Institute of Public Administration
MSc in Computer Science
Systems Management
Module Assignment 2013

Name: David Breen
Student Number: 12254329

User Manual to Demonstrate Setting Up a Local Area Network Using Windows Server 2008

Contents **Page**

Task A - Initial Setup of the 4 Machines **2**

1. Setting up the Virtual Machines 2
2. Set up of Windows Server 2008 using the full GUI install 6
3. Set up of Windows Standard Core 11
4. Set up of Windows 7 14
5 Testing Connectivity 17

Task B - Configure the Forest Settings **18**

1. Configure Server1 to be a domain controller 18
2. Configure Server2 to be a second domain controller 23
3.Configure MS-Core to be a member server 25
4. Configure Client1 to be a workstation member 27
5. Check the machines are configured correctly 28

Task C - Disk Management **29**

1. Install 2 additional hard disks 29
2. Mirror the Operating System to Disk 1 30
3. Create a Spanned volume on all 3 disks 31

Task D - Creating and Organisational Unit Structure **34**

1. Create the Organisational Units 34
2. Create the Users 36
3. Configure the logon hours for all the users 37

Task E - Grouping Policy **39**

1. Group users in each OU 39
2. Prevent the users in Marketing from being able to see the IT OU 41
3. Create 3 Group Policies 45

Task G - Print Servers **59**

1. Configure Server1 as a print server 59
2. Publish HP910 and HP915 printers in Active Directory 65

Task H - File Servers **70**

1. Setup MS-Core as a file server 70
2. Configure MS-Core for Windows Remote Administration 72
3. Access MS-Core from Client2 using remote desktop 73

Task I - DHCP Servers **75**

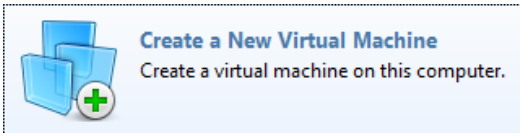
1. Install DHCP on Server2 75
2. Configure Client 1 to obtain its IP Address from DHCP 81
3. Disable DHCP services to see the results 82

Task J - Decommission Server2 assuming it has become unbootable **84**

References **87**

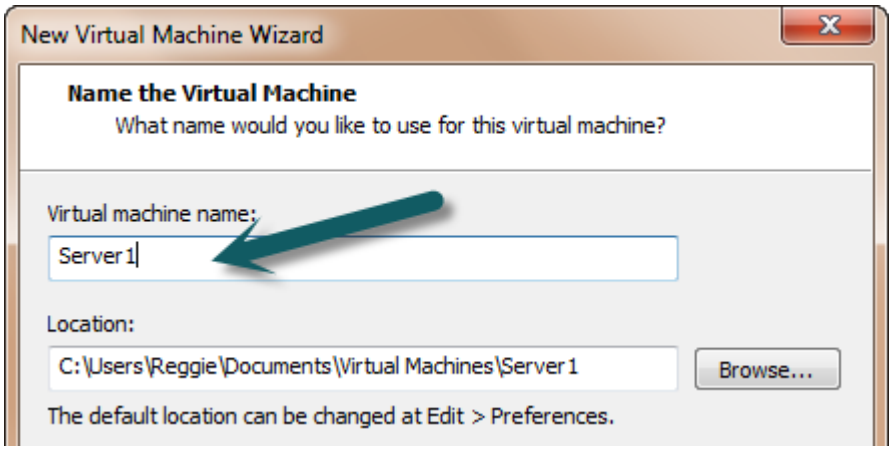
Task A - Initial Setup of the 4 Machines

1. Setting up the Virtual Machines

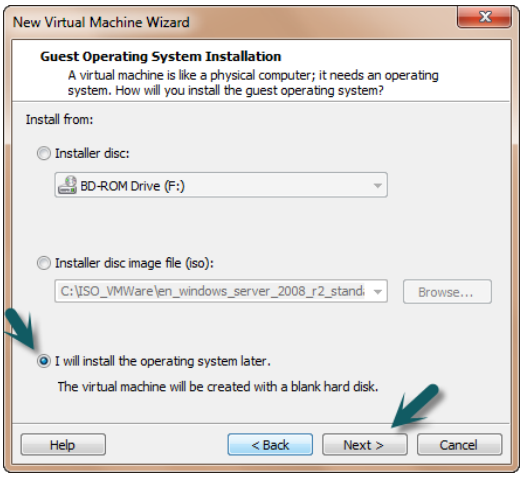


- Open VMWare Workstation
- Click **Create a New Virtual Machine**

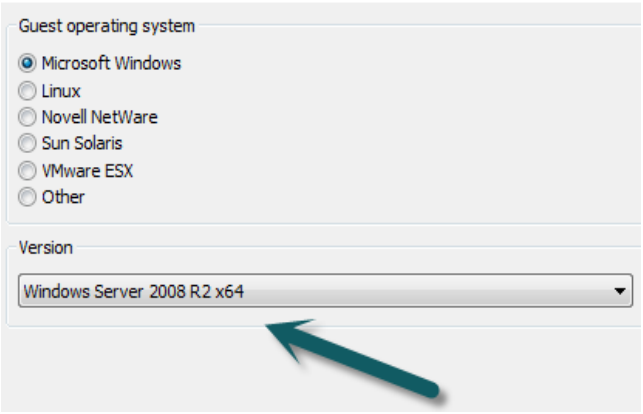
- Choose **Typical** instalation and click **Next**



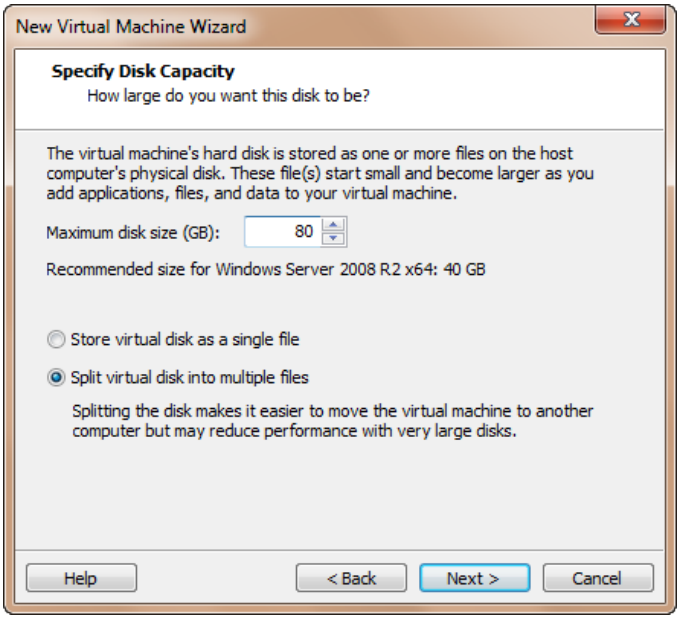
- Enter a name for the Virtual Machine and click **Next**



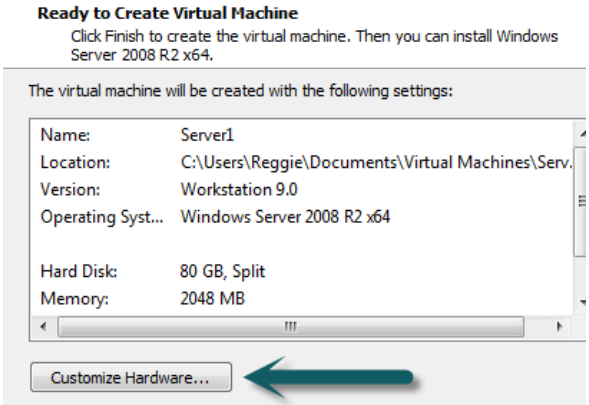
- Choose to install the operating system later and click **Next**



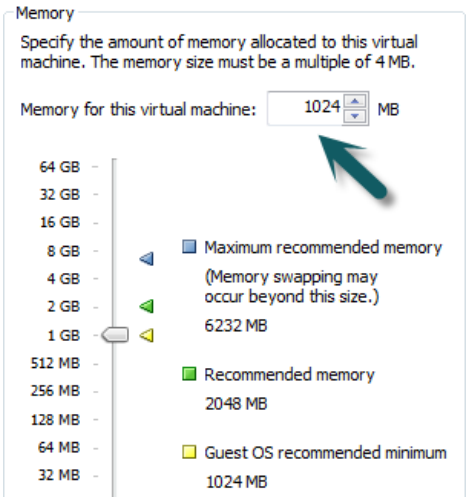
- Choose the operating system you wish to install and click **Next**



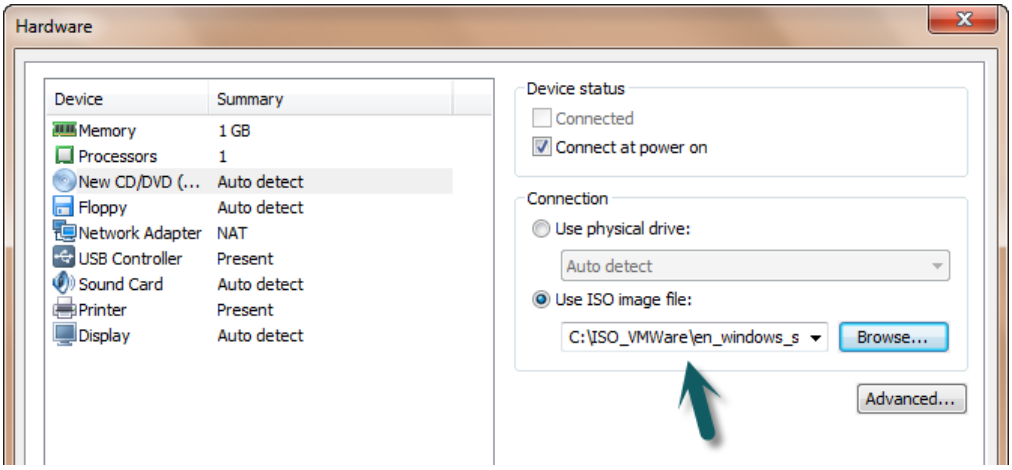
- Choose the size of the hard disk. In this manual all our servers will be 80GB and all the Clients will use the recommended size dictated by VMWare Workstation.
- Choose to split virtual disk into multiple files. This will allow the disk to grow only as files are added and not to physically assign the full size of the virtual disk. This is called thin provisioning.
- Click **Next**



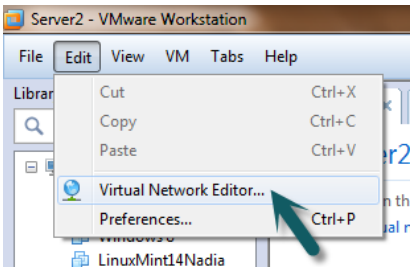
- Choose **Customize Hardware** to adjust the hardware options.



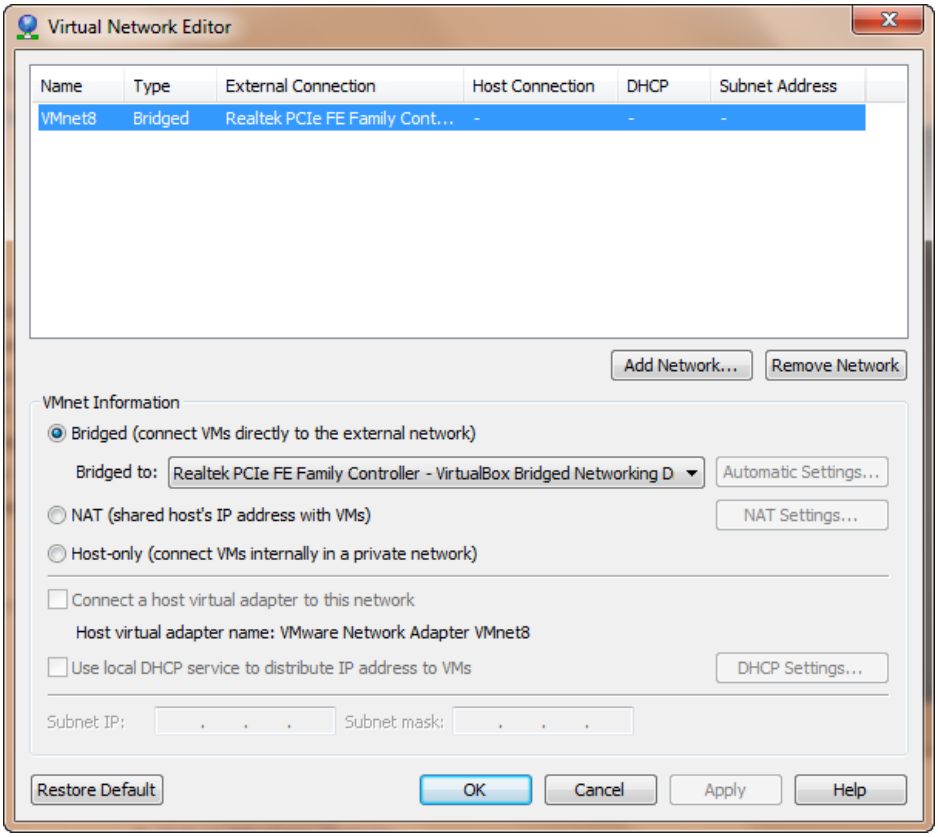
- Click the memory tab and change the memory to an appropriate level for your own system.
- Note: Multiple machines will be running at the same time so do not have memory set too high running speed will be affected.



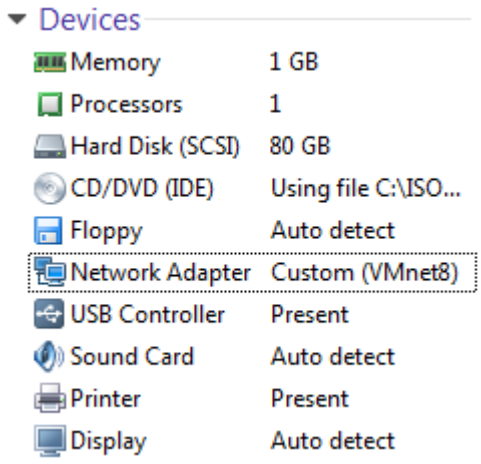
- Click on thhe CD/DVD tab and choose **Use ISO image file:**
- Browse to the location of the ISO image file of the operating system you wish to install
- The iso image is now mounted in the CD drive and will be used to install the operating system when powered on for the first time.



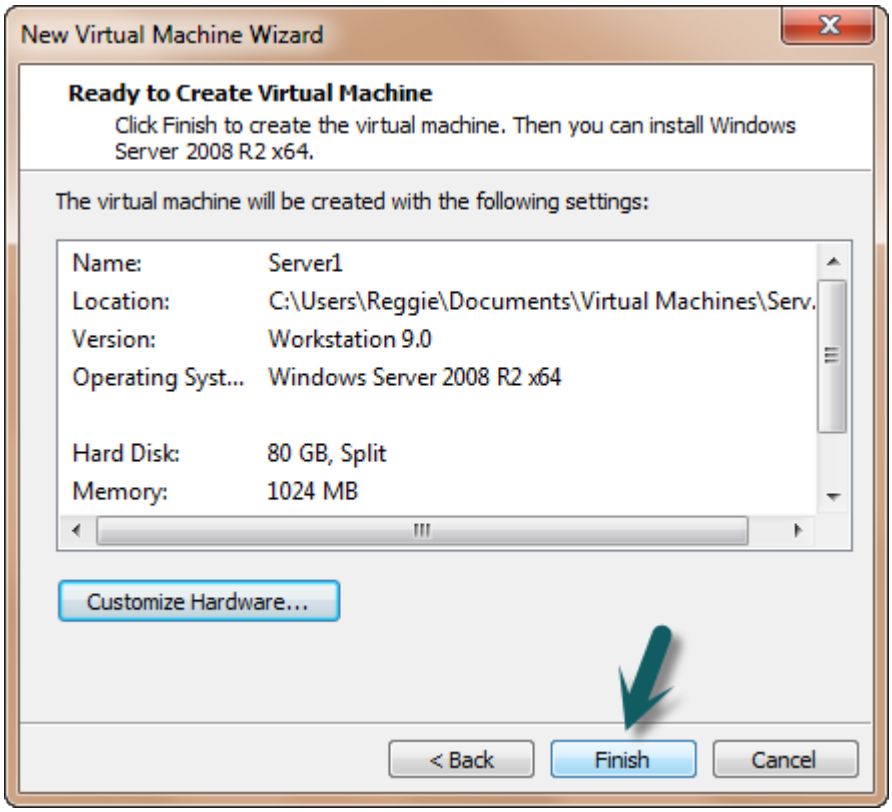
- To set up a common network for the machines Click **Edit** and **Virtual Network Editor**



- Click **Add Network** and choose one of the available names. e.g. **VMnet8**
- Choose a **Bridged** connection
- Choose one of the Bridged Networking Drivers.. see above
- Click OK



- Click the **Networ k Adapter** tab and choose the Custom adaptor created above.
- All the machines created in this manual should use this custom adaptor. Therefore if any changes are to be made to the adapter they can be made at this point. E.g. adding internet connectivity. Thus preventing the need to make the changes individually to each machine.

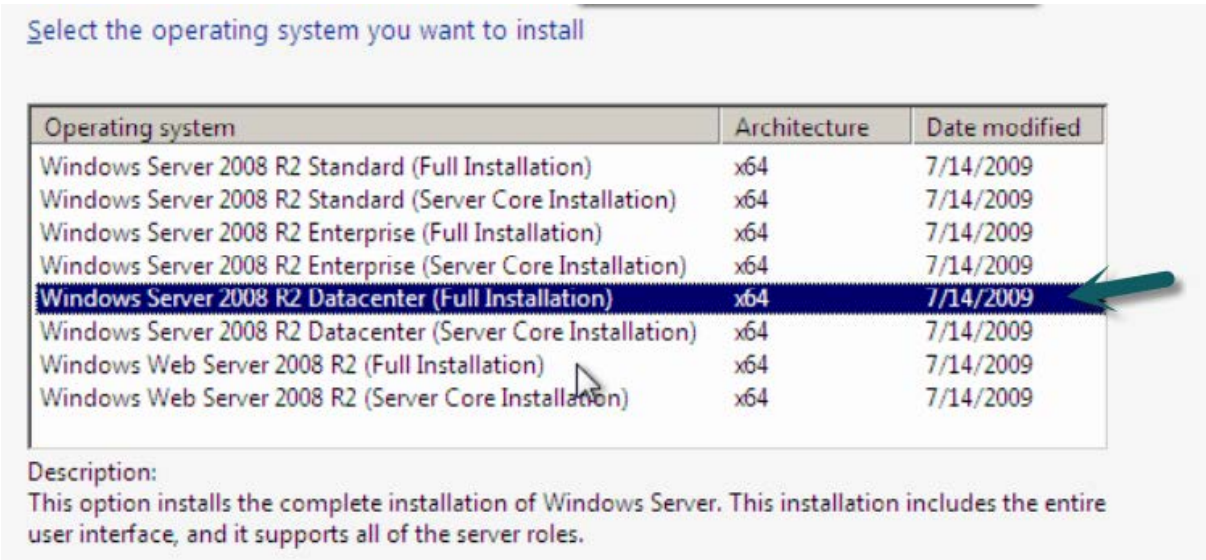


- Review the settings of the virtual machine and if correct click **Finish**
- Click Power on this virtual machine
- The system will now boot from the iso image file mounted in the CD drive.

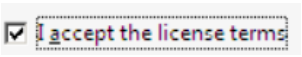
2. Set up of Windows Server 2008 using the full GUI install

- Power on the machine and click **Install now**

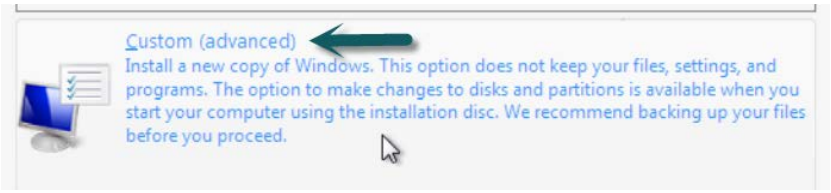
- Change the Language settings as appropriate and click **Next**



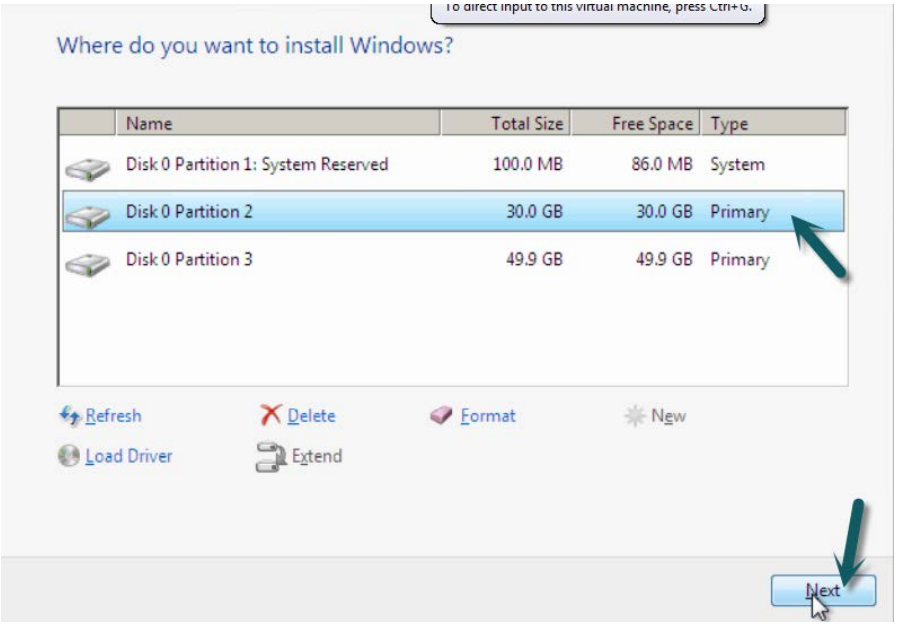
- Choose the appropriate version of Windows Server 2008 to install, in this manual the installation of Windows Server 2008 R2 Datacenter is demonstrated. The process for the other versions are practically identical.
- Click **Next**



- Check the **I accept the licensing terms** and click **Next**

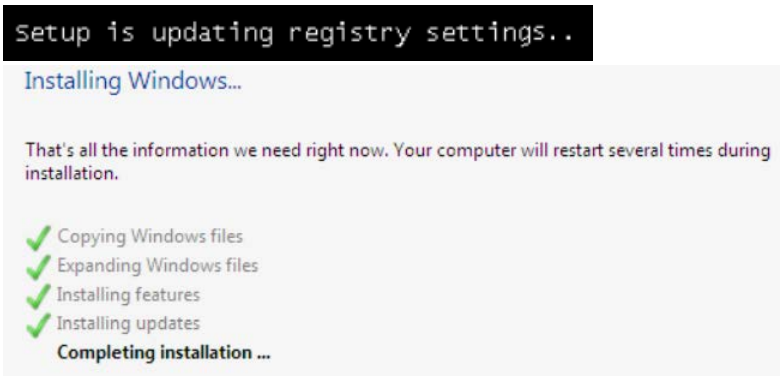


- Click on the **Custom (advanced)**



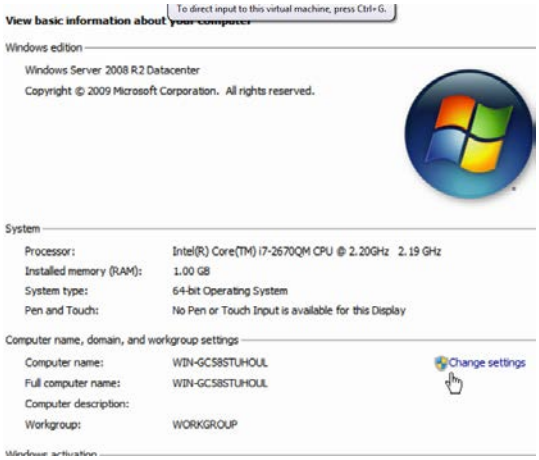
- Click **Advanced Disk Options** then **New** to add partitions to the disk
- 100MB will be reserved for the system automatically

- Make 2 more partitions, a 30GB partition for the operating system and use the rest to be used for programs and files
- Highlight the **30GB partition** to be used for the operating system and click **Next**.

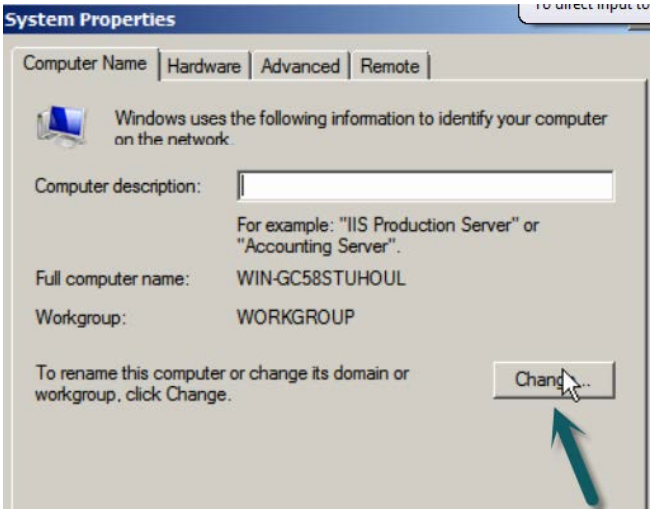


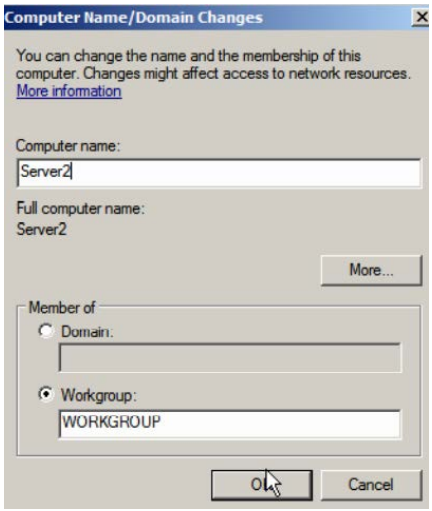
- The installation will finish on its own now, the computer may restart a couple of times during this process

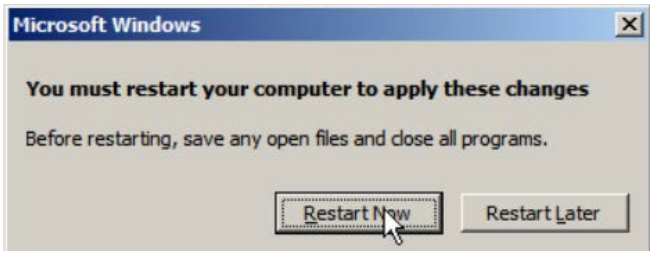
- When the computer runs for the first time the user will be required to change the Administrator password. The password must meet minimum complexity requirements which are:
- must be at least 6 characters in length
- must contain letters from three of the following four categories: Uppercase letters, lowercase letters, basic 10 digits(0-9), non-alphabetic characteries (e.g. !,$,%,&)
- reference Microsoft Technet technet.microsoft.com/en-us/library/cc264456.aspx



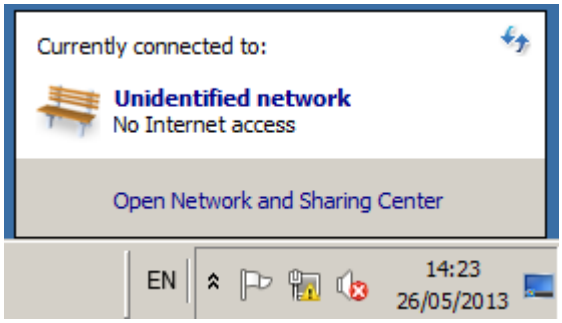
- It may be advisable to change the computer name to something meaningful within the organisation. Click the **Start** button at the bottom left of the desktop.
- Right click on **Computer** and click **Properties**
- Click **Change Settings**



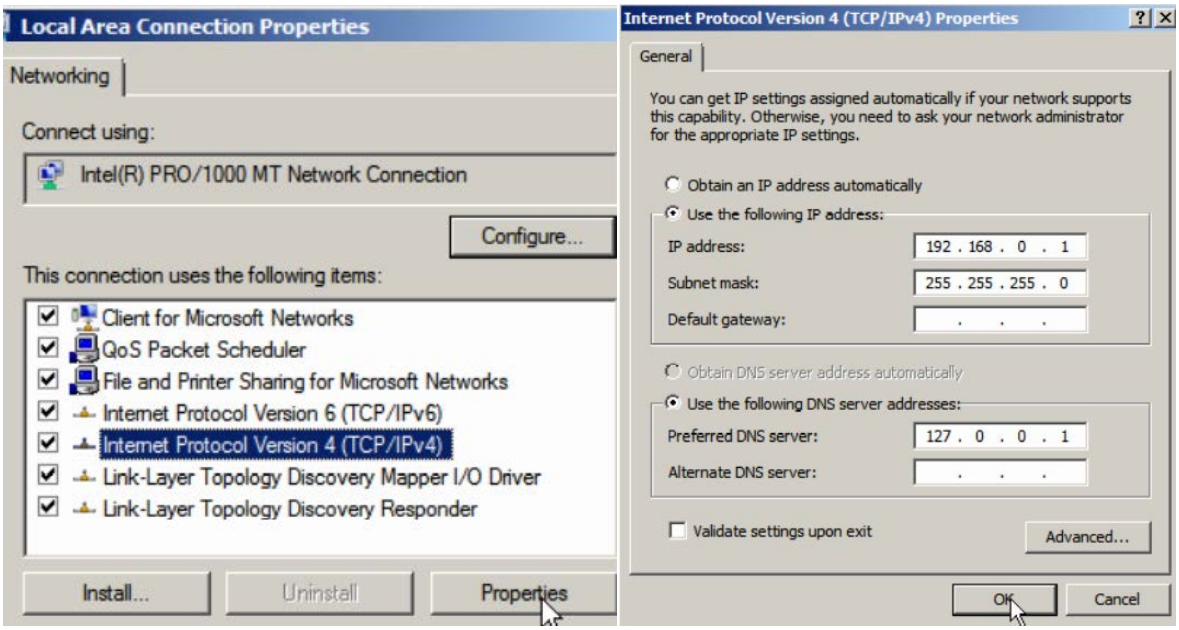




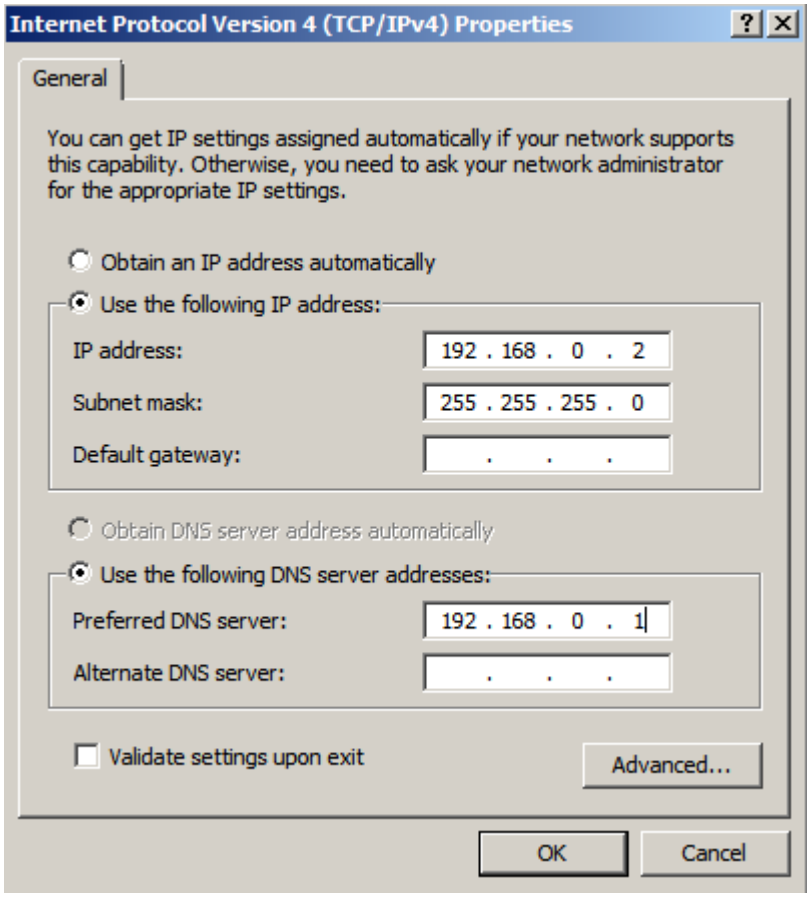
- To change computer name Click **Change** as shown on above screenshot
- Enter the new name of the computer and click **Ok**
- You will now be asked to restart the computer, Click **Restart Now** to apply these changes.



- To configure the IP settings, click on the network icon in the toolbar (see above screenshot
- Click on **Open Network and Sharing Center**
- Click **Change adapter settings**



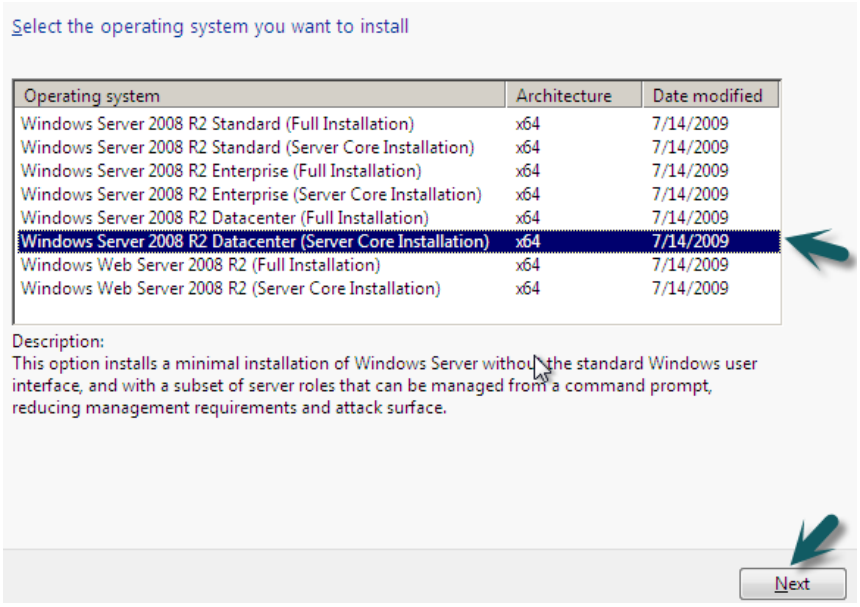
- Highlight **Internet Protocol Version 4(TCP/IPv4)**
- Click **Properties**



- Change the settings to the desired settings (see above)
- Click **OK**

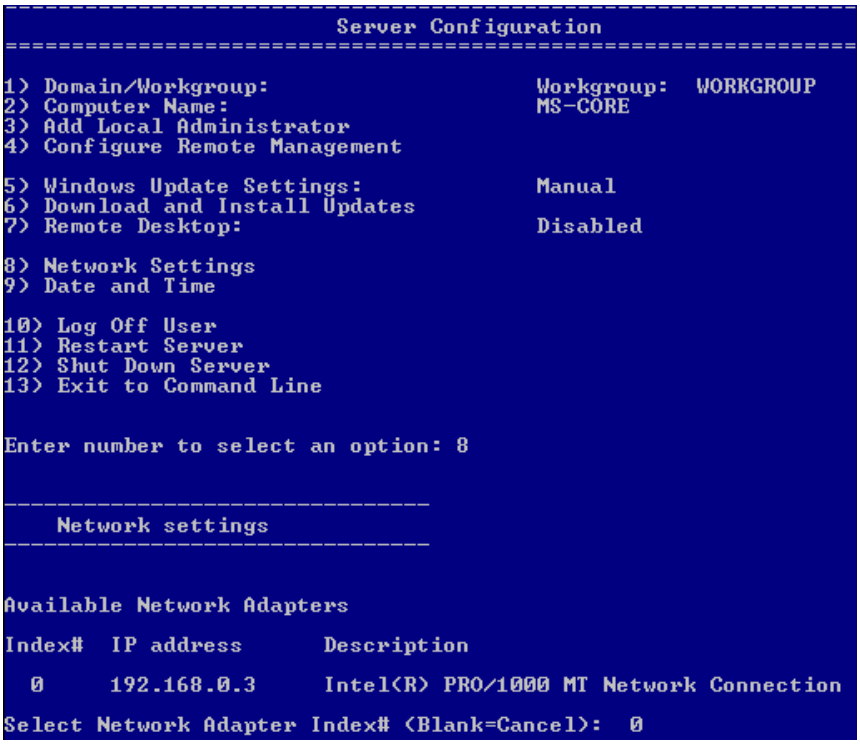
3. Set up of Windows Server 2008 R2 Datacenter Server Core

- The instalation of Windows Server Core is very similar to the previous full installation. The only difference being that instead of choosing the Full Installation you choose the **Server Core Installation**. See screenshot below

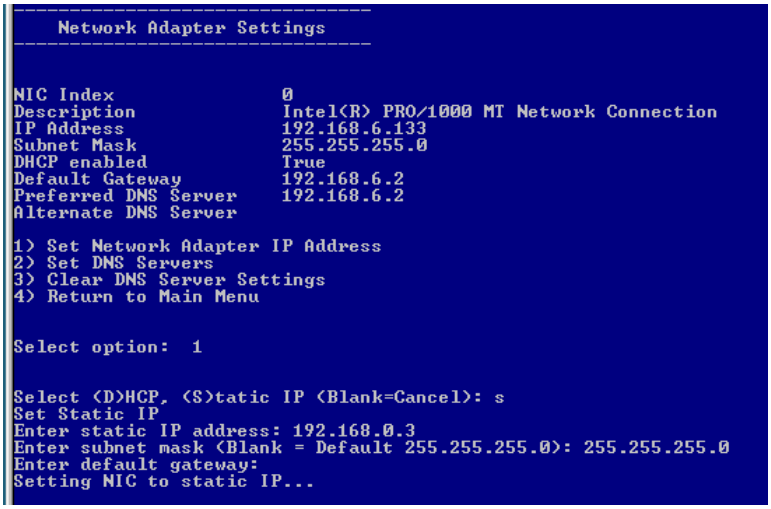


- Once installed the user interface is a TUI environment like the screenshot below.

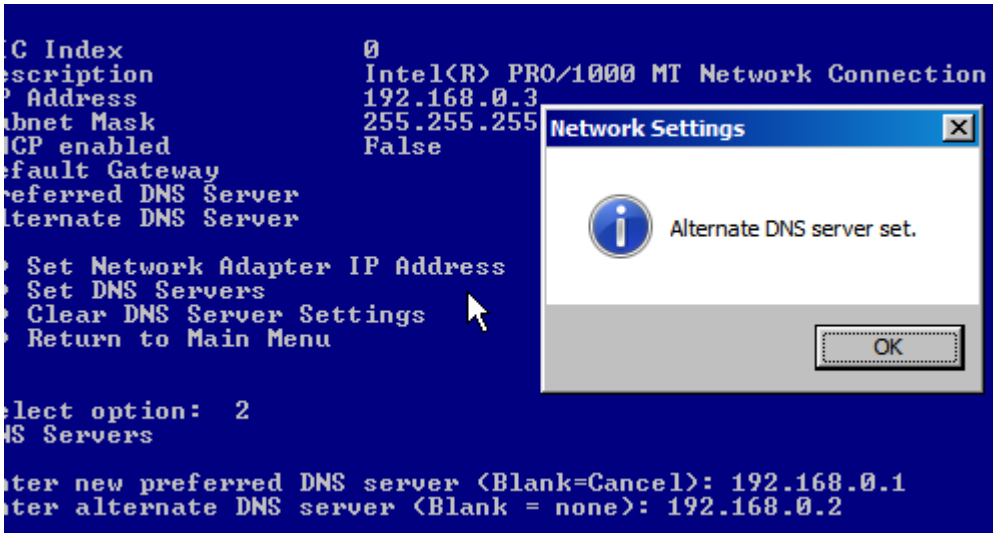
- Type **Sconfig.cmd** into the command prompt and press **Enter**



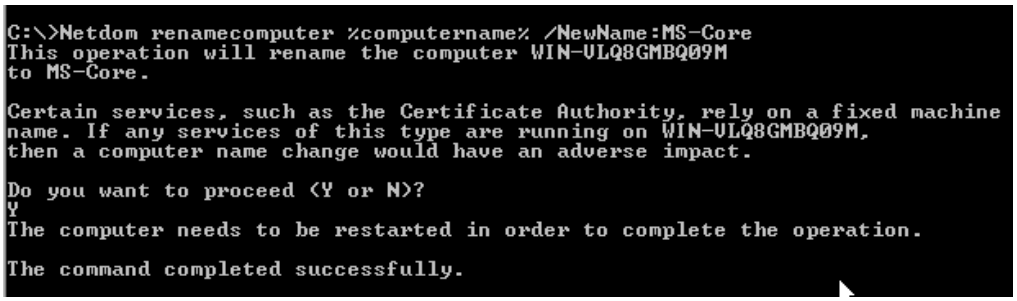
- Enter the number **8** and press **Enter** to modify the Network Settings
- Select the appropriate network adapter from the list of Available Network Adapters and press **Enter** (see above screenshot)



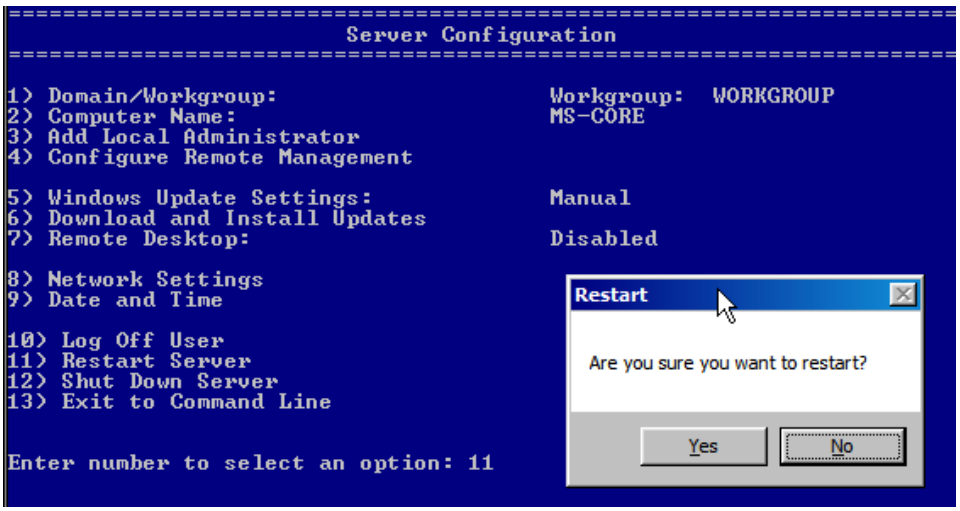
- Enter **1** and press **Enter** to set the ip address settings
- Enter **S** and press **Enter** to set to the computer to a static IP address
- Enter the IP address of the machine and press **Enter**
- Enter the subnet mask for the network, leave blank for default: 255.255.255.0
- Leave the default gateway blank and press **Enter**. This would be the ip address of the router to the internet. In this manual we are not going to need to connect to the internet.



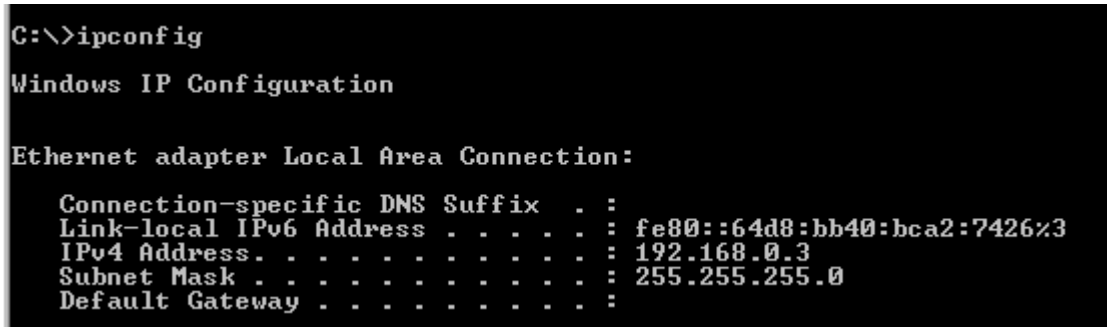
- Enter **2** and press **Enter** to set the Domain Name Server details
- Enter the IP address of the preferred DNS server and press **Enter**
- Enter the IP address of the Alternate DNS server and press **Enter**
  Note: For the purposes of this manual Server1 and Server2 will be the Domain Name Servers for the domain.



- To rename the computer to something meaningful on the network enter the following command:
  Netdom renamecomputer %computername% /NewName:MS-Core
- Enter **Y** to proceed when prompted



- Enter the server Configuration by again using the sconfig command as before
- Enter **11** to restart the computer.
- Click **Yes**



- Upon restart the new settings can be checked using the ipconfig command, (see above)

- For troubleshooting purposes later when connecting the computers to the domain it is useful to be able to ping the machines from each other. By default in server core these are blocked by the firewall. To enable them enter the following command:

netsh advfirewall firewall add rule name="ICMPv4 Inbound" dir=in action=allow enable=yes profile=any localip=any remoteip=any protocol=icmpv4:8,any interfacetype=any edge=yes

Note-

It is best practice to use the **netsh advfirewall** command over the **netsh firewall** command.
[1]Microsoft Technet says:
"The firewall team is pushing everyone to using netsh advfirewall because netsh firewall cannot:

- enable groups of rules
- create rules for services

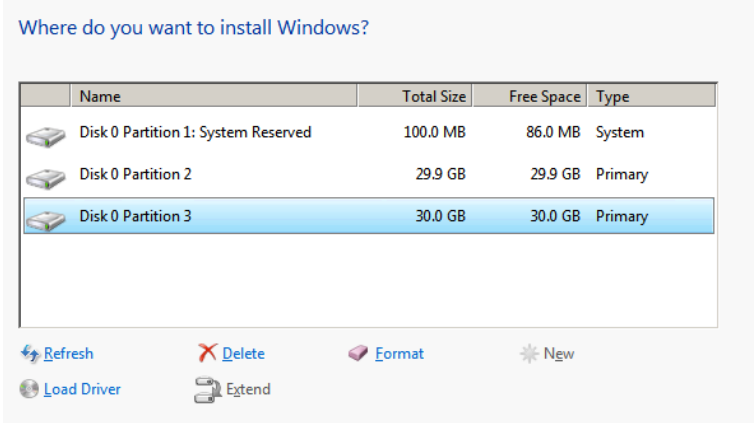
- create rules that support multiple filtering criteria

I don't see any disadvantages for using the above netsh command in Windows Server 2008, but based on the netsh advfirewall push and netsh firewall limitations I would guess there will be changes in the future." - Microsoft Technet

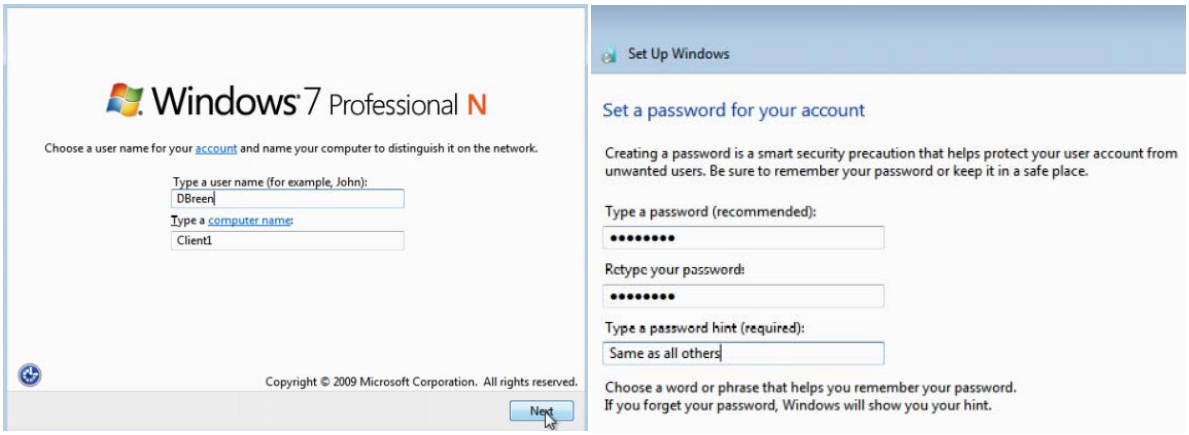
4. Set up of Windows 7

- Set the language settings as appropriate and click **Next**
- Click **Install now**
- Check the **I accept the licence terms** box and click **Next**

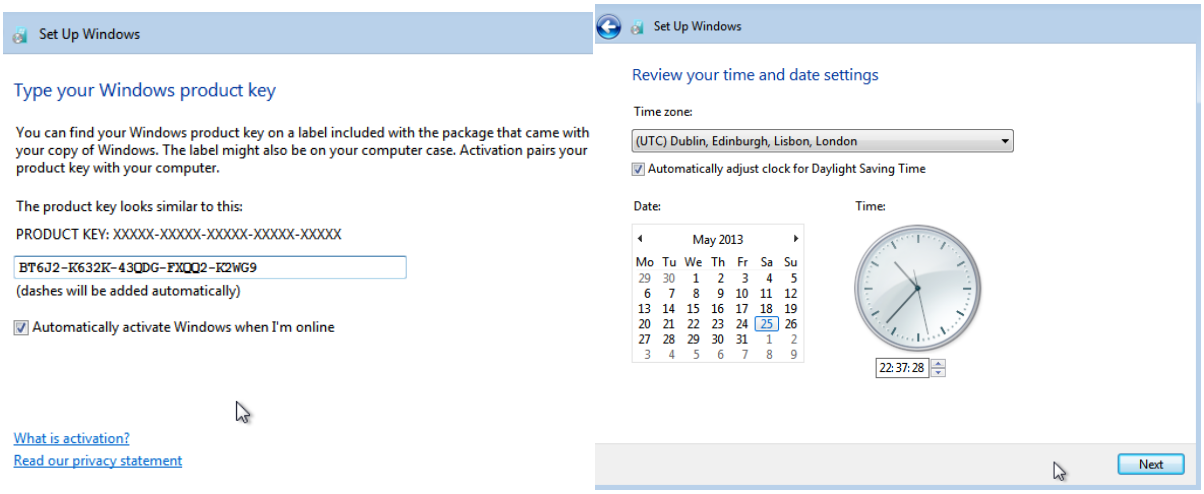
- Click the custom install
-



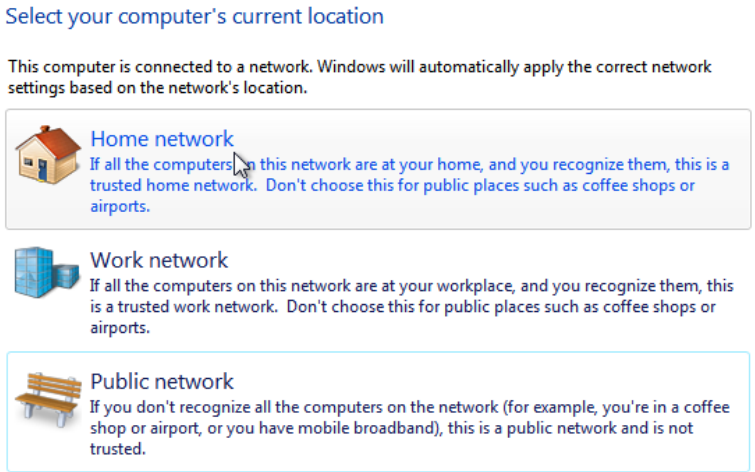
- Set up the partitions in exactly the same way with the Server 2008 install



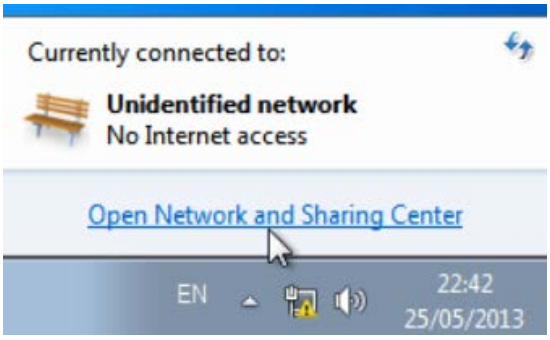
- Enter a username for your user account and a unique name for the computer. e.g. Client 1
- Set the password for the account you created and click **Next**

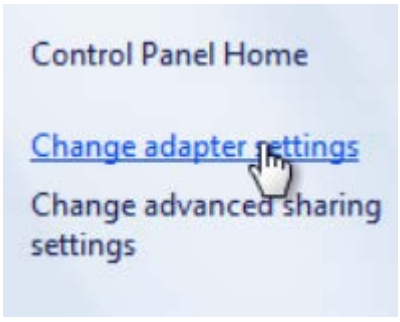


- Enter the product key and click **Next**
- Set the appropriate Time and Date Settings and click **Next**

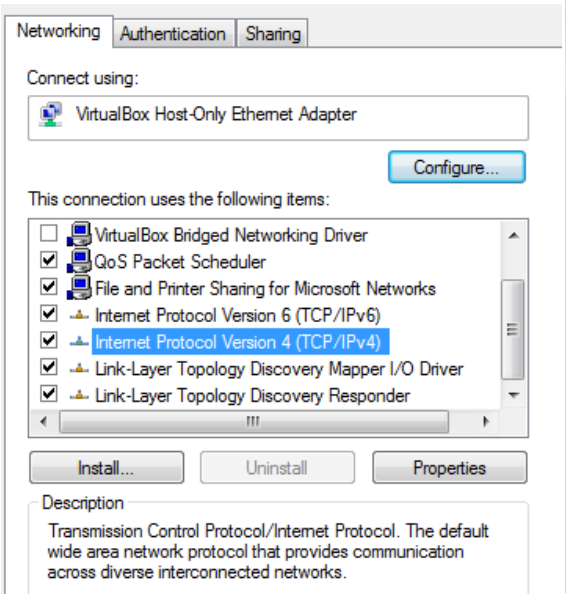


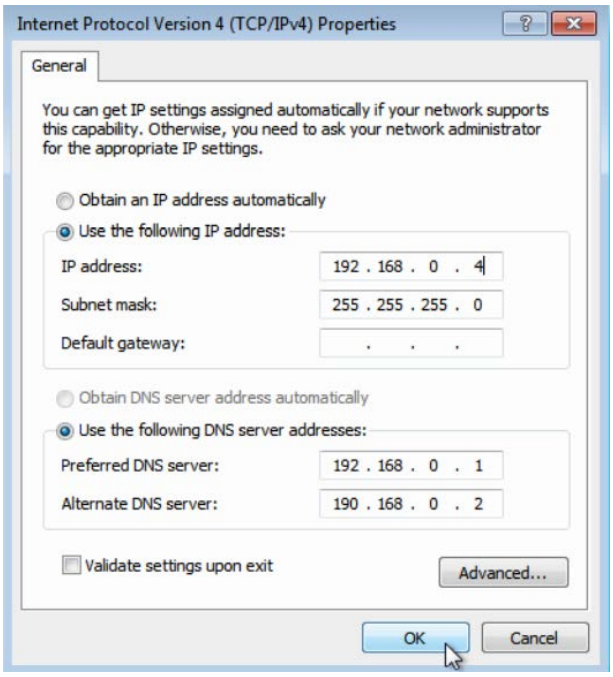
- Choose the type of network you are using, e.g. Work Network





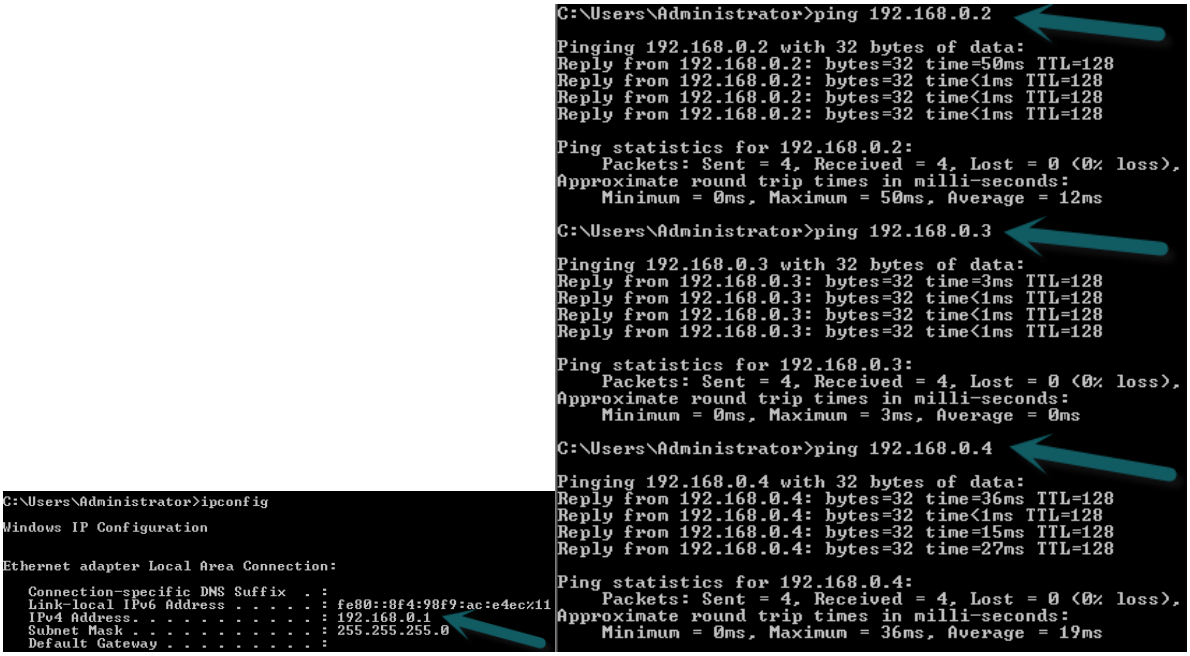
- To configure the IP settings, click on the network icon in the toolbar (see above screenshot
- Click on **Open Network and Sharing Center**
- Click **Change adapter settings**





- Highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**
- Set the IP address, Subnet mask, Preferred DNS and Alternate DNS server addresses as appropriate. (see above screenshot)

5 Testing Connectivity



All the machines are now set up with their IP address assigned statically as follows

Server1 - 192.168.0.1

Server2 - 192.168.0.2

MS-Core - 192.168.0.3

Client1 - 192.168.0.4

The computers should now be ready to communicate on a network. Before setting up the Active Directory domain this connectivity can be tested using the ping command. All the computers should be able to ping each other. See above screenshot - Server1 is able to ping all three other machines.

Task B - Configure The Forest Settings

In this section we will set up the forest settings as follows:

- The forest will contain a single domain called MSCONV.IPA
- Server1 and Server2 will be set up as Domain Controllers
- MS-Core will be set up as a member server
- Client will be set up as a workstation member

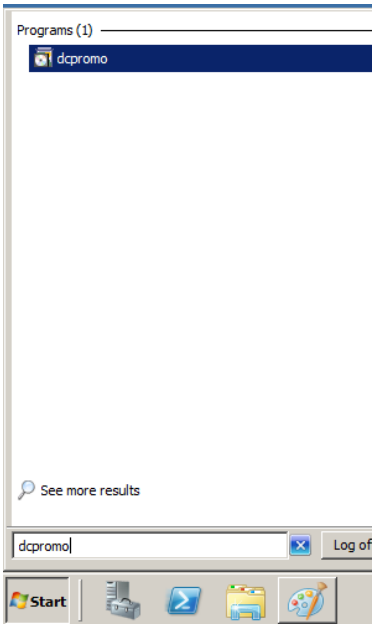
There are many benefits of using a single domain. [2] Mastering Windows Server 2008 R2 lists three :

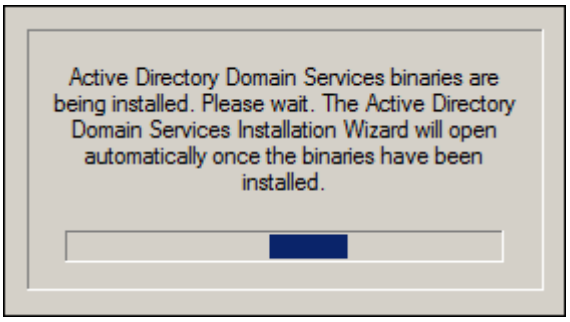
" **Least expensive** Every domain starts with a single domain controller and usually includes a second DC for redundancy. Each additional domain requires additional servers, incurring costs for hardware and software plus the added costs of the IT professionals like you needed to manage them.
Easier to manage A single domain is easier to manage than multiple domains. Each additional domain includes additional accounts, groups, group policies, and other details that must be managed.
Simpler disaster recovery You only need to plan for the recovery of a single domain. Backups only need to be done for a single domain, and the overall disaster recovery plan is simpler."

1. Configure Server1 as a domain controller

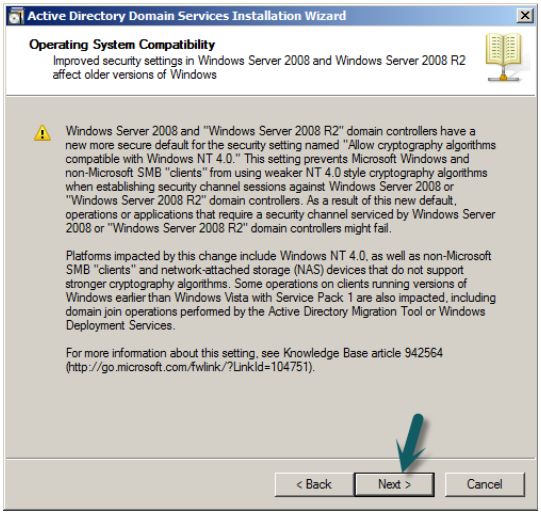
The first computer to set up a forest will be set as the Primary Domain Controller (PDC). It will also hold all the operations master roles for the forest.
Microsoft Technet says:
[3]"Domain controllers that hold operations master roles are designated to perform specific tasks to ensure consistency and to eliminate the potential for conflicting entries in the Active Directory database. AD DS defines five operations master roles: the schema master, domain naming master, relative identifier (RID) master, primary domain controller (PDC) emulator, and infrastructure master."

This first Domain Controller will be in charge of all replication to subsequent Domain Controllers and all subsequent Domain Controllers will send any updates to the directory to the PDC. This means that it will be by far the busiest machine in the domain and therefore should have the best and fastest hardware possible. Subsequent domain controllers can be used to balance the load and provide redundancy in case of hardware failure.

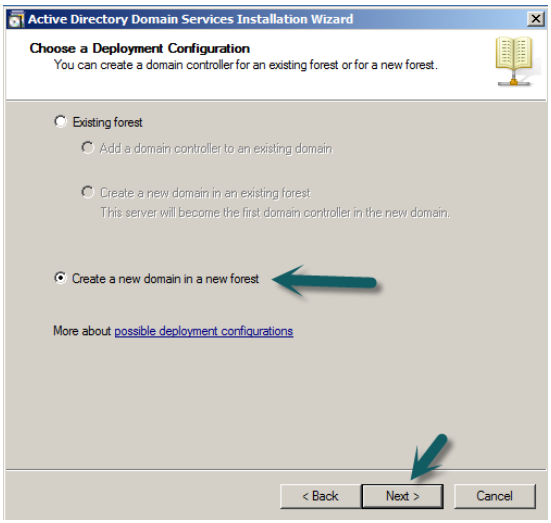




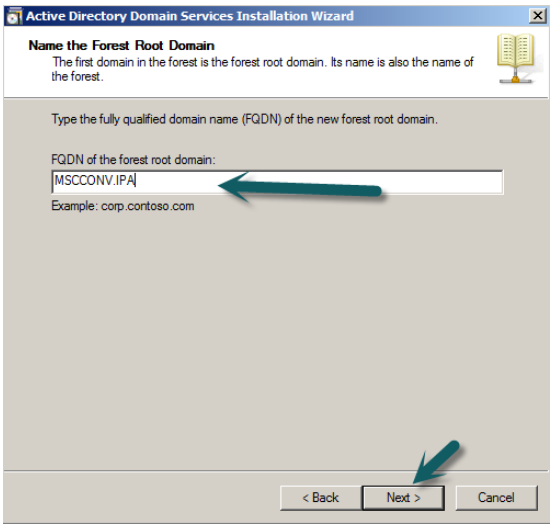
- Click **Start** and type **dcpromo** into the search box and click **dcpromo**
- Active Directory Domain Services will be installed if not already on the system

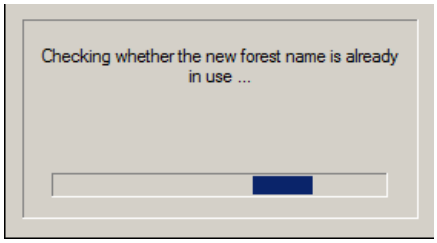


- Click **Next** on the next two screens, see above screenshots

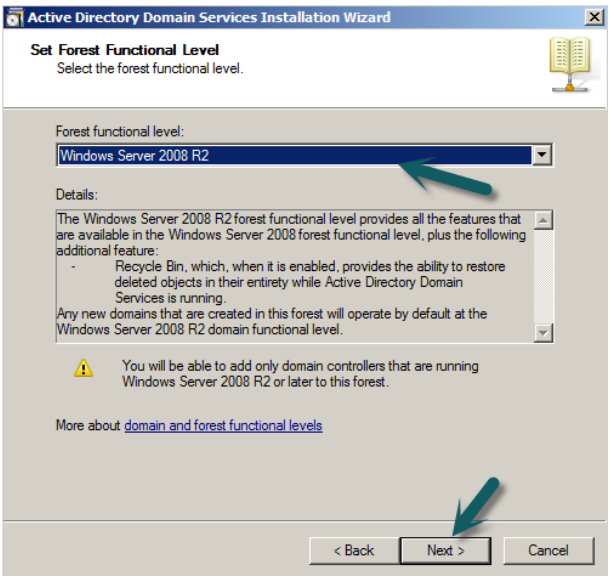


- Choose to **Create a new domain in a new forest**
- Click **Next**

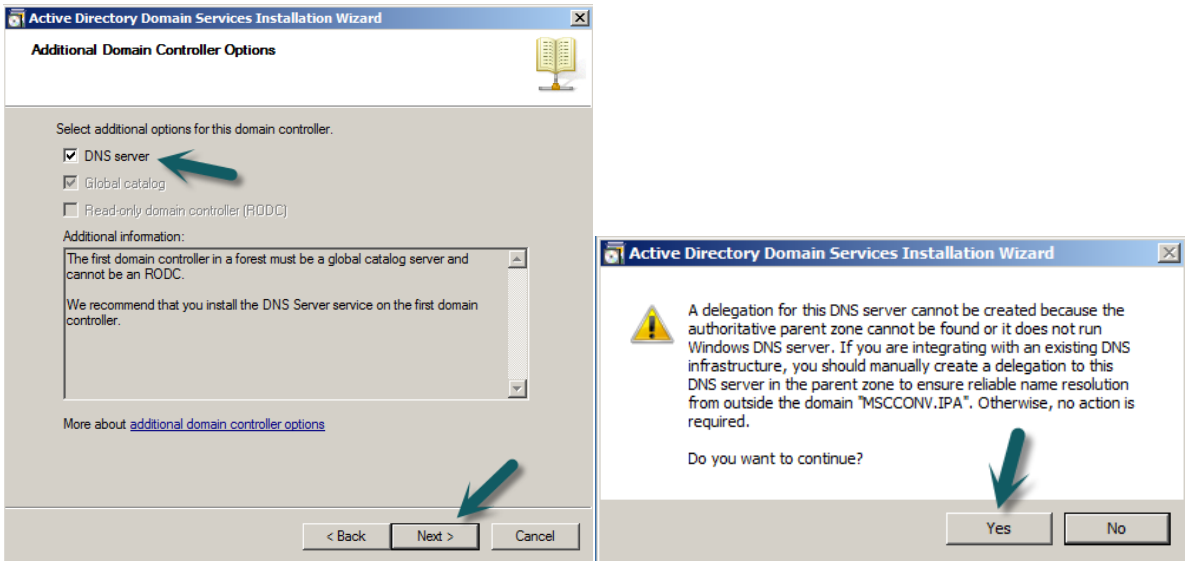




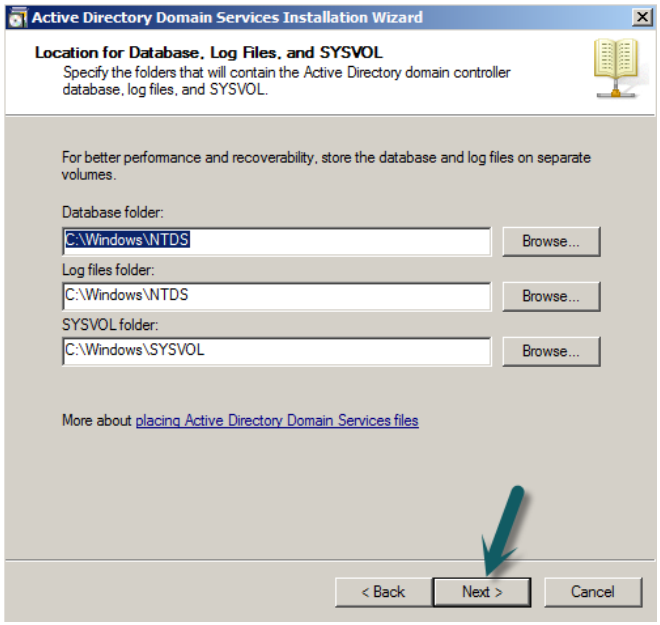
- Enter the Fully Qualified Domain Name (FQDN) and Click **Next**
- In this manual we will use the FQDN **MSCCONV.IPA**



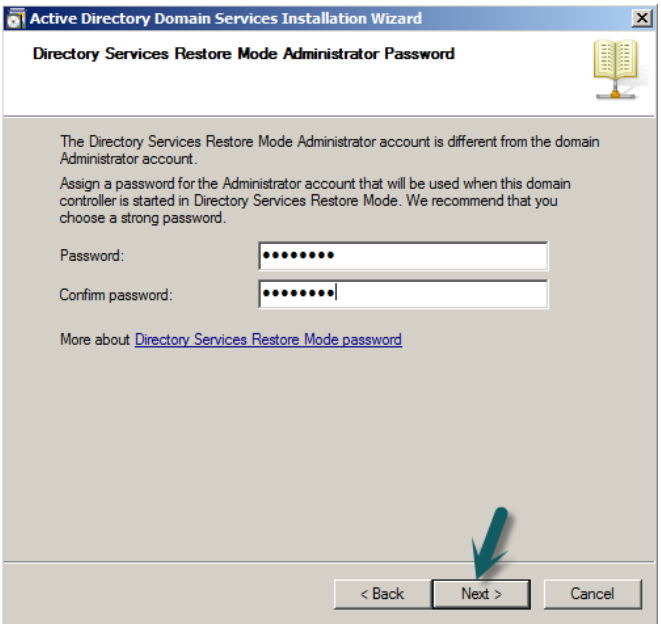
- Choose the Functional level for the Domain Controllers. This will be the minimum level for any additional Domain Controllers to be added to the network in the future. Its is possible to promote a functional level of the domain to a higher level but its not possible to demote to a lower level.
- Click **Next**



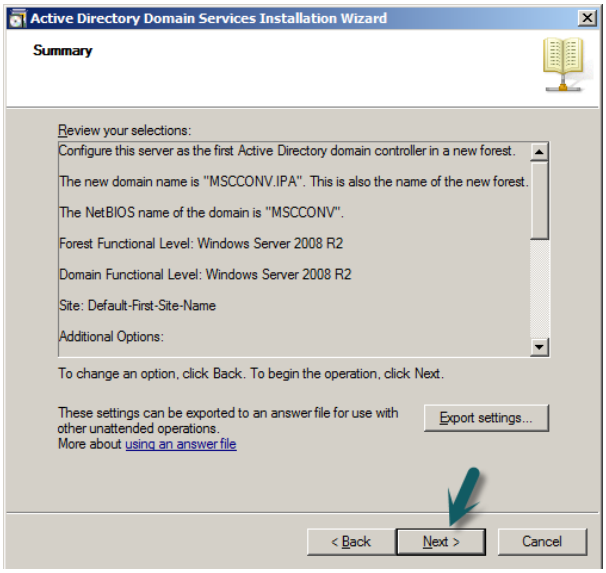
- Check the **DNS server** box as an additional option for the domain controller
- Click **Next**
- Click **Yes** to continue

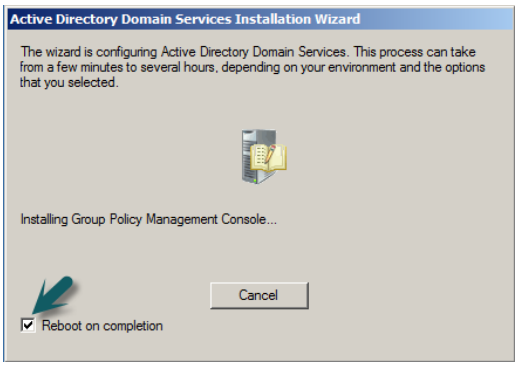


- Leave the Locations for Database, Log Files and SYSVOL in the default locations and click **Next**

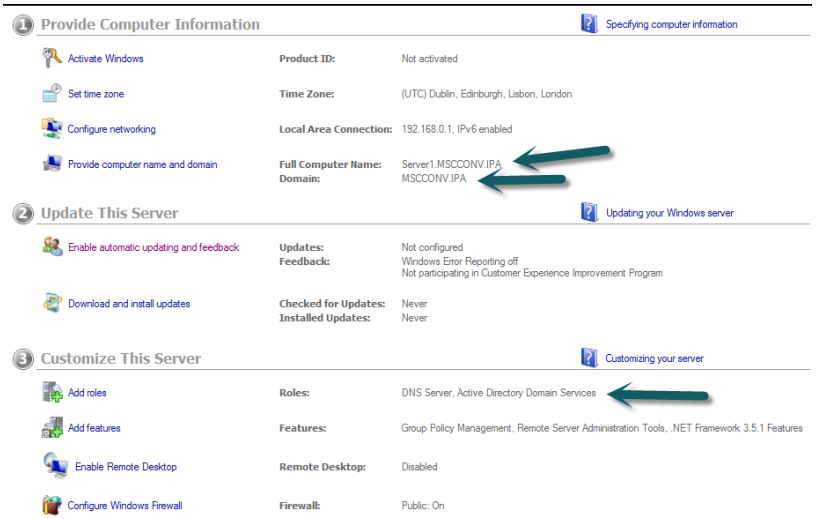


- Enter a unique password, different from the Administrators password as the Directory Services Restore Mode Administrator Password
- Click **Next**





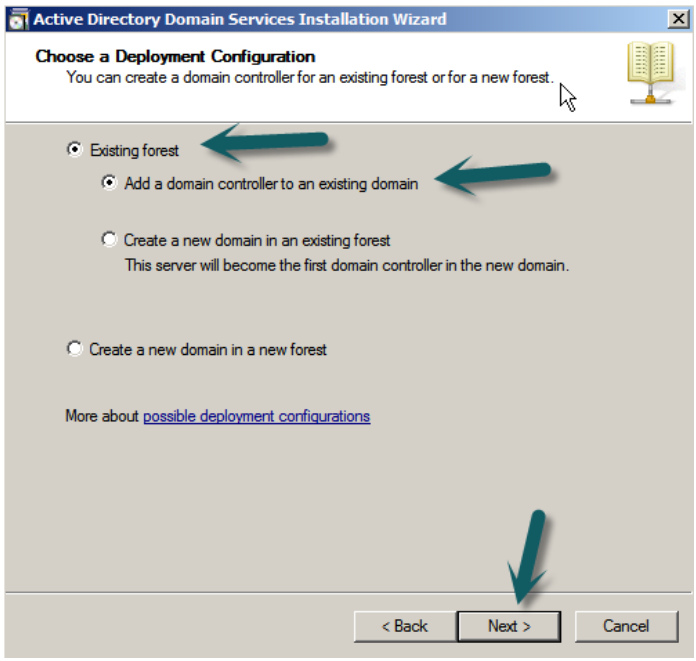
- Check the Summary screen is correct and click **Next**
- Check the **Reboot on completion** box and wait for the wizard to finish installing and configuring Active Directory. The computer will reboot when finished.



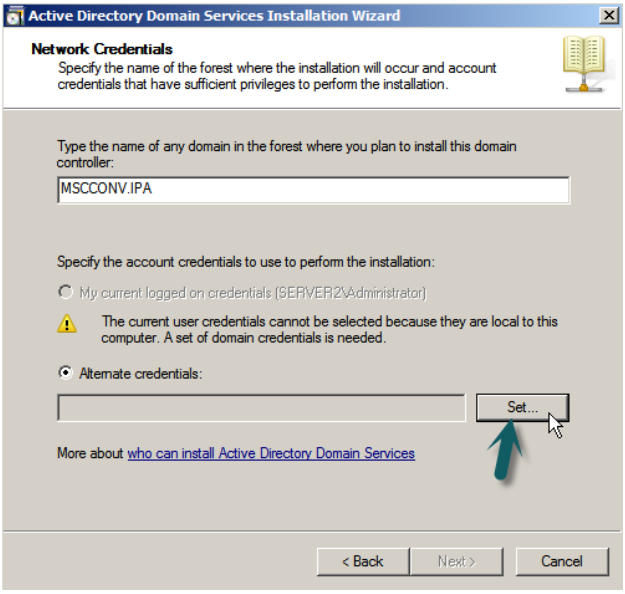
- Upon reboot the logon screen should look like the above screenshot. You are now logging on to the domain and not onto the local computer as before.
- The startup screen will show the computer information, see screenshot above. The computer should have the roles of DNS Server and Active Directory Domain Services.
- The Full computer name should have the domain as part of it now and the domain should be listed.

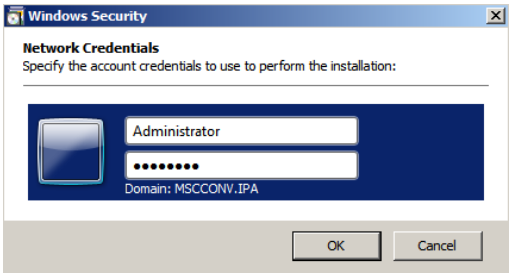
2. Configure Server2 to be a second domain controller

- Log into Server2 as an administrator
- Start dcpromo in the same way as before
- Click **Next** on the next two screens

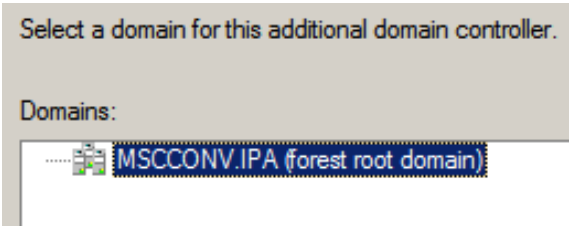


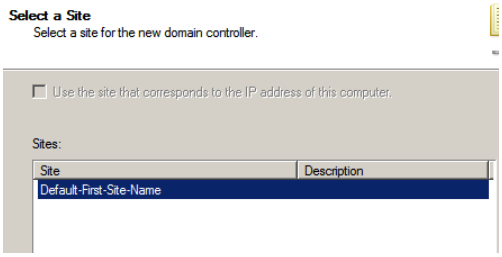
- Choose **Existing forest**
- Choose to **Add a domain to an existing domain**
- Click **Next**



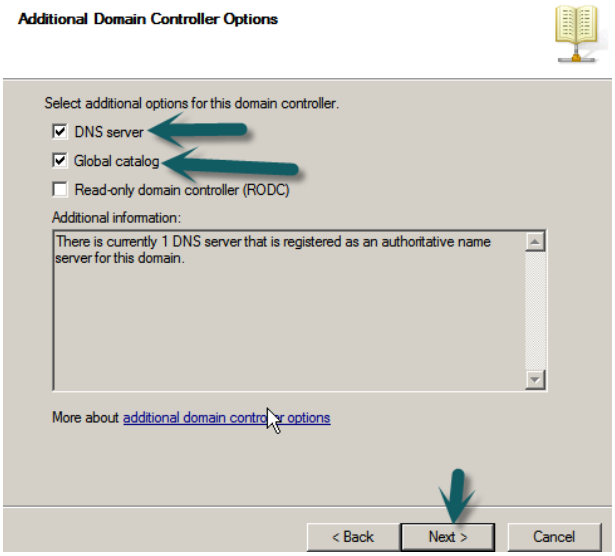


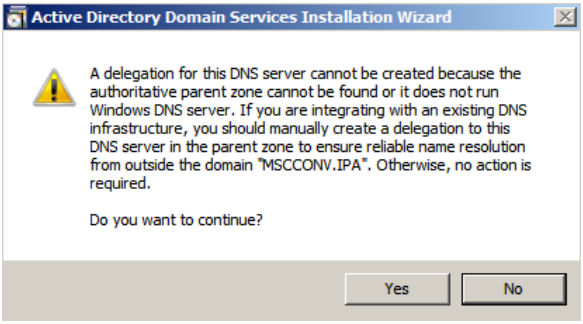
- Enter the Fully Qualified Domain Name of the domain. (Same as for Server1)
- Click **Set** to set the credentials to login to the domain with
- Enter the credentials of an administrator of the Domain and click **OK**





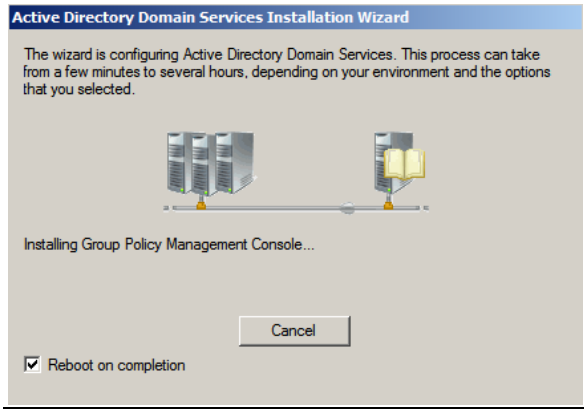
- Highlight the domain. (should be the only domain on the list) and click **Next**
- Highlight **Default First Site Name** and click **Next**





- Check the **DNS server** box to use this Domain Controller as an alternative DNS server
- Check the **Global catalog** box to set the DC to replicate the global catalog

- Uncheck the **Read-Only domain controller** box as we want this to be a fully fledged domain controller
- Click **Next**
- Click **Yes** on the error box to continue

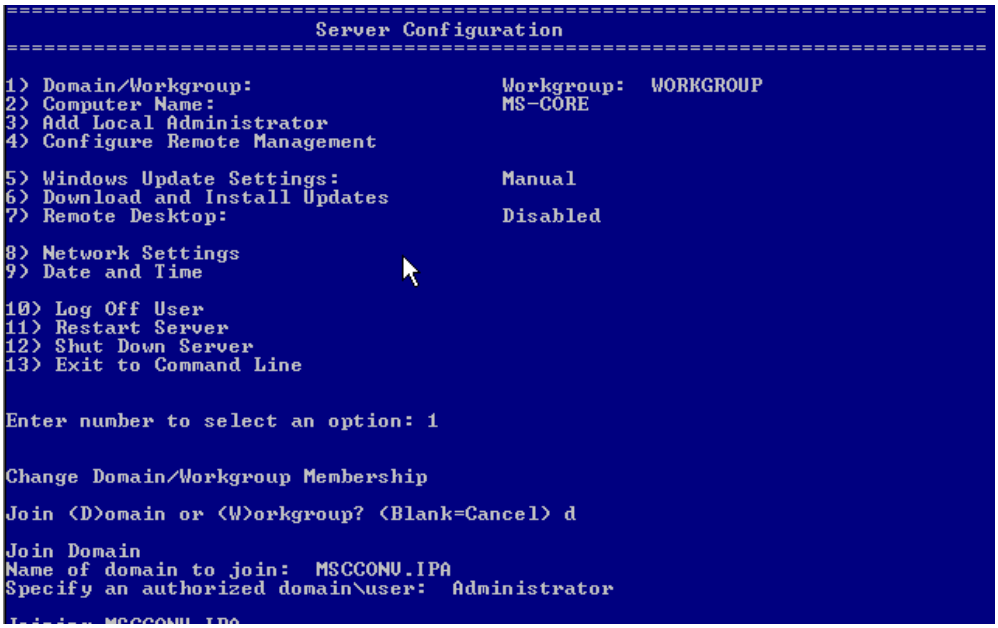


- Finish the installation exactly the same way as for Server1 and reboot when finished

3.Configure MS-Core to be a member server

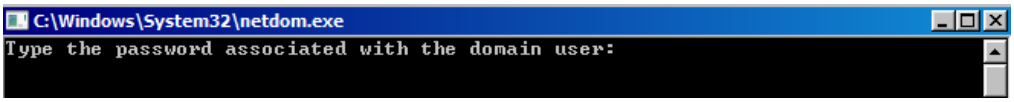
The Server Core is a lighter weight version of windows server 2008. It users a Text User Interface (TUI). Microsoft [4]" stripped Windows Server 2008 to the bare minimum requirements to run an operating system."
Microsoft promoted the product for the following reasons:

[5] "**Reduced maintenance** Less code has fewer updates to perform.
Reduced attack surface Without the fluff, there is less to attack. Roles and features can be installed as needed and the limited number of services will reduce the areas for attack.
Reduced performance requirements Server Core takes fewer CPU cycles and less hard disk space. So, the opportunity to repurpose hardware is increased with this option."

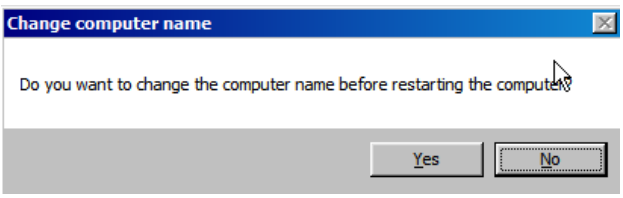


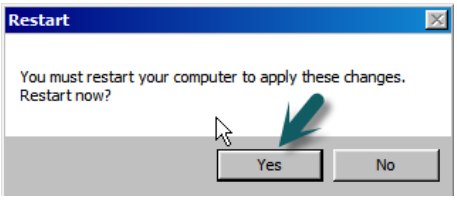
- Log into MS-Core as an administrator

- Type **sconfig** into the command prompt and press **Enter** to start the Server Confiiguration utility.
- Type **1** and press **Enter** to change domain/workgroup settings
- Type **D** and press **Enter** to join a new Domain
- Enter the name of the domain, e.g. MSCCONV.IPA and press **Enter**
- Enter a username for an administrator of the domain, e.g. Administrator and press **Enter**



- Enter the password for the administrator and press **Enter**

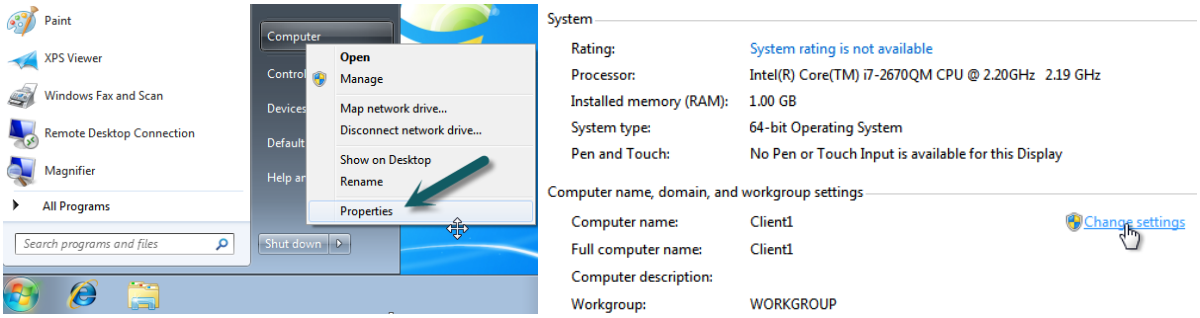




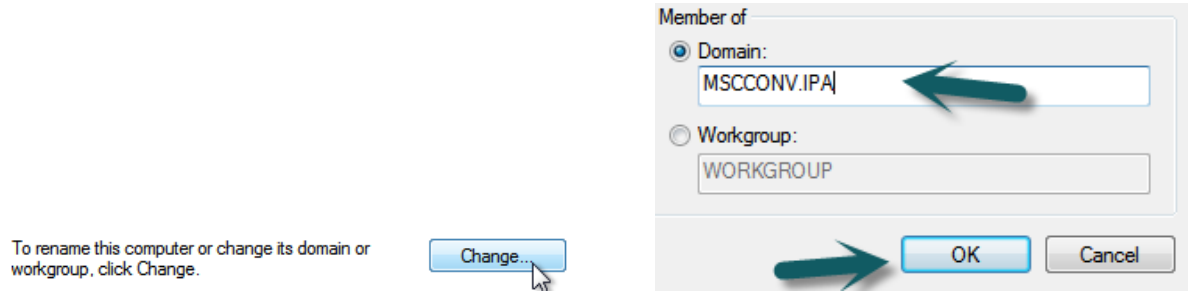
- As we have already changed the name of the computer click **No** when asked do we want to change its name
- Click **Yes** to restart the computer

4. Configure Client1 to be a workstation member

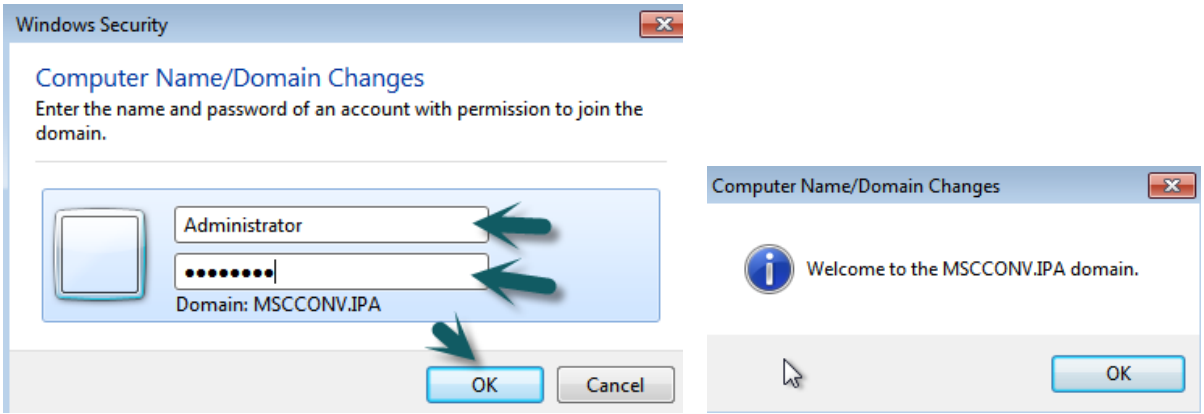
This is the basic method used to join clients using any of the windows operating systems to the domain. Its basically the same process with slight changes for older operating systems.



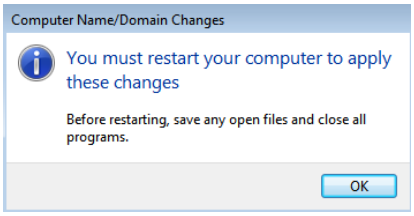
- Right click on **Computer** in the start menu and choose **Properties**
- Click **Change settings**

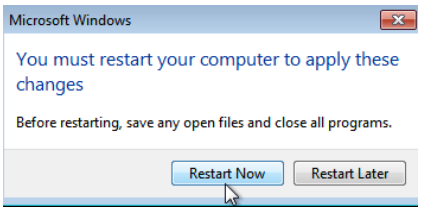


- Click **Change**
- Enter the name of the Domain, e.g. MSCCONV.IPA
- Click **OK**



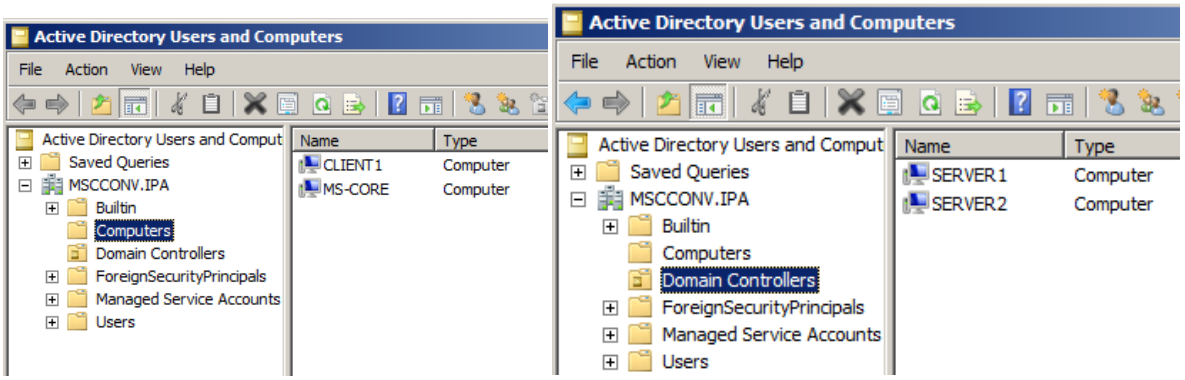
- Enter a domain administrator's credentials and click **OK**
- You are now part of the domain





- Restart the computer to apply the changes

5. Check the machines are configured correctly

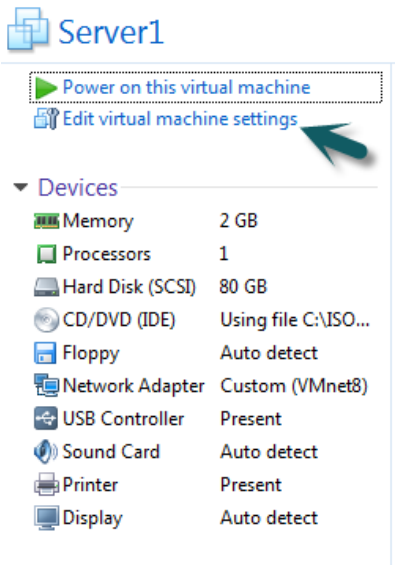


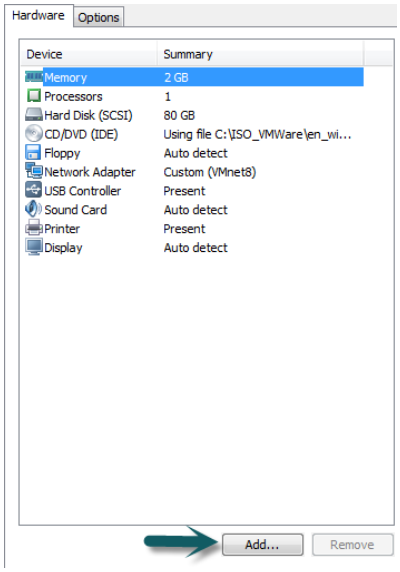
- In the start menu, click **Administrative Tools** then **Active Directory Users and Computers**
- To check to see if the Domain Controllers and Workstations have been added to the domain highlight the tabs. If they have been set up properly they should appear in the window, (see above screenshots)

Task C - Disk Management

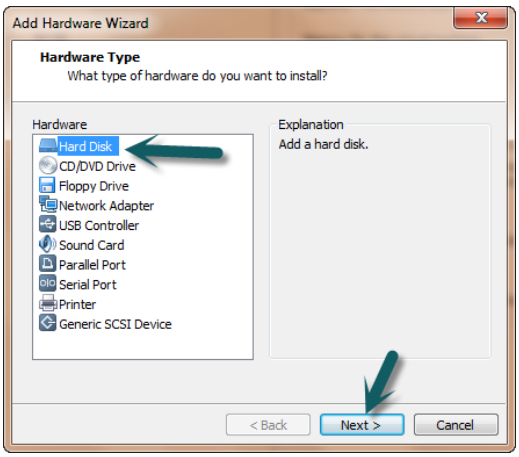
There are many options nowadays for disk management. The use of dynamic disks has allowed for advanced features such as:
simple volumes, mirrored , spanned volumes, striped volumes and RAID 5 volumes.

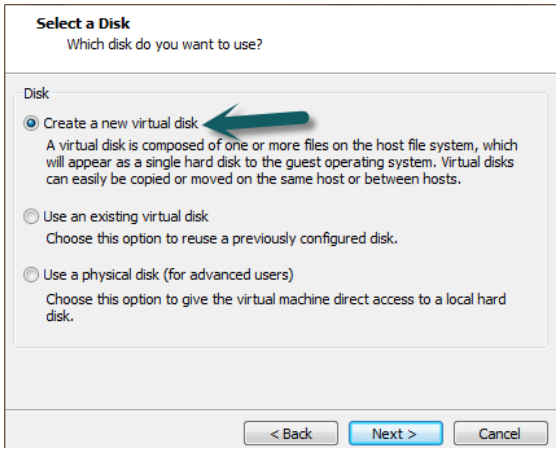
1. Install 2 additional hard disks



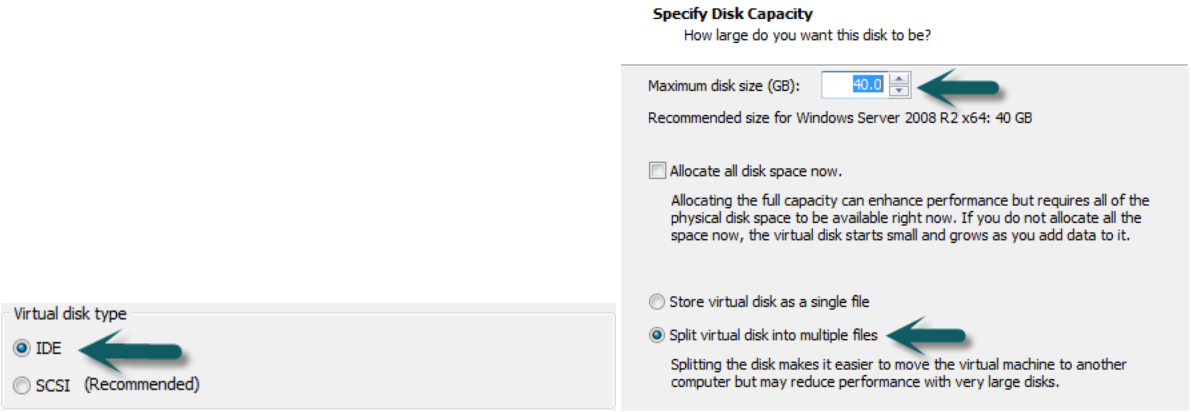


- Open VMWare Workstation and highlight the appropriate machine
- To add a new hard disk, click **Edit virtual machine settings**
- Click **Add**

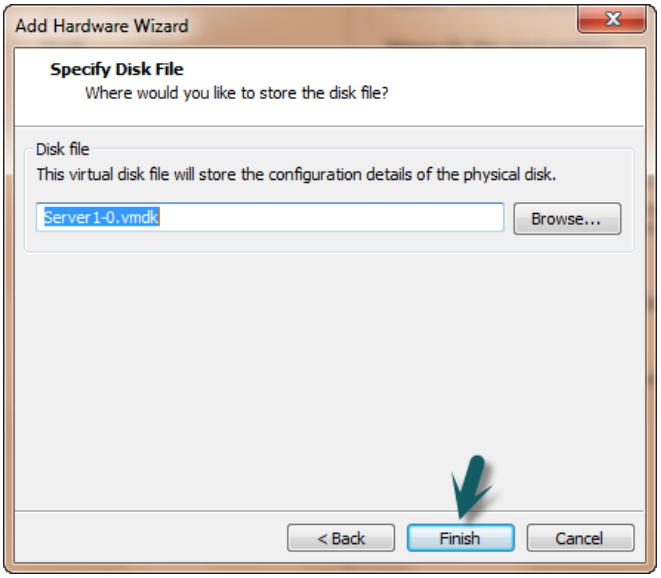


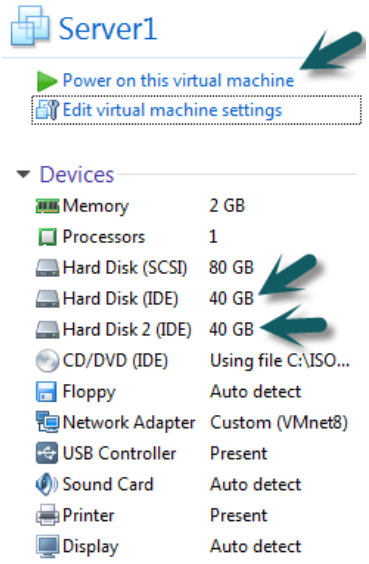


- Select **Hard Disk** and click **Next**
- Select **Create a new virtual disk** and click **Next**



- Choose **IDE** for the virtual disk type and click **Next**
- Set **Maximum disk size (GB)** to the desired size and choose to **Split virtual disk into multiple files**
- Click **Next**

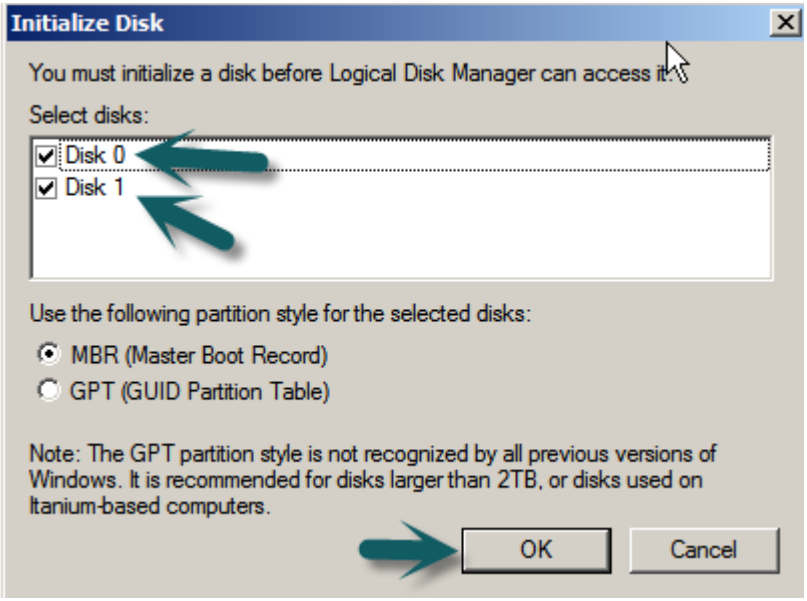




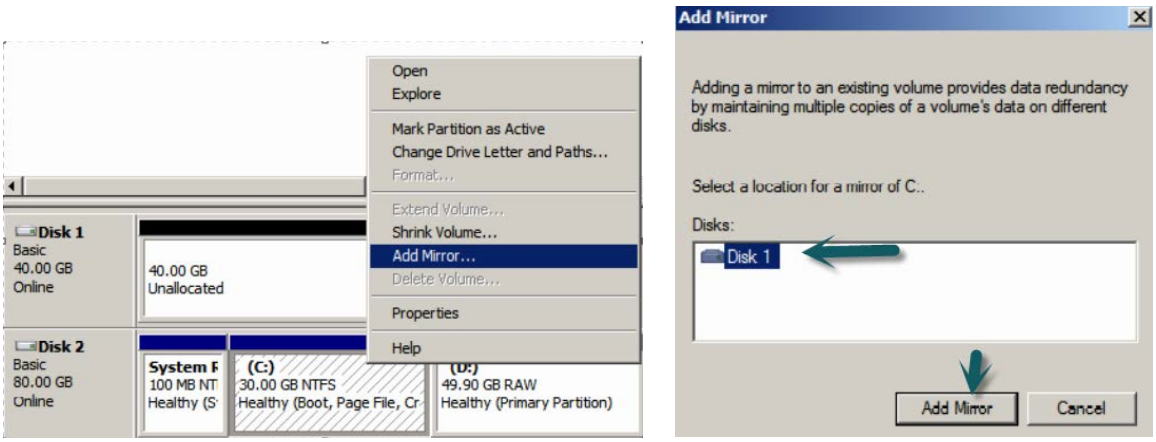
- Leave the filename as the default, don't change it and click **Finish**
- The new hard disks should be now visable on the summary screen, see above screenshot

2. Mirror the Operating System to Disk 1

A mirrored volume is just a simple copy of the volume wrote to another disk. This allows for redundancy, i.e. if one volume becomes corrupt the other take over and no data will be lost. Microsoft says:
[6]" A mirrored volume is a fault-tolerant volume that provides data redundancy by using two copies, or mirrors, of the volume to duplicate the data stored on the volume. All data written to the mirrored volume is written to both mirrors, which are located on separate physical disks."



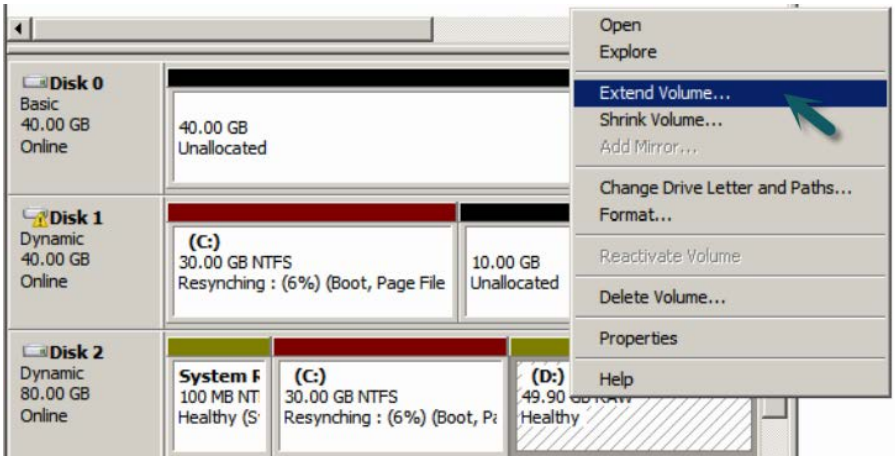
- Power on the virtual machine
- The **Initialize Disk** screen will pop up when logged in
- Check the box beside both new disks
- Choose **MBR (Master Boot Record)** as the partition style for the selected disks. GPT is more suitable for larger disks, i.e. >3TB



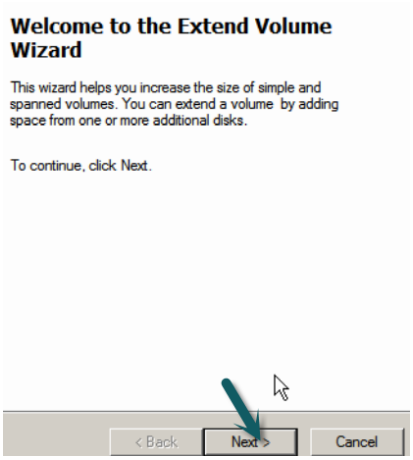
- Right click on the bootable partition with the Operating system installed on it
- Click **Add Mirror**
- Highlight the Disk to hold the mirror and click **Add Mirror**
- The volume will be mirrored into the chosen disk.

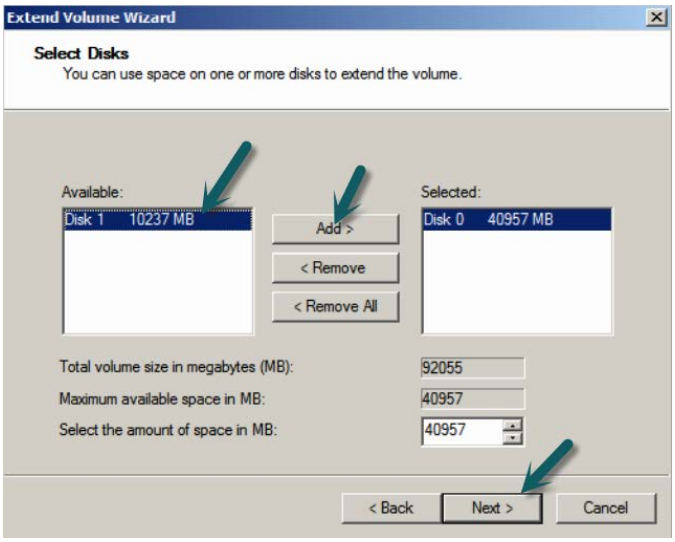
3. Create a Spanned volume on all 3 disks

A spanned volume is one that encompasses free space from multiple physical disks(up to 32 disks). It allows you to use the free space on multiple disks to create one single volume with one drive letter. Spanned volumes offer no redundancy or no performance improvement over simple volumes.

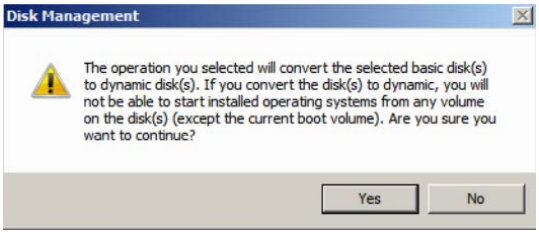


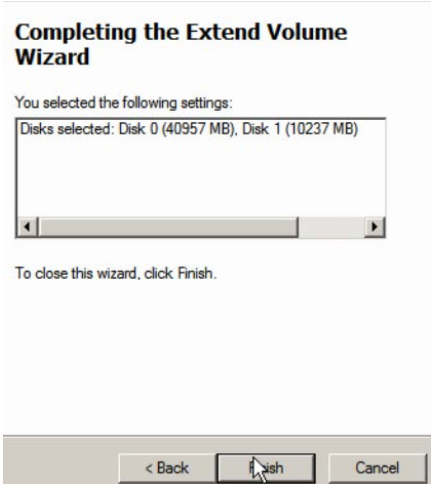
- Right click on the volume you wish to span accross the 3 disks, e.g. D:



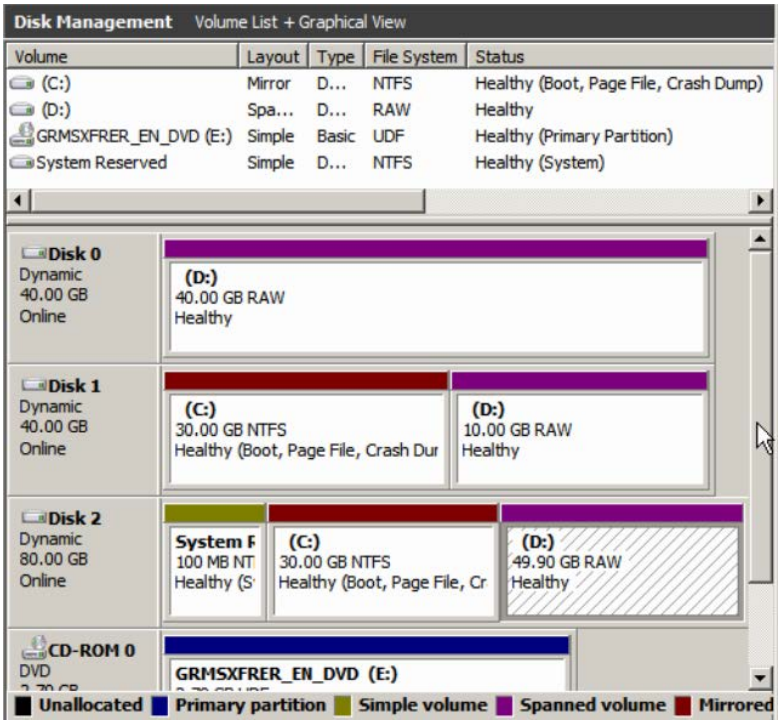


- Click **Next** to start the wizard
- Highlight Disks to be added to the volume and click **Add**
- When both disks are added to the **selected** list
- Click **Next**





- Click **Yes** on the warning popup. The disks will be converted to dynamic disks
- Click Finish to complete the wizard



- The mirrored volumes and spanned volume are now shown graphically on the Disk Management screen within the server manager. See above screenshot

Task D - Creating an Organisational Unit Structure

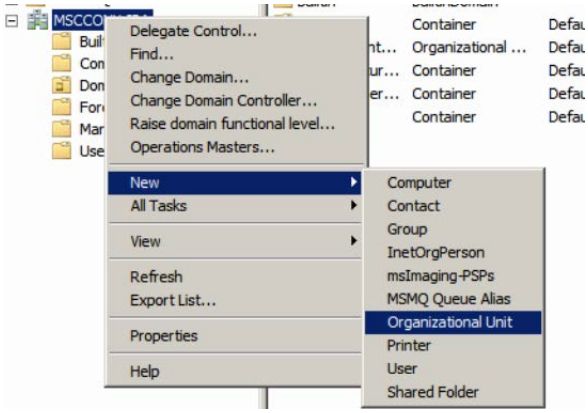
Active Directory offers an opportunity to structure the directory in a way that mimics the logical structure of the organisation. It does this by using Organisational Units(OU's). To make an administrator's life easier, OU's should be structured in a way that allows for easier:
7"

- Management through Group Policy
- Administrative delegation " (Mastering Windows Server 2008 R2, Minasi M)

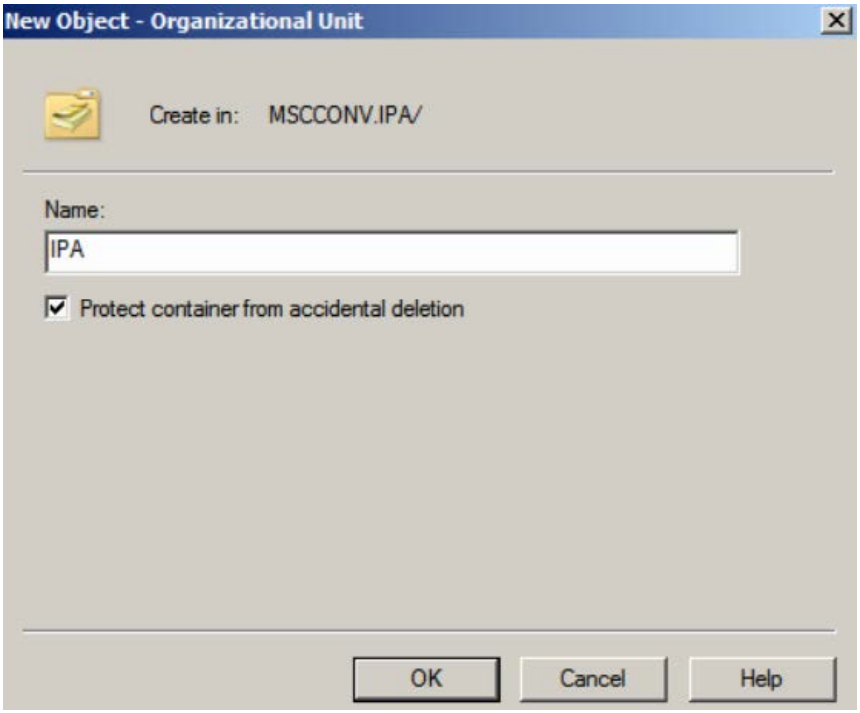
Objects stored within an OU will, by default, inherit any Group Policy Objects linked to the parent. Time should be taken to work out the best way to structure the OU's.

1. Create the Organisational Units

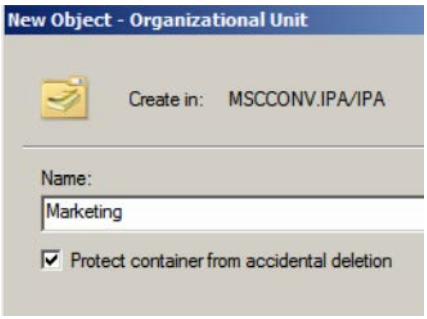
- On the desktop click **Start**
- In the search bar enter **Active Directory Users and Computers**
- Click on the icon to start the utility

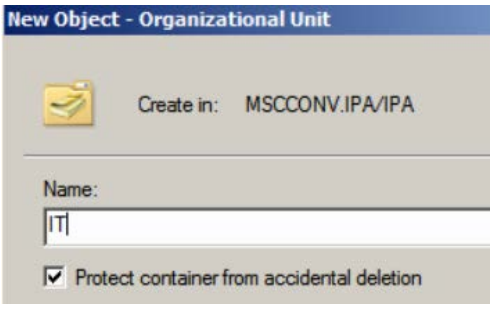


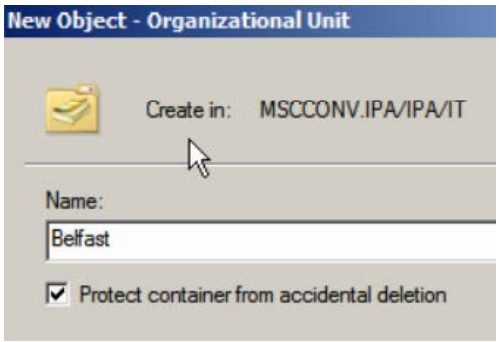
- Right click on the domain, click **New** and click **Organisational Unit** to create a new organisational unit within the domain



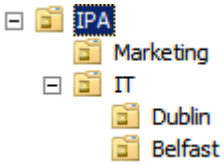
- Enter the name for the Organisational Unit and click **OK**







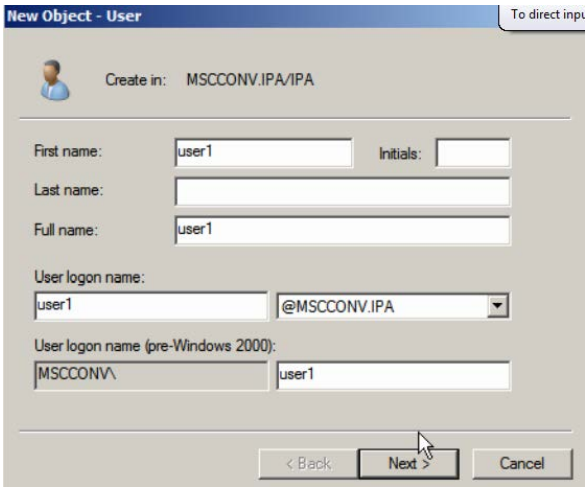
- Within the new **IPA** organisational unit create **Marketing** and **IT** organisational units
- Within the **IT** organisational unit create **Dublin** and **Belfast** organisational units

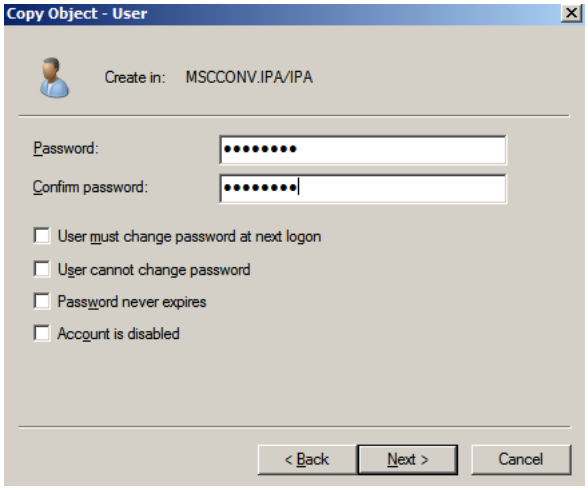


- The organisational unit structure should look like the above screenshot when finished

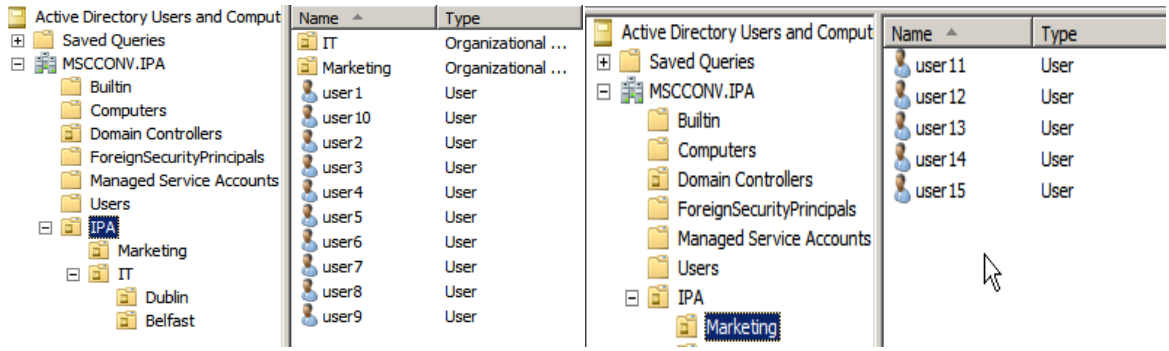
2. Create the Users

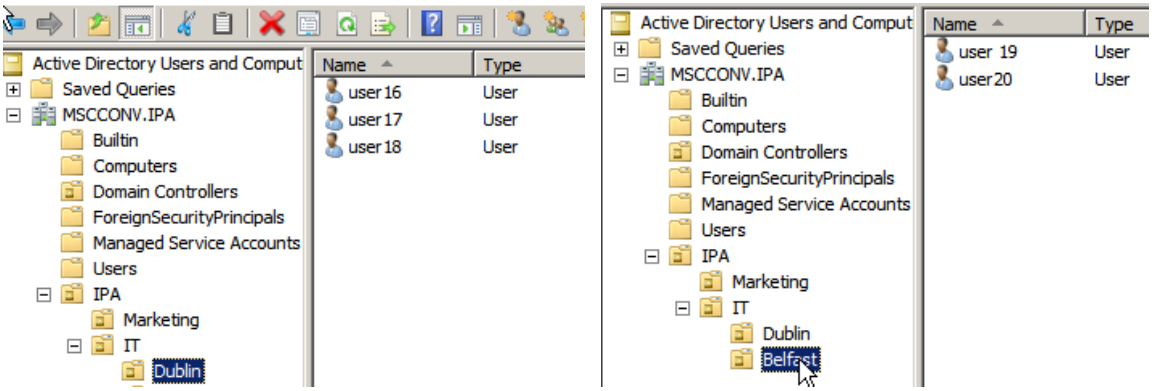
- Highlight the organisational unit you wish to create users in
- Click the  icon at the top of the screen to create a new user





- Enter the users details and click **Next**
- Enter a password for the user
- Uncheck all the option boxes and click **Next**

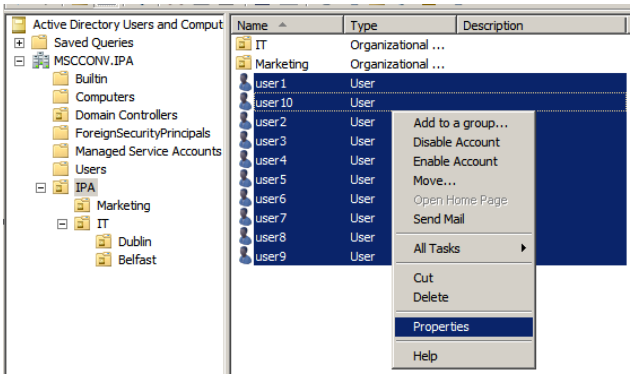




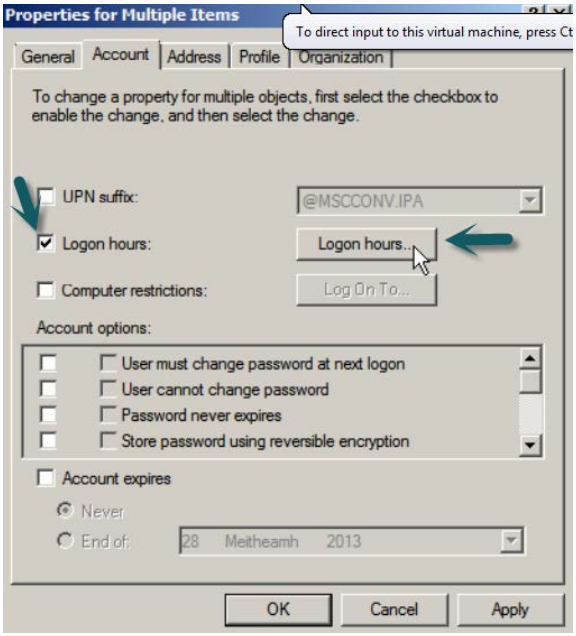
- Create 10 users within the **IPA** organisational unit
- Create 5 users within the **Marketing** organisational unit
- Create 3 users within the **Dublin** organisational unit

- Create 2 users within the **Belfast** organisational unit

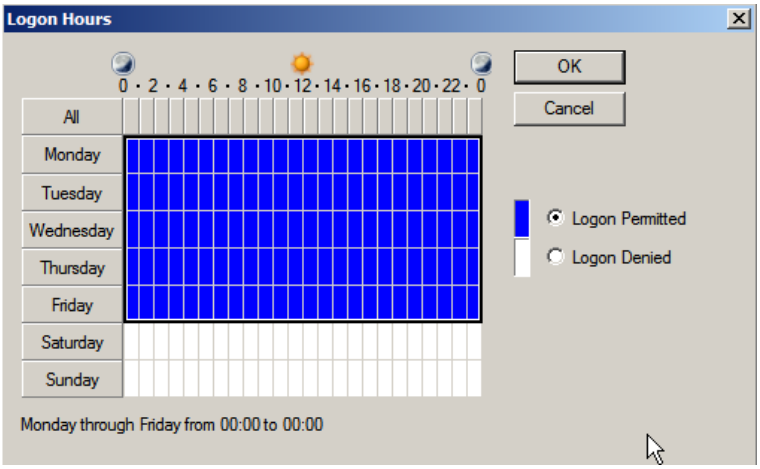
3. Configure the logon hours for all the users



- To change multiple users permitted logon hours highlight the multiple users and click **Properties**



- Click on the **Account** tab
- Tick the **Logon hours** option box
- Click the **Logon hours** button



- Use the mouse to highlight the area on the chart when the users should not be allowed to log on
- Click the Logon Denied option. The selected area should turn white
- Click **OK**
- Click **Apply**
- Repeat these steps for the users in the other organisational units

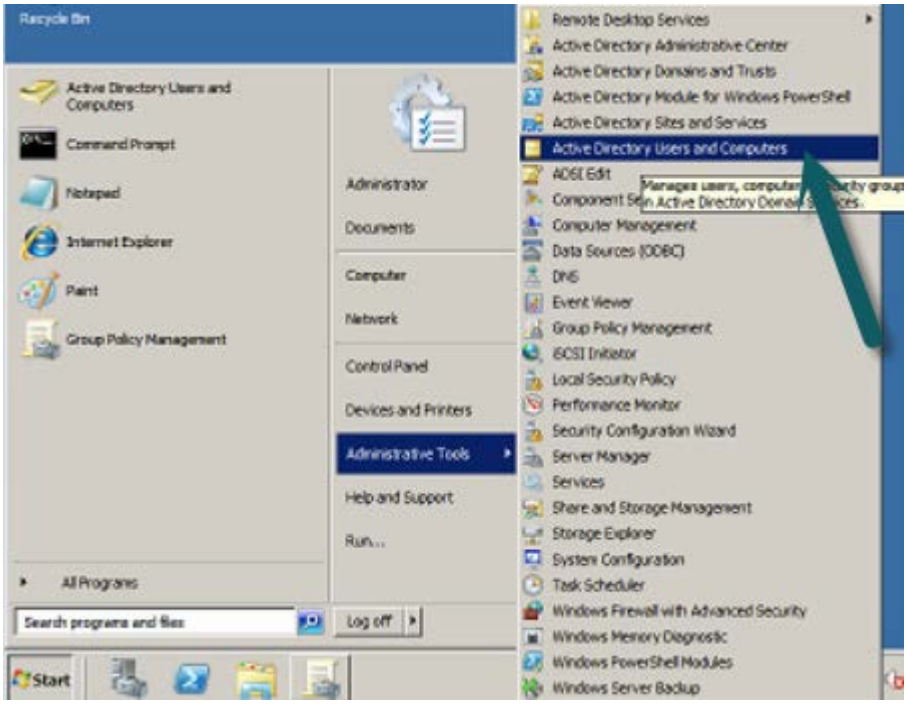
Task E - Grouping Policy

Microsoft Technet says:
[8]"Group Policy is an infrastructure that allows you to implement specific configurations for users and computers."

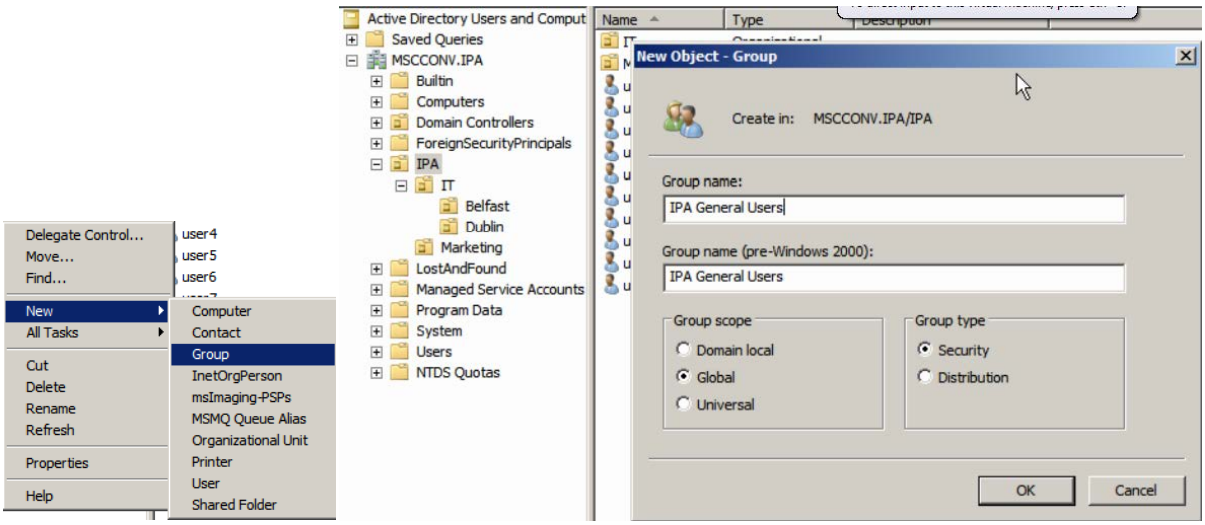
Group Policy provides a way to control the working environment for all the users and computers in the domain. It is enforced using Group Policy Objects(GPO's). A GPO is created and linked to an OU. Any settings in the GPO are applied to the users/computers inside the scope of the OU, i.e. either inside the OU or inside a nested OU. There are over 5000 different settings which can be applied to either the Users or Computers within the scope of a GPO.

1. Group users in each OU

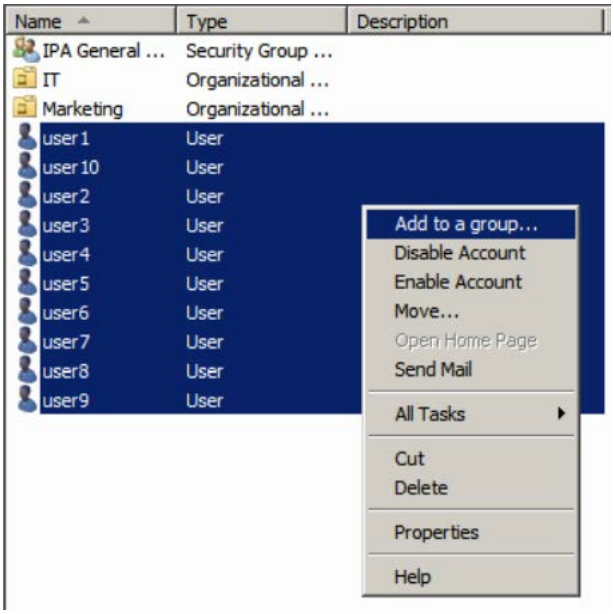
It is best practice not to apply permissions to users and instead to make the users part of a group and apply permissions to the group. This cuts down on administrative work, instead of assigning permissions to every single user, just assign the rights to a security group and make the user a member of the group. If the user leaves or changes department he/she can be easily removed from the group again.



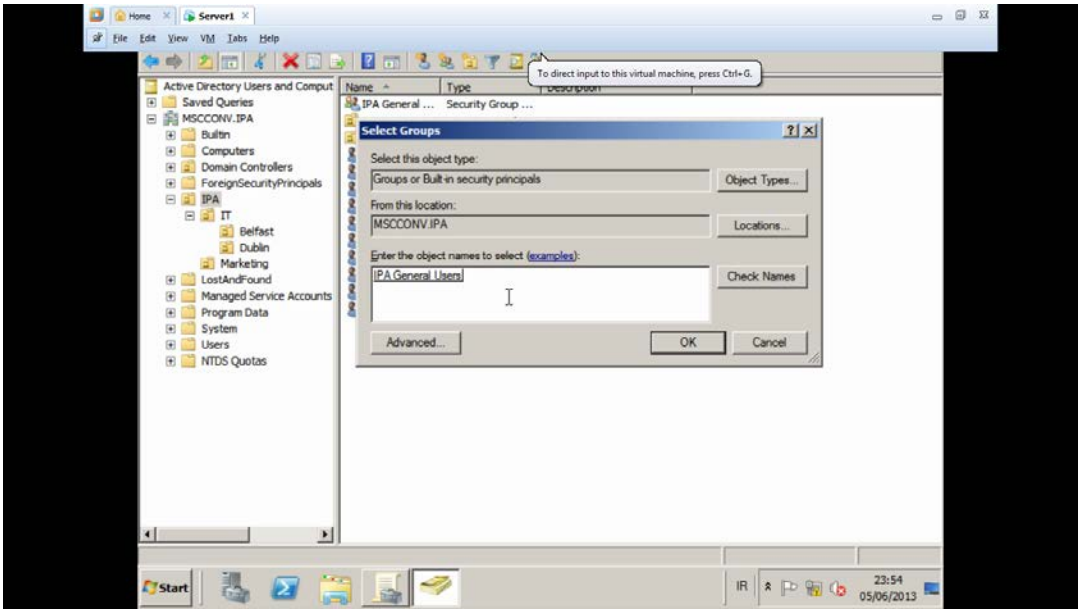
- Click **Start->Administrative Tools->Active Directory Users and Computers**



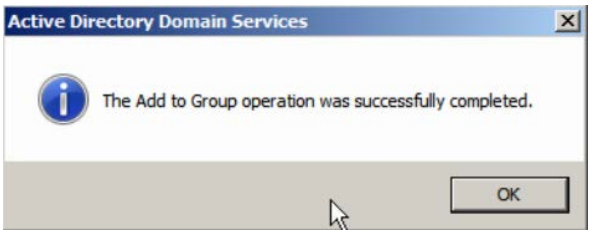
- To Create a new group within the **IPA Organisational Unit(OU):**
- **Right Click** on the **IPA** OU icon and select **New -> Group**
- Enter a meaningful name for the group
- Make sure Group Scope is **Globla** and Group Type is **Security**
- Click **OK**



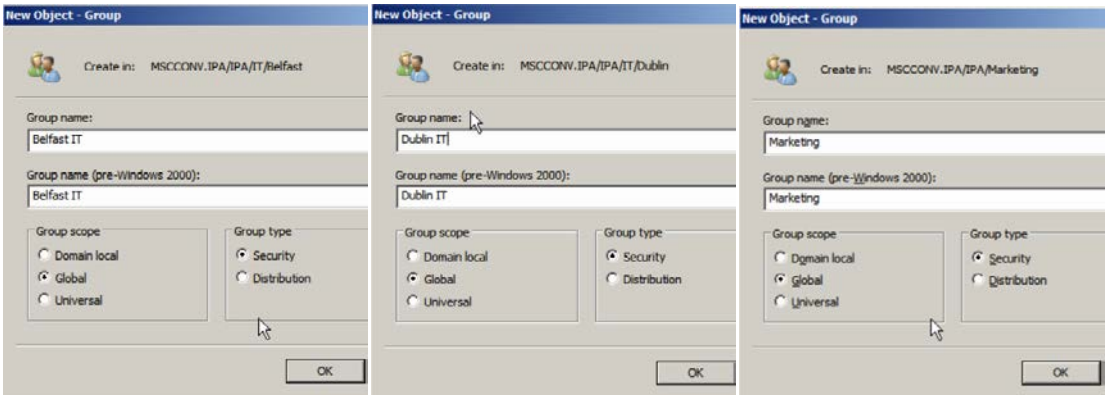
- To add multiple members to the group, highlight the desired members
- Right Click and select **Add to a group...**



- Type the name of the group, e.g. IPA General Users and click **Check Names**
- If the group exists it should appear underlined, see above screenshot
- Click **OK**



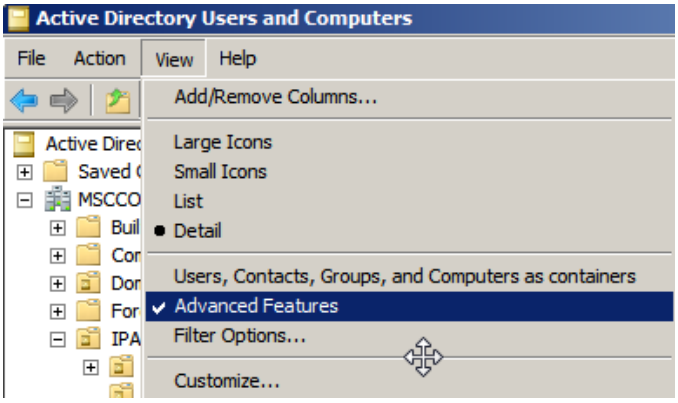
- The selected users are now members of the group



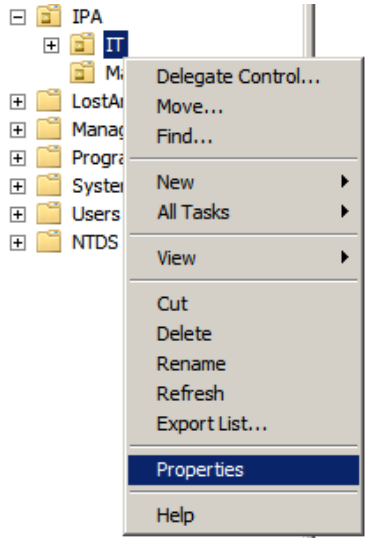
- Create groups in the Belfast, Dublin and Marketing Organisational Units and populate them with the appropriate users in the same way as before.

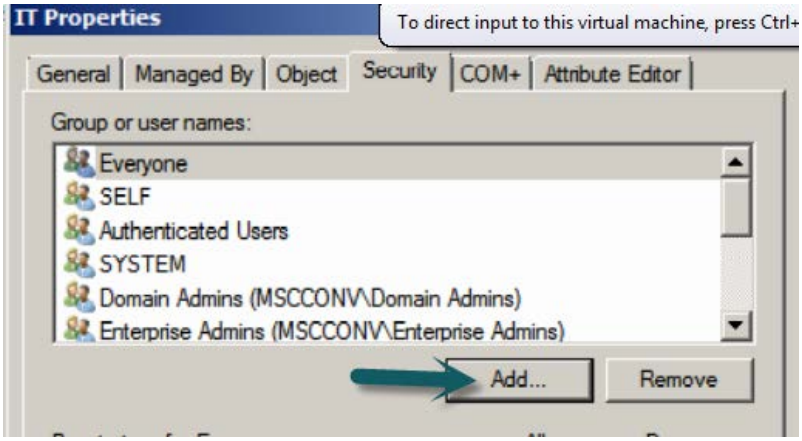
2. Prevent the users in Marketing form being able to see the IT OU in Active Directory

There are may reasons you might wish to hide one group of users from another, e.g. for privacy or security reasons. It is done using the NTFS permissions applied to the OU you wish to hide as follows:

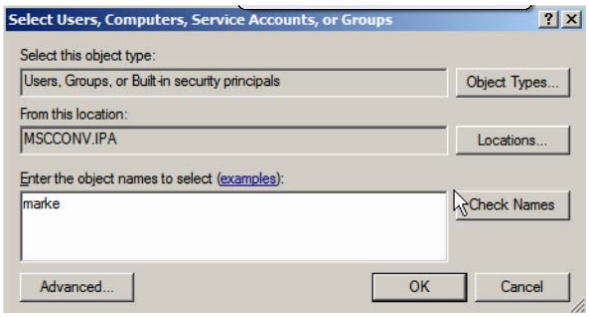


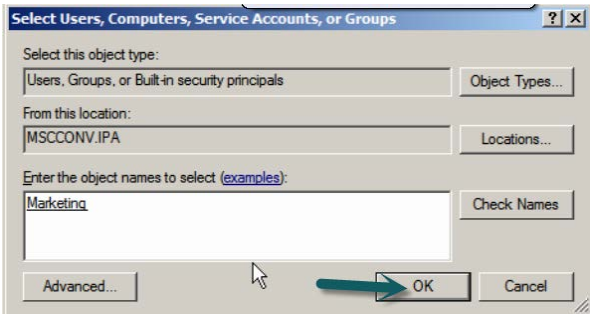
- In Active Directory Users and Computers, click View and click Advanced Features to enable more options, in this case the security tab within the OU Properties.



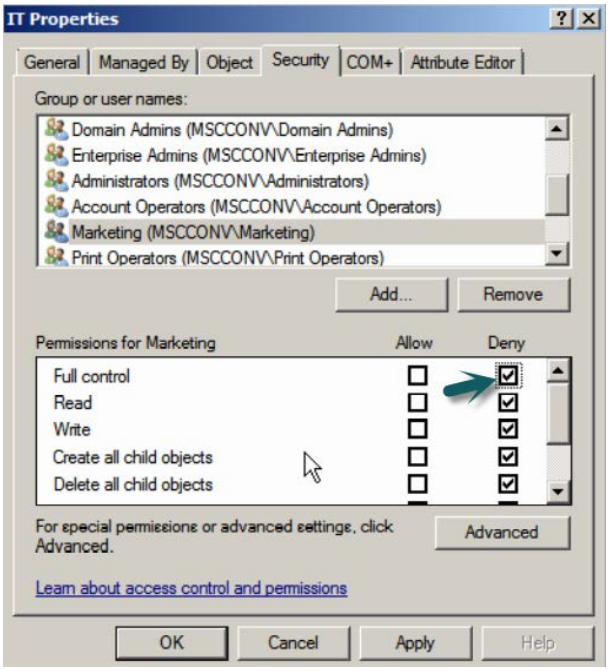


- Right click on the **IT** Organisational Unit and choose **Properties**
- Click the **Security** tab
- Click **Add**

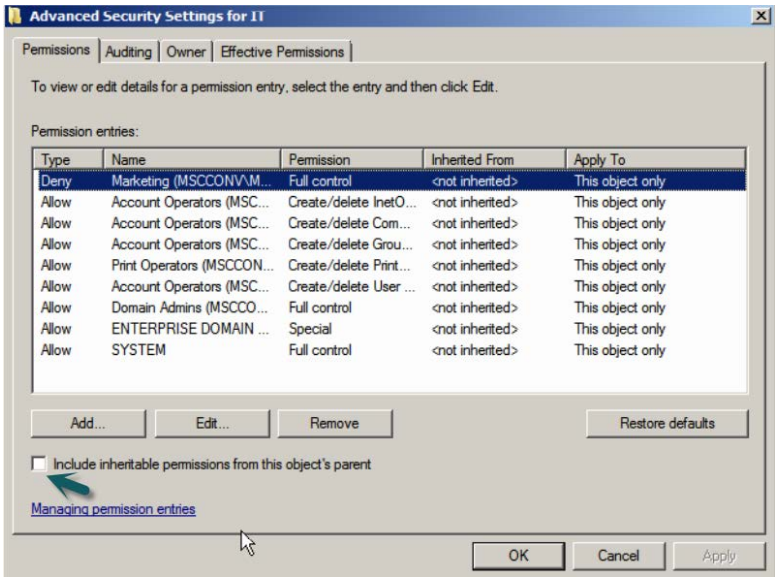




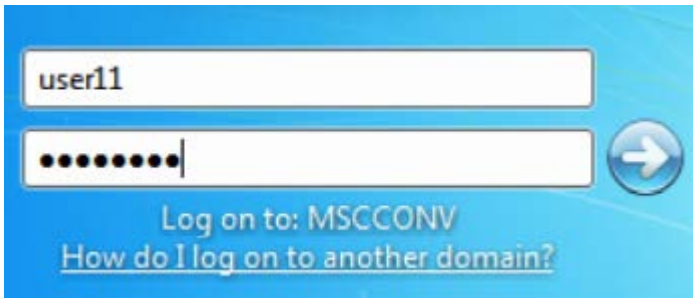
- Enter the first few characters of Marketing and click **Check Names**
- The **Marketing** group should appear underlined in the white box
- Click **OK**



- Highlight the **Marketing** group
- Check the **Deny** box beside **Full Control**. This should check all the deny boxes thus denying the marketing group any access to the IT OU

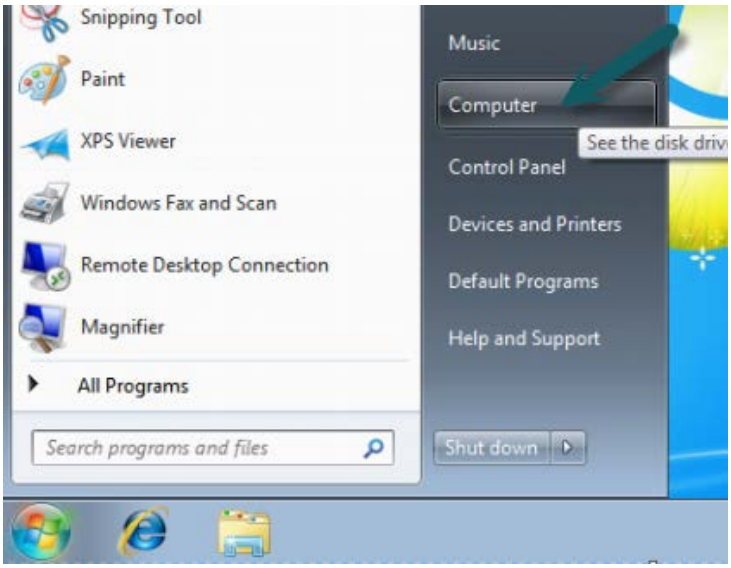


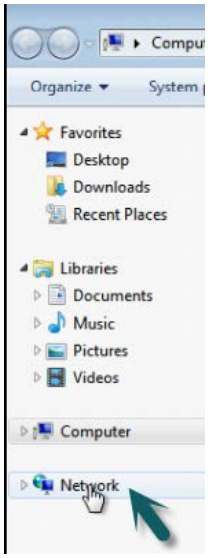
- Click on Advanced
- Uncheck the **Include inheritable permissions from this obect's parent**



- To check that the IT OU has been hidden from Marketing users:

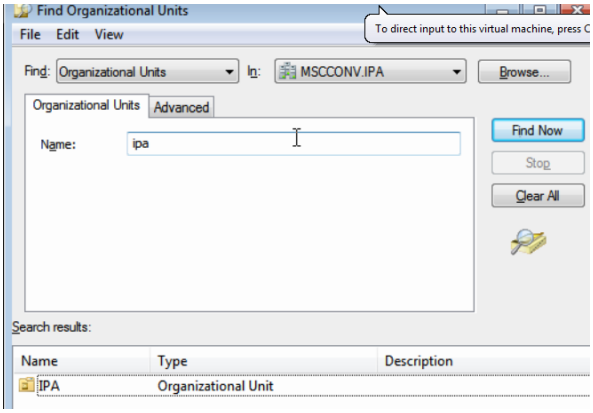
- Log in to Client1 as a marketing user i.e. users 11 - 15. It is possible to check on a server machine but that would mean giving an ordinary user the rights to log on to a domain controller machine and would not be good practice.

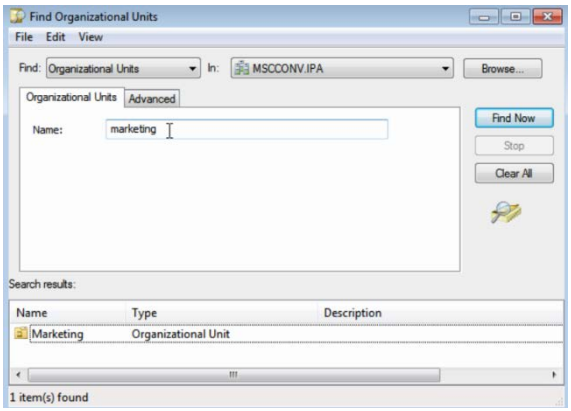




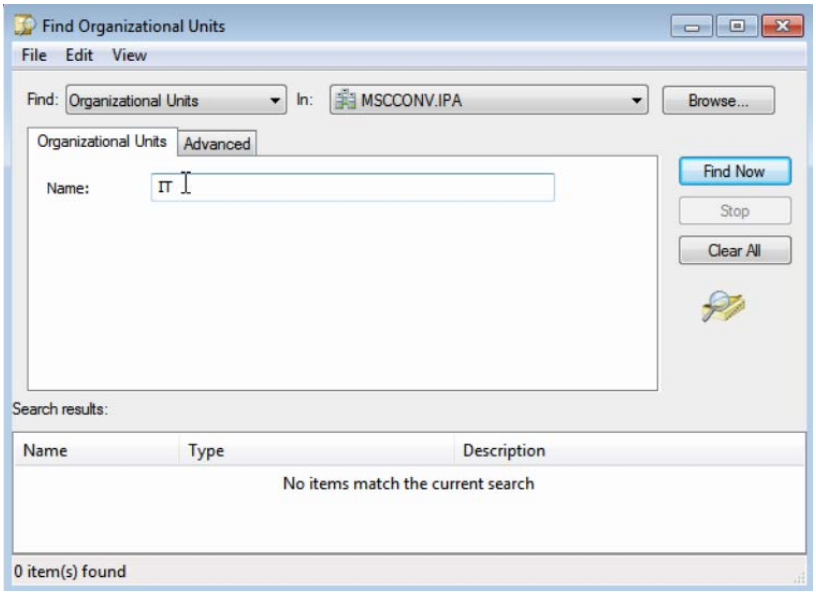
- Click **Start -> Computer**
- Click on **Network**

- Click **Search Active Directory**





- Search for the Organisational Units **IPA** and **Marketing**.
- They should be found and visible at the bottom



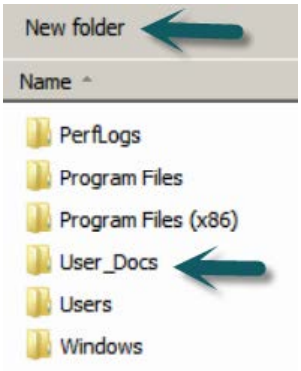
- Search for the Organisational Unit **IT**
- As the user has not got permission to view the OU nothing should be found

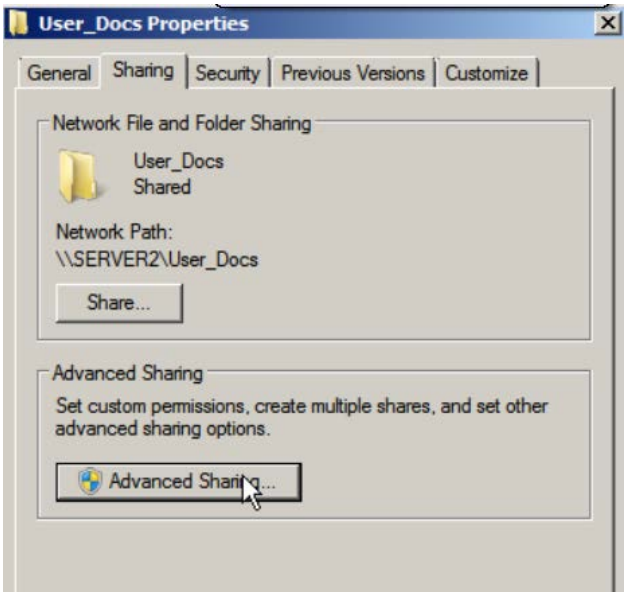
3. Create 3 Group Policies

Group policies are created using Group Policy Objects which can be linked to [9]"sites, domains, and OUs, allowing Group Policy settings to be applied to users and computers." In this section we will demonstrate the creation and linking of 3 of these GPO's.

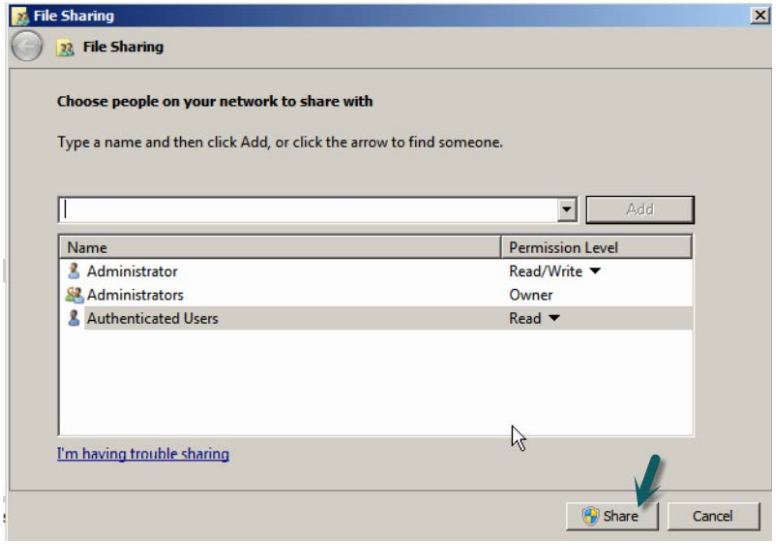
(a) Group policy to forward the my documents folder from those using Client1 to a folder on the root of Server2.

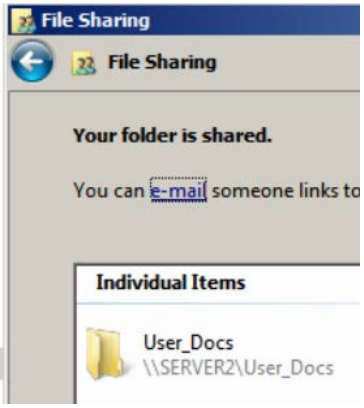
In this example we will assume the users of Client1 are those who work in Belfast IT, i.e those in the security group Belfast IT, user 19 and 20. A possible reason for forwarding the my documents folder to Server2 would be that the company wants to conserve space on Client1.



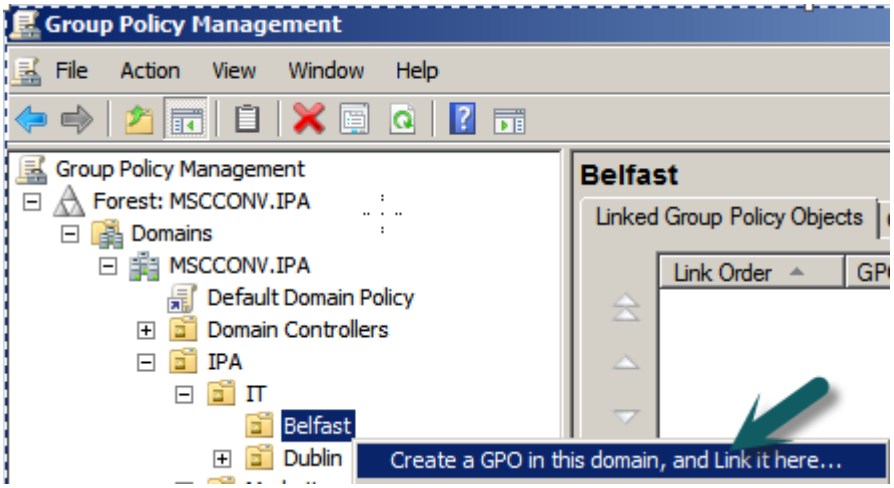


- First we must create a folder in Server2 to redirect the my documents folder to.
- Create a new folder on the C:/ of Server2 and call it **User_Docs**
- Right click on the folder and click on the **Sharing** tab
- Click **Share**

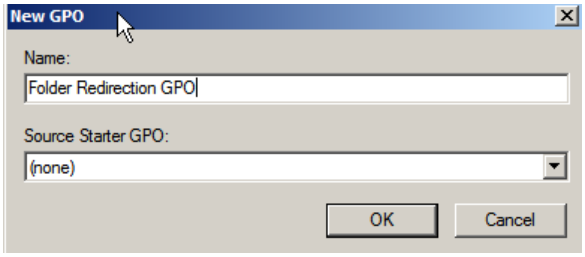




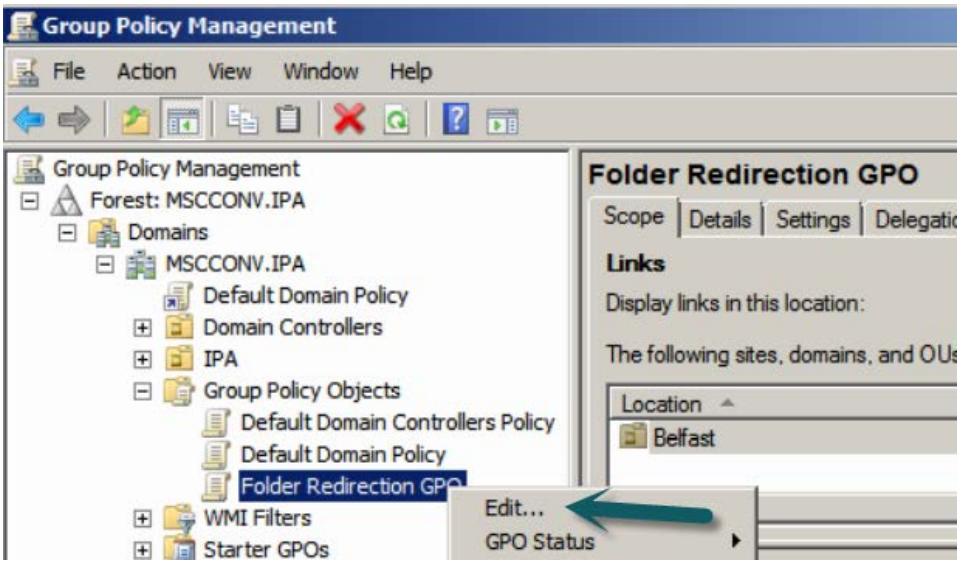
- Add Authenticated users to the share and give them Read permissions. The users will only have NTFS permissions for their own my documents folder.
- Click **Share.** The folder is now shared.



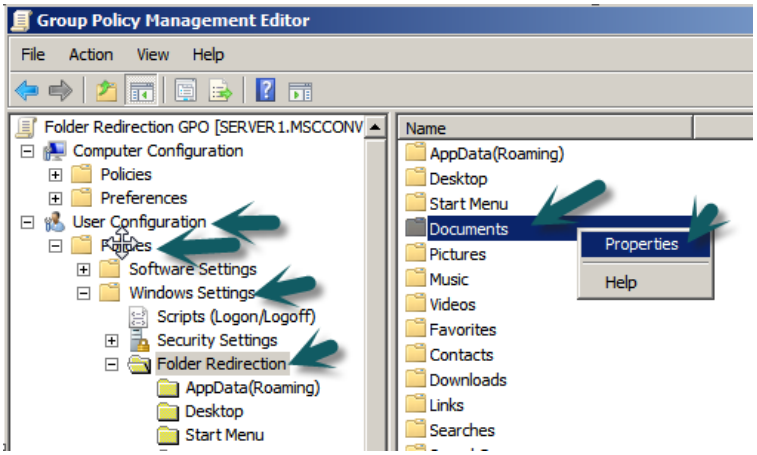
- Open **Gropu Policy Management** by clicking **Start->Administrative Tools-> Group Policy Management**
- We are creating a group policy to apply to the users in Belfast so we create a GPO and link it to the Belfast OU by right clicking on **Belfast OU** and clicking **Create a GPO in this domain and link it here...**



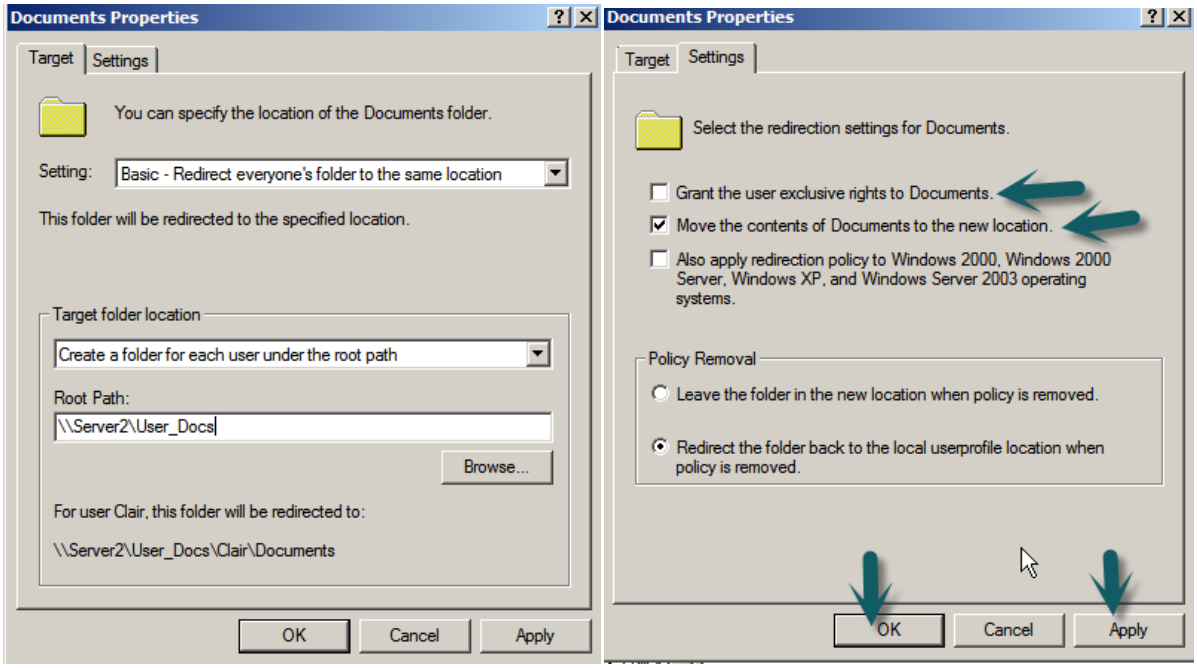
- Name the new GPO with a meaningful name i.e **Folder Redirection GPO**



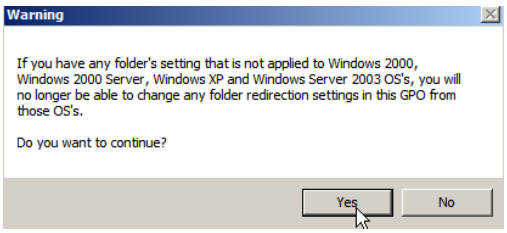
- To edit the configuration of the GPO, right click on it and click **Edit**



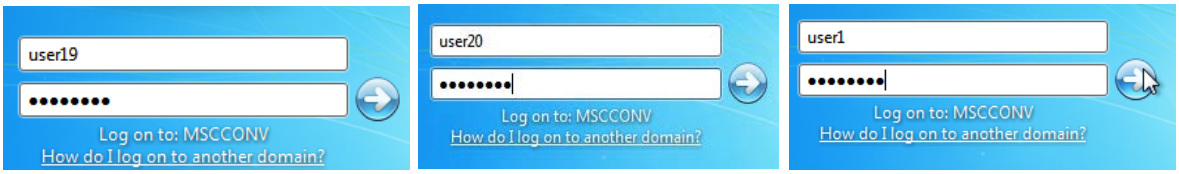
- Follow the path **User configuration->Policies->Windows Settings->Folder Redirection**
- Right Click on **Documents** and click **Properities**



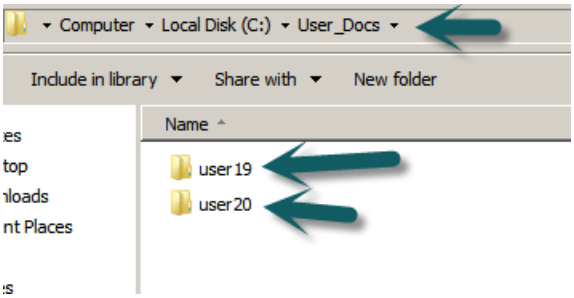
- Choose **Basic - Redirect everyone's folder to the same location**
- Choose to **Create a folder for each user under the root path**
- Specify the root path as **\\Server2\User_Docs**
- Click the **Settings** tab
- Untick **Grant the user exclusive rights to Documents**
- Choose what ever options suit your situation best for the other options
- Click **Apply** and **OK**



- Click **Yes** on the warning window. This warning concerns windows 2000 computers.

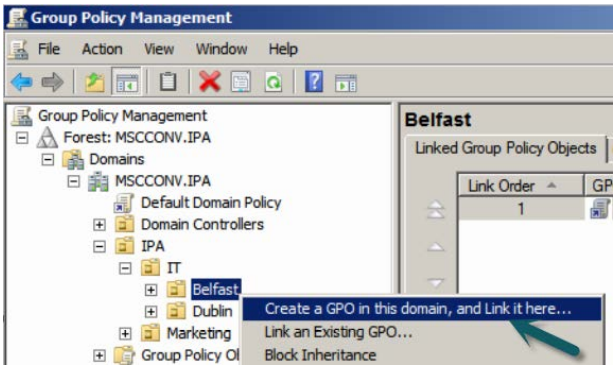


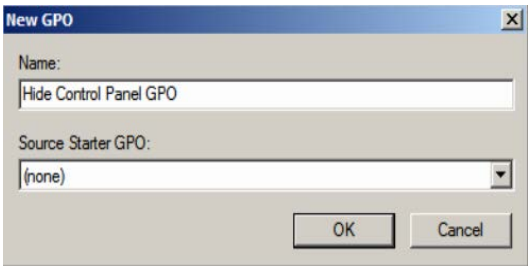
- To test the GPO has been applied, log in to Cliient1 as the Belfast IT users, i.e users 19 and 20
- The my documents should be forwarded to Server2 when you log on
- Also to make sure it doesnt apply to all users, log in as some other users, e.g. user 1. Their folders should not be redirected



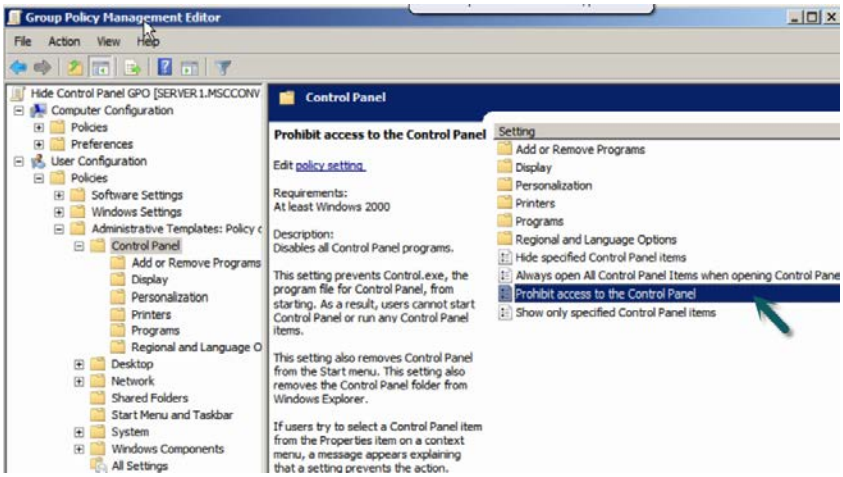
- Log on to Server2 and and navigate to the **User_Docs** folder. There should be folders inside for the two members of the Belfast IT group. There should be no other folders inside for any of the other users.

(b) Group policy to prevent users in Belfast from accessing the control panel with the exception of user20

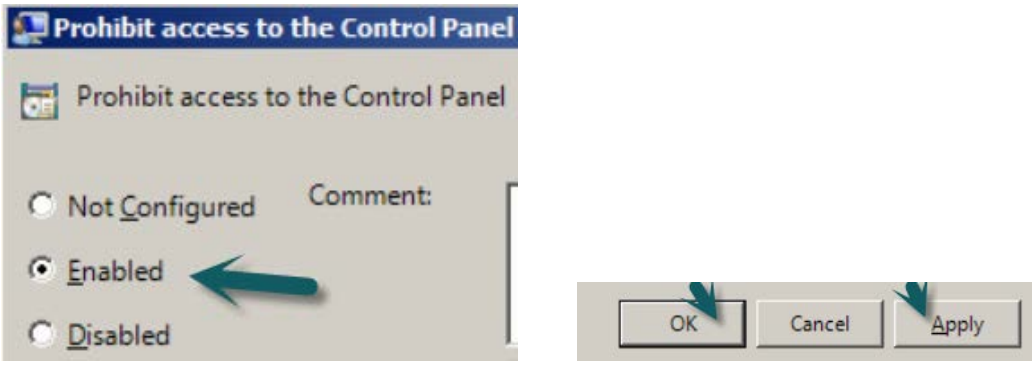




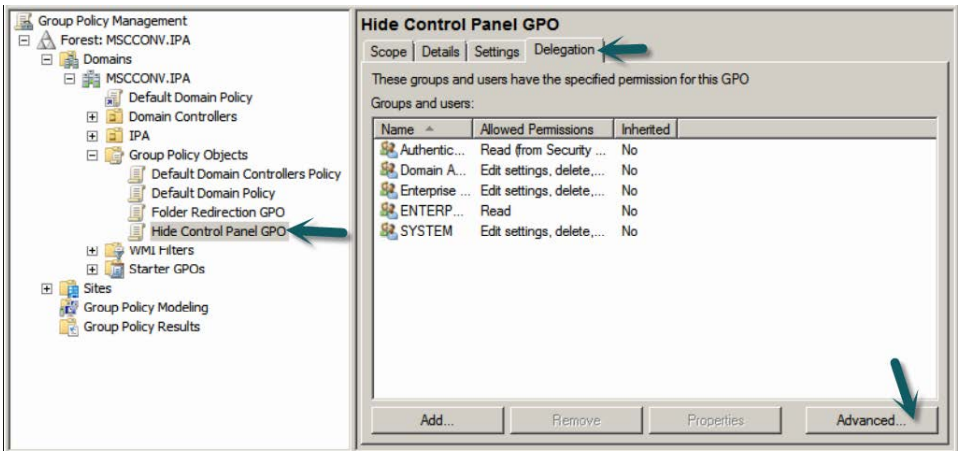
- Open The **Group Policy Management** console like before
- Right click on the **Belfast** OU and choos **Create a GPO in this domain, and Link it here...**
- Name the GPO something meaningfull, e.g. **Hide Control Panel GPO** and click **OK**



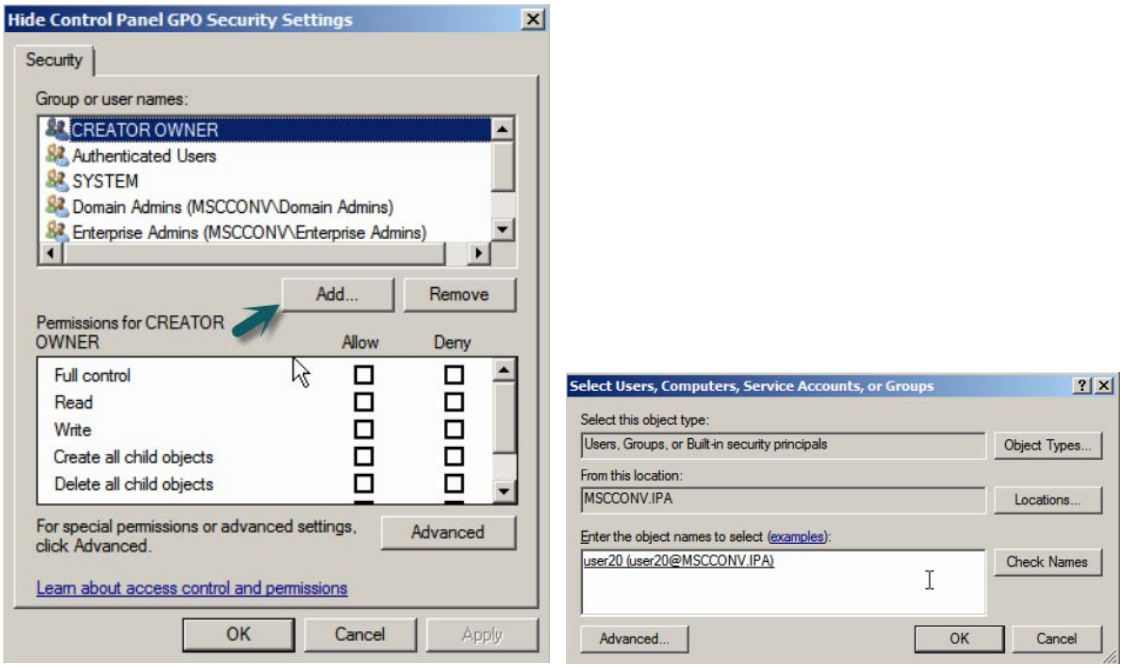
- Right click on the newly created GPO and click **Edit** to open the Group Policy Management editor
- Follow the path: **Hide Control Panel GPO -> User Configuration->Policies->Administrative Templates->Control Panel**
- Highlight **Control Panel**
- Double Click **Prohibit access to the Control Panel**



- Choose the **Enabled** option box to enable the policy
- Click **Apply** then **OK**



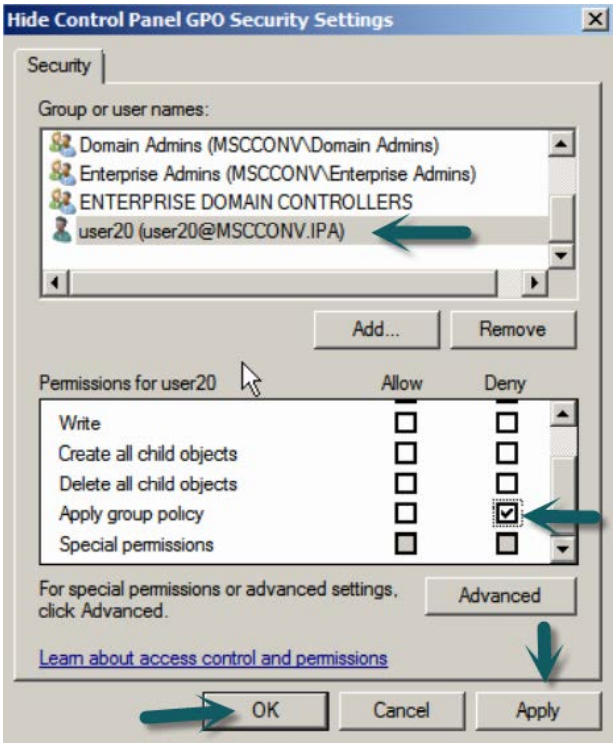
- To add and exception for user20 so the policy doesn't apply for them:
- In the Group Policy Management Console highlight the **Hide Control Panel GPO**
- Click the **Delegation** tab and click **Advanced**



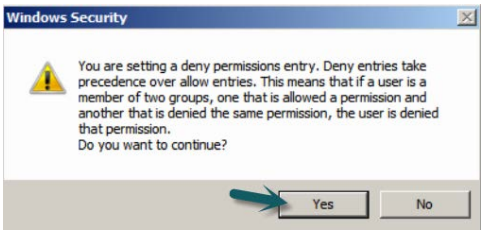
- Click **Add**

- Enter the name of the user/group you wish to and click **Check Names**.
- Click **OK**

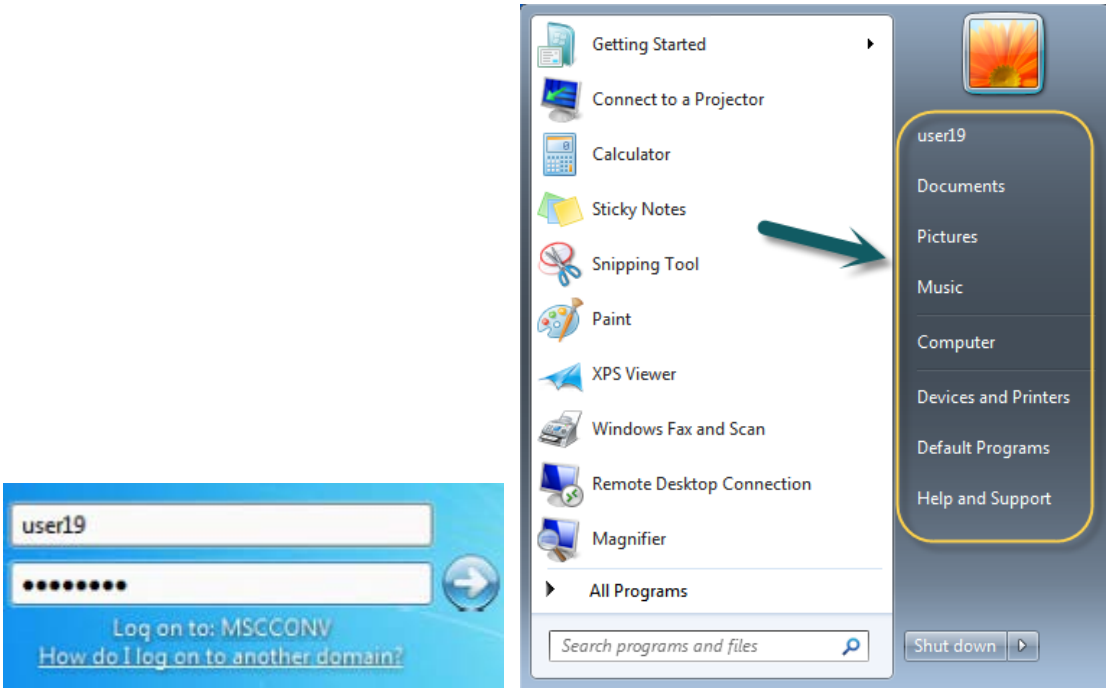
NB- It is better practice create exceptions for security groups rather than for users.



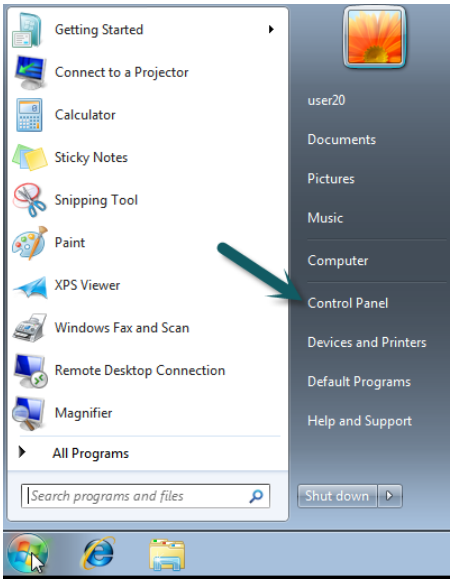
- Highlight the user and check the **Deny** box beside **Apply group policy**
- Click **Apply** then **OK**



- Click **Yes** on the warning screen to continue



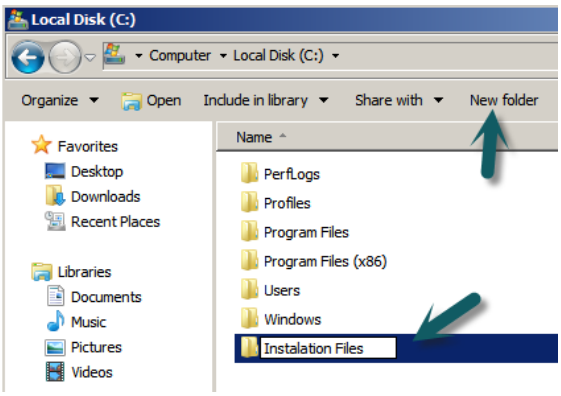
- Log on as a user from Belfast. i.e. user19
- To check the GPO has been applied properly click the **Start Menu**. The Control panel should not be present if the GPO has been applied properly



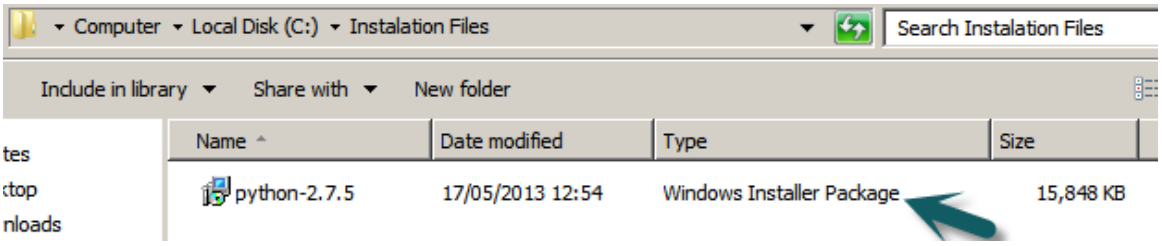
- To check the exception has been applied log on as user20.
- Open the start menu and the Control Panel should be present if the exception is working

(c) Group policy to publish an MSI file from the C drive to all the users in Dublin

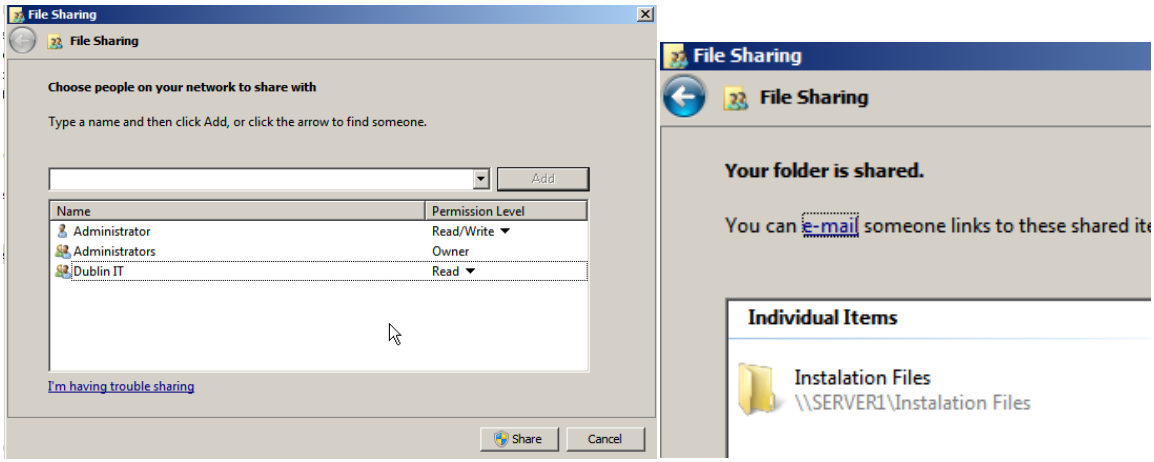
An MSI file is a Microsoft Installer file is a file used to install a program on a windows machine using Windows Installer. It is a very user friendly way of installing a program. In this case we will demonstrate the publishing of an msi file to the control panel the users in Dublin. Group Policy can be a very effective tool in rolling out new software/software updates over a network. Instead of publishing the file to the control panel for the users to install themselves, the msi file could be set to deploy itself automatically and silently when the user logs on to the network or when anyone logs on to a computer.



- First we must create a folder to hold the .msi file on the C drive and share it to the Dublin Group
- Open **My Computer** then the **Local Disk (C:)**
- Click **New Folder** and call the new folder something meaningful, e.g. **Installation Files**

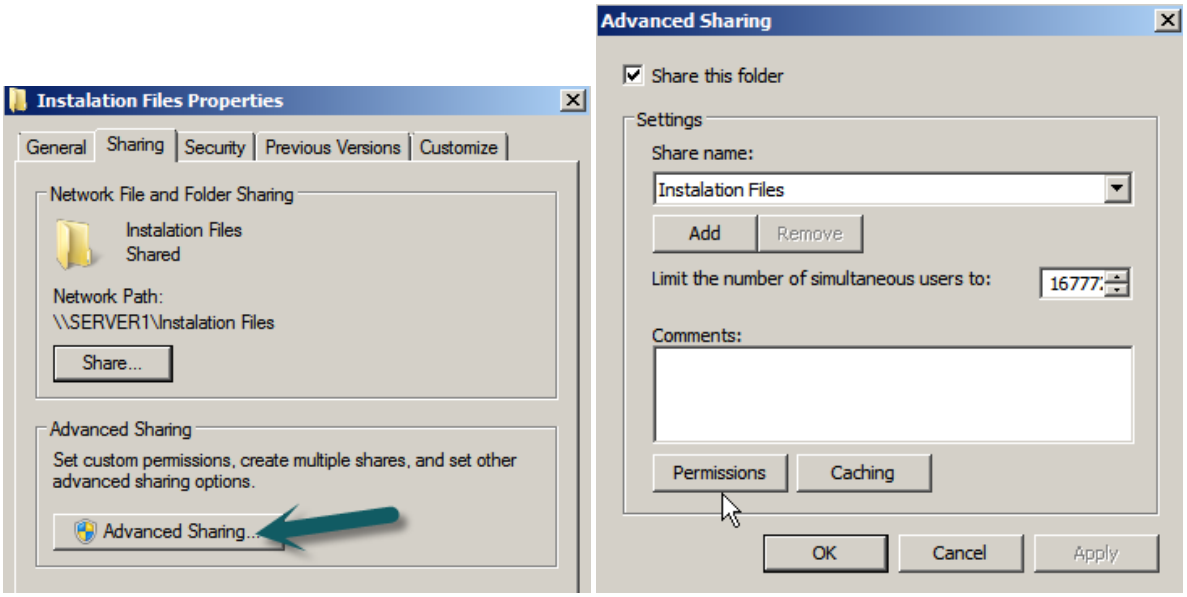


- Copy and Paste the desired .msi file into the folder

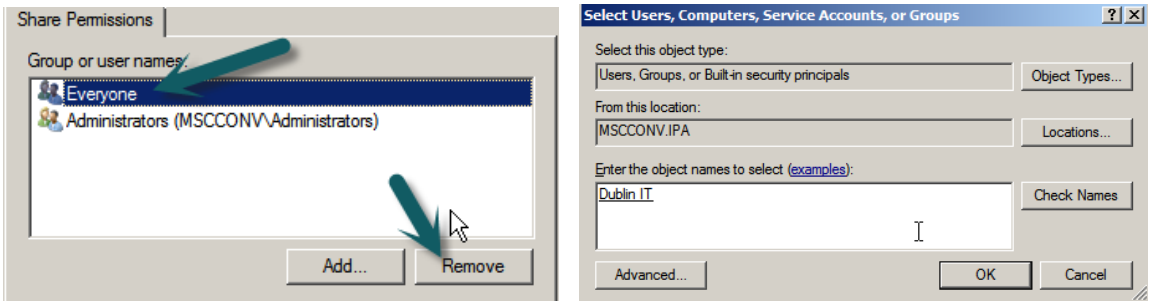


- Right click on the folder and click **Share**

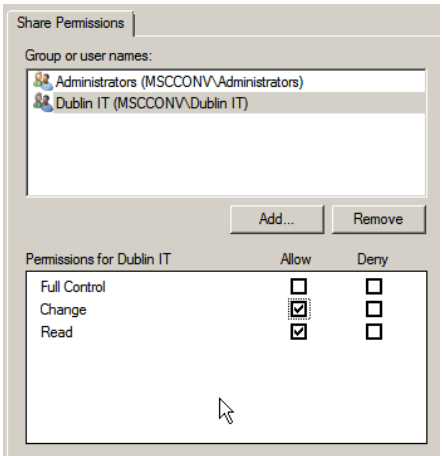
- Add the Dublin IT security group to the share
- Click **Share**
- The folder is now shared. Note the network path of the shared folder as it will be needed when creating the Group Policy Object



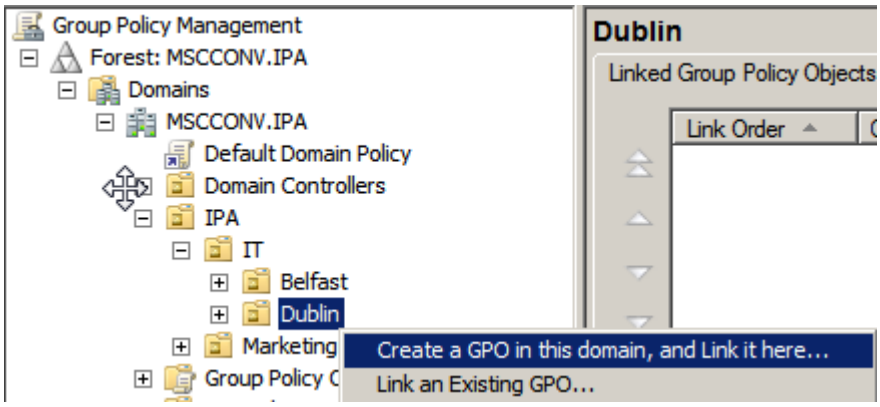
- To fine tune the permissions for the share, right click on the folder and click **Properties**
- Click the **Sharing** tab and click **Advansed Sharing**
- Click **Permissions**



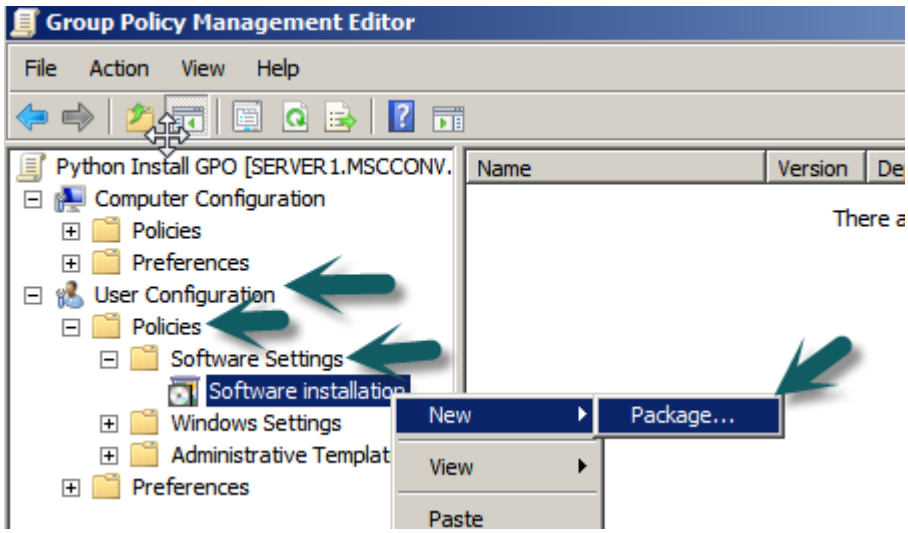
- Remove the **Everyone** security group and add the **Dublin IT** tab
- Click **OK**



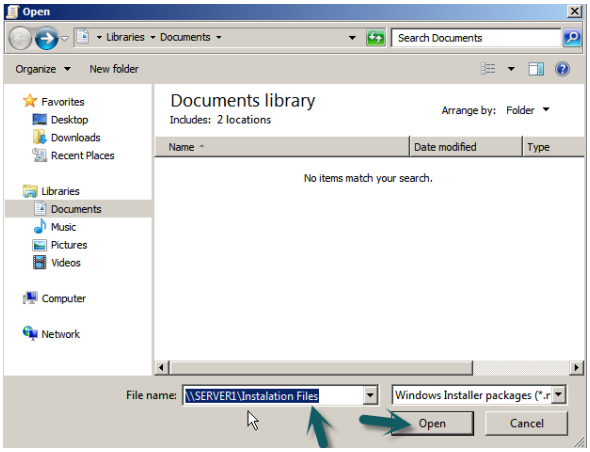
- Highlight the **Dublin IT** group
- Give the group **Change** and **Read** permissions
- Click **OK**

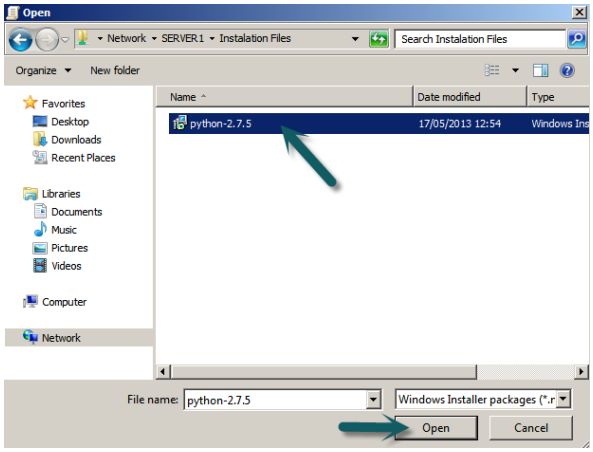


- Open the Group Policy Management console
- Right click on the **Dublin** OU and click **Create a GPO in this domain, and Link it here...**

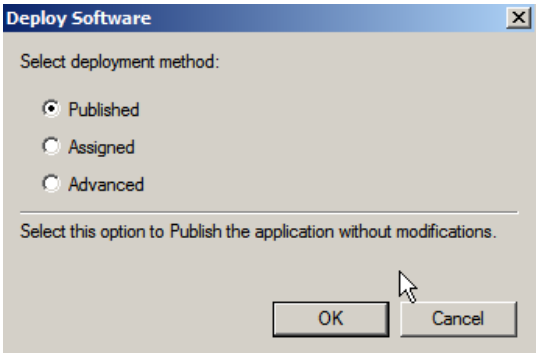


- To configure the new GPO, right click on it and click **Edit** to open the **Group Policy Management Editor**
- Follow the path **User Configuration->Policies->Software Settings**
- Right click on **Software installation**, then **New->Package**



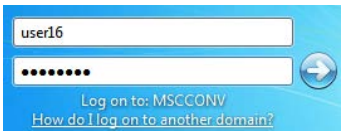


- Enter the Network path of the shared folder we created and click **Open**, e.g **\\SERVER1\Instalation Files**
- Highlight the .msi file you wish to publish and click **Open**

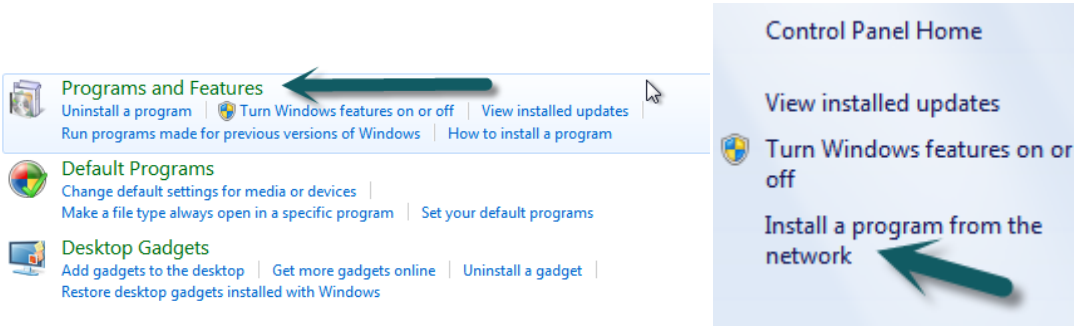


- Choose to **Publish** the application. This will add it to the list of programs which can be installed over the network in the control panel
- Click **OK**

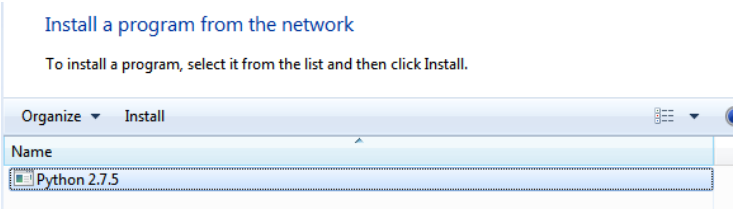
Note- To automatically install the program when the user logs on we would choose **Assigned,** or for further more advanced options we would choose **Advanced**



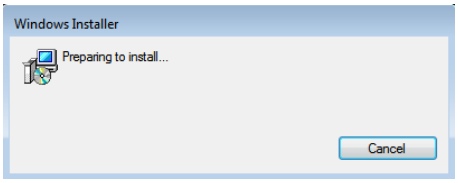
- To test the Group Policy has been enforced for the Dublin IT users, log in to a client machine with a Dublin IT user, e.g. **user16**
- Open the **Control Panel** and click on **Programs**



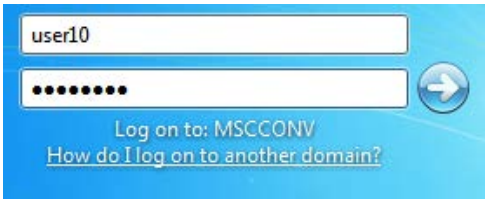
- Click **Programs and Features**
- Click **Install a program from the network**

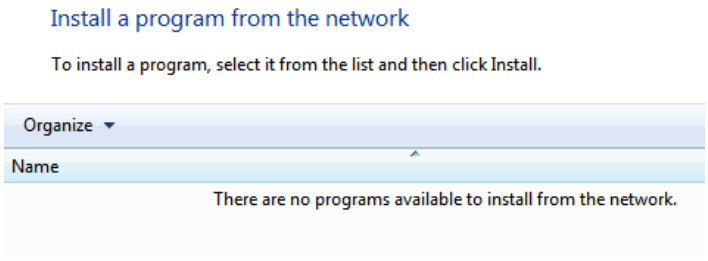


- The program should be available to install over the network
- Double click on the program and the Windows Installer wizard will start.



- Follow the instructions of the wizard and the program will now be installed on the client computer.





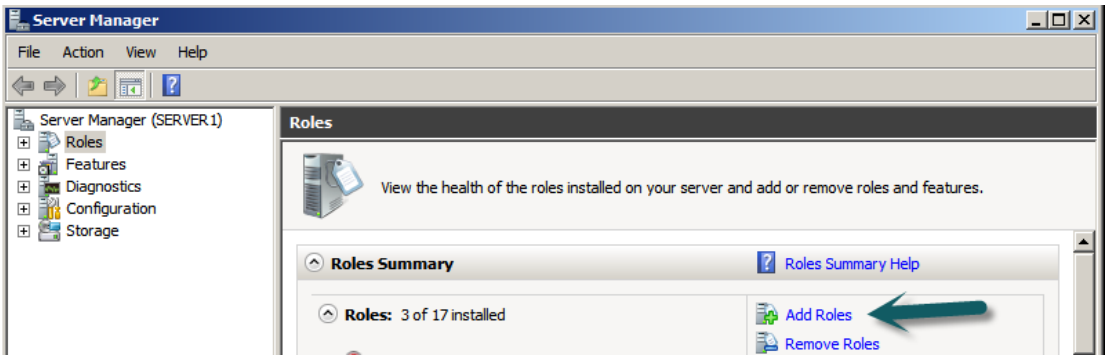
- To show the program is not available for other users who are not part of the **Dublin IT** group log in as any other user, e.g. **user10**
- Follow the same steps as above, the program should not be available to install from the network.

Task G - Print Servers

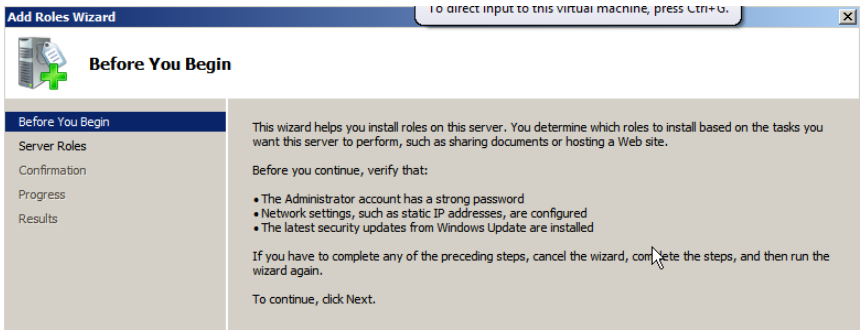
Adding the print server role to a Windows Server 2008 machine allows the use of the print management console (PMC). The PMC is a utility that allows [10]"you to do *everything* printer related from a single console". Tasks that can be performed from the PMC include the following:

- Add new drivers
- View printers using custom filters
- Manage printer settings and drivers
- Monitor printer status and configure alerts
- Connect to remote print servers so you can do all this for your entire enterprise

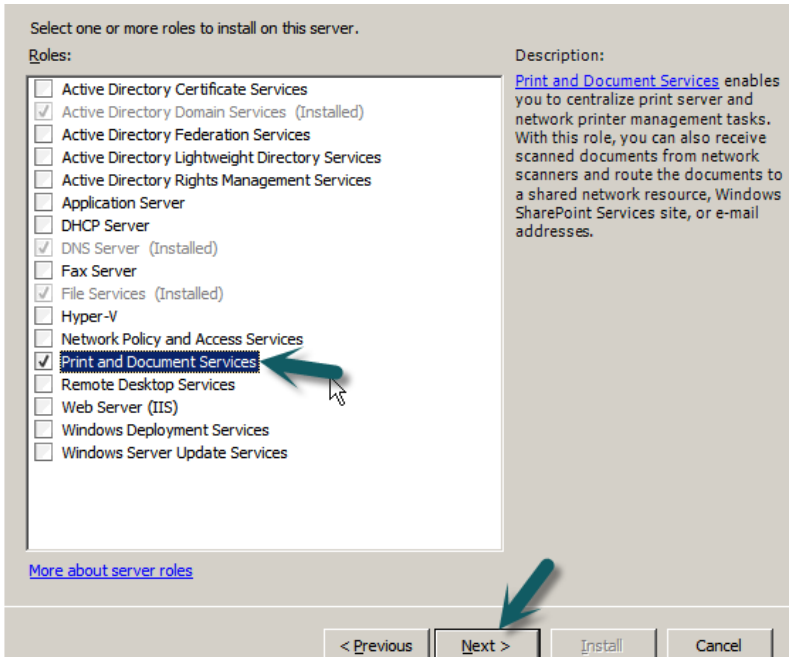
1. Configure Server1 as a print server



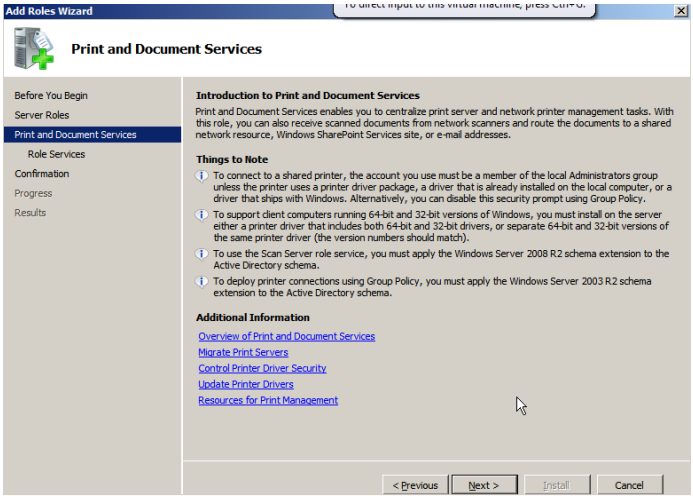
- Open the **Server Manager** by clicking **Start->Administrative Tools->Server Manager**
- Click **Add Roles** to start the **Add Roles Wizard**



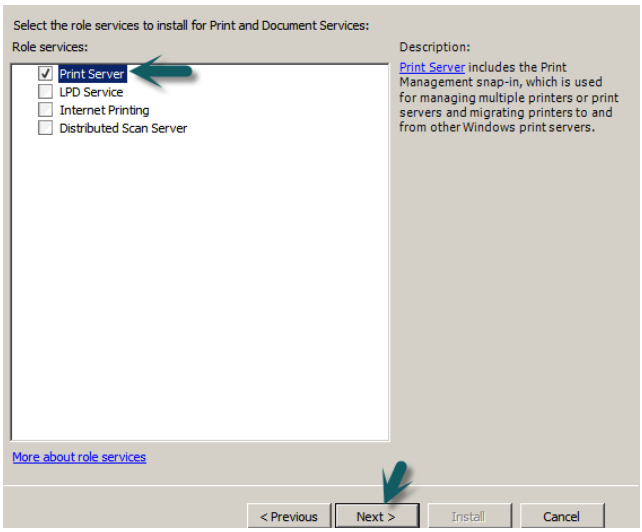
- Click **Next** on the first screen to continue



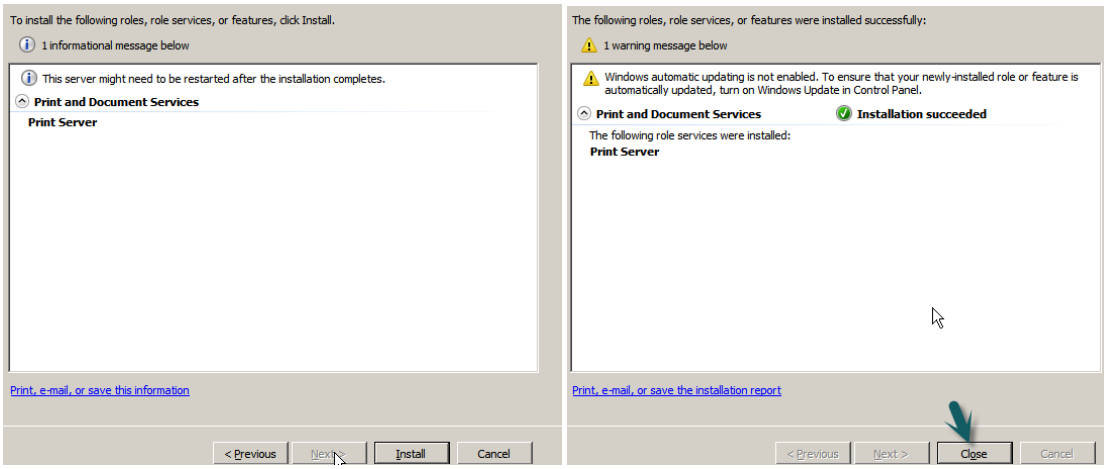
- Check the box beside **Prin and Document Services** and click **Next**



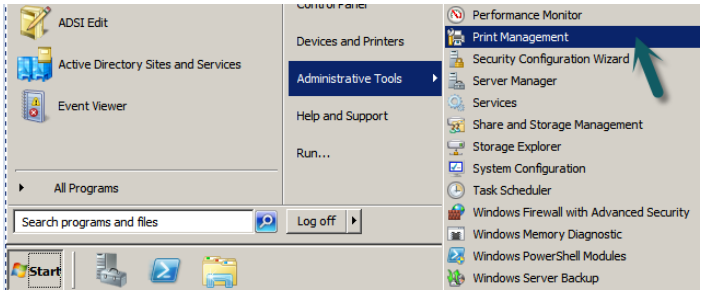
- Click **Next** to continue



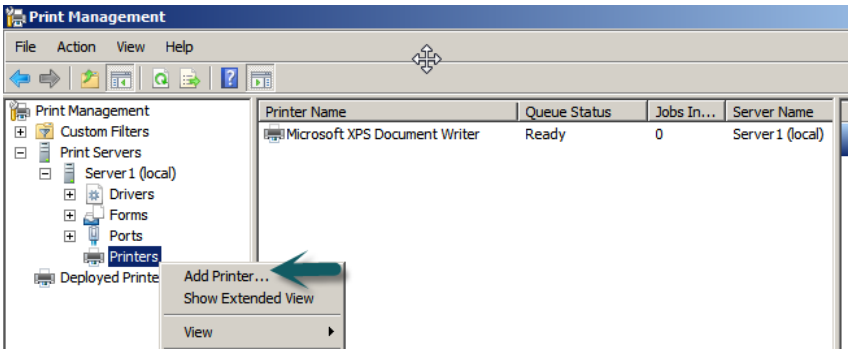
- Check the **Print Server** box and click **Next**



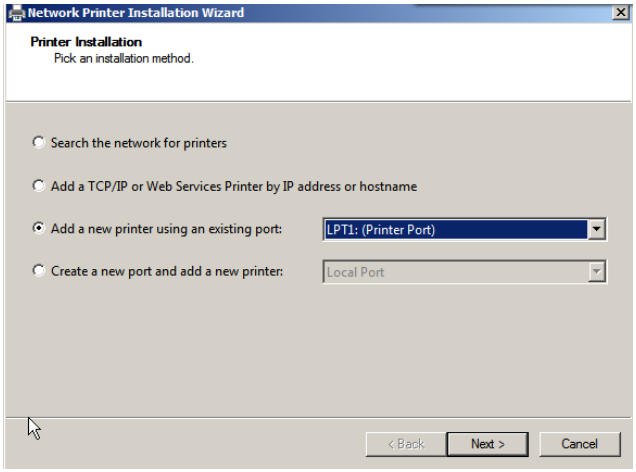
- Click **Install** to install the print server software
- Click **Close** when the installation is complete



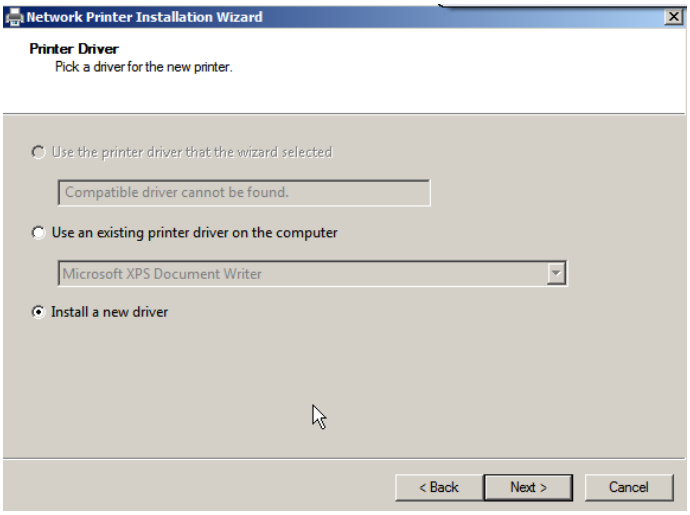
- Open the **Print Management** console, **Start->Administrative Tools->Print Manager**



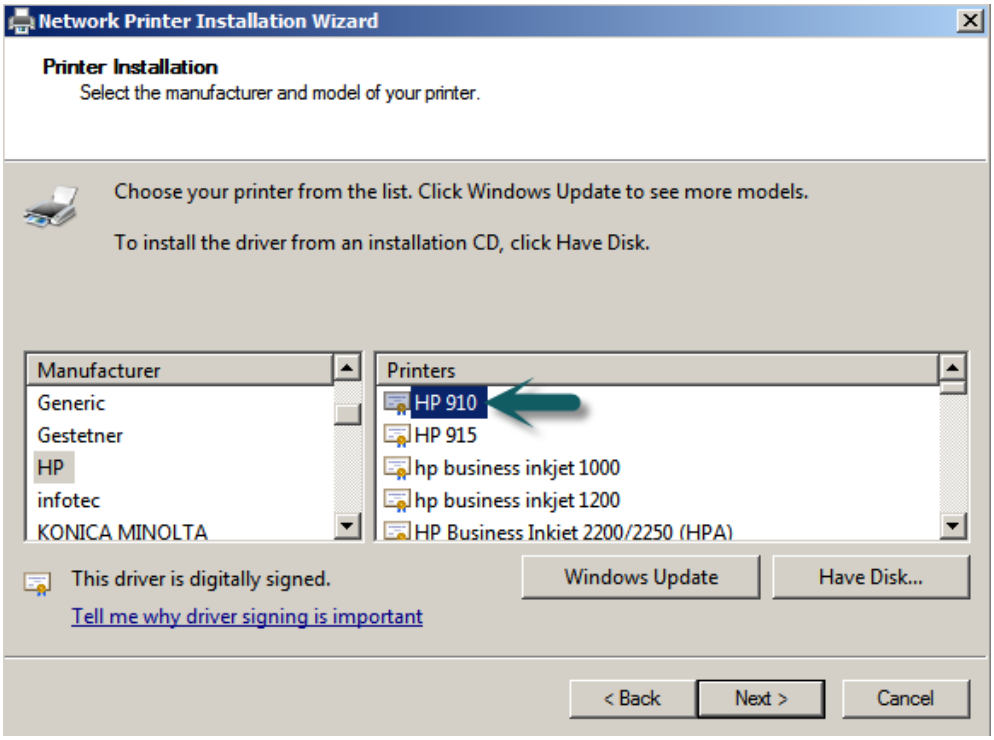
- Right click on **Printers** and click **Add Printer**



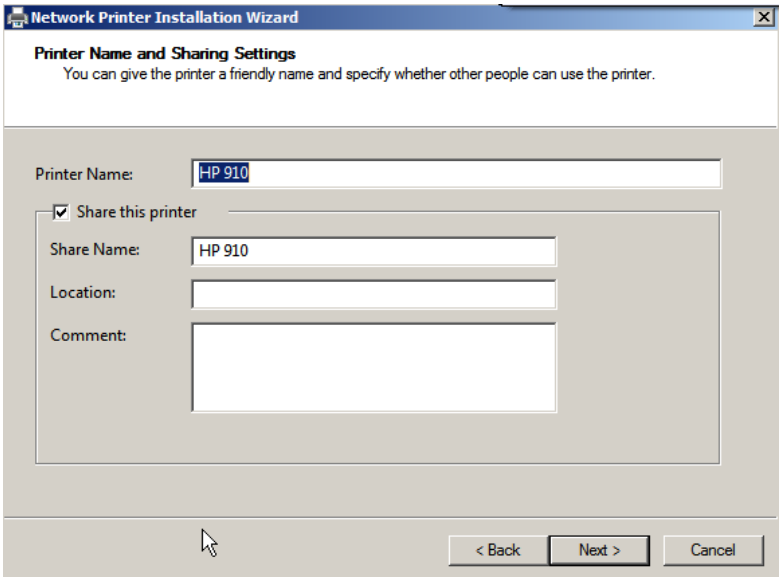
- Choose to **Add a new printer using an existing port** and choose any of the vacant ports, e.g. LPT1(Printer Port)
- Click **Next**



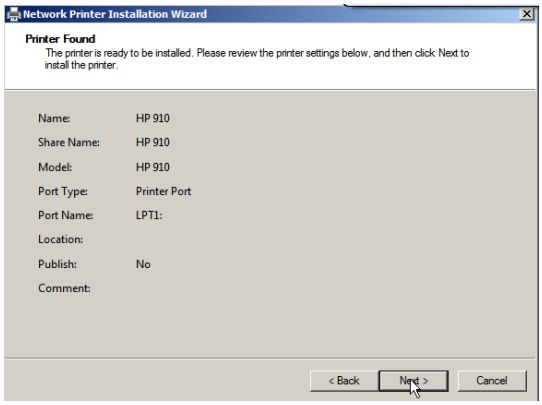
- Choose to install a new driver and click **Next**



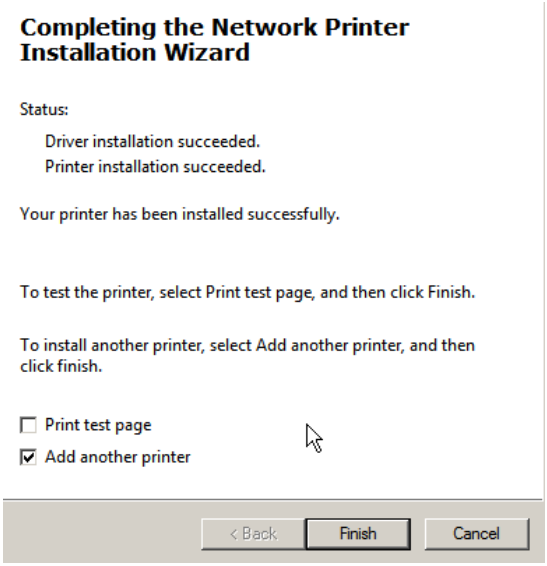
- Choose the model of printer you wish to install, e.g **HP 910**
- Click **Next**



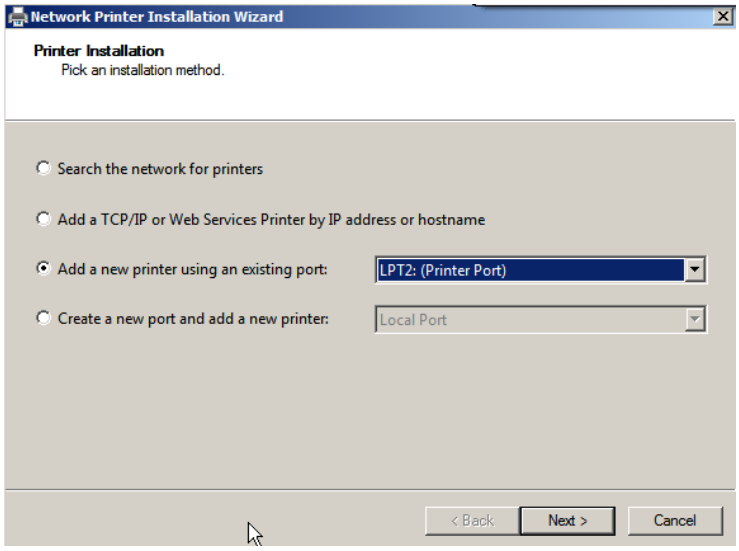
- Give the printer a meaningful name and make sure the **Share this printer** box is checked
- Click **Next**



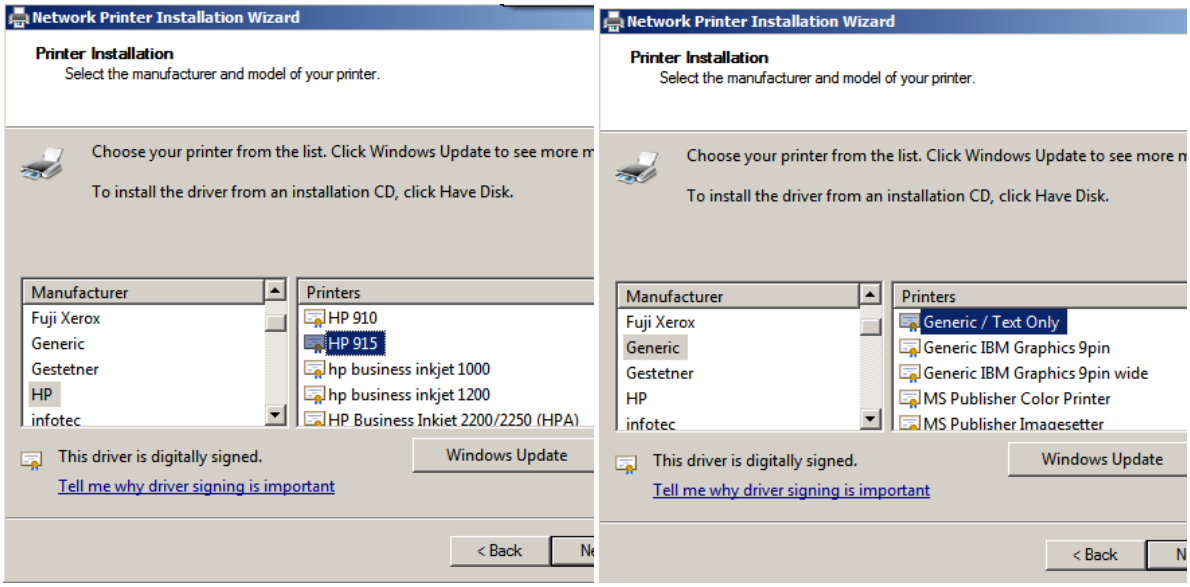
- Click **Next**



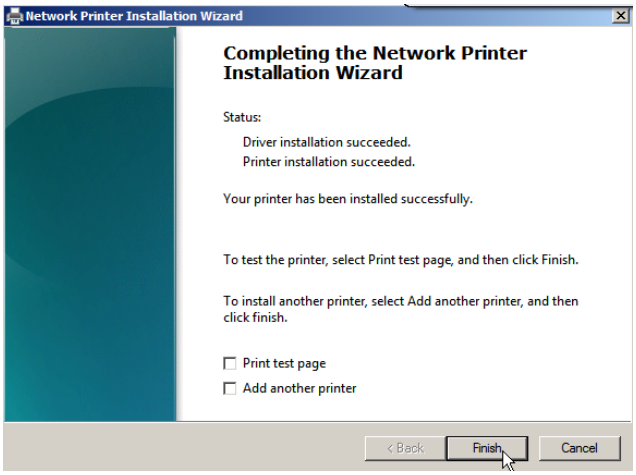
- Check the **Add another printer** box and click **Finish**



- Repeat the process to add another printer,
- Change the port to a different unused port for each new printer.

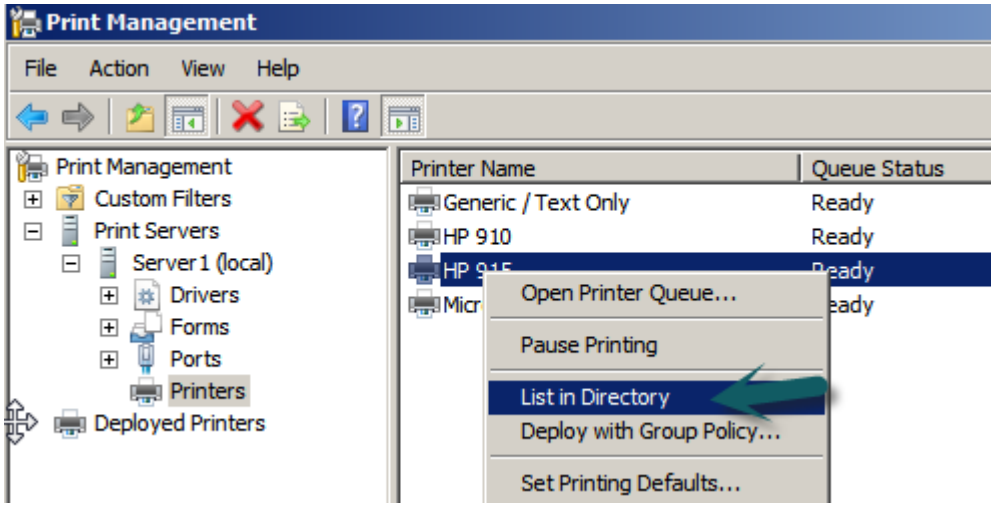


- In this example we have installed two additional printers: **HP915** and a **Generic / Text Only** printers



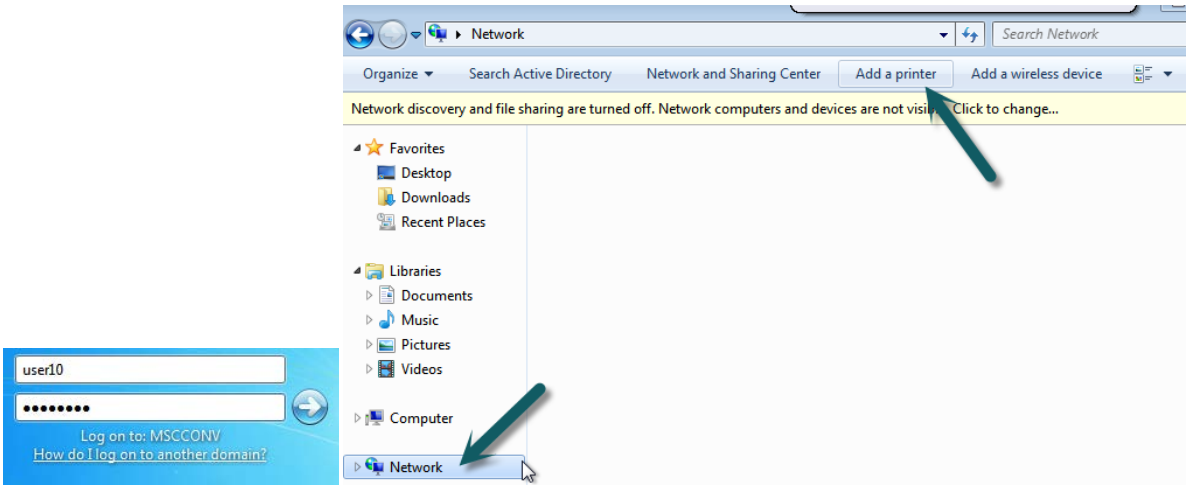
- When finished adding printers click **Finish**

2. Publish HP910 and HP915 printers in Active Directory

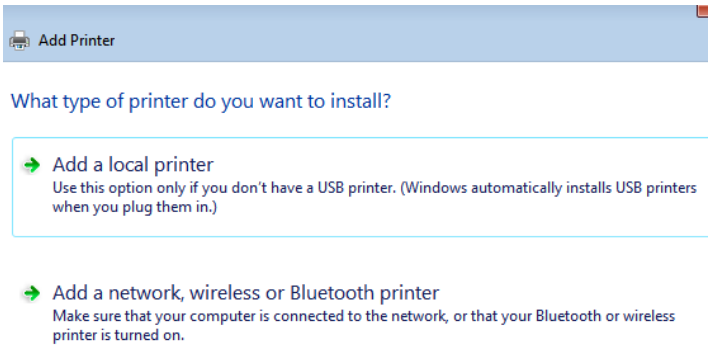


- To publish the printers in the directory:

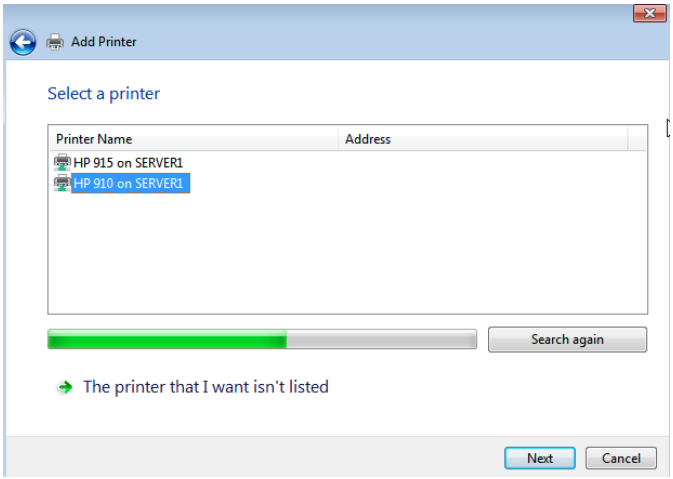
- Open the **Print Management** console
- Click the **Printer** icon on the right hand side window
- Right click on the printer and click **List in Directory**
- Repeat for any printers you wish to publish, in this case we have listed only the 2 HP printers



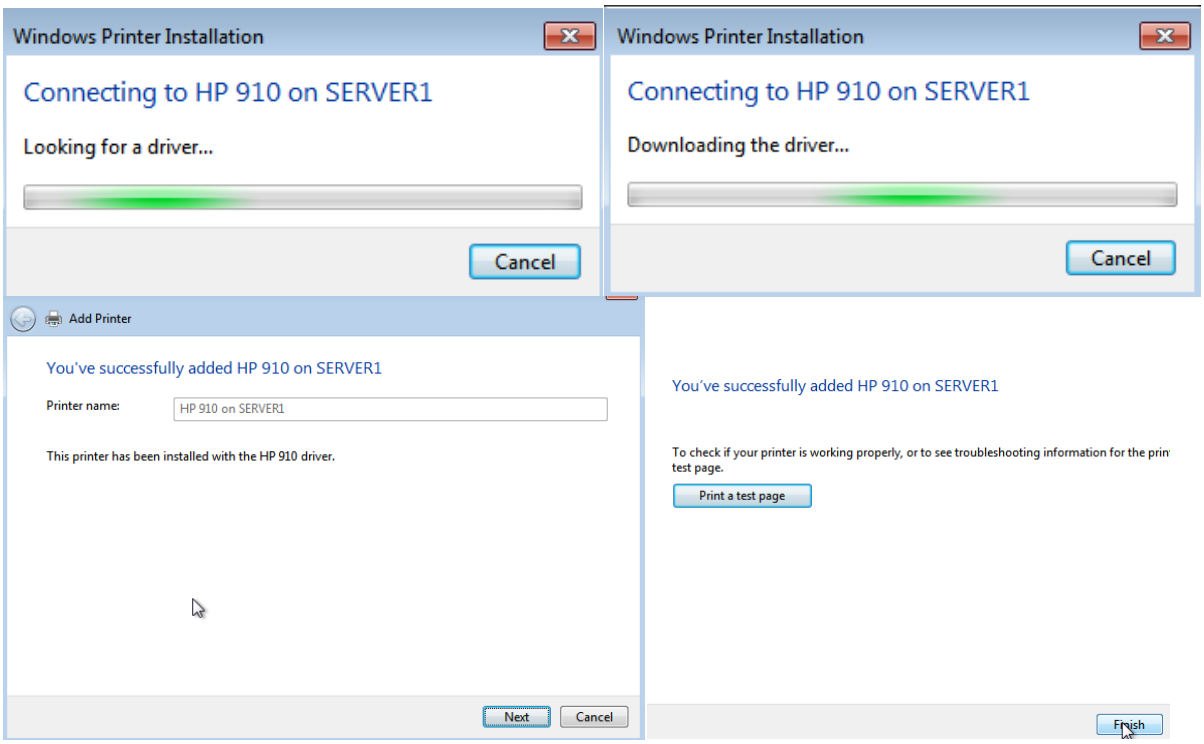
- The printers are now published in Active directory and can be easily accessed by any user in the domain
- To test this, **logon** to the domain on the **client1** machine
- Open **My Computer** and click **Network**
- Click **Add a printer**



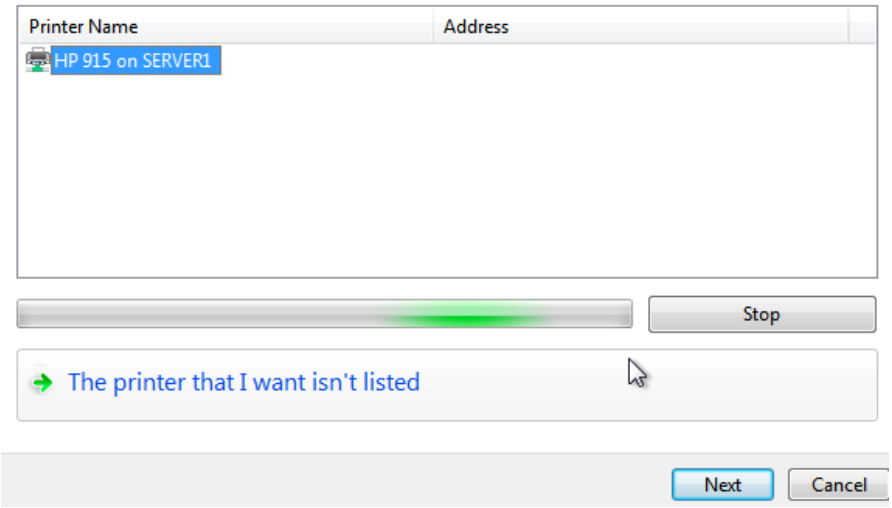
- Click **Add a network, wireless or Bluetooth printer** and click **Next**



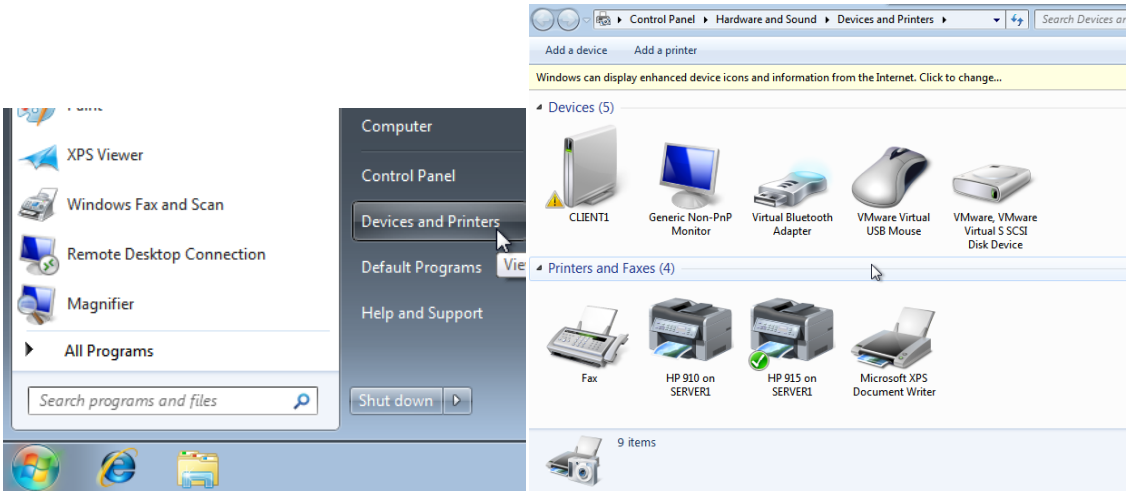
- The wizard will search Active Directory for any published printers and list them
- Highlight one of the printers and click **Next**



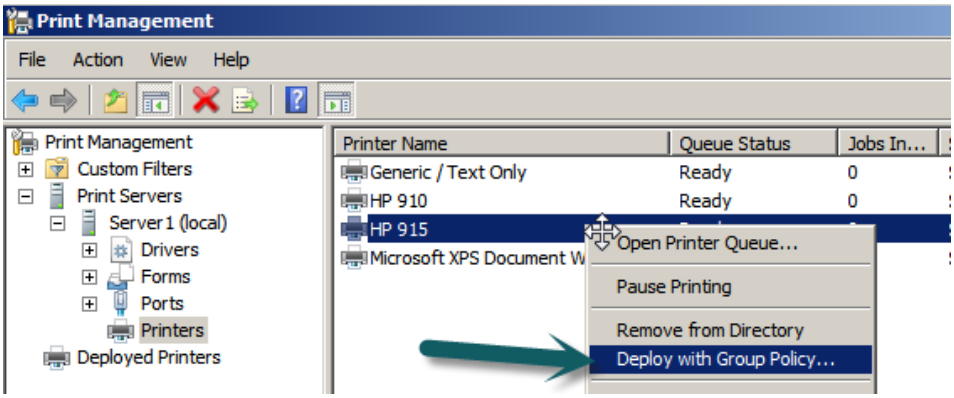
- When the drivers are installed give the printer a meaningful name, e.g. HP910 on SERVER1 and click **Next**
- Click **Finish**



- Repeat the process for the other HP Printer



- To test the printers are available for use click on the **Start menu** and click **Devices and Printers**
- The printers icons should be visible in the printers and faxes section



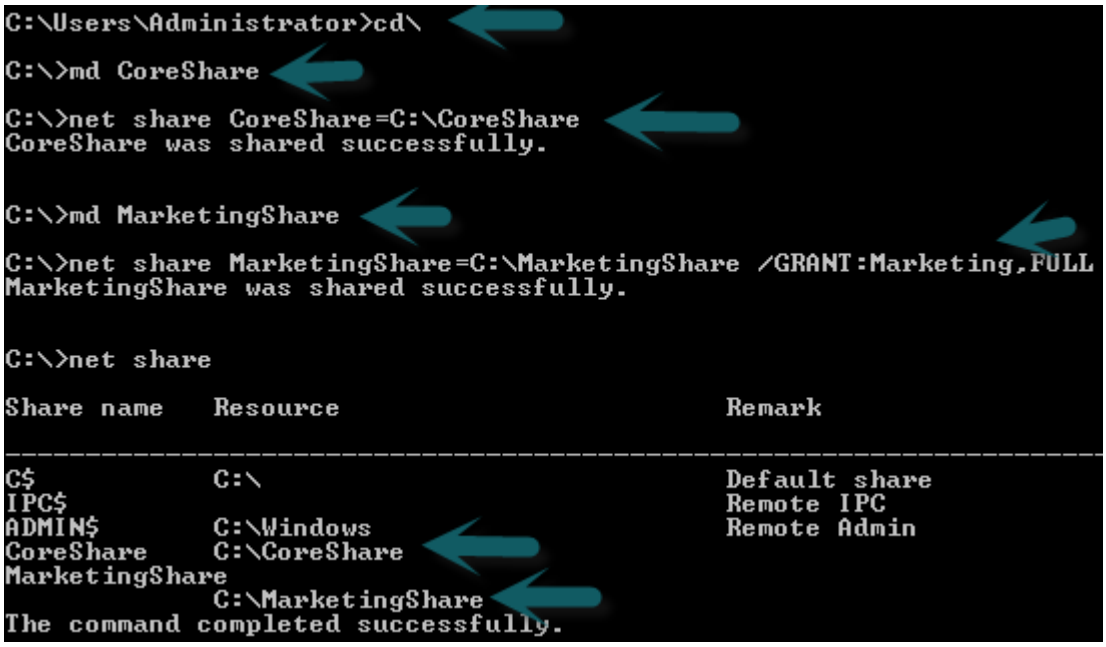
Note- Another option for installing the printer on user machines is to deploy the printer using a group policy object (GPO). To do this you right click on the printer in the Print Manager console and click Deploy with Group Policy. You should create a new GPO and link it to the OU's that contain the users/computers who wish to deploy the printers to

Task H - File Servers and Remote Connections

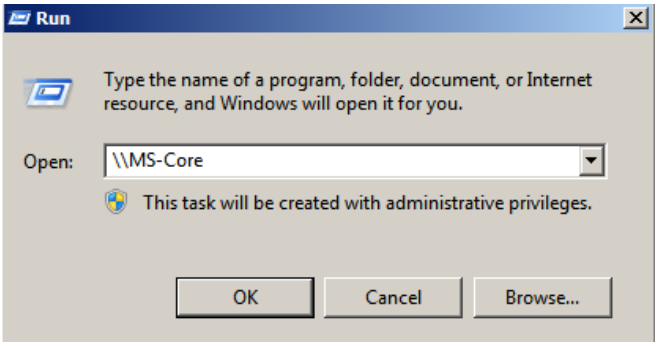
1. Setup MS-Core Server as a File Server

By default a Server Core installation has already got basic file services installed. Additional file service features can be installed by using the commands:
[11](Microsoft Technet)
"For File Replication Service, type the following at a command prompt:
Dism /online /enable-feature /featurename:FRS-infrastructure
For Distributed File System service, type:
Dism /online /enable-feature /featurename:DFSN-Server
For Distributed File System Replication, type:
Dism /online /enable-feature /featurename: DFSR-Infrastructure-ServerEdition
For Services for Network File System (NFS), type:
Dism /online /enable-feature /featurename:ServerForNFS-Base
or:
Dism /online /enable-feature /featurename:ClientForNFS-Base "

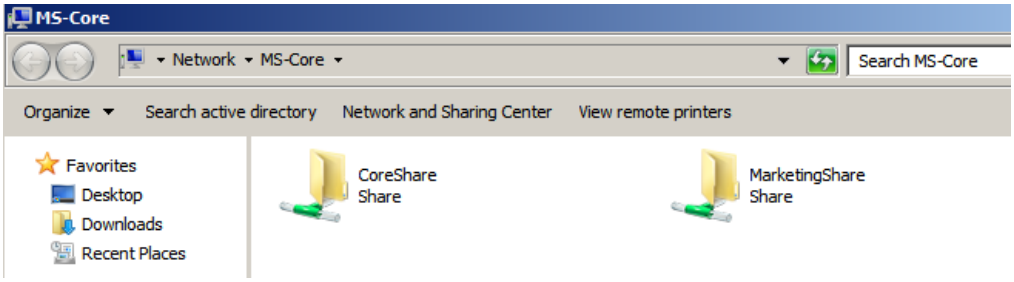
This task does not require any of the above features so we can start by creating the folders to be shared.



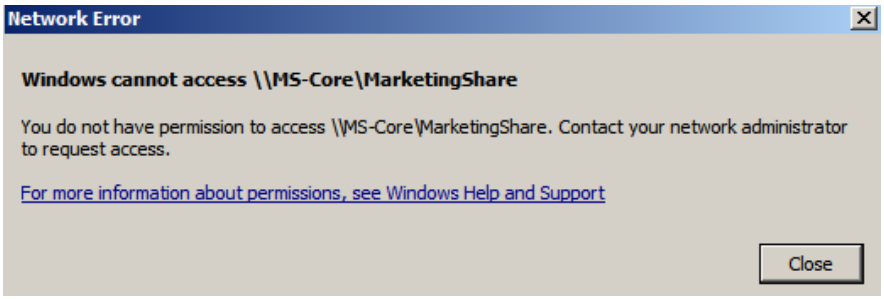
- Login to the MS-Core Machine
- Create a new directory using the **md** command-> see above screenshot
- Share the new folder using the **net share** command-> see above screenshot
- Create another new directory which will be created with share permissions for the marketing group only
- Share using the **net share** command as before but append **/Grant:Marketing,FULL** to grant full share permissions to the marketing group
- Enter **net share** to the command line to show what shares are active from this computer
- Notice the two created shares should be listed here



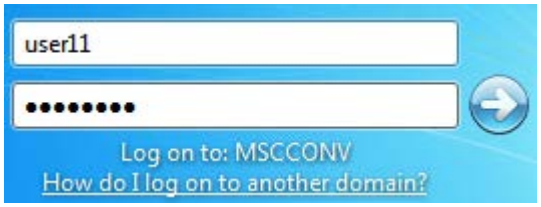
- To test the shares have been created correctly, log in to one of the server machines
- Click **Start->Run**
- Type **\\MS-Core** and click **OK**



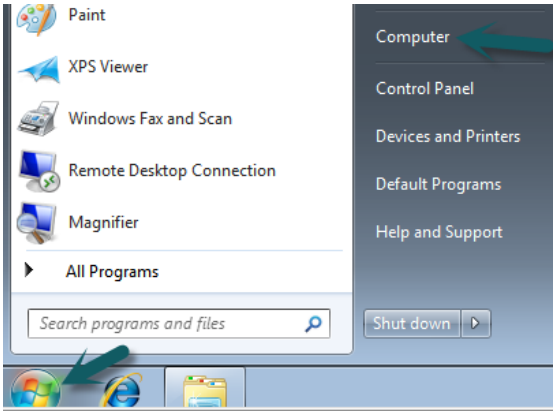
- The two shares should be visible



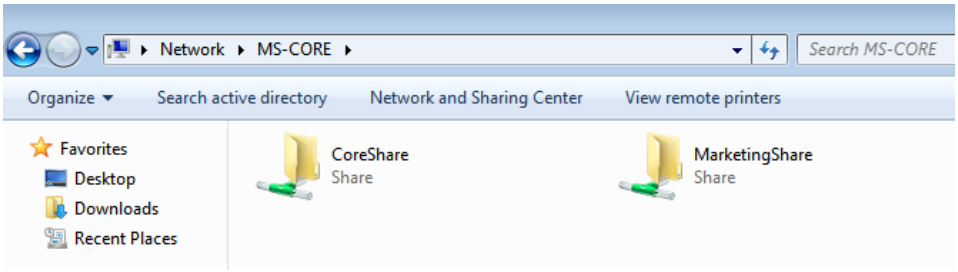
- As the **MarketingShare** was created with share permissions for the **Marketing** group you should not have access to it unless you log in as a member of the marketing group



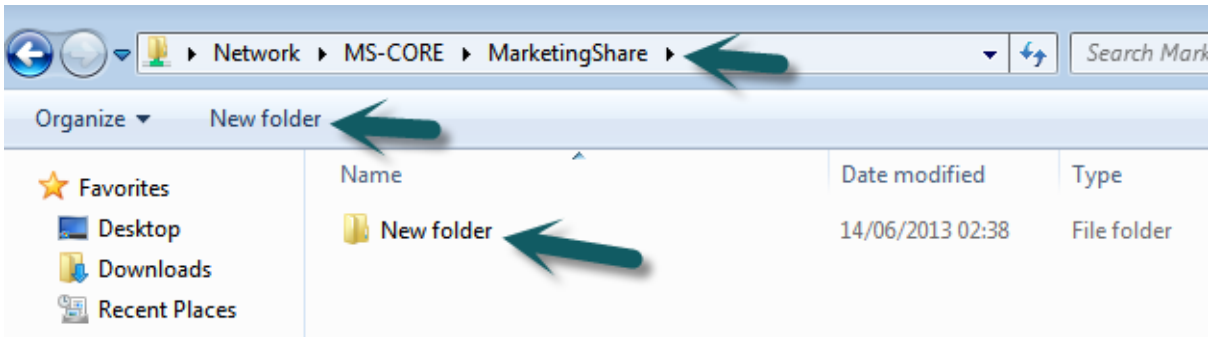
- To test this log in to a client machine as a member of the **Marketing** group, e.g. **user11**



- Click **Computer** on the **Start Menu**
- In the address bar at the top, type **\\MS-CORE**



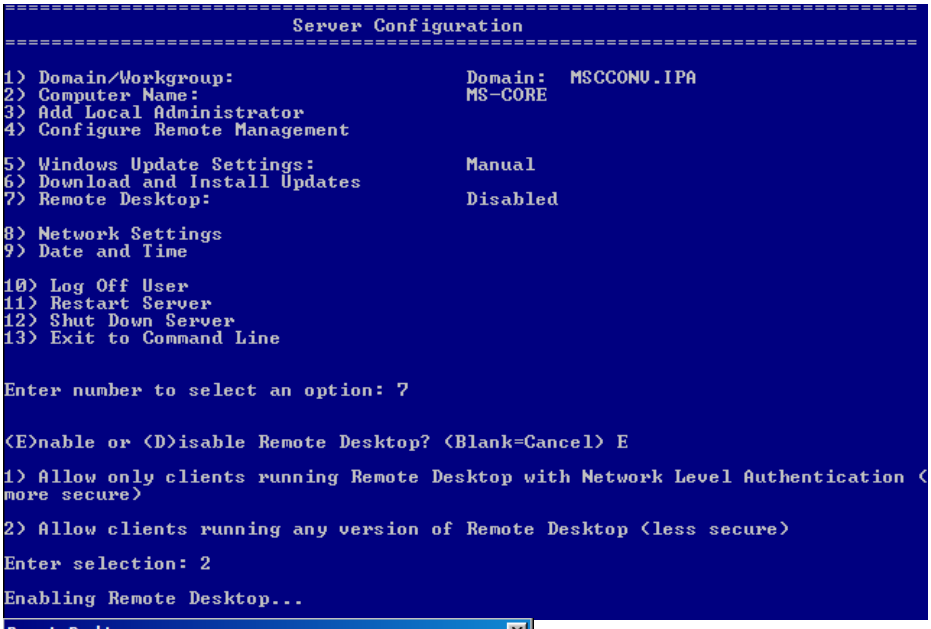
- Open **MarketingShare**

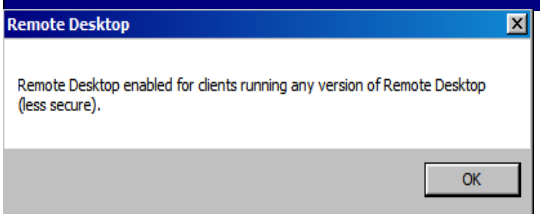


- As you are logged in as a member of the marketing group you have recieved full share permissions
- To test this create a new folder in the share

2. Configure MS-Core for Windows Remote Administration

Remote Administration is when you log into a computer remotely, i.e. from another computer and perform administrative tasks. In server environments it is a very important tool. In large enterprises the servers will usually be locked away in a secure temperature controlled room with restricted access. In these circumstances an administrator will need the facility to log on to a server and perform maintenance. A good way to do this is by using software such as remote desktop which is installed on both machines and allows the user to log on to one machine to the other. Other examples of remote administration software are: LogMeIn, GotoMyPC, Radmin, WebEx PCNow and many more. Remote Desktop is the Microsoft version and the version demonstrated below.

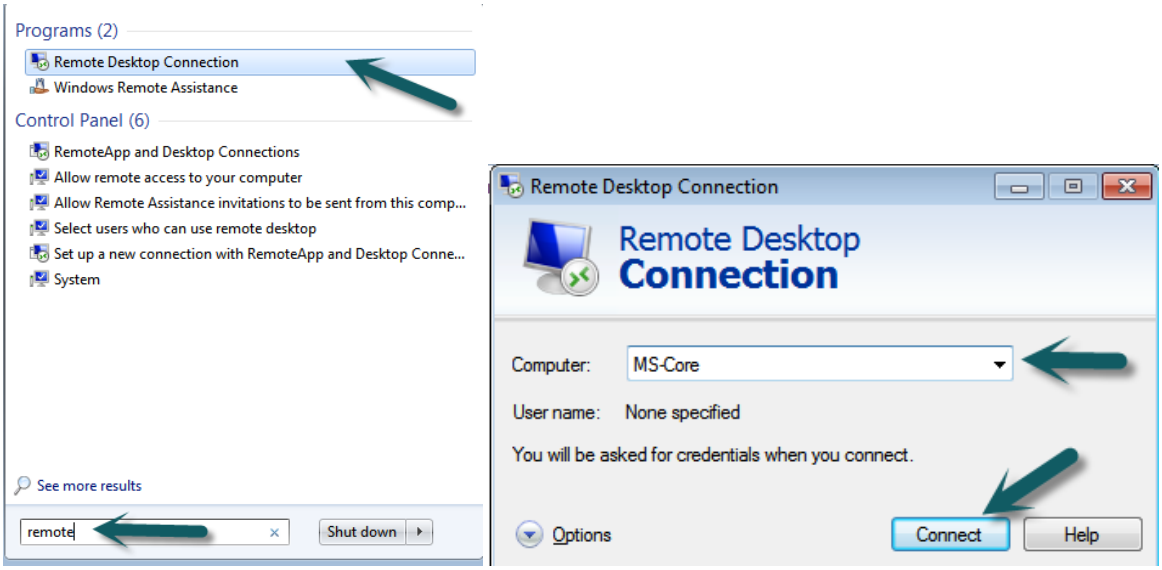




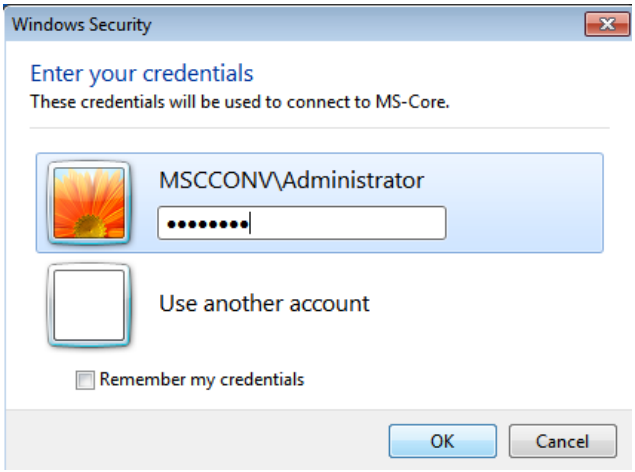
- Log into MS-Core and run the server configuration tool using the command **sconfig**
- Type **7** and press **Enter** to configure Remote Desktop settings
- Type **E** and press **Enter** to enable Remote Desktop
- Enter **1** to only allow clients running Remote Desktop with Network Level Authentication
  or
  Enter 2 to allow clients running any version of Remote Desktop
- Click **OK**

3. Access MS-Core from Client2 using Remote Desktop

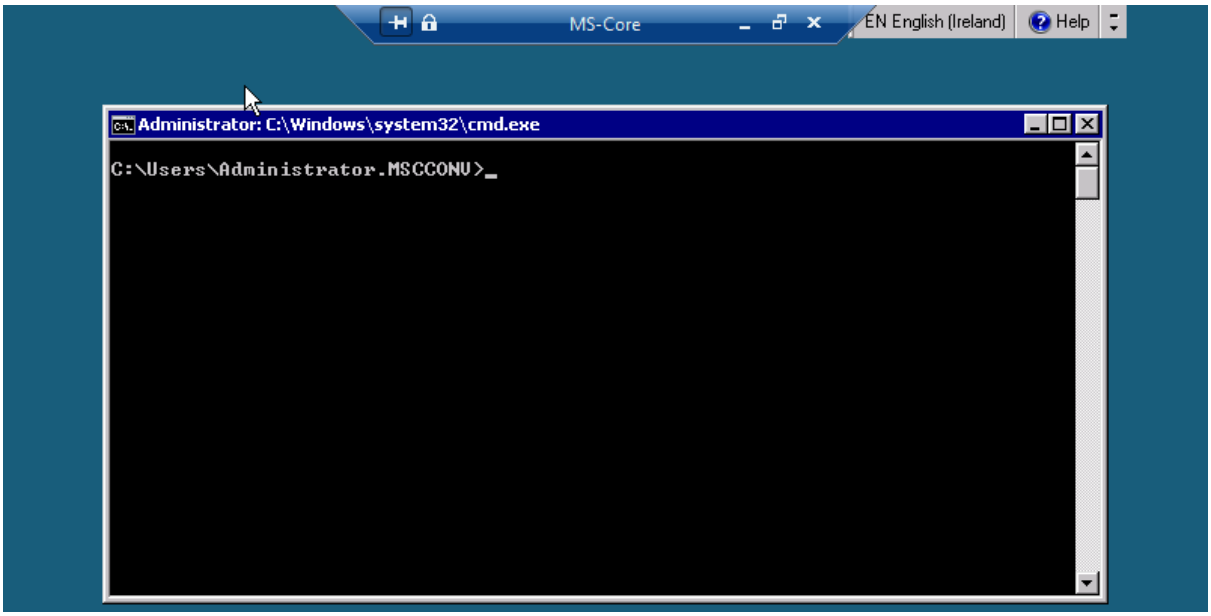
- Log into Client1 using a domain administator's account



- Open **Remote Desktop Connection** by typing remote desktop in the search bar on the start menu
- Enter **MS-Core** as the computer you want to connect to
- Click **Connect**



- Enter valid credentials to log in to MS-Core
- Click **OK**

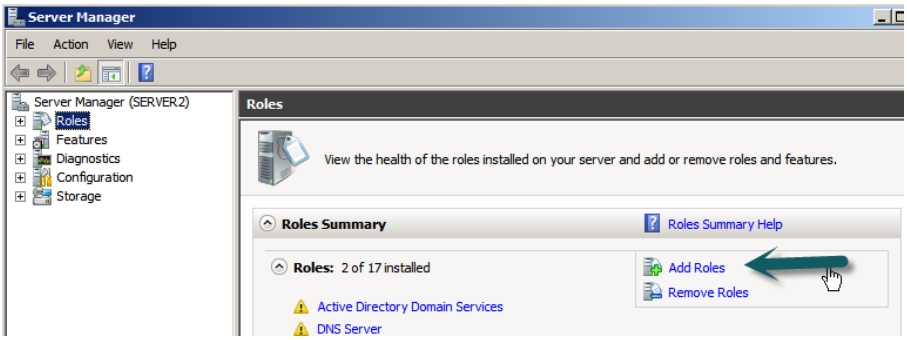


- You should now be connected remotely to MS-Core

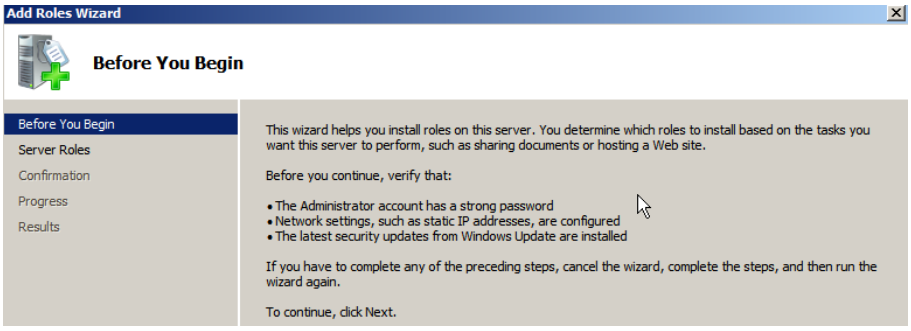
Task I - DHCP Servers

DHCP (Dynamic Host Configuration Protocol) is a way of dynamically configuring the network settings of computers on a network. Instead of statically assigning each computer on a network, dhcp allows computers to be set up to look for the DHCP server and 'ask' for IP, subnet mask, default gateway and DNS server addresses. The DHCP server will then lease out an IP address to the client for a specific period of time. The addresses the DHCP server gives out will be taken from a pool of available IP addresses configured by the administrator. The main reason an administrator would roll out DHCP would be to reduce workload. Each computer doesn't have to be configured for static IP addresses.
DHCP by definition will mean that IP addresses for the computer's on a network will be changing constantly. This could be a security issue as we may need to know who is responsible for any changes made. The DHCP role in Server 2008 allows the logging of IP addresses which stores the information about who was using each IP address at what time.

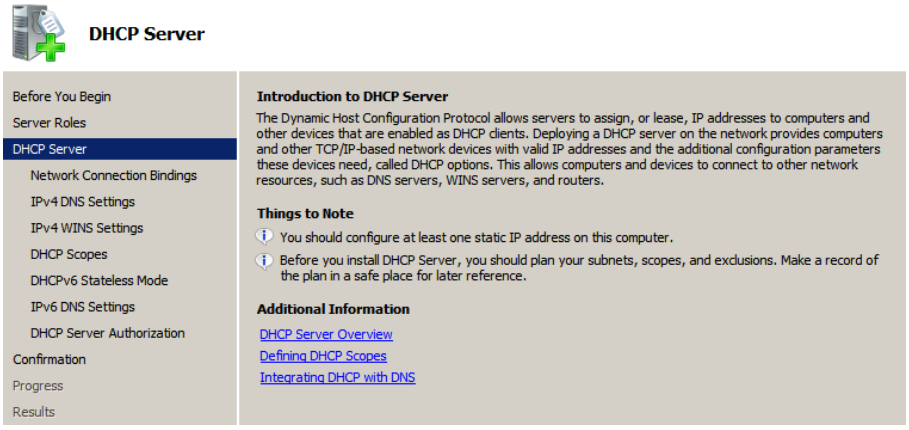
1. Install DHCP on Server2



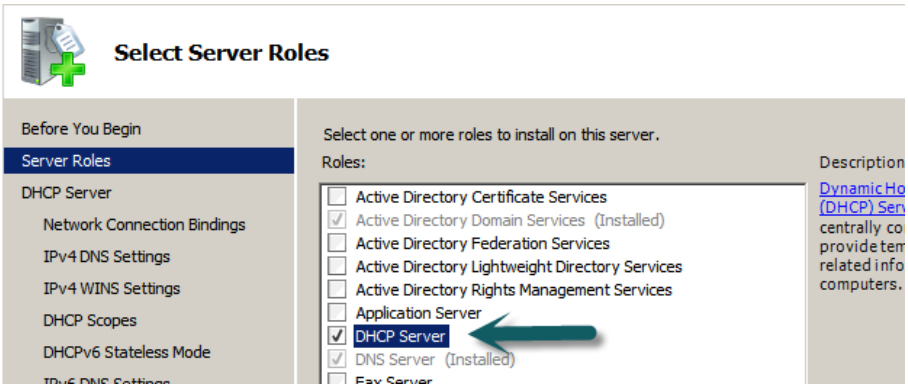
- Open the **Server Manger** and click **Add Roles**



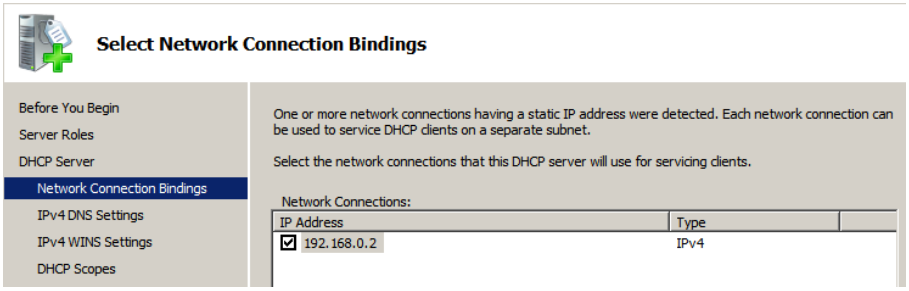
- Click **Next**



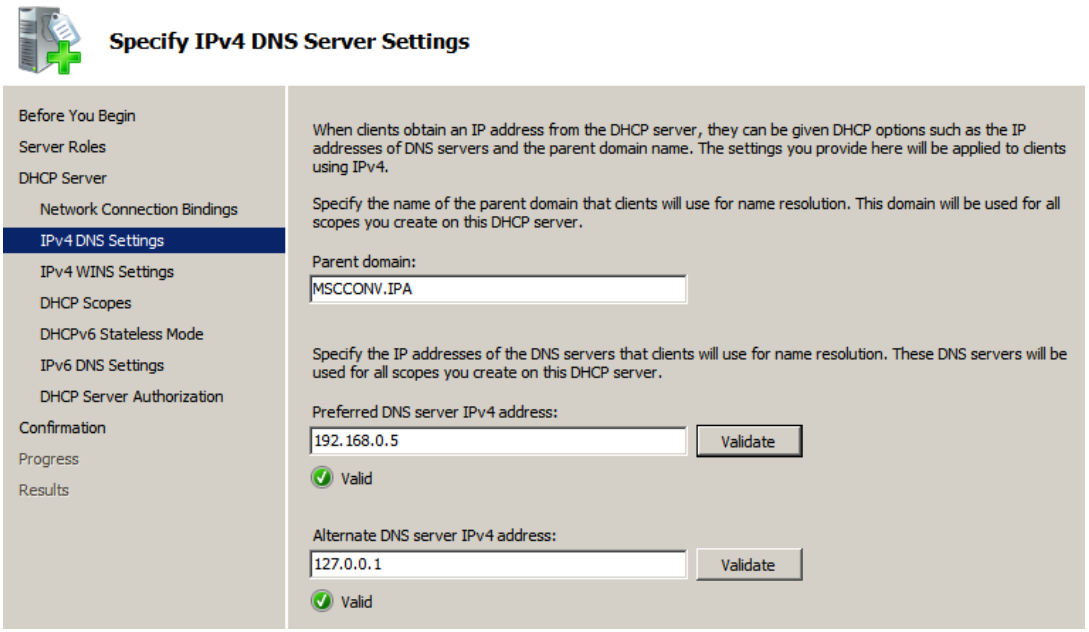
- Click **Next**



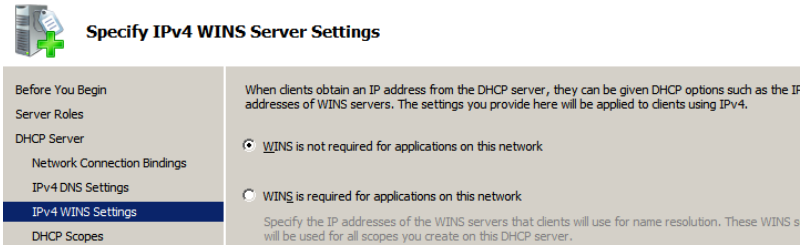
- Tick the box next to **DHCP Server** and click **Next**



- Tick the box beside the Server2's IP address
- Click **Next**

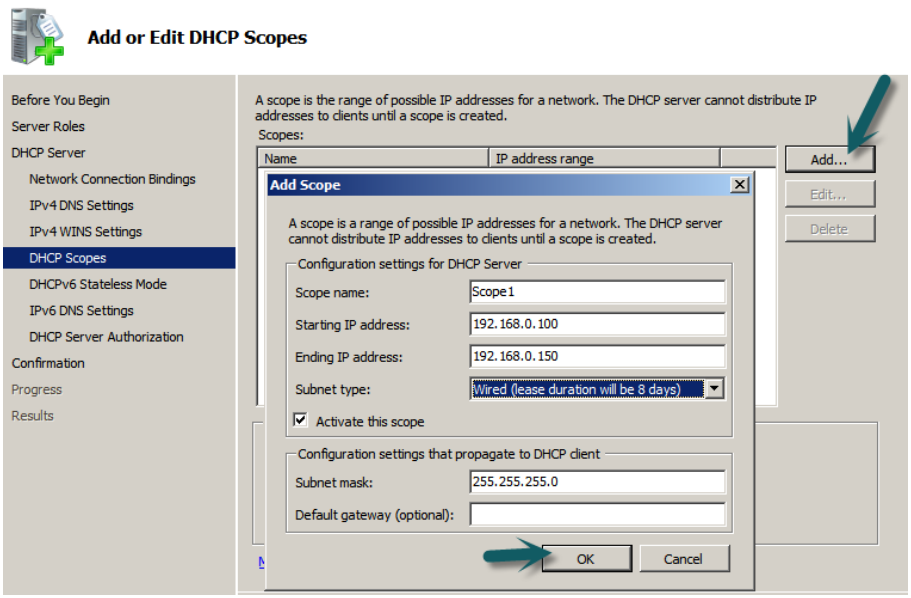


- Enter the name of the domain, i.e. MSCCONV.IPA
- Enter the DNS settings for the network
- Click **Validate** beside each IP address to validate that it is a DNS server
- Click **Next**

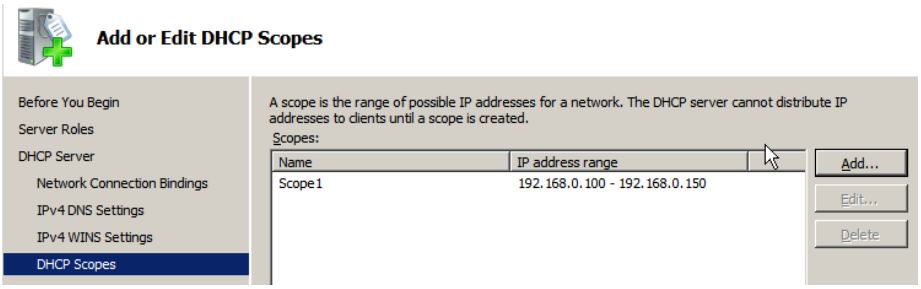


- Choose **WINS is not required for applications on this network**
- Click **Next**

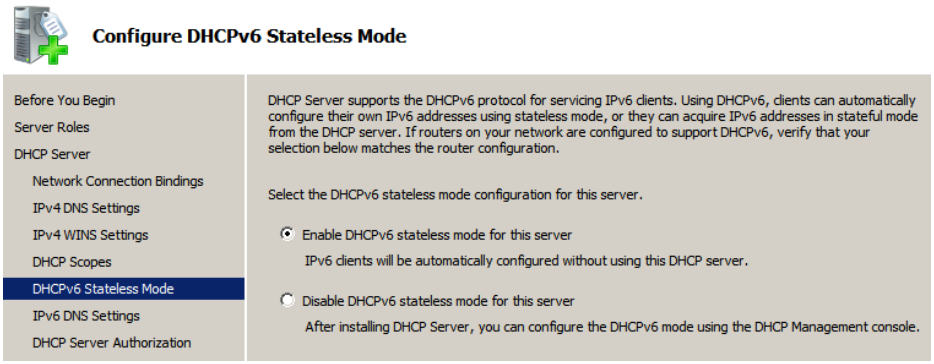
Note- If there is a WINS server on the network you should choose the other option and enter the IP address of the WINS server machine



- Click **Add** to add a new scope of IP Addresses for the server to give to clients
- Enter a name for the scope, the starting IP address and Ending IP address
- Choose the subnet type, in this case its a **Wired** network. This allows the lease time each IP address will be 8 Days. If Wireless is selected the lease time is 8 hours
- Tick the **Activate this scope** box
- Enter the **Subnet mask** for the network
- If applicable enter a **Default Gateway** (usually the address of the router used to connect to the internet)
- Click **OK**

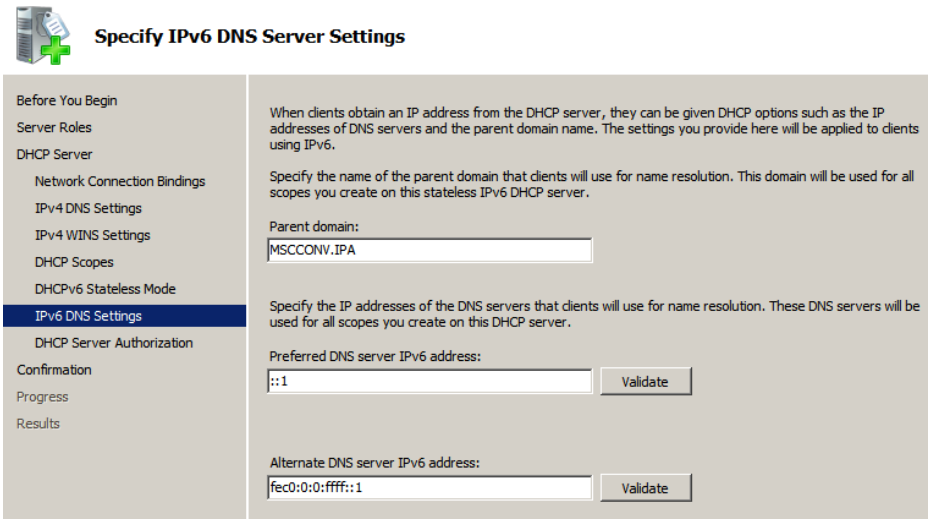


- Click **Next**

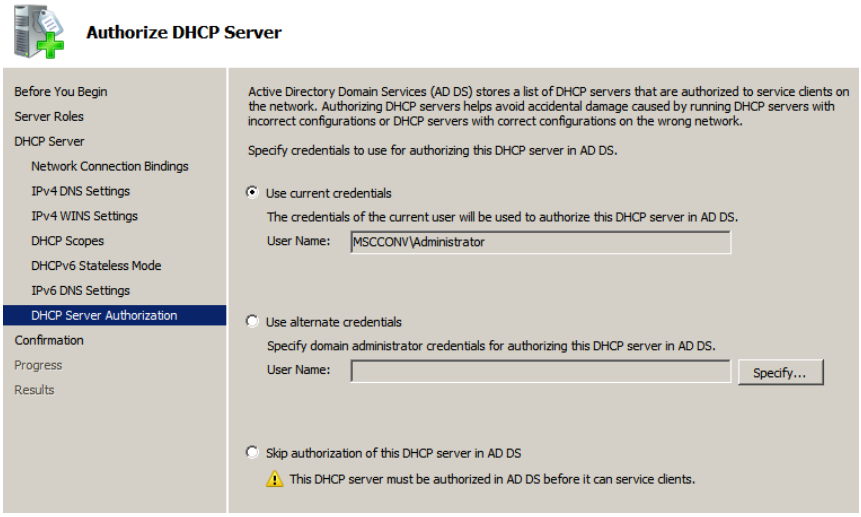


- Choose to **Enable DHCPv6 stateless mode for this server**
- Click **Next**

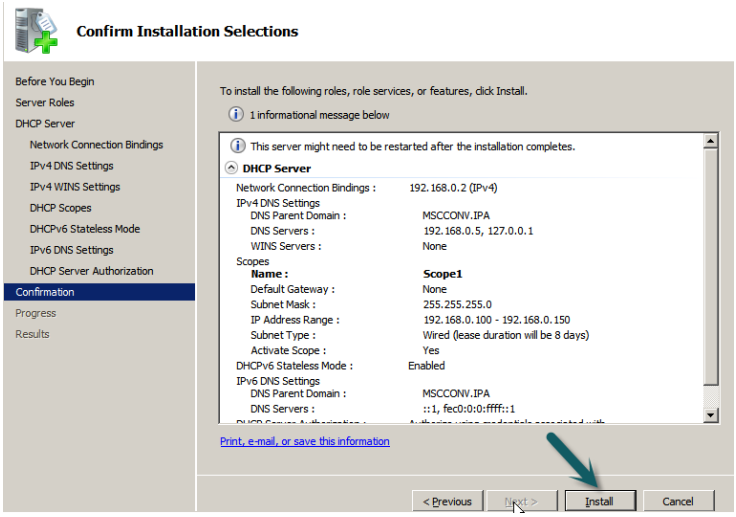
Note- This option means that IPv6 clients will be automattically configured without using the DHCP server



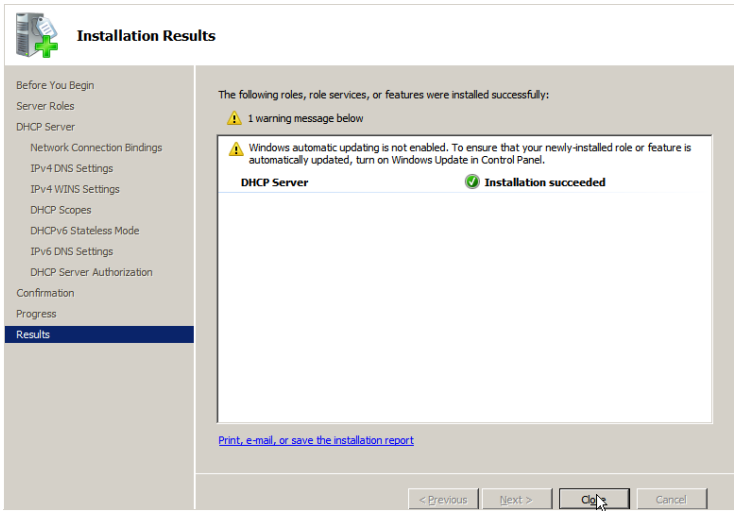
- Leave the default values for **IPv6 DNS Settings**
- Click **Next**



- If you are logged in as an domain administrator choose to **Use current credentials** to authorize the DHCP Server.
- If you are not logged in as a domain controller choose to **Use alternate credentials** and enter the credentials
- Click **Next**

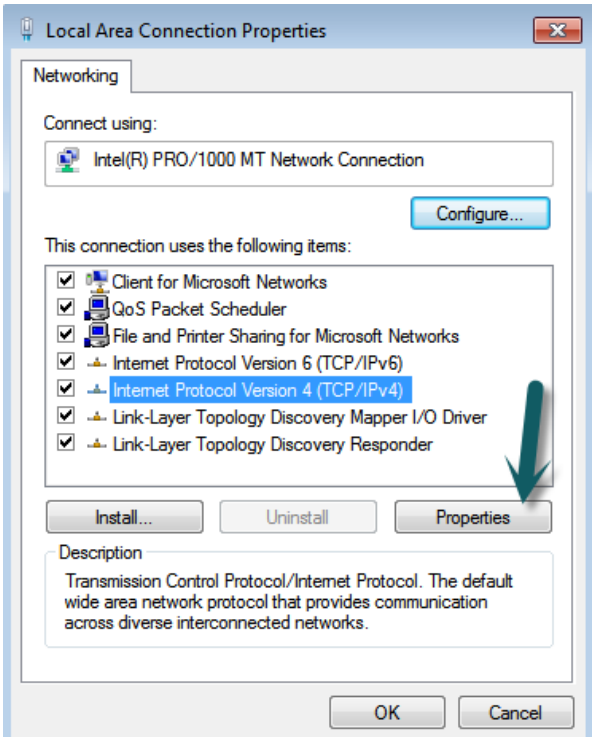


- Check the summary is correct and click **Install**

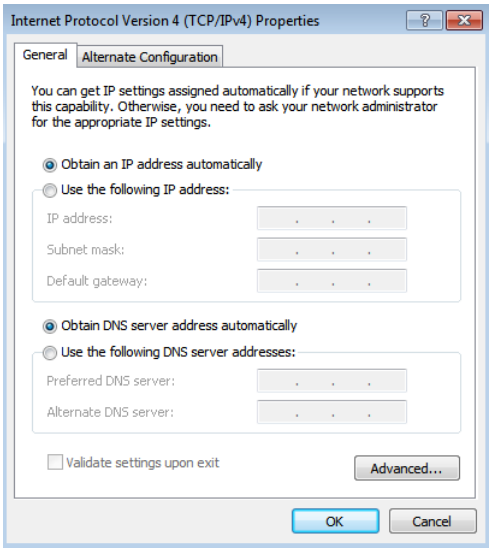


- When the installation completes successfully click **Close**

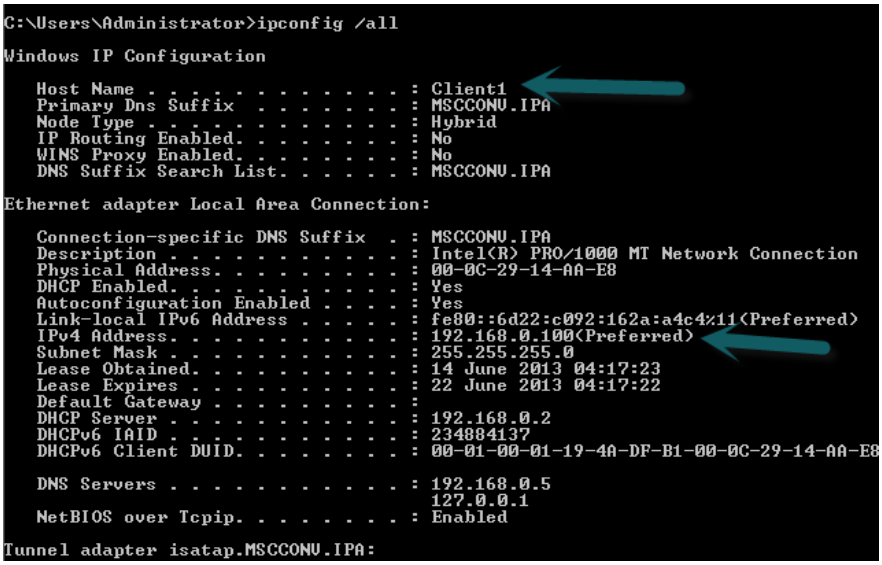
2. Configure Client1 to obtain its IP address from DHCP



- Log on to Client1 as an administrator
- Open the **Local Area Connection Properties** the same way as in Task A
- Highlight **Internet Protocol Version 4(TCP/IPv4)**
- Click **Properties**



- Choose to **Obtain an IP address automatically**
- Choose to **Obtain DNS server address automatically**
- Click **OK**



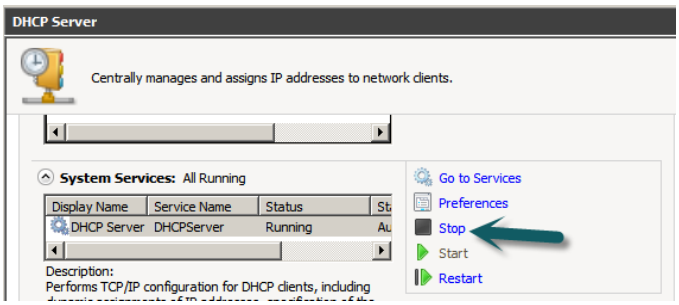
- To check the machine is now receiving an IP Address from the DHCP server:
- Open the command prompt from the client1 machine
- Enter the command **Ipconfig /all**
- The full IP address details of the computer will be shown on screen. Check to see that the **IPv4 Address** is within the scope set up for the DHCP server. If it is, the DHCP Server is working correctly.

3. Disable DHCP services to see the results

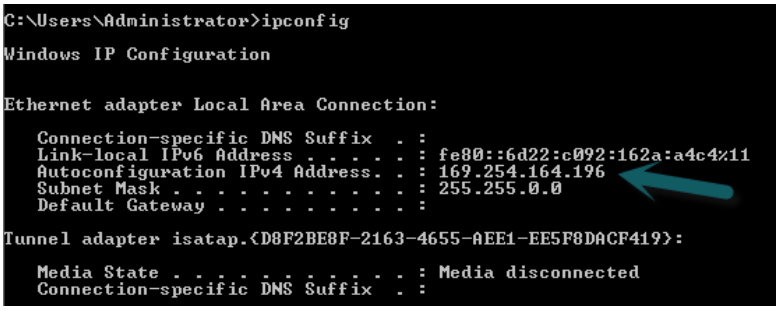
[12] Webopedia states:

"When a client boots up, it first looks for a DHCP server in order to obtain an IP address and a subnet mask. If the client is unable to find the information, it uses APIPA to automatically configure itself with an IP address from a range that has been reserved especially for Microsoft. (169.254.0.1-169.254.255.254 and subnet mask of 255.255.0.0)"

This means if we disable DHCP services and the client machine is still left configured to obtain its IP address dynamically then the client will configure itself with an address in the APIPA(Automatic Private IP Addressing) range.



- Open the server manager in Server2 and click **Roles**
- Click on **DHCP**
- Scroll down and click **Stop** to stop DHCP services



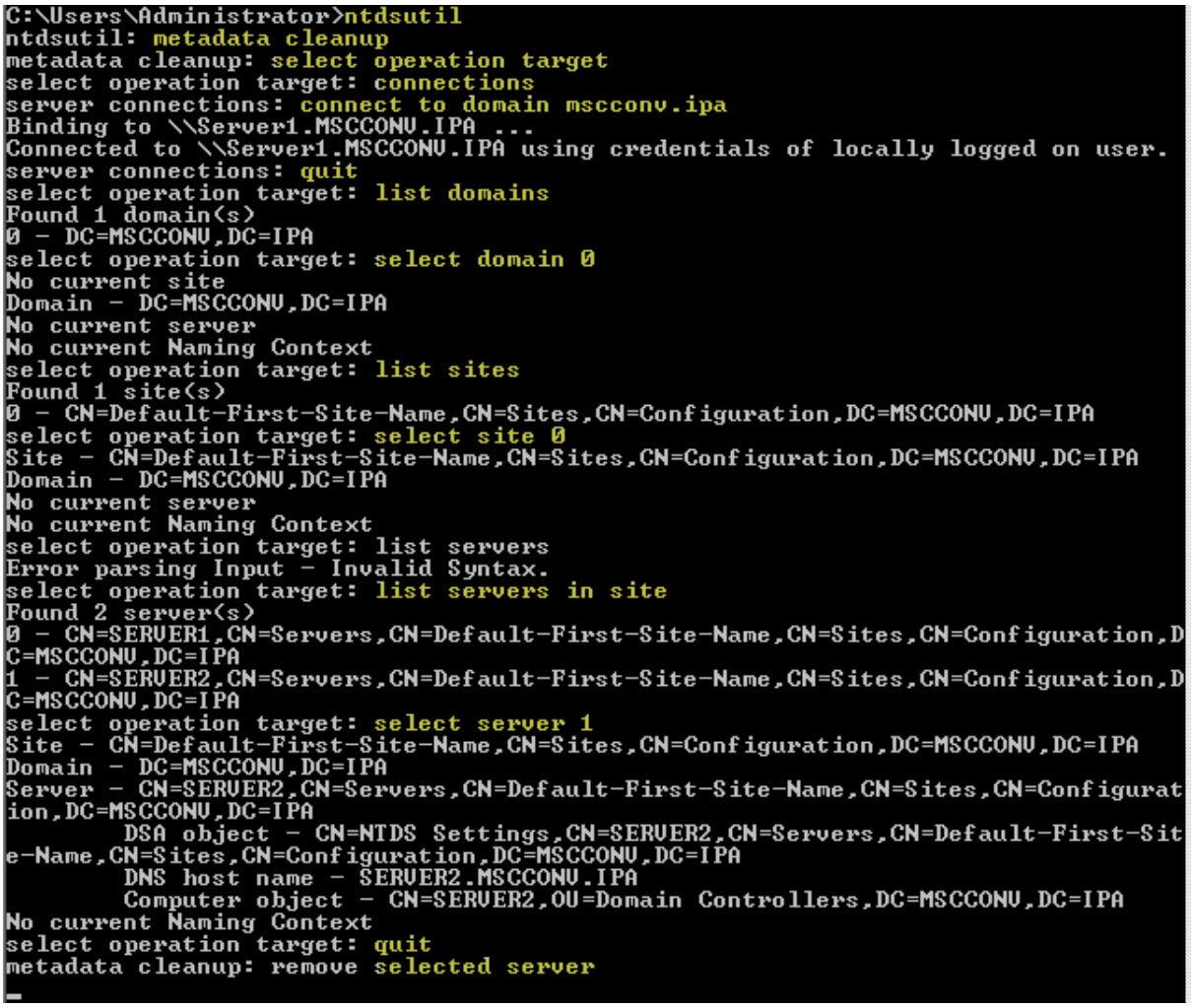
- Log in to **Client1** and open the **Command prompt**
- Now that there is no DHCP server available the computer should assign itself an APIPA address. See above screenshot

Task J - Decommission Server2 assuming it has become unbootable

If Server 2 becomes unbootable, the first step would be to physically decommission the server to make sure it can not be fixed and then reintroduced to the domain later as it would be a security risk to have a rogue DC on a domain and in the wrong hands could be very damaging. This can be done most easily by drilling holes through the hard disk.

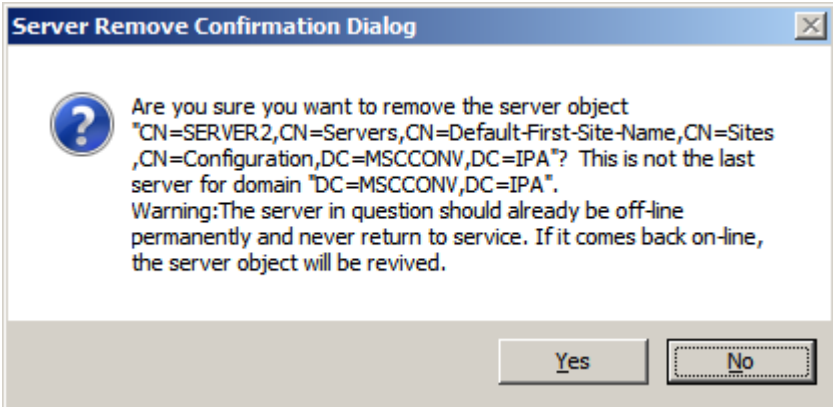
Next step is to remove all traces of the server from the domain. We could just delete the DC from Active Directory Users and Computers but this does not remove everything, there is still information about the failed DC left over and it is best practice to remove this metadata when decommissioning a Domain Controller that has become unbootable.

iSiek's blog about Microsoft Windows services states
[13]" But Active Directory still knows about it and uses that DC for AD data replication which can cause errors. To prevent replicating data between broken DC and the rest, you need to perform **metadata cleanup**. This can be done using **ntdsutil** on any workstation/server in a network. You just need to have Domain Admin account to do that."

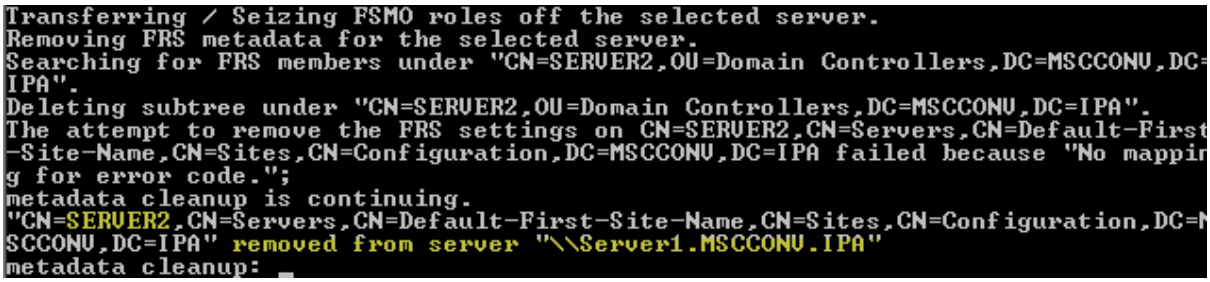


- Log into Server1 and open the **command line**
- Type **ntdsutil** and press **Enter**

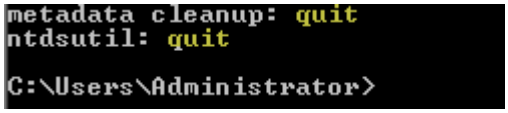
- Type **metadata cleanup** and press **Enter**
- You now have to choose the Domain, Site and the Domain Controller you want to remove from the Active Directroy metadata.
- Type **select operations target** and press **Enter**
- You now must connect to the domain.
- Type **connections** and press **Enter**
- Type **connect to domain mscconv.ipa** and press **Enter**
- To move back out one level type **quit** and press **Enter**
- Now we can choose the domain the DC is in
- Type **list domains** and press **Enter**
- In this case there will only be one domain found and it will be number 0 on the list
- Type **select domain 0** and press **Enter**
- Now we can choose the site the DC is in
- Type **list sites** and press **Enter**
- Again there will be only one site in this case
- Type select site 0 and press **Enter**
- Now we can list all the Domain controllers in the selected site
- Type **list servers in site** and press **Enter**
- Find the number of the DC you wish to remove from Active Directory, in this case the number is 1
- Type **select server 1** and press **Enter**
- We now have all the data needed to perform the metadata cleanup
- Type **quit** and press **Enter** to go up back one level
- Type **remove selected server** and press **Enter**



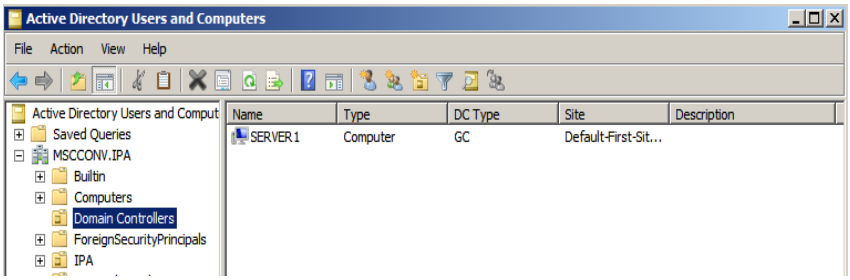
- Click **Yes** to continue



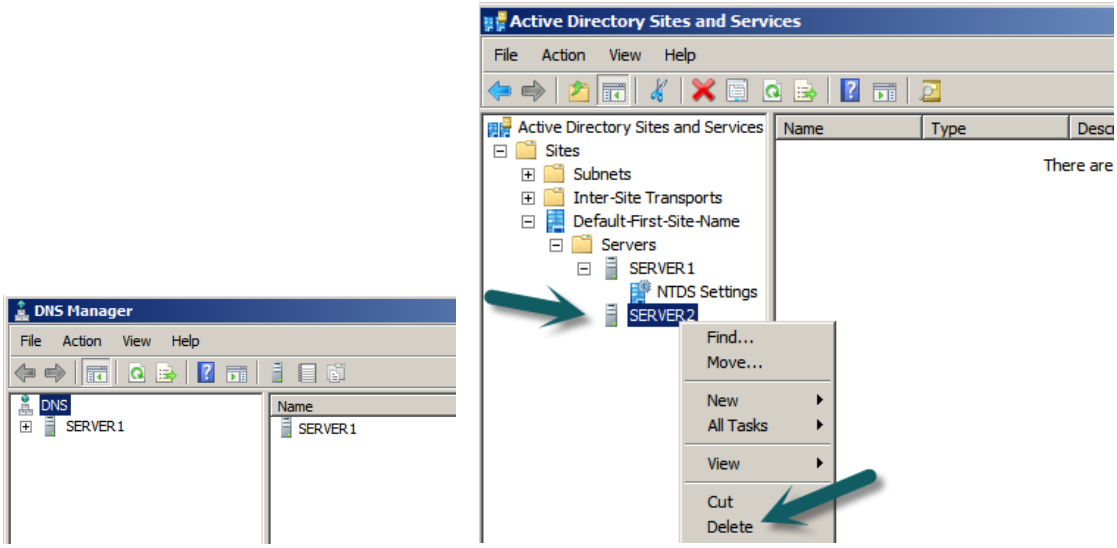
- You should now see that the metadata has been removed from the Active Directory. See above screenshot



- Type **quit** and press **Enter** twice to exit to the command prompt



- To test that the DC has been removed open **Active Directory Users and Computers**
- Open the **Domain Controllers** Orgainisational Unit
- Server2 should be gone from the list



- Open the **DNS Manager** and make sure Server2 has been removed from the list of DNS servers
- Open **Active Directory Sites and Services**
- Navigate to **Sites->Default-First-Site-Name->Servers**
- If Server2 is still left in the site, right click on **Server2** and click **Delete**
- All traces of the unbootable Domain Controller should now be removed

References

[1] Microsoft Technet (2013, June). Ping: netsh firewall vs advfirewall: http://social.technet.microsoft.com/Forums/en-US/winservercore/thread/56cd9ed2-24ea-4ddf-90fc-c37de99296bc

[2]Minasi, M (2010). Mastering Windows Server 2008. Wiley Publishing (p231)

[3]Microsoft Technet (2013, June). Domain Controller Roles: http://technet.microsoft.com/en-us/library/cc786438%28v=WS.10%29.aspx

[4] Minasi, M (2010). Mastering Windows Server 2008. Wiley Publishing (p112)

[5] Minasi, M (2010). Mastering Windows Server 2008. Wiley Publishing (p231)

[6] Microsoft Support(2013, June). Using Mirrored Volumes: http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_diskconcepts_17.mspx?mfr=true

[7] Minasi, M (2010). Mastering Windows Server 2008. Wiley Publishing (p250)

[8] Microsoft Technet (2013, June). Group Policy: http://technet.microsoft.com/en-us/windowsserver/bb310732.aspx

[9] Microsoft Technet (2013, June). Group Policy Collection http://technet.microsoft.com/en-us/library/cc779838%28v=ws.10%29.aspx

[10] Minasi, M (2010). Mastering Windows Server 2008. Wiley Publishing (p546)

[11] Microsoft Technet (2013, June). Installing a server role on a server running a Server Core installation of Windows Server 2008 R2: Overview http://technet.microsoft.com/en-us/library/ee441260%28v=ws.10%29.aspx

[12] Webopedia (2013, June). APIPA http://www.webopedia.com/TERM/A/APIPA.html

[13] Isiek's Blog about Microsoft Windows Services (2013, June). Metadata cleanup for broken Domain Controller http://kpytko.pl/2011/08/29/metadata-cleanup-for-broken-domain-controller/