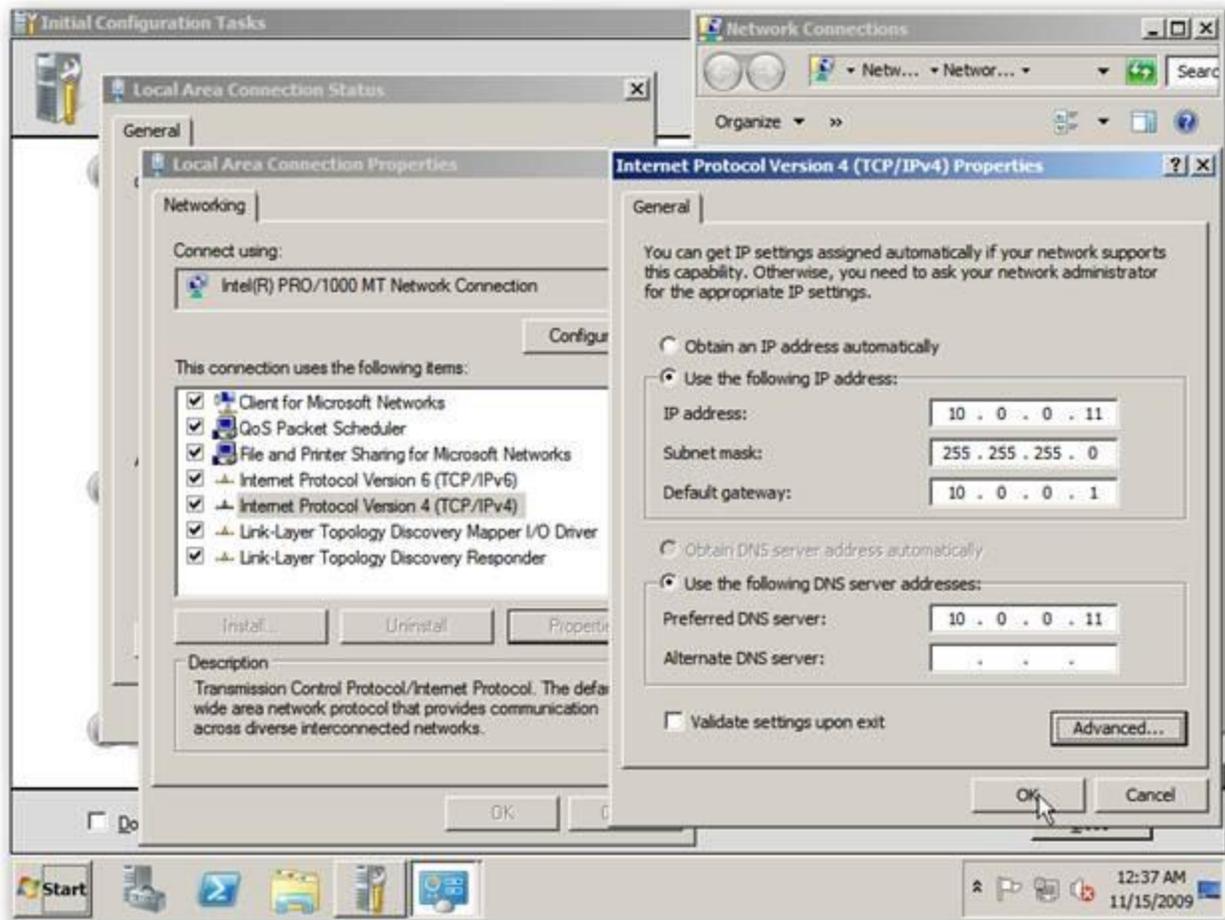
One of the first things we want to correct is the time, so choose *Set time zone*. Make sure that you set the time zone first, because the date and time will shift after.



Next we want to choose *Configure Networking*. The first server installed in a network needs to be a Domain Controller, and since they require a static IP, we are going to need to set one up now. Double-click on *Local Area Connection*, and once the information box pops up, click on *Properties*.



Click on *Internet Protocol Version 4* in the Networking box, then click *Properties*. Change the radial button to *Use the following IP address:* and then enter the settings for your specific server and network IP addresses. When you're finished, click *OK* to save those settings.



Finished!

Part 3. Adding Roles

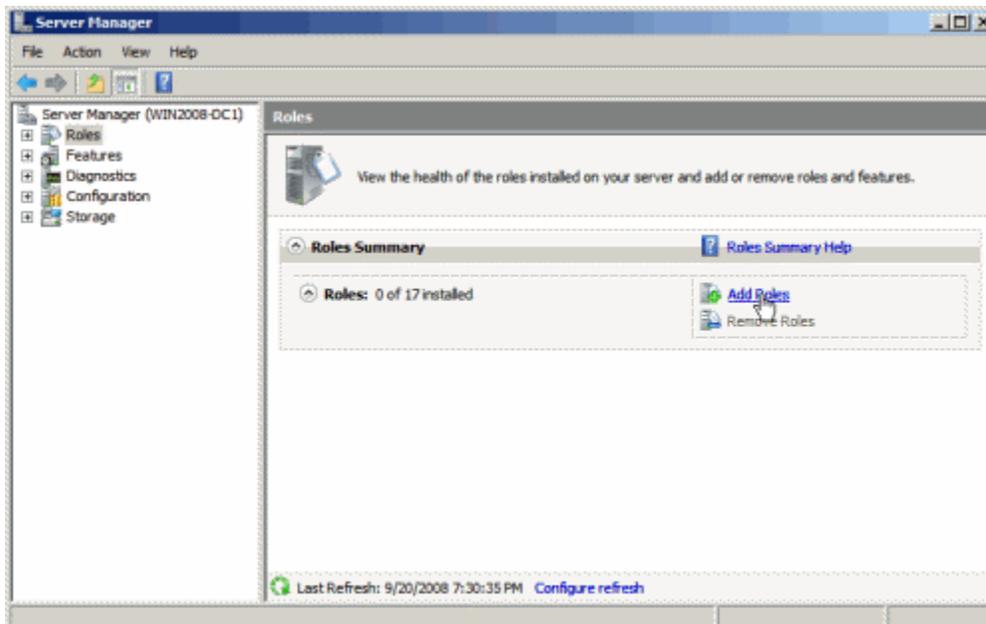
1. Installing Active Directory Domain Services (AD-DS) with DNS

In Windows Server 2008, unlike previous server operating Systems, there is an additional step that needs to be taken before running DCPROMO to promote the server to Domain Controller and installing Active Directory on it. This step is the installation of Active Directory Domain Services (AD-DS) role on the server. In fact, the AD-DS role is what enables the server to act as a Domain Controller, but you will still need to run DCPROMO the regular way.

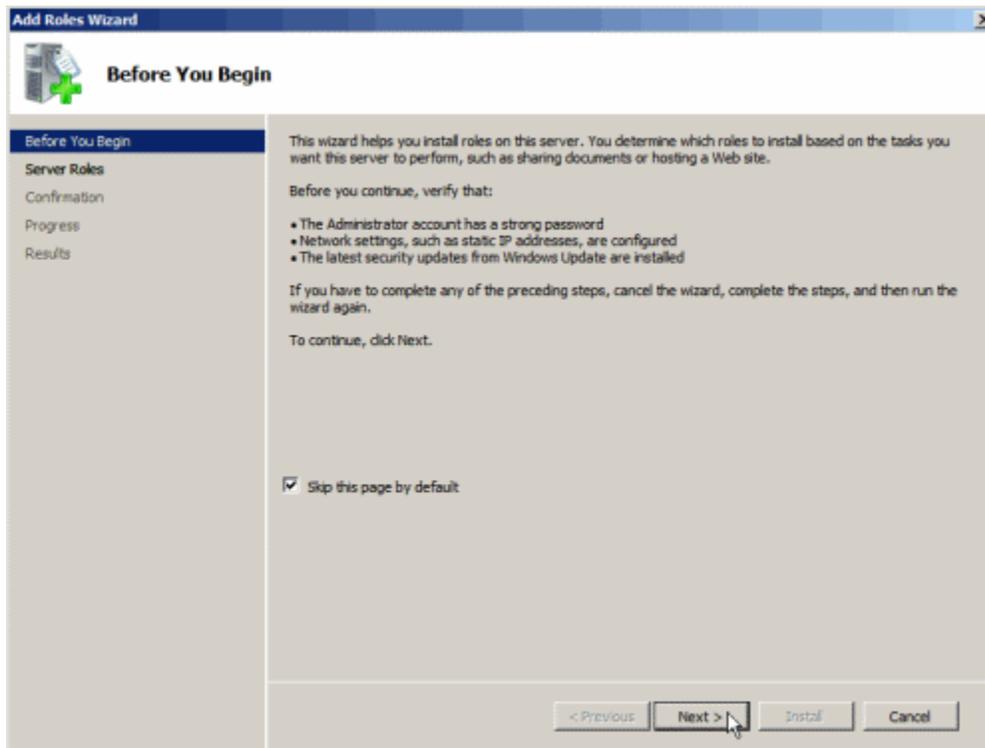
Server Manager/Initial Configuration Tasks

Roles can and should be added from Server Manager (but they can also be initiated from the Initial Configuration Tasks wizard that auto-opens the first time you log on to the server).

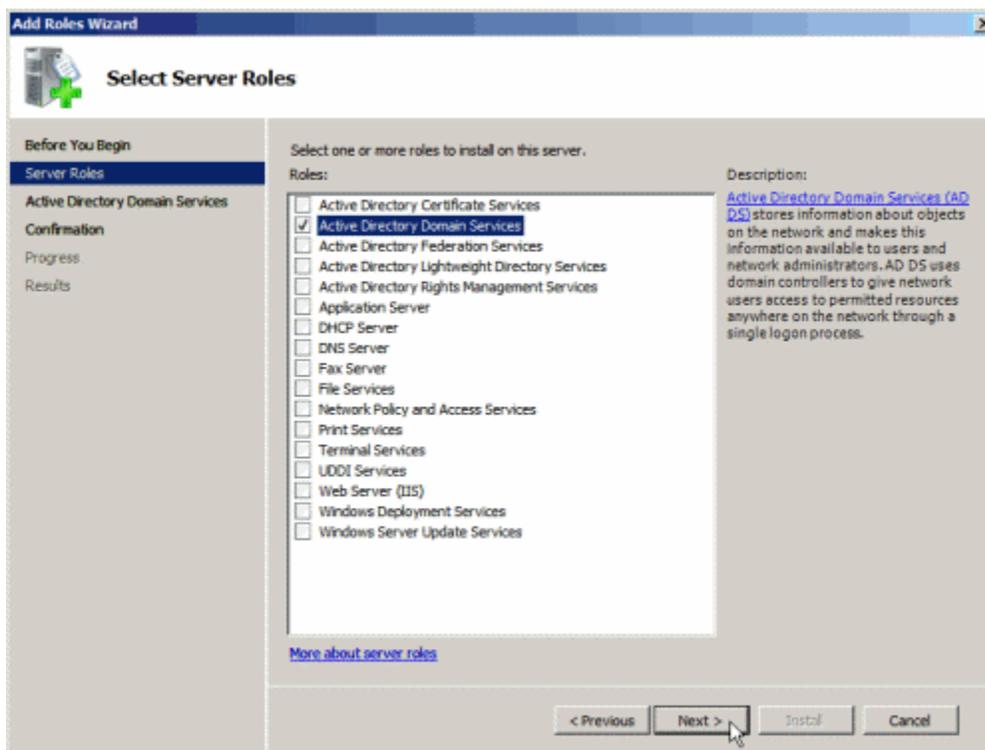
1. Open **Server Manager** by clicking the icon in the Quick Launch toolbar, or from the Administrative Tools folder.
2. Wait till it finishes loading, then click on **Roles > Add Roles** link.



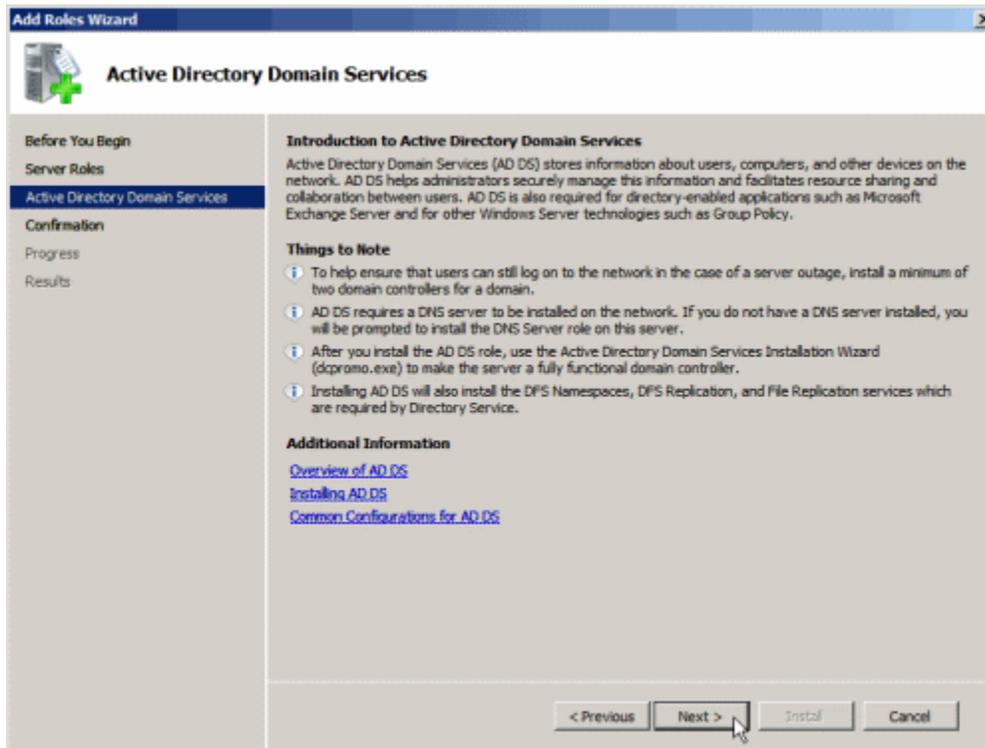
3. In the **Before you begin** window, click **Next**.



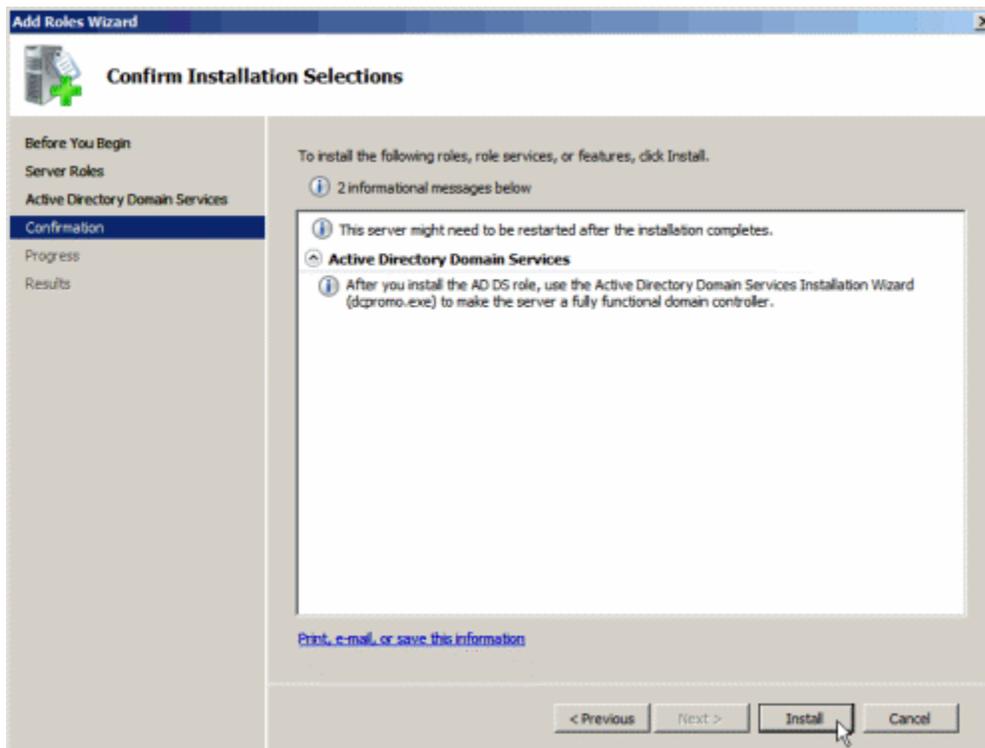
4. In the Select Server Roles window, click to select **Active Directory Domain Services**, and then click **Next**.



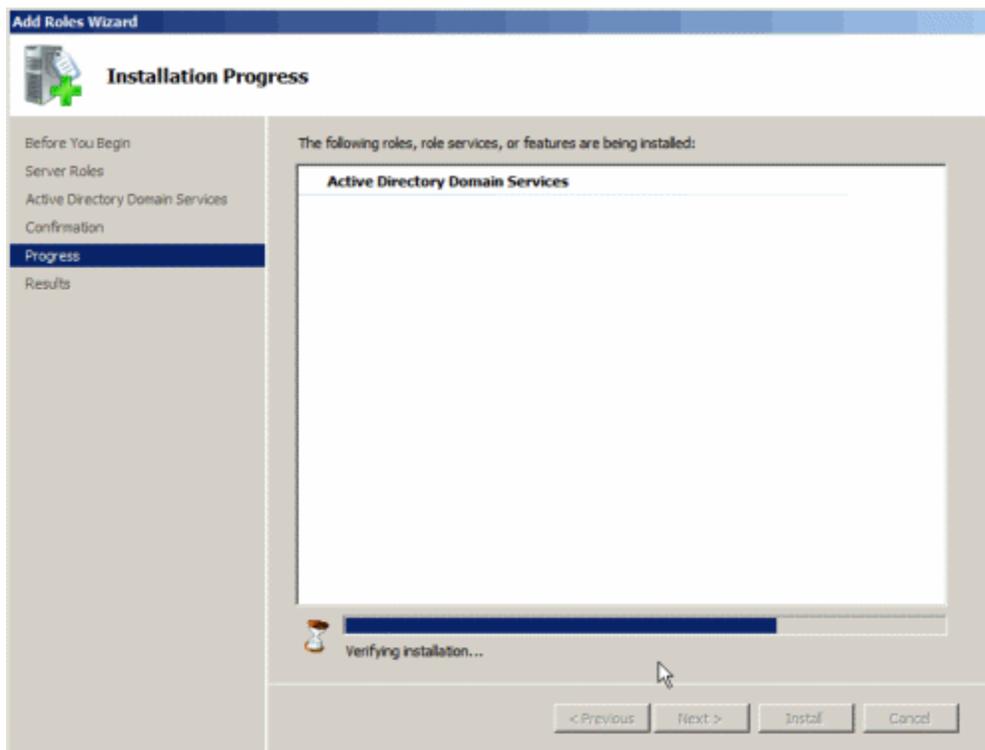
5. In the Active Directory Domain Services window read the provided information if you want to, and then click **Next**.



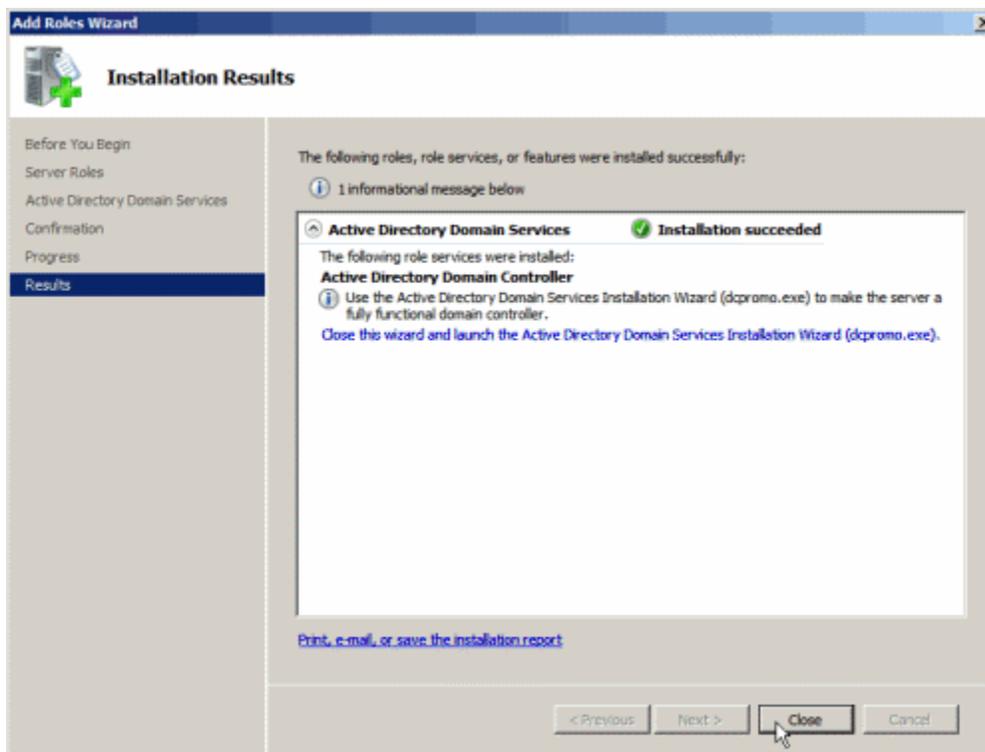
6. In the Confirm Installation Selections, read the provided information if you want to, and then click **Next**.



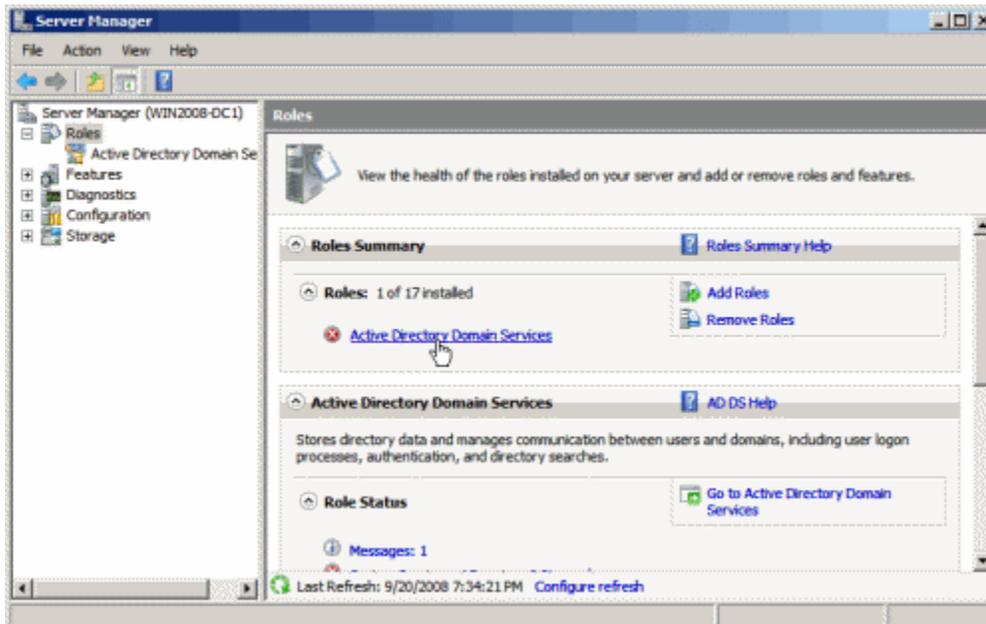
7. Wait till the process completes.



8. When it ends, click **Close**.

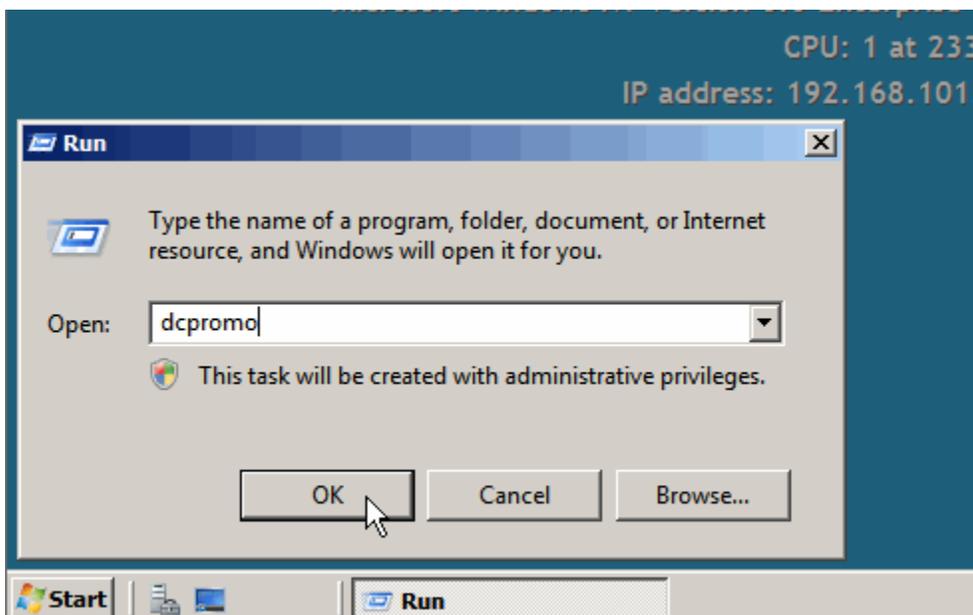


9. Going back to Server Manager, click on the **Active Directory Domain Services** link, and note that there's no information linked to it, because the DCPROMO command has not been run yet.



10. Now you can click on the DCPROMO link, or read on.

To run DCPROMO, enter the command in the **Run** command, or click on the DCPROMO link from **Server Manager > Roles > Active Directory Domain Services**.

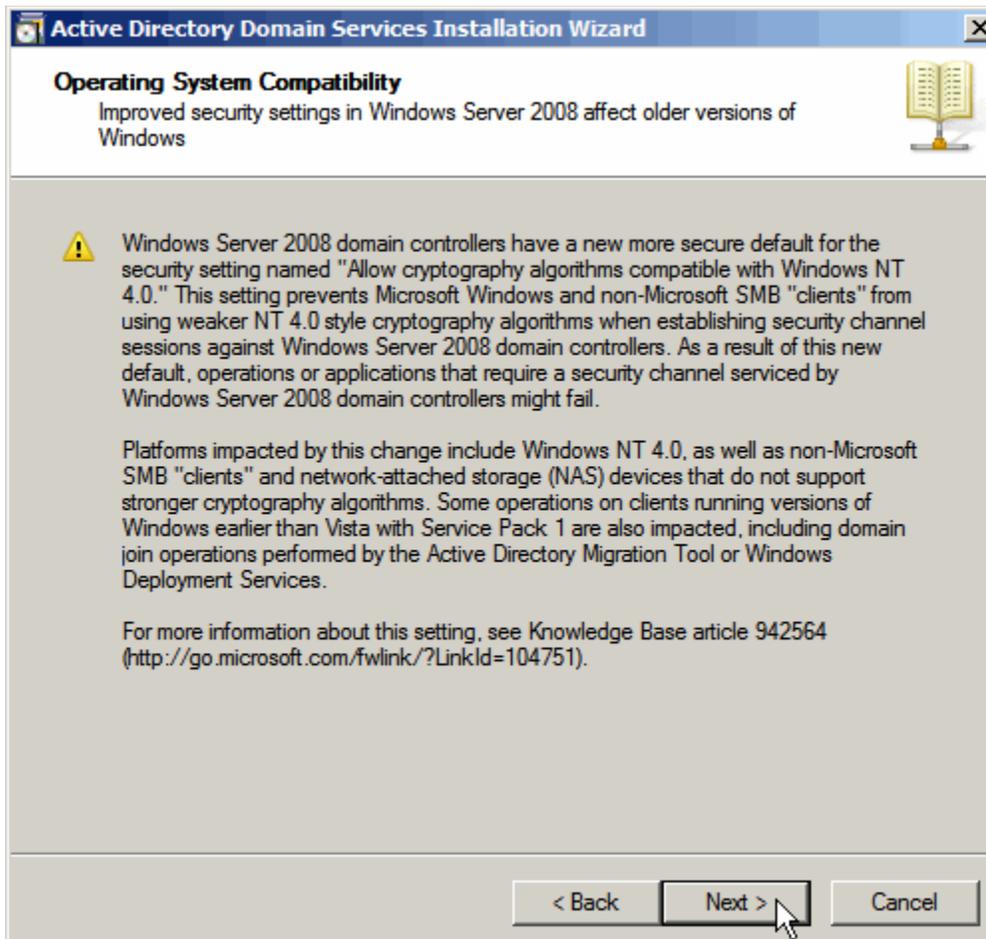


2. Depending upon the question if AD-DS was previously installed or not, the Active Directory Domain Services Installation Wizard will appear immediately or after a short while. Click **Next**.

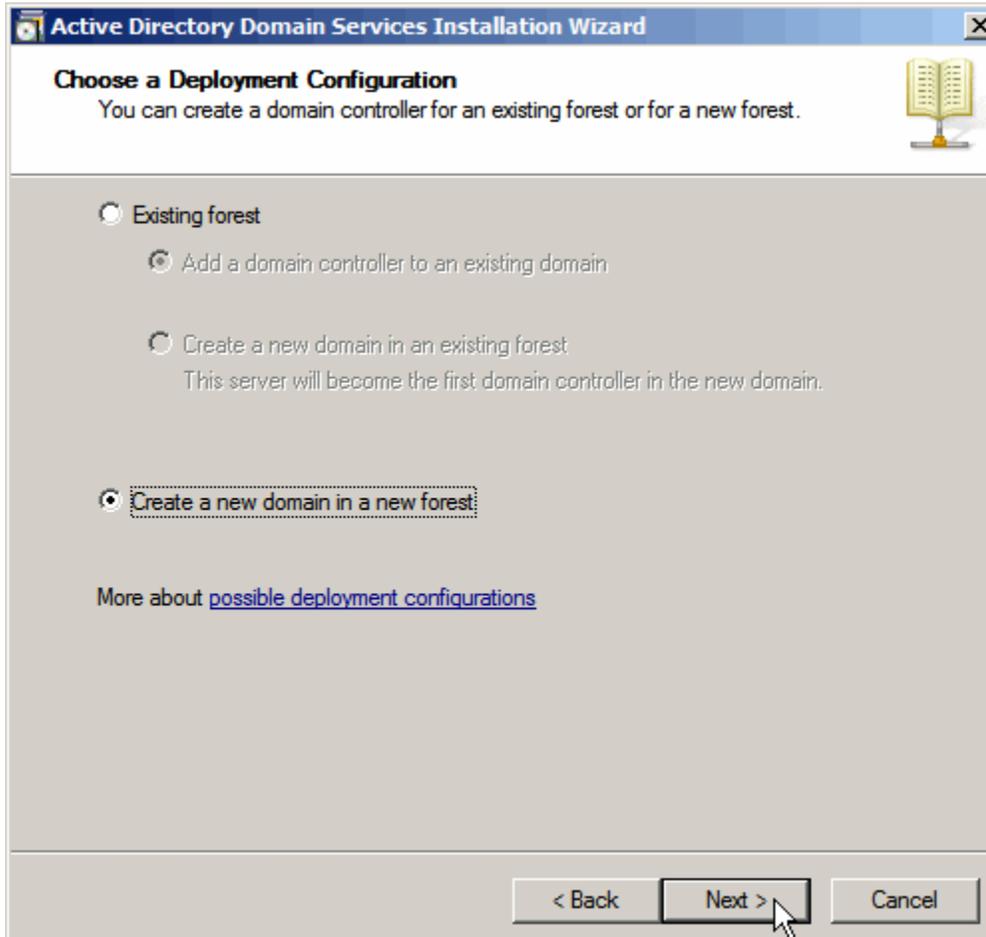


Note: The Advanced features of DCPRMO will be discussed in a future article.

3. In the Operating System Compatibility window, read the provided information and click **Next**.



4. In the Choosing Deployment Configuration window, click on "**Create a new domain in a new forest**" and click **Next**.

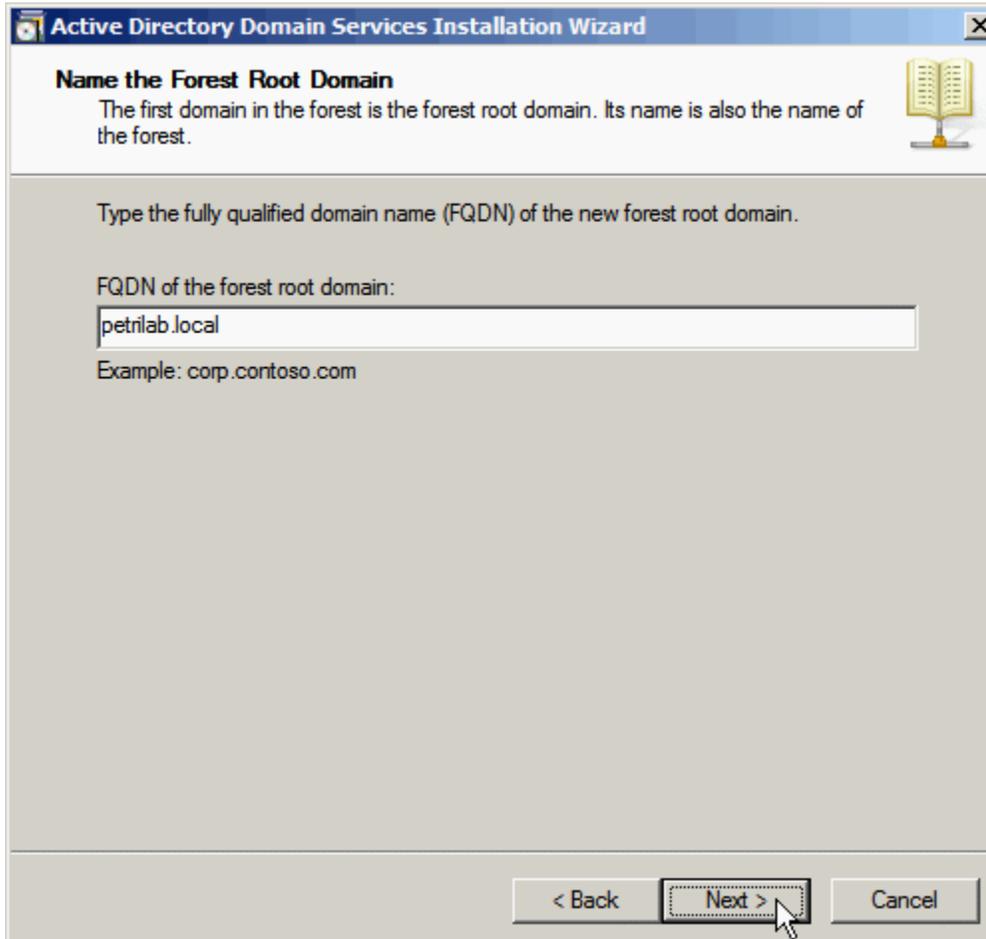


Note: It's possible that the Administrator password was not set; a dialog box may pop up after pressing next, in which case you will need to go to the Computer Management Console to set the administrator password.

1. Start → Administrative Tools → Computer Management
2. Locate and click on Local Users and Groups
3. Find and right click on Administrator. Select Set Password and then type in a password.
4. You should now be able to proceed with the DNS installation.

Keep in mind that you are more than likely logged in as 'a' user administrator account and not the actual Administrator account that's referred to in the dialog. These are two separate things and shouldn't be confused. The local users and groups will move to **Active Directory Users and Computers** once DNS has completed installing and will no longer be found in Computer Management.

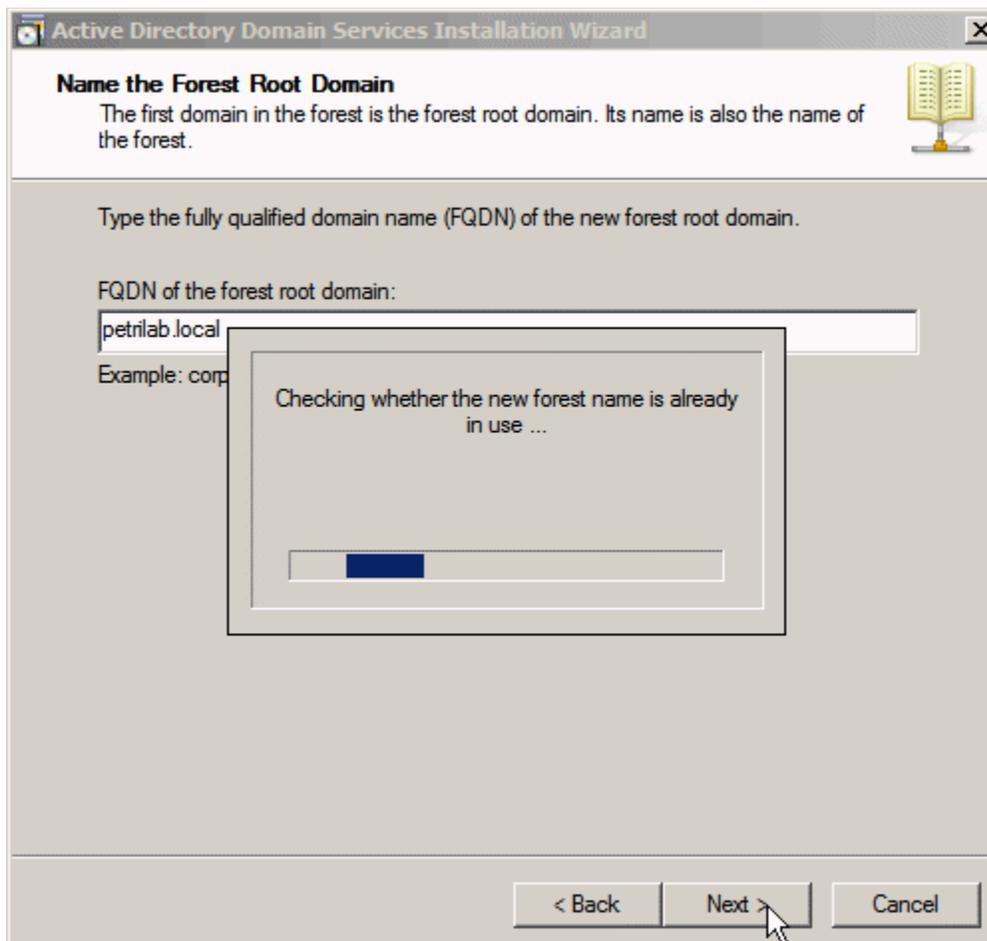
5. Enter an appropriate name for the new domain. Make sure you pick the right domain name, as renaming domains is a task you will not wish to perform on a daily basis. Click **Next**.



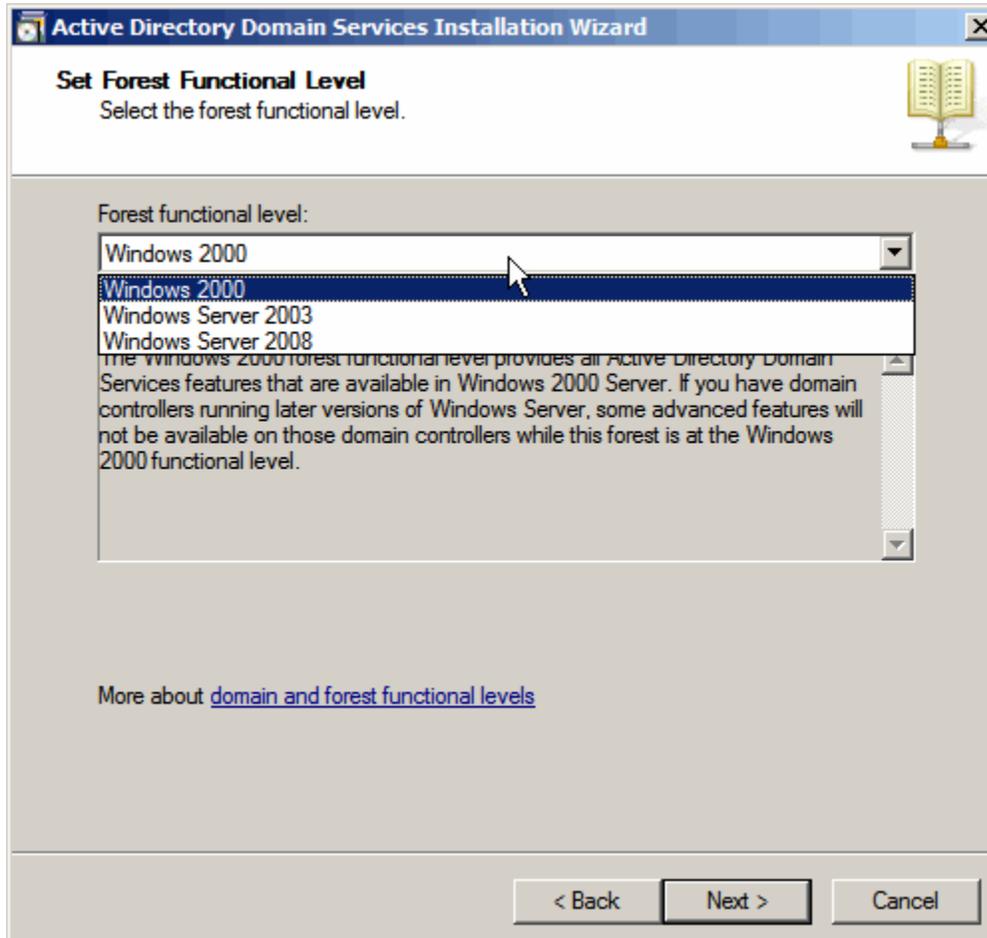
The screenshot shows the 'Active Directory Domain Services Installation Wizard' window. The title bar reads 'Active Directory Domain Services Installation Wizard'. The main heading is 'Name the Forest Root Domain'. Below the heading, there is a descriptive text: 'The first domain in the forest is the forest root domain. Its name is also the name of the forest.' To the right of this text is an icon of an open book. Below the text, there is a prompt: 'Type the fully qualified domain name (FQDN) of the new forest root domain.' A text input field contains the value 'petrilab.local'. Below the input field, there is an example: 'Example: corp.contoso.com'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. A mouse cursor is pointing at the 'Next >' button.

Note: Do NOT use single label domain names such as "mydomain" or similar. You MUST pick a full domain name such as "mydomain.local" or "mydomain.com" and so on.

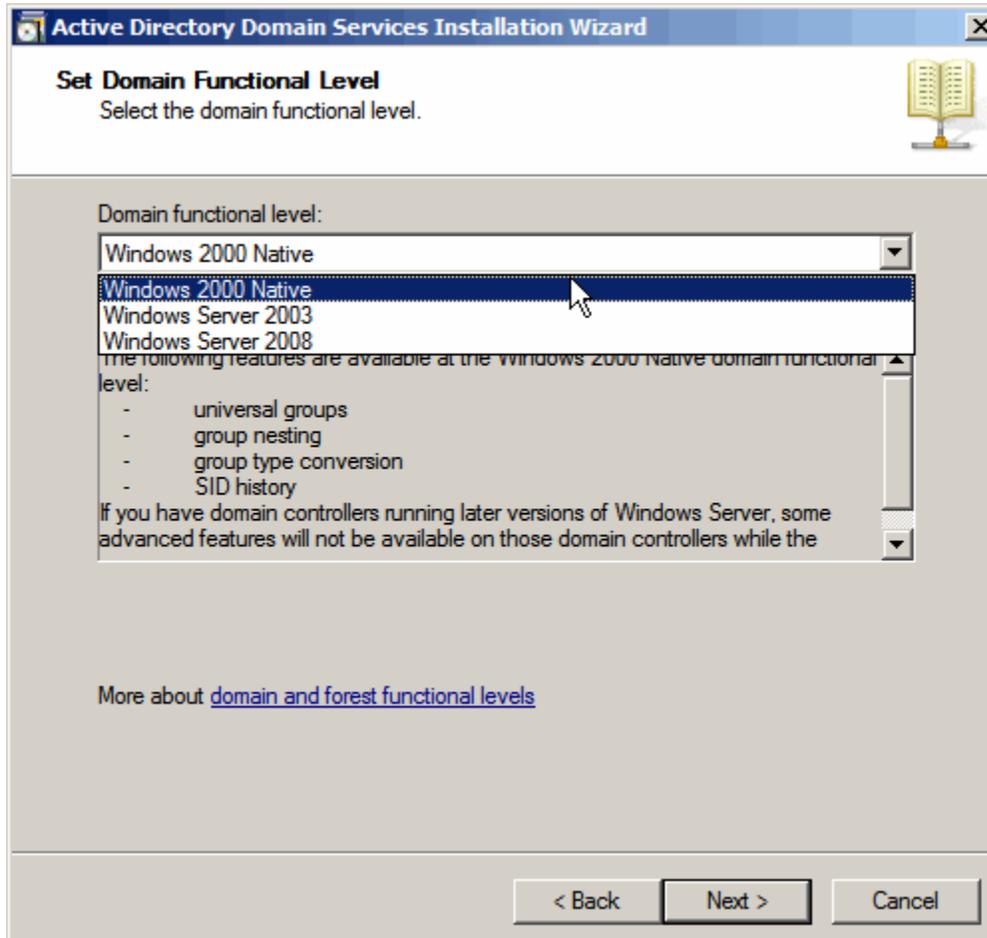
The wizard will perform checks to see if the domain name is not already in use on the local network.



6. Pick the right forest function level. Windows 2000 mode is the default, and it allows the addition of Windows 2000, Windows Server 2003 and Windows Server 2008 Domain Controllers to the forest you're creating.

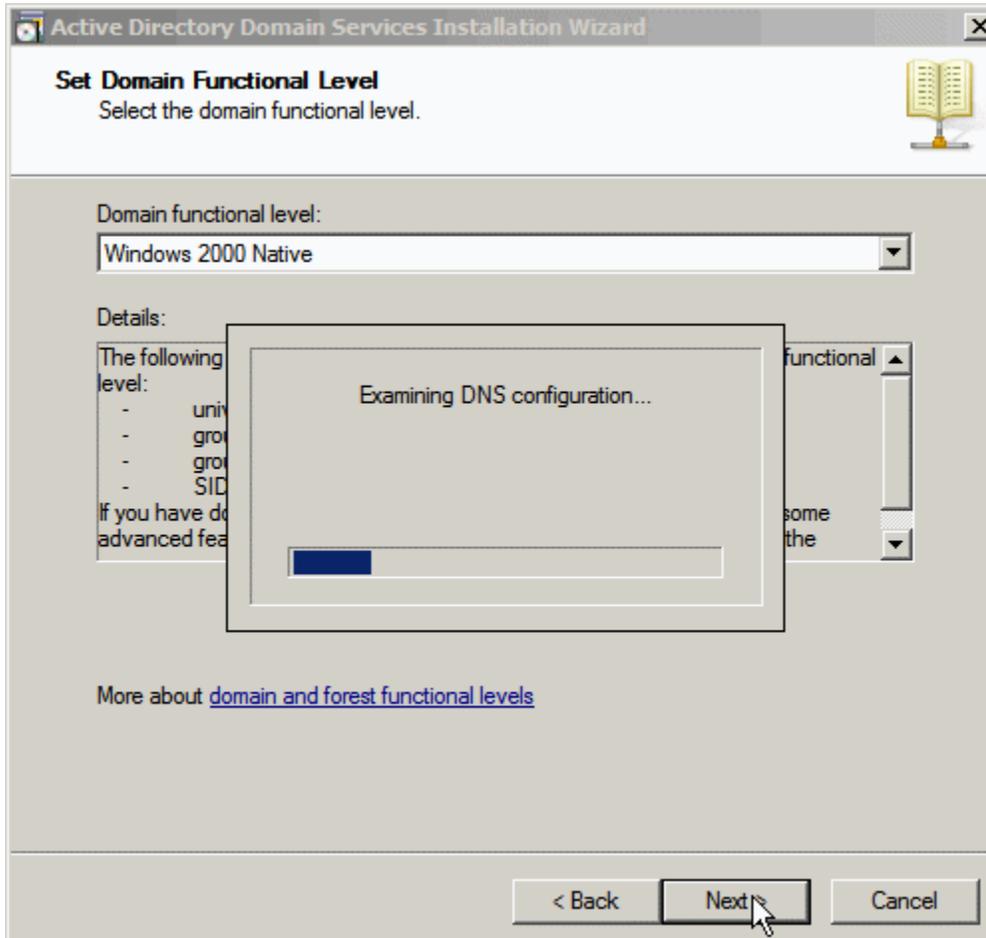


7. Pick the right domain function level. Windows 2000 Native mode is the default, and it allows the addition of Windows 2000, Windows Server 2003 and Windows Server 2008 Domain Controllers to the domain you're creating.



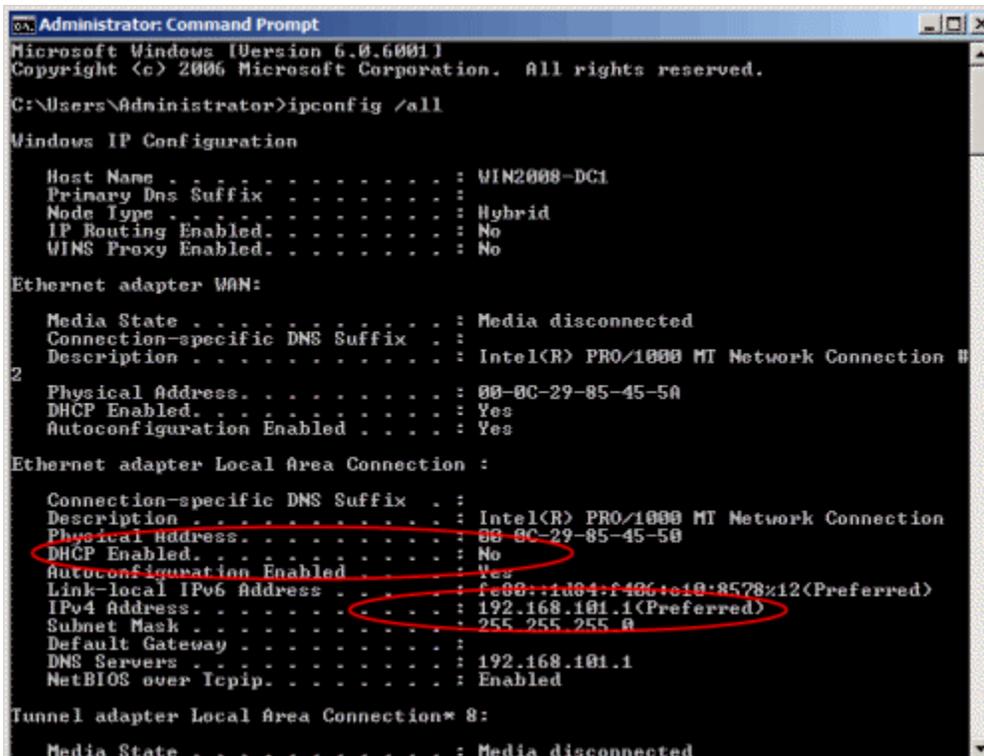
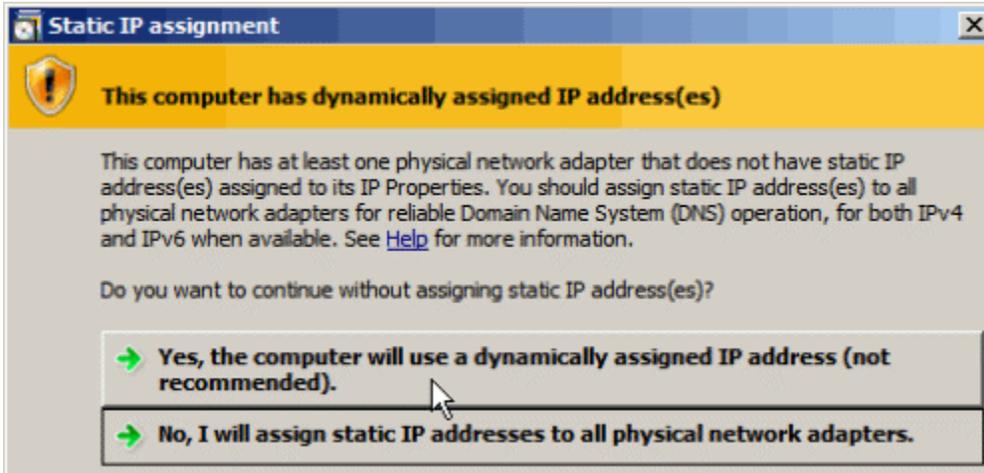
Note: If you select "Windows Server 2008" for the forest function level, you will Not be prompted to pick a domain function level.

8. The wizard will perform checks to see if DNS is properly configured on the local network. In this case, no DNS server has been configured, therefore, the wizard will offer to automatically install DNS on this server.

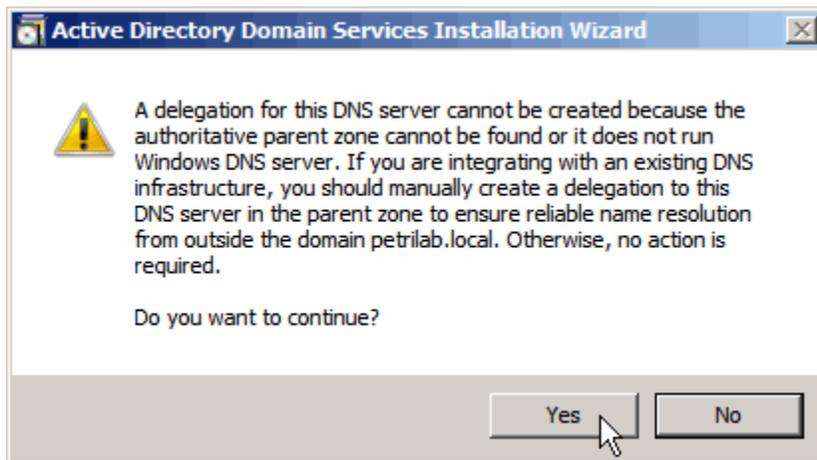


Note: The first DCs must also be a Global Catalog. Also, the first DCs in a forest cannot be a Read Only Domain controller.

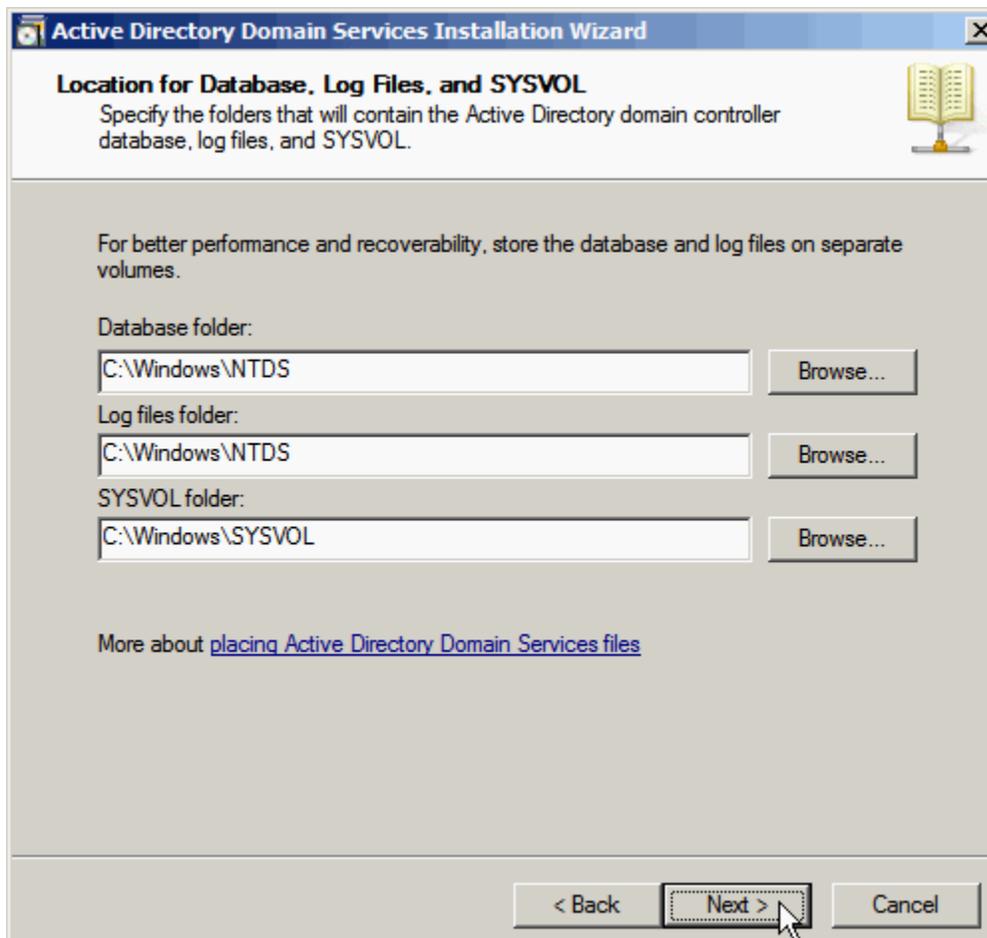
9. It's most likely that you'll get a warning telling you that the server has one or more dynamic IP Addresses. Running **IPCONFIG /all** will show that this is not the case, because as you can clearly see, I have given the server a static IP Address. So, where did this come from? The answer is IPv6. I did not manually configure the IPv6 Address, hence the warning. In a network where IPv6 is not used, you can safely ignore this warning.



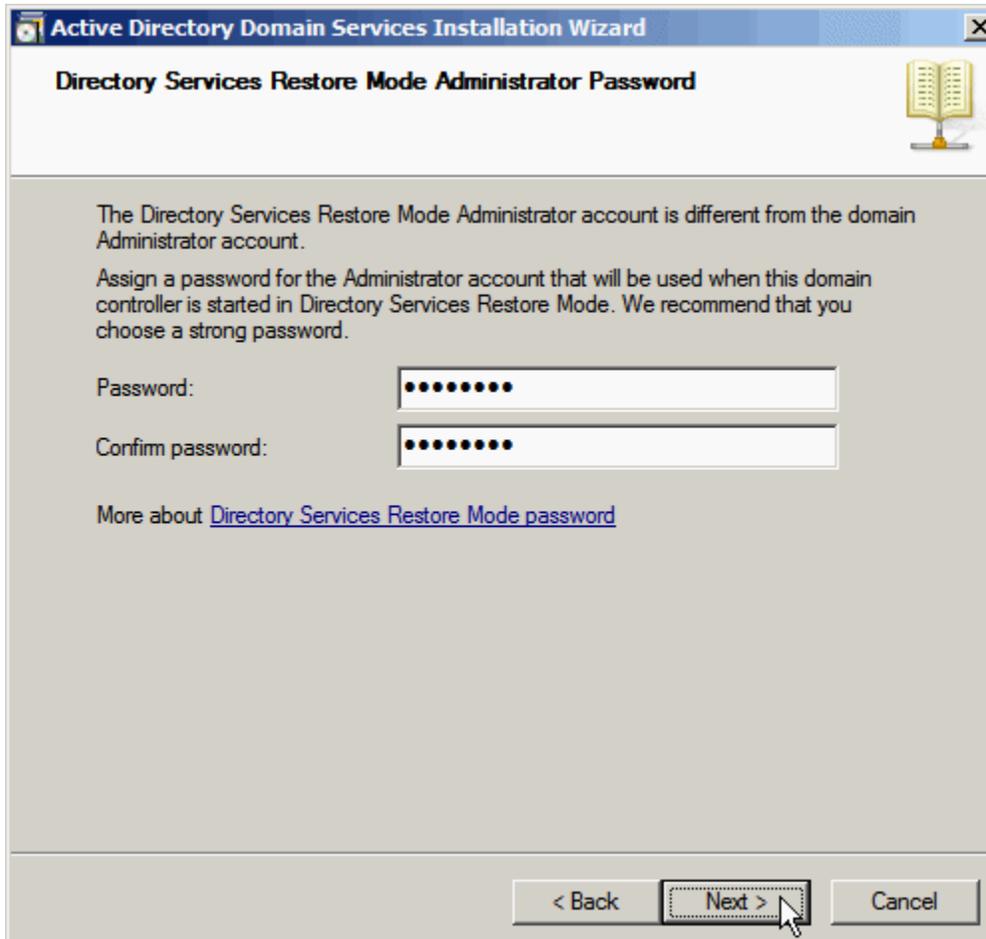
10. You'll probably get a warning about DNS delegation. Since no DNS has been configured yet, you can ignore the message and click **Yes**.



11. Next, change the paths for the AD database, log files and SYSVOL folder. For large deployments, carefully plan your DC configuration to get the maximum performance. When satisfied, click **Next**.

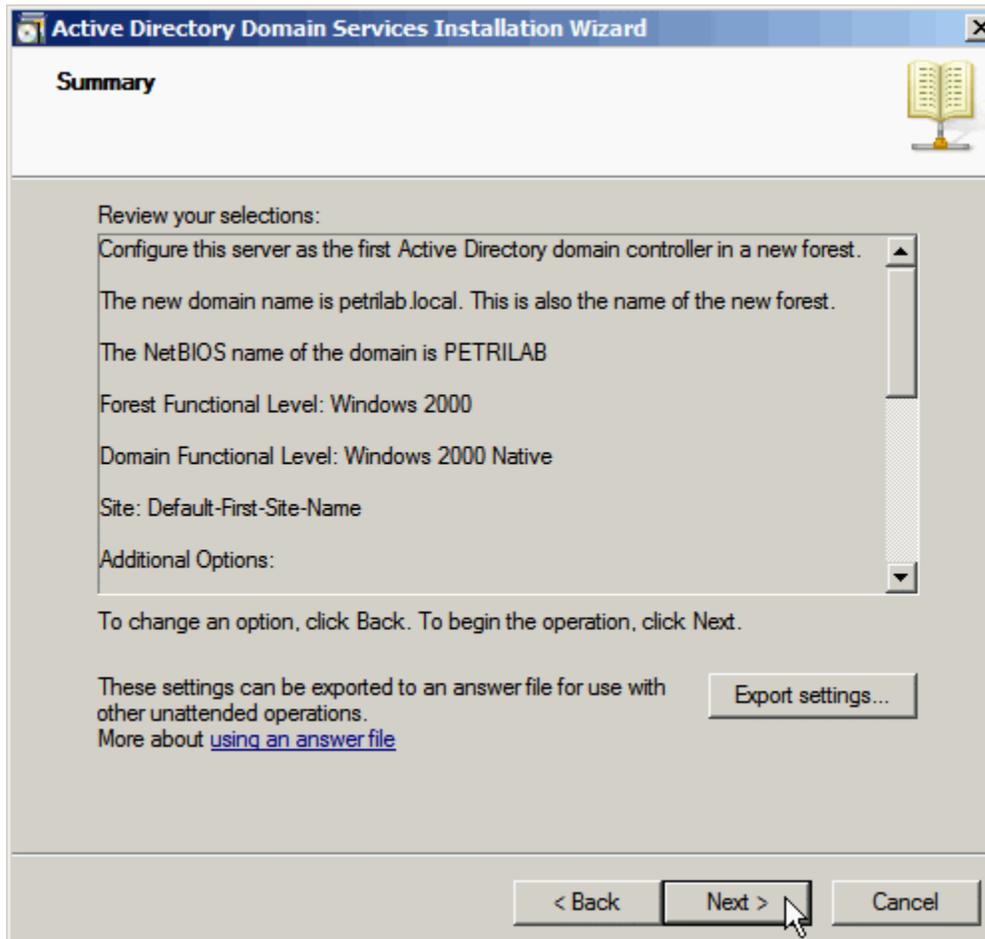


12. Enter the password for the Active Directory Recovery Mode. This password must be kept confidential, and because it stays constant while regular domain user passwords expire (based upon the password policy configured for the domain, the default is 42 days), it does not. This password should be complex and at least 7 characters long. I strongly suggest that you do NOT use the regular administrator's password, and that you write it down and securely store it. Click **Next**.

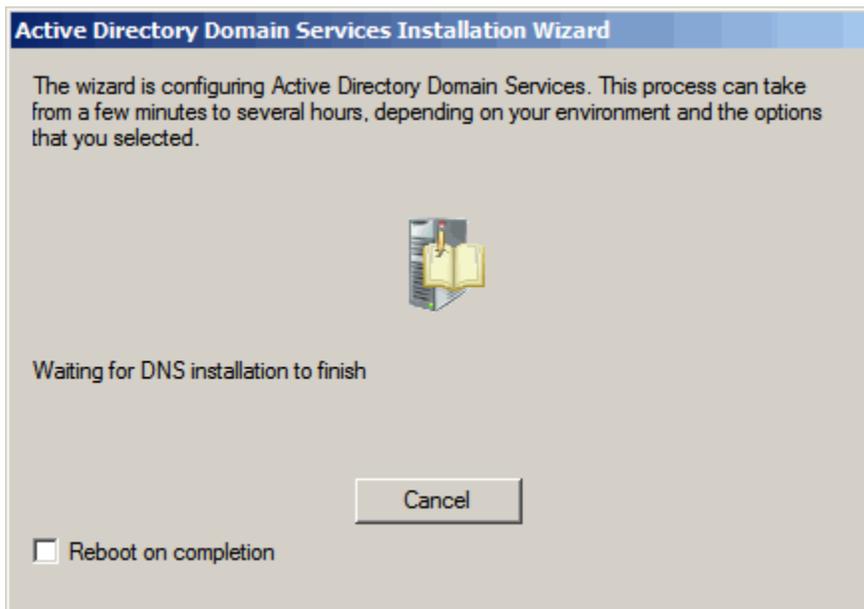


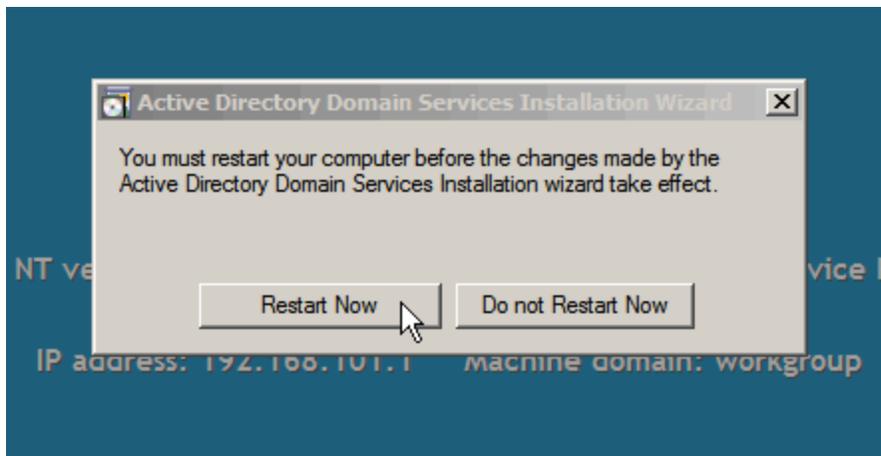
The screenshot shows a Windows-style dialog box titled "Active Directory Domain Services Installation Wizard". The main heading is "Directory Services Restore Mode Administrator Password". To the right of the heading is an icon of an open book. Below the heading, there is explanatory text: "The Directory Services Restore Mode Administrator account is different from the domain Administrator account. Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password." There are two input fields: "Password:" and "Confirm password:", both containing seven black dots. Below the fields is a blue hyperlink: "More about [Directory Services Restore Mode password](#)". At the bottom, there are three buttons: "< Back", "Next >" (which is highlighted with a mouse cursor), and "Cancel".

13. In the Summary window review your selections, and if required, save them to an unattend answer file. When satisfied, click **Next**.



14. The wizard will begin creating the Active Directory domain, and when finished, you will need to press **Finish** and reboot your computer.



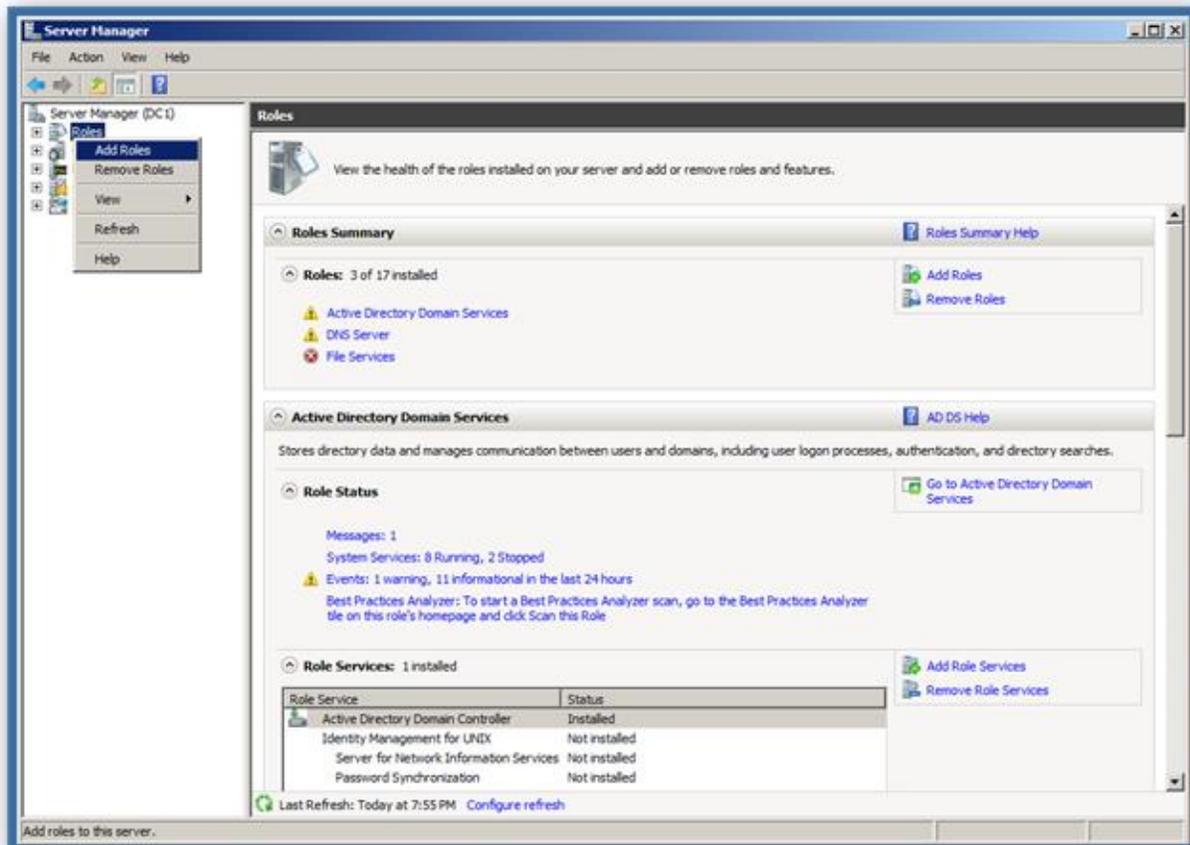


Note: You can automate the rebooting process by checking the Reboot on Completion checkbox.

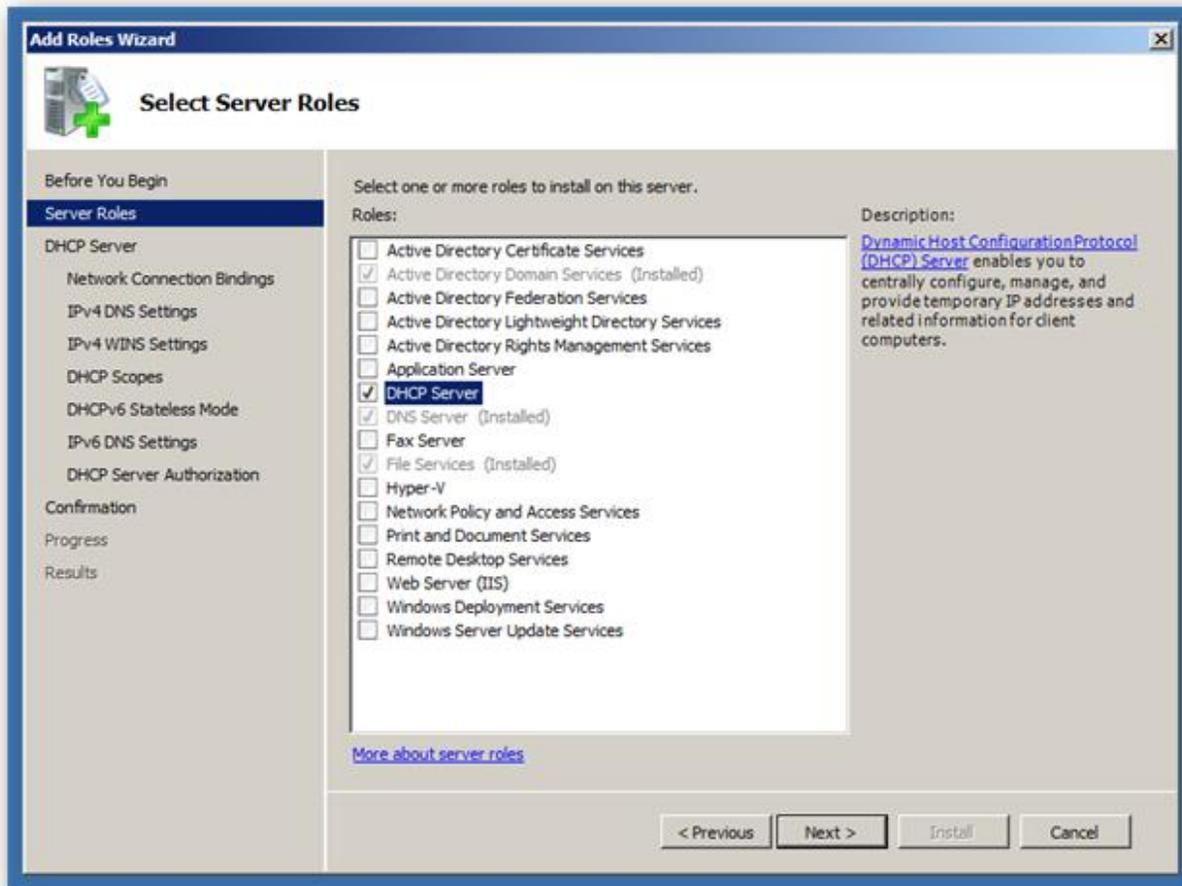
Your server now acts as a Domain Controller. Make sure you properly back it up. You can test functionality by using AD management tools such as Active Directory Users and Computers, examine the Event Logs, services and folders and shares that have been created.

2. Installing Dynamic Host Configuration Protocol (DHCP)

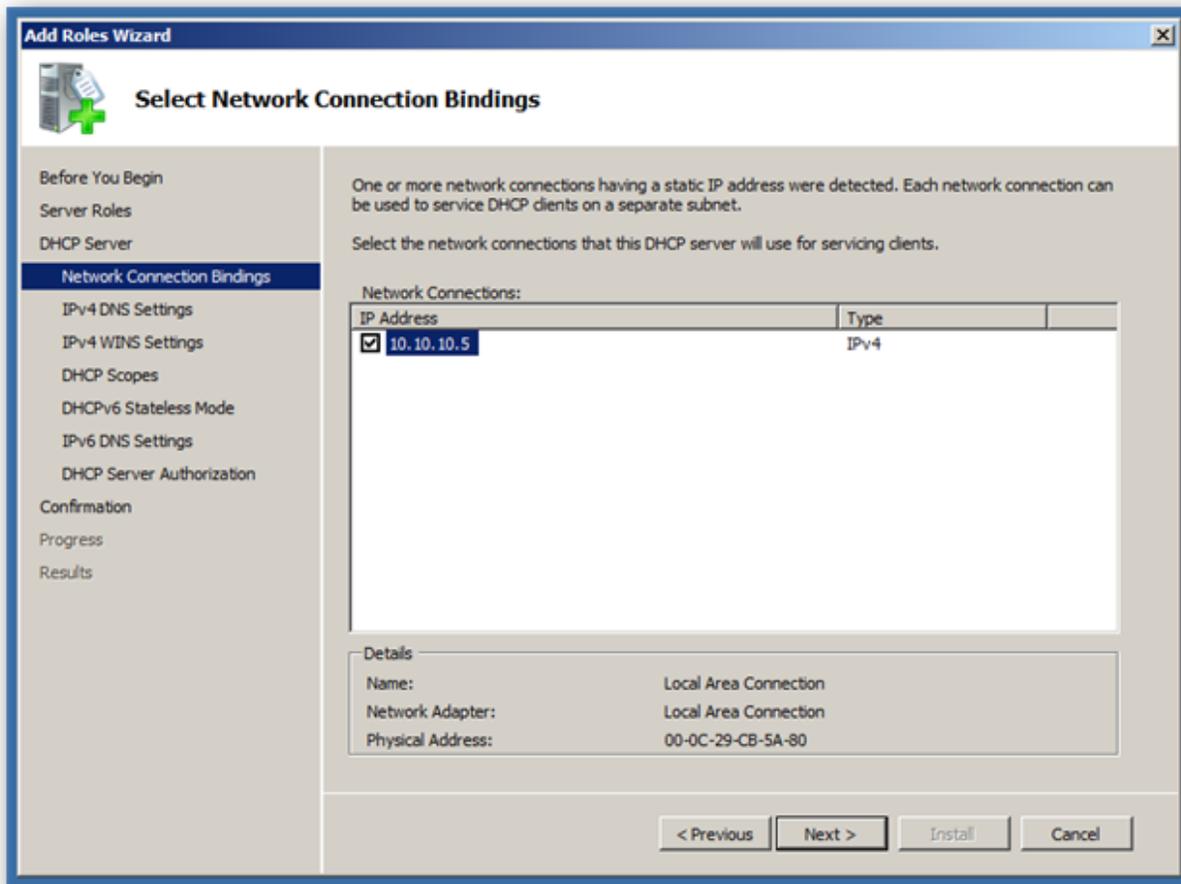
To get started, fire up the Server Manager, right click on roles, and then select add roles.



You will be prompted with the normal "Before You Begin" screen, and after clicking Next you'll be able to choose DHCP Server.



Next you'll want to select the network connection to bind the DHCP protocol to.



Put in the IP address of your DNS Server, which in this case is the same machine—but be careful not to put the loopback address (127.0.0.1) as this will be the address your clients will go to for name resolution.

The screenshot shows the 'Add Roles Wizard' window with the title 'Specify IPv4 DNS Server Settings'. The left sidebar contains a list of steps: 'Before You Begin', 'Server Roles', 'DHCP Server', 'Network Connection Bindings', 'IPv4 DNS Settings' (highlighted), 'IPv4 WINS Settings', 'DHCP Scopes', 'DHCPv6 Stateless Mode', 'IPv6 DNS Settings', 'DHCP Server Authorization', 'Confirmation', 'Progress', and 'Results'. The main area contains the following text and fields:

When clients obtain an IP address from the DHCP server, they can be given DHCP options such as the IP addresses of DNS servers and the parent domain name. The settings you provide here will be applied to clients using IPv4.

Specify the name of the parent domain that clients will use for name resolution. This domain will be used for all scopes you create on this DHCP server.

Parent domain:

Specify the IP addresses of the DNS servers that clients will use for name resolution. These DNS servers will be used for all scopes you create on this DHCP server.

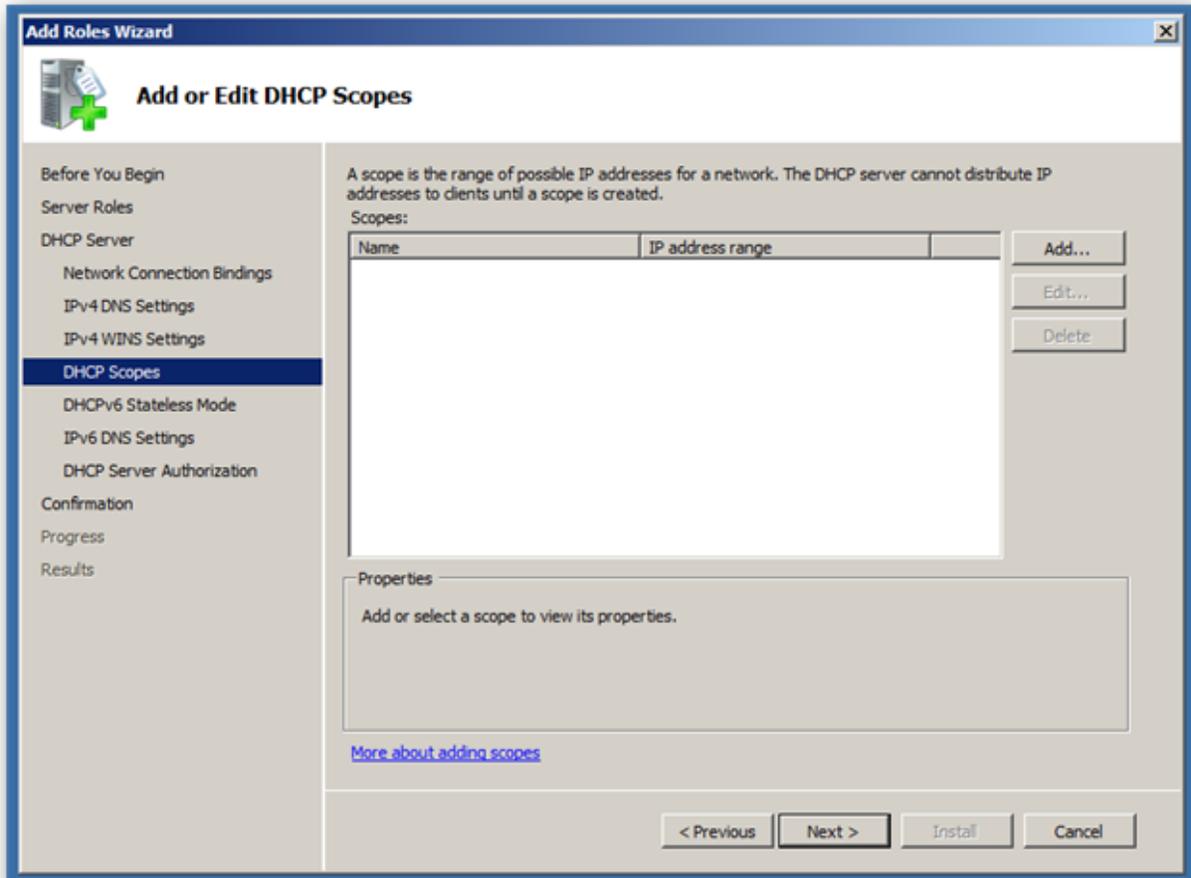
Preferred DNS server IPv4 address:

Alternate DNS server IPv4 address:

[More about DNS server settings](#)

At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

Click next again to skip the WINS setup, this will bring you to creating a DHCP Scope, where you can click the Add button.



Now you need to:

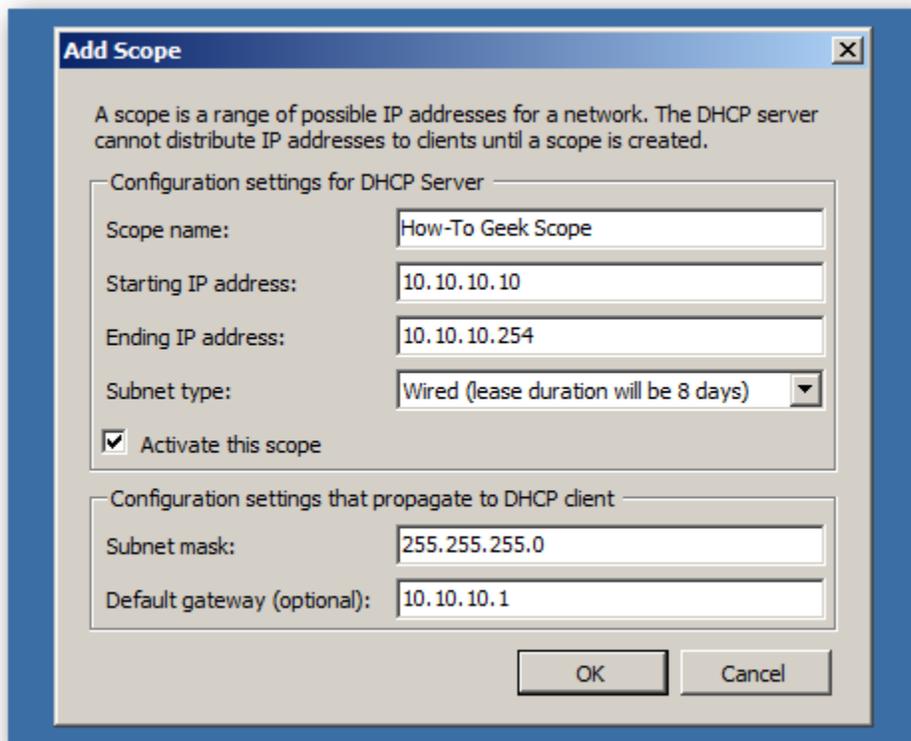
Give your scope a name

Enter the first address that you want available to clients to use

Enter the last address that you want available to clients to use

Enter the subnet mask (usually 255.255.255.0)

Enter the IP address of your default gateway (usually your router IP at .1)



The image shows a screenshot of the 'Add Scope' dialog box in the Windows DHCP console. The dialog box has a title bar with the text 'Add Scope' and a close button. Below the title bar, there is a descriptive text: 'A scope is a range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.' The dialog is divided into two sections: 'Configuration settings for DHCP Server' and 'Configuration settings that propagate to DHCP client'. In the first section, the 'Scope name' is 'How-To Geek Scope', 'Starting IP address' is '10.10.10.10', 'Ending IP address' is '10.10.10.254', and 'Subnet type' is 'Wired (lease duration will be 8 days)'. There is a checked checkbox for 'Activate this scope'. In the second section, the 'Subnet mask' is '255.255.255.0' and the 'Default gateway (optional)' is '10.10.10.1'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Add Scope

A scope is a range of possible IP addresses for a network. The DHCP server cannot distribute IP addresses to clients until a scope is created.

Configuration settings for DHCP Server

Scope name: How-To Geek Scope

Starting IP address: 10.10.10.10

Ending IP address: 10.10.10.254

Subnet type: Wired (lease duration will be 8 days)

Activate this scope

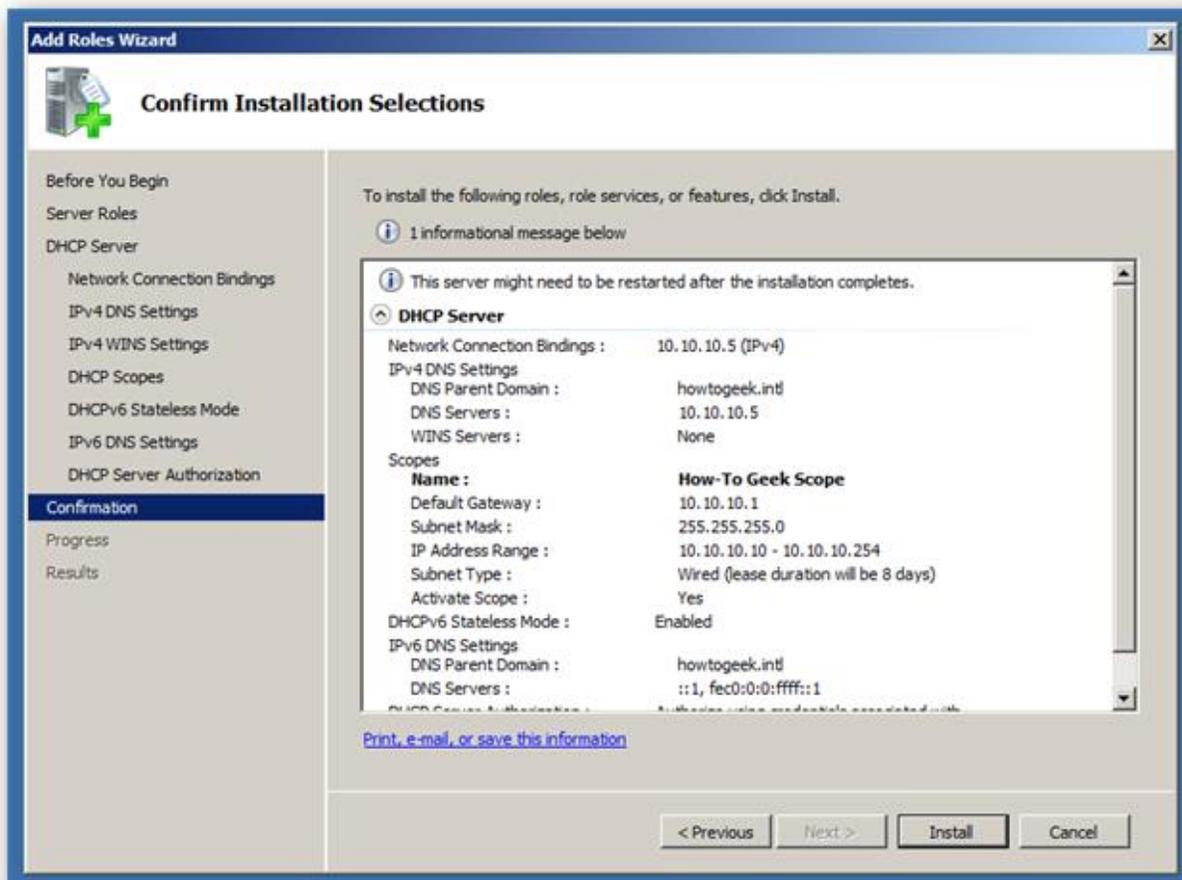
Configuration settings that propagate to DHCP client

Subnet mask: 255.255.255.0

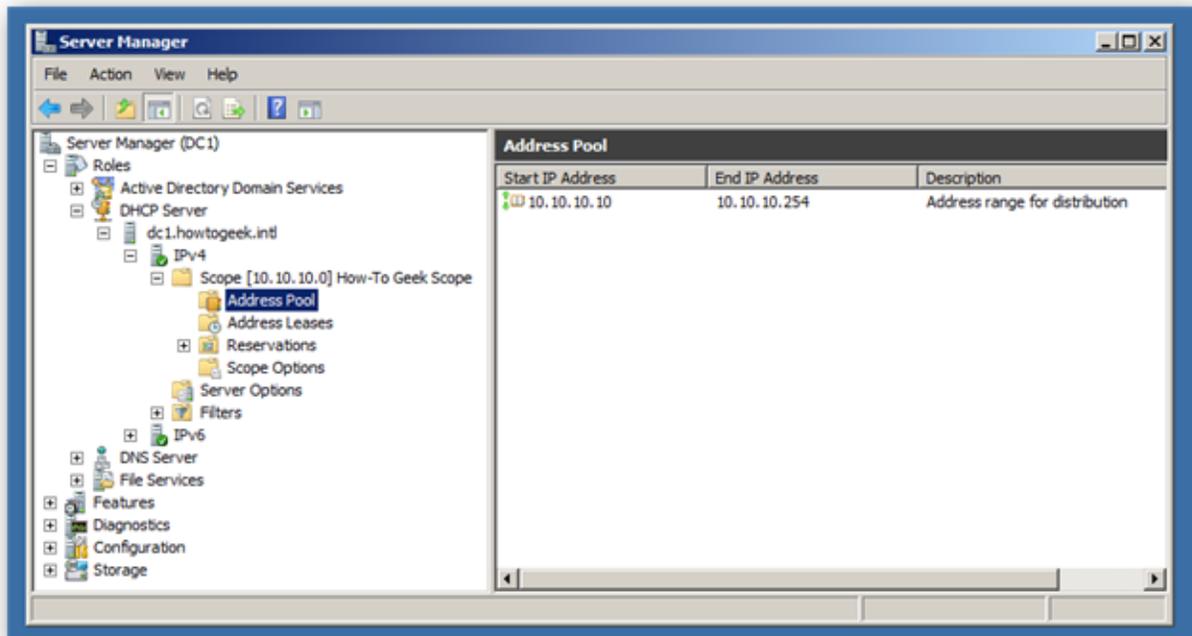
Default gateway (optional): 10.10.10.1

OK Cancel

Once you have clicked on OK, you can click next 4 times to get to the confirmation screen where you can finally click install.



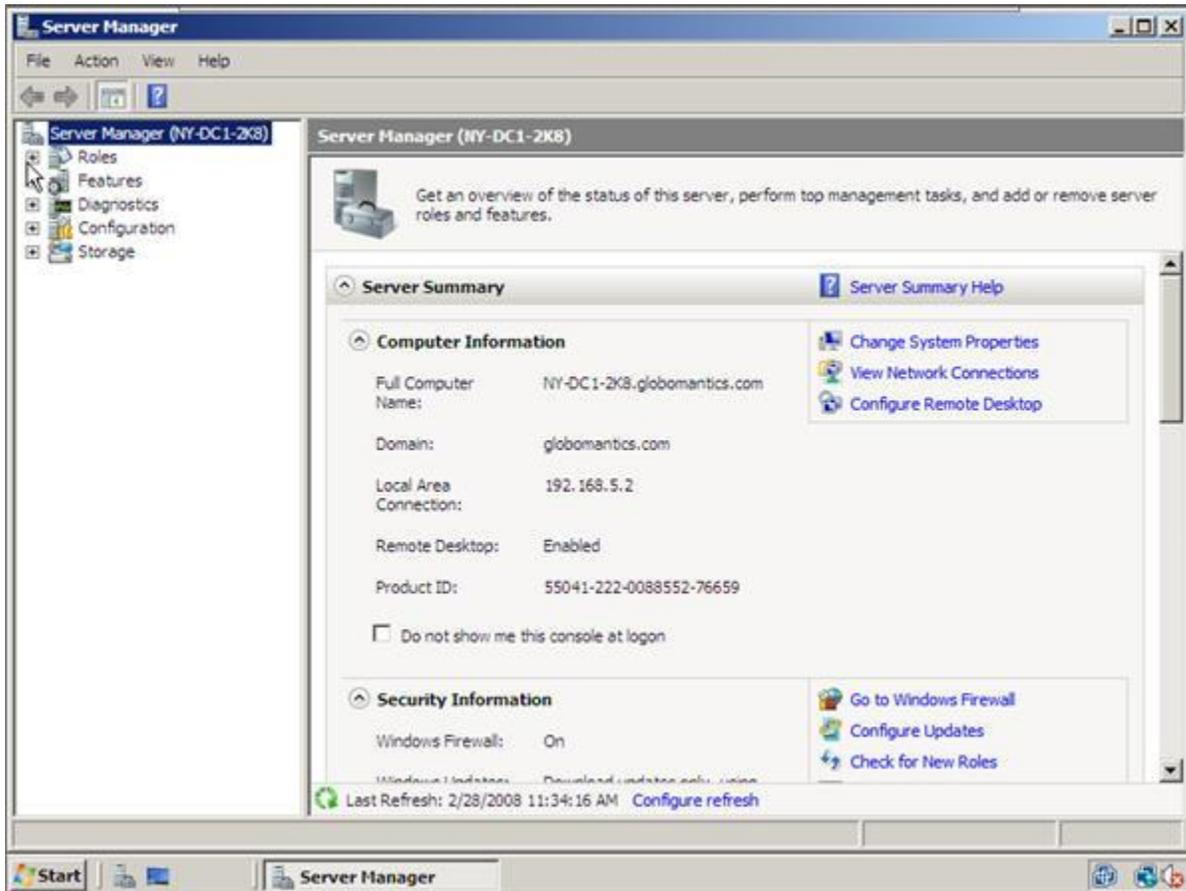
Once the installation is complete your DHCP will be functioning, and you can start managing your DHCP server right away.



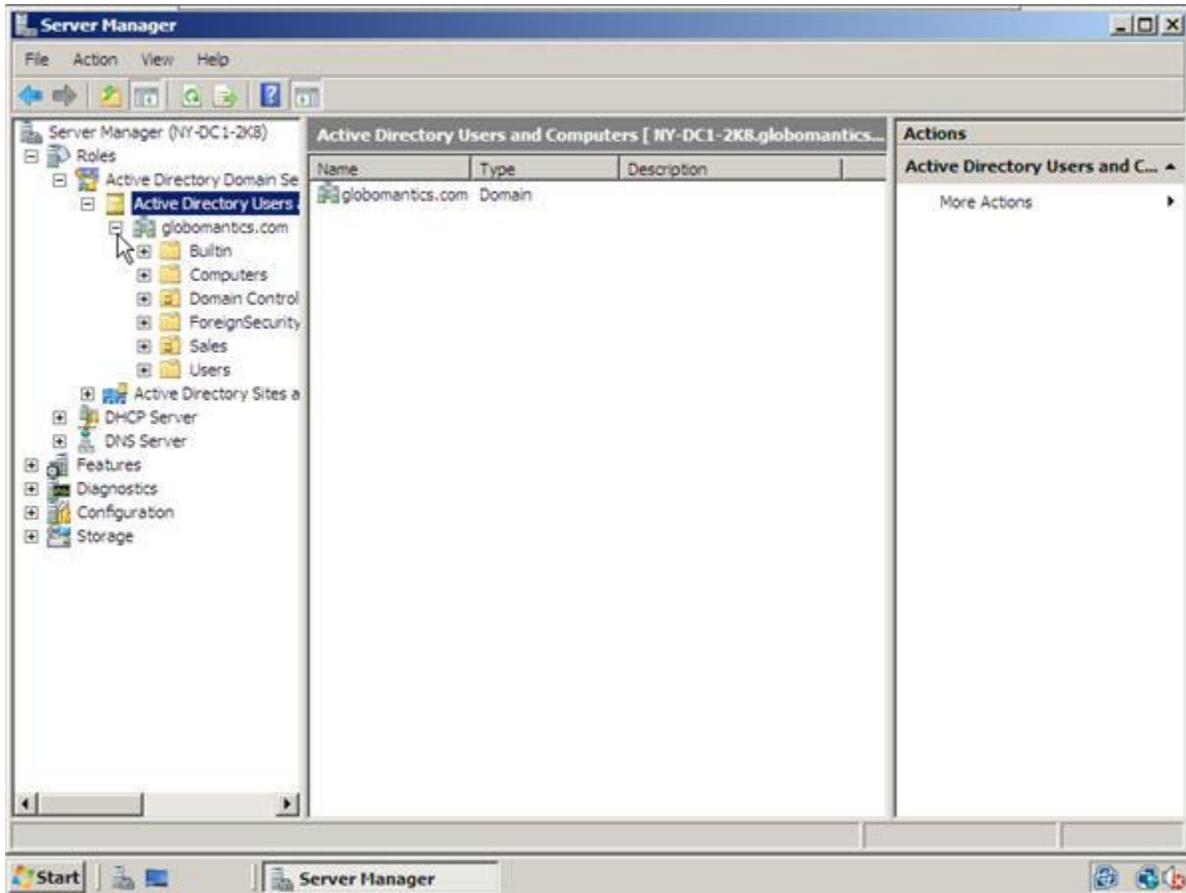
Part 3. Account Management

a. How To Create a New User Account in Active Directory

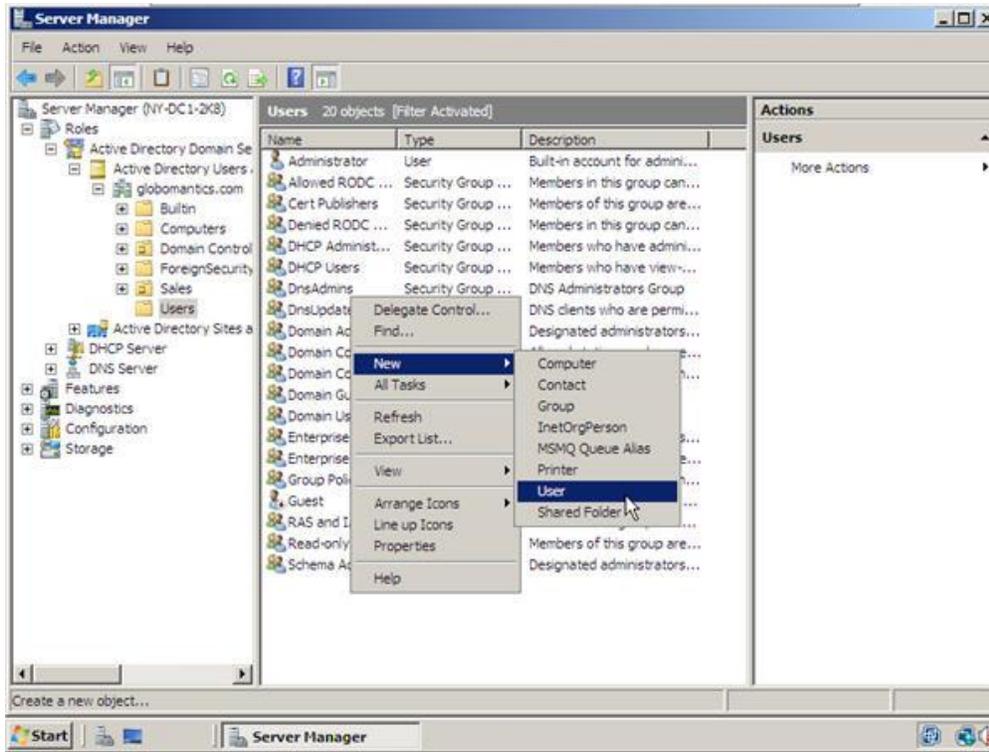
1. To start let's go ahead and open up Server Manager



2. Next we will open up the **Roles** section, next to **Active Directory Users and Computers** section and finally the **Active Directory Users and Computers**. You should now see your domain name.

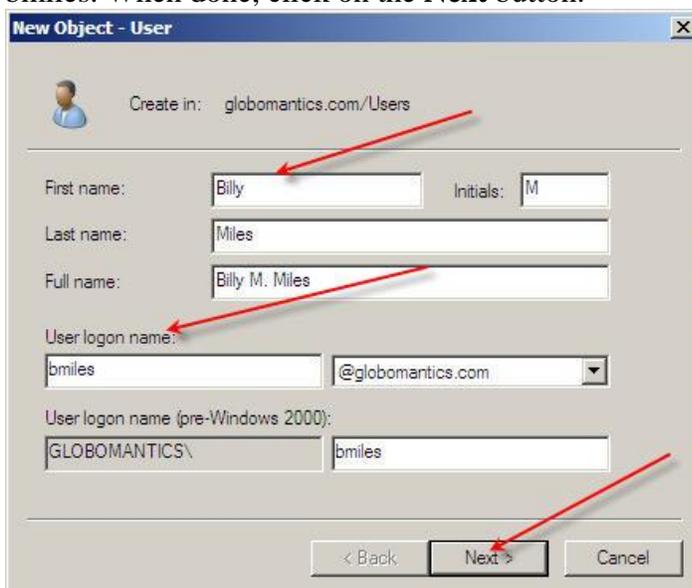


3. We are going to click on our **Users** section where we are going to create a new User Account. To do so, right-click on the blank section, point to **New** and select **User**.



4. In this window you need to type in the user's first name, middle initial and last name. Next you will need to create a user's logon name.

In our example we are going to create a user account for Billy Miles and his logon name will be bmiles. When done, click on the **Next** button.



5. In the next window you will need to create a password for your new user and select appropriate options.

In our example we are going to have the user change his password at his next logon. You can also prevent a user from changing his password, set the password so that it will never expire or completely disable the account.

When you are done making your selections, click the **Next** button.

The screenshot shows a Windows-style dialog box titled "New Object - User". At the top left is a user icon and the text "Create in: globomantics.com/Users". Below this are two password input fields: "Password:" and "Confirm password:", both containing masked characters. There are four checkboxes: "User must change password at next logon" (checked), "User cannot change password", "Password never expires", and "Account is disabled". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

6. And finally, click on the **Finish** button to complete the creation of new User Account.

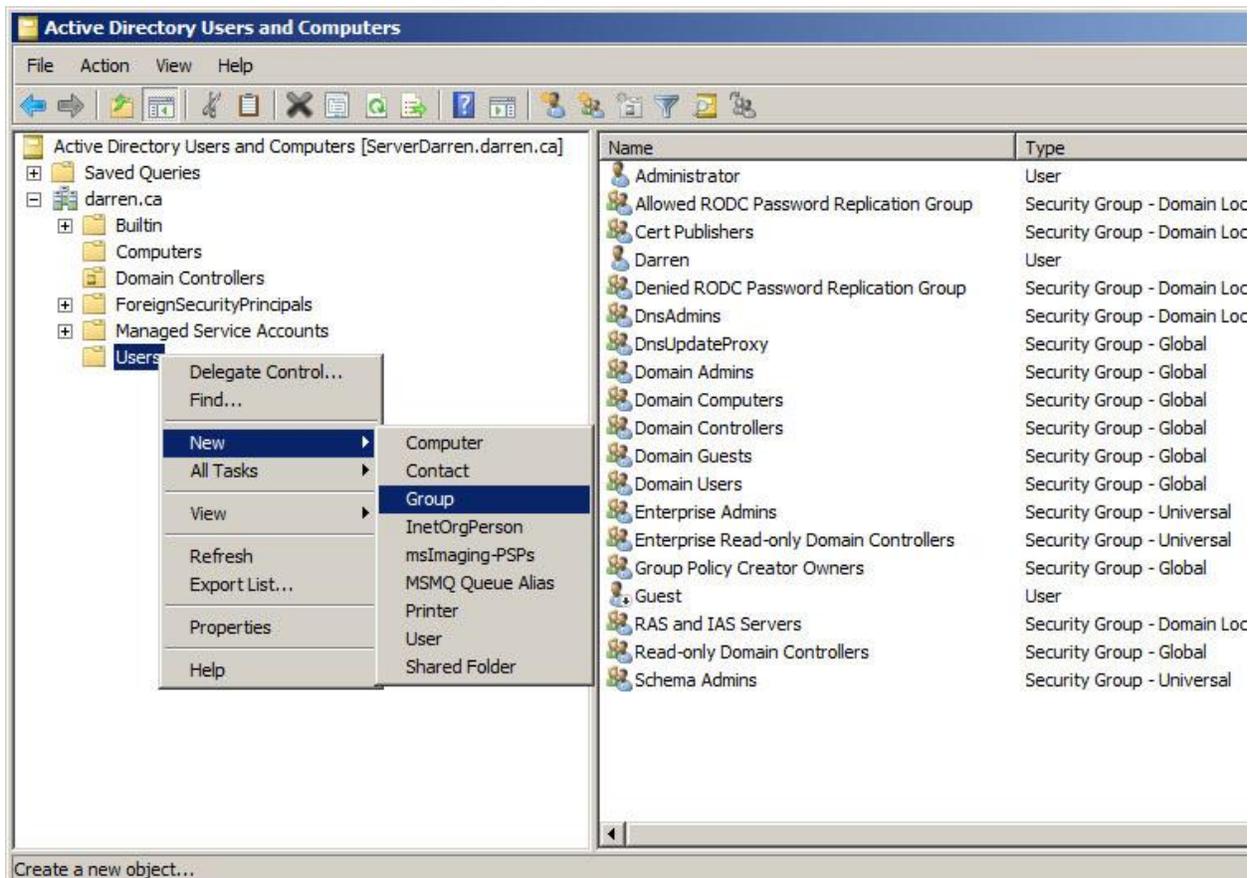


b. How To Create a New User Group Account and add Users to the group in Active Directory

Active Directory Users and Computers

Adding a new user group

1. Go to Start → Administrative Tools → Active Directory Users and Computers
2. Expand a domain name in the left column
3. Highlight Users and select New → Group
4. Type in a Group Name and leave the Group Scope on Global and Group Type on Security.
5. Click OK and a new Group has been added to the right hand column list.



Active Directory Users and Computers

Adding user(s) to a group

Note: There are a few ways one could go about doing this, pick one that's the easiest and least painful to do.

1. Go to Start → Administrative Tools → Active Directory Users and Computers
2. Expand a domain name in the left column
3. Mouse click on Users in the left column to show Users and Groups in the right column
4. Refer to the methods provided below to continue.

Method 1:

1. Hold Control key + click and select individual users that you're going to add to a group and right click **Add to Group**. Type in the group name and click Check Names then click OK.

Method 2:

1. Double click the group name or right click and select **Properties**
2. Click on the **Member Of** tab and click on Add to start adding the users to this group. Click Check Names to verify the names that have been added and then click OK.

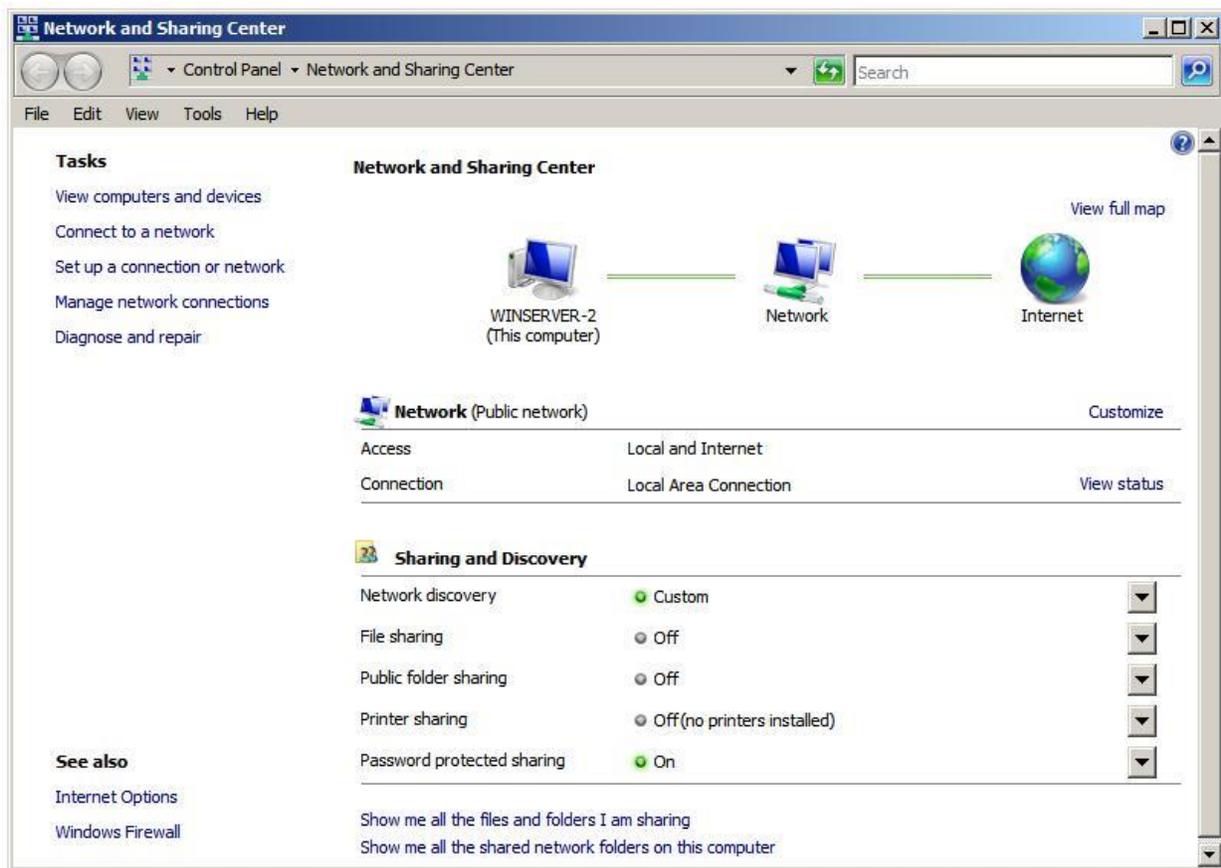
Method 3:

1. Select individual user names and double click or right click and select **Properties**.
2. Locate and click on the **Member Of** tab for that individual user.
3. Click on the **Add** button to add the group or groups for that individual user account. Ok.

Part 5. Sharing

Enabling File Sharing

File sharing in Windows Server 2008 R2 is managed from the *Network and Sharing Center*, accessed by selecting *Start -> Network* and clicking on the *Network and Sharing Center* button in the toolbar. Once invoked, the Network and Sharing Center will list the current file sharing configuration and options as illustrated in the following figure:



To enable public file sharing, click on the down arrow next to the *Public folder sharing* in the section entitled *Sharing and discovery*. This will provide the following list of public folder sharing options:

- **Turn on sharing so anyone with network access can open files** - Allows network users to open, but not delete, modify or create files in the server's public folder.

- **Turn on sharing so anyone with network access can open, change and create files** - Allows network users to open, modify, delete and create files in the public folder.
- **Turn off sharing (people logged on to this computer can still access this folder)** - Allow public folder access only to those users locally logged on to the server. Network users are denied access.

Similarly, *standard file sharing* can be configured by click the down arrow next to *File sharing*. When unfolded, this panel provides the option to either enable or disable standard file sharing on this server. When enabled, a dialog will appear providing the option to make the shared folders available only to the private network on which the system resides, or to make sharing available to public networks. The choice here depends on the requirements of the organization but for security purposes it is typically best to limit sharing to the private network unless external access is required.

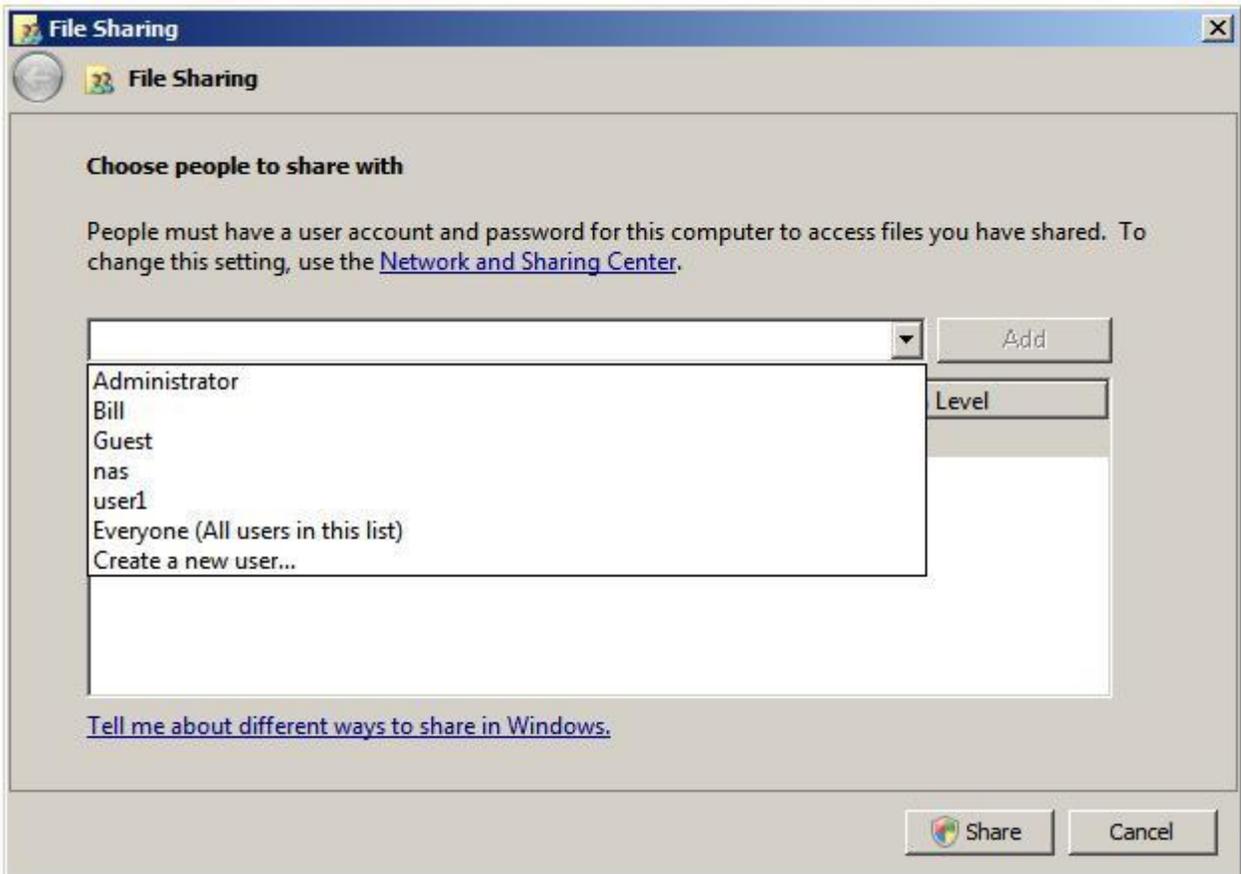
The *Network and Sharing Center* also allows password access to shared folders to be configured. When the arrow next to *Password protected sharing* is selected the options to enable or disable password protection sharing are provided. When enabled on workgroup servers, only users with user accounts and passwords on the server will be able to access shared files and folders.

Creating Shared Folders with Windows Explorer

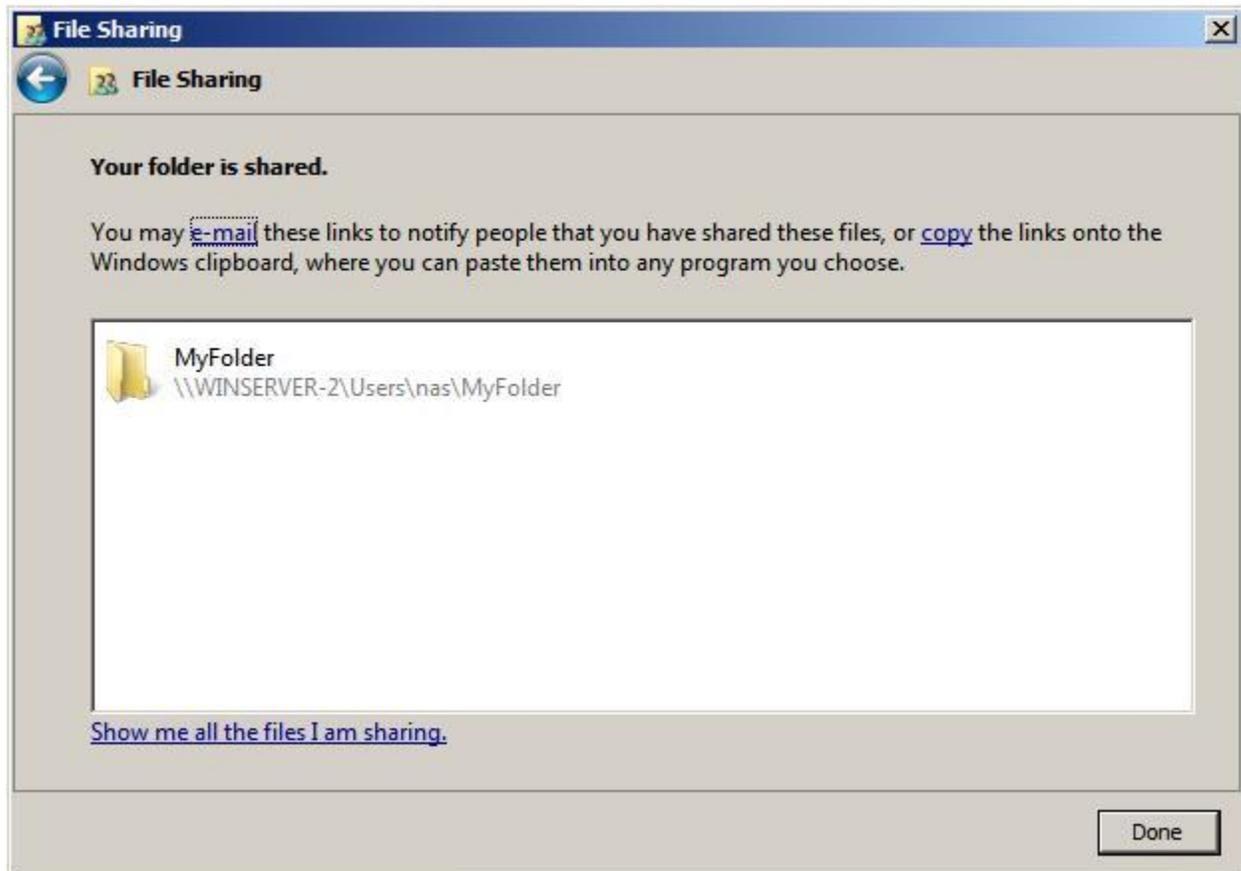
Shared folders can be configured using Windows Explorer, simply by navigating to the folder to be shared, right clicking on the folder and selecting *Properties* from the menu. In the properties dialog, click on the *Sharing* tab to display and modify the current shared folder settings as illustrated in the following figure:



Within the sharing property panel, click on the *Share...* button to access the *File Sharing* dialog. Within this dialog, the users who may access this shared folder are specified. If file sharing has been restricted to users with local accounts and passwords, a list of users can be obtained by clicking on the down arrow. In this situation, select and add users, or select *Everyone* if access is to be made available to all users with local accounts:

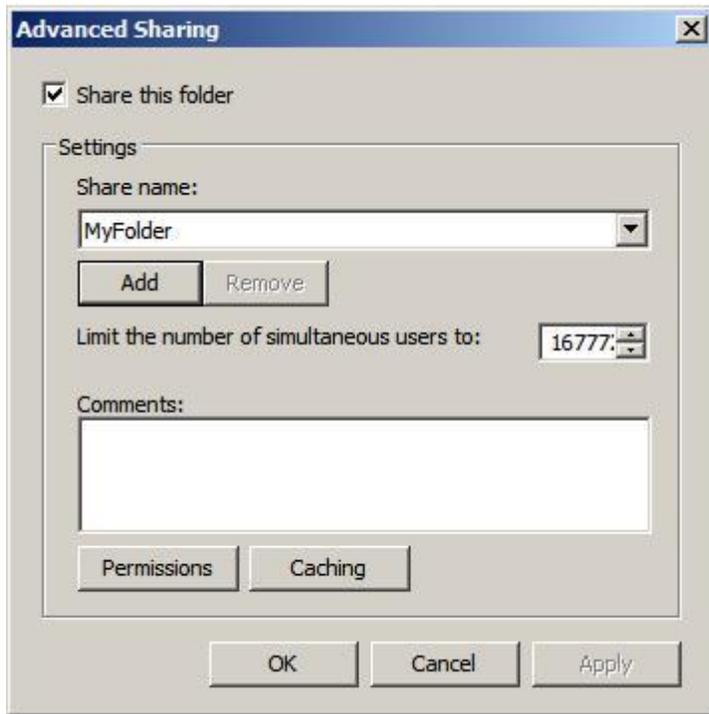


Once these settings are complete, click on the *Share* button to initiate the file sharing process. Once this initial phase of the share setup is complete a dialog will appear announcing this fact, listing the full Universal Naming Convention (UNC) path to the shared folder and providing the option to email users to notify them of this fact:

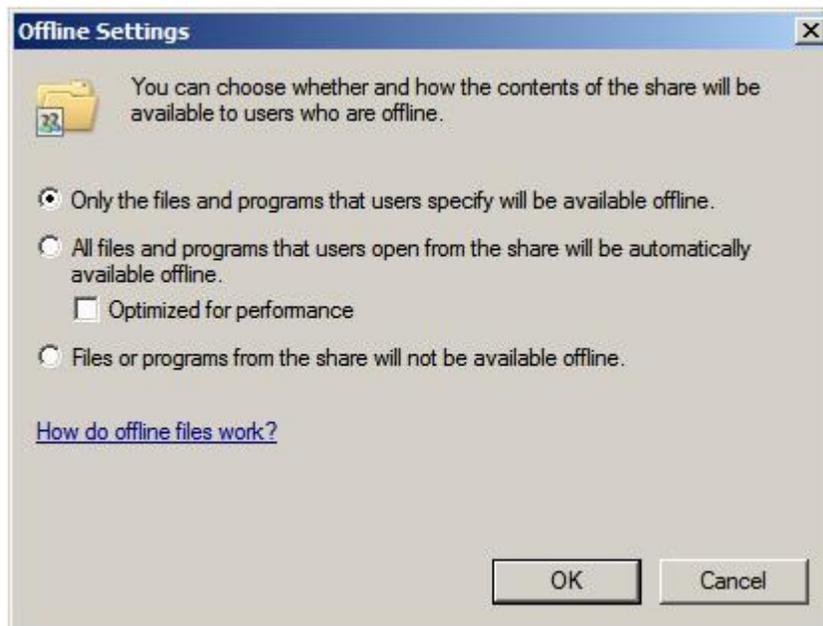


Having specified which users will have access to the folder the next step is to enable the sharing of the folder, specify *share permissions* and configure a *Share Name* by which the folder will be referenced and accessed. In addition caching of shared files can be configured. Caching allows users to maintain local copies of shared files so that they can be accessed *off-line* (for example when the server hosting the files is not available to the user's local system). With caching configured, local copies of shared files are stored on the user's local system so that they can be accessed without a connection to the server. When a connection is re-established, any changes made to the local copy of the file are synchronized with the original copy on the server.

To configure these settings, click on the *Advanced Sharing* button to display the following dialog:



In this dialog, set the *Share this folder* option to enable the sharing of the folder. Once this has been selected the *Share name* field and associated button will activate enabling a share name to be entered. By default the name of the folder being shared will be displayed, although this may be changed to another name if desired. If the number of concurrent users accessing a shared folder is of concern, modify the number of simultaneous users accordingly. Enter optional comments about the share before clicking on *Caching* to configure the *off-line* file settings. This will invoke the *Offline Settings* dialog where a number of options are available including allowing each user to specify which files they would like to be able to access off-line, only having files that users actually access available off-line and disabling off-line sharing all together:



Understanding and Configuring Share Permissions

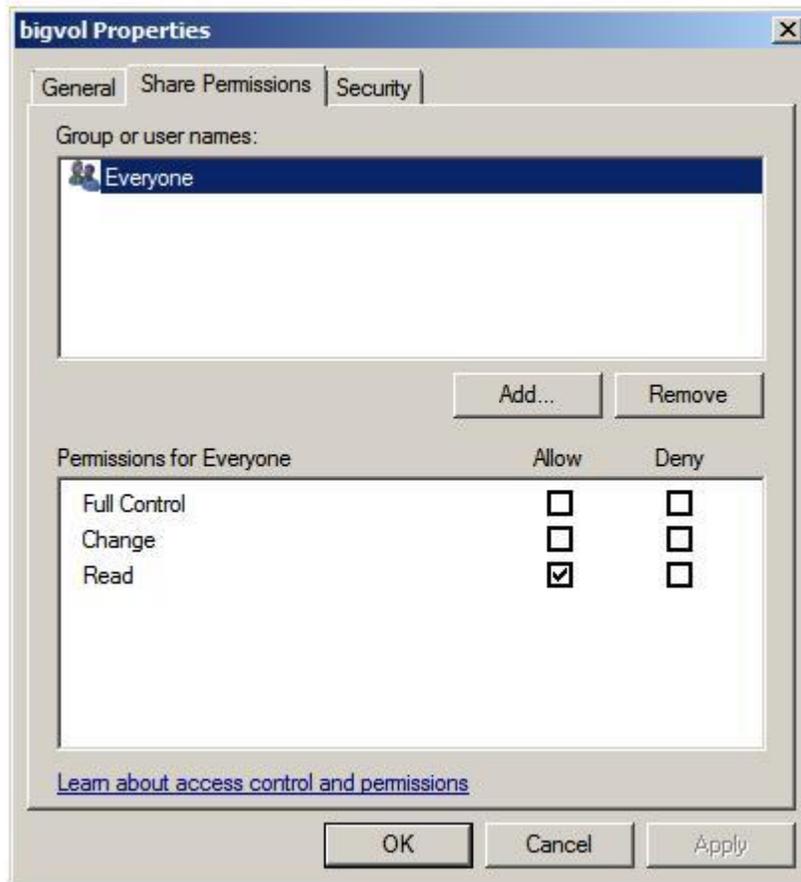
As outlined at the beginning of this chapter, Windows Server 2008 R2 provides two levels of permissions for shared files and folders, namely *share permissions* and *file and folder permissions*. Share permissions are applied when access is made via the network. When shared files and folders are accessed locally from the server on which they reside these permissions serve no purpose. File and folder permissions, on the other hand, take effect both when accessing files and folders both locally and over the network. In the case of network access to shared files and folders, the share permissions are applied first, followed by any file and folder permissions. The key issue to note is that file and folder permissions provide a far greater level of control over access than the more general permissions options provided by share permissions. In this section, share permissions will be covered.

Share permissions are granted on a per user and per group basis. In addition to allowing a cap on the number of concurrent users accessing a share to be defined, share permissions also provide three permission options, each of which can be set to *Allow* or *Deny*:

- **Full Control** - Grants the specified users permission to change file and folder permissions, execute, read, modify, create and delete files and sub-folders.
- **Change** - Grants users permission to change file and folder attributes, read, modify, execute, create and delete files and sub folders.
- **Read** - Grants users permission to read and execute files and view and access file lists and sub-folders.

Permissions are cumulative in that a user will inherit the permissions of all the groups of which he or she is a member. If a permission is *Denied*, however, it overrides any cases where that permission may have been granted. For example, if a user is a member of a group where full control is provided over a folder, and also a member of a second group where full control is specifically denied, the user will be denied full control regardless of the fact that it was granted in the first group.

To configure share permissions, start Computer Management, connect to a remote server if not working on local shares, unfold System Tools and select *Shares* to list all currently shared folders. To configure share permissions for a folder, select it from the list, right click and select *Properties*. In the properties dialog select the *Share Permissions* tab as illustrated in the following figure:



This screen displays the current share permissions and provides the ability to configure additional permission controls. To change the settings for a currently configured group or user select the user from the list, modify the permissions accordingly and click on *Apply* to commit the changes.

To add permissions for a specific user or group click the *Add* button and enter one or more users or groups into the text box (separating multiple entries with a semi-colon) and click on *Check Names* to verify the names are correct. Click on *OK* to return to the properties dialog where the added users and groups will appear in the list. Once again, select each name in turn and configure the desired share permissions. Finally, click *Apply* to commit the new permissions.

Part 6. Resources

- a. <http://www.petri.co.il/how-to-install-windows-server-2008-step-by-step.htm>
- b. <http://www.howtogeek.com/50036/how-to-install-windows-server-2008-r2/>
- c. <http://www.petri.co.il/installing-active-directory-windows-server-2008.htm>
- d. <http://www.howtogeek.com/99723/how-to-set-up-dhcp-in-server-2008-r2/>
- e. <http://www.trainsignal.com/blog/windows-server-2008-active-directory-users>
- f. http://www.techotopia.com/index.php/Configuring_Windows_Server_2008_File_Sharing