Systems Management Assignment

ANDREW DOYLE

STUDENT NUMBER: 12252388

LECTURER: TOM BRETT

18/06/2013

COMPLETED AS PART OF THE MSc COMPUTER SCIENCE (CONVERSION) AT UNIVERSITY COLLEGE DUBLIN (IN CONJUNCTION WITH THE IPA)

INTRODUCTION

Introduction

Navigating to utilities

Throughout this manual, you will be instructed to type in the search bar to find a utility to work with. This is the author`s personal preference, however, there it is important to be aware that there is often multiple ways to navigate to the same location.

Additional Information Boxes

You will be greeted with many information boxes as shown below. This usually serves to provide additional, non-essential information that you may find useful for a further understanding of the topic at hand, often with links or reference to recommended reading.

Executing Commands

You will also work with command boxes as shown below, these boxes highlights long commands that you will execute at the command prompt. It is important to enter commands exactly as they appear, and to pay particular attention to spaces which you may otherwise neglect to notice.

CMD	Run this command

Screenshots

Screenshots are included at important stages throughout this manual, which will help ensure that you are executing the accompanying instructions correctly. You may view a full list of the images included in Appendix A.

Links to recommended reading

When websites are referenced in this manual, EBook users will have the ability to navigate to the relevant link if the text is highlighted in blue and underlined.

TASK A – INSTALLATION OF OPERATING SYSTEMS

A0 - Task Introduction

In this section, you will be guided through the installation of a Windows Server 2008 R2 operating system and also a Windows Server 2008 R2 Core system. It is assumed that you already have a Windows 7 system in place. During the installation process a 30GB partition will be set aside for the installation of the operating systems.

When the systems have been installed, they will be renamed, and they will be statically assigned IP addresses. By not specifying a default gateway, the network will be private as required.

It is critical that you follow the instructions throughout this manual step by step to avoid making a mistake. As discussed by Spears (2002, p.413), the saying, "the longest way around is the shortest way home", is salient.

Windows Server 2008 R2

Windows Server 2008 R2 is the second release of Windows Server 2008, adding additional features and improvements to the first release. Microsoft (2010, p.6) set out a number of reasons to upgrade from Server 2008 to 2008 R2, including the following:

- Scaling Features
  - Support for up to 256 logical processors
- Hyper-V improvements
  - Ability to access up to 64 logical CPUs on the host computer (double the initial capability)
- Reduced power consumption
  - Unused processor cores are not used when not required
- Improved Windows PowerShell
- Upgraded Web Server
- Remote Desktop enhancements
- Enriched mobile user experience

Windows Server 2008 R2 Server Core

As outlined by Tulloch (2009, p.1), "Server Core provides you with a minimal installation of Windows Server 2008 that supports installing only certain server roles".

It is a Text-based user interface (TUI) whereby you issue commands to carry out tasks. However, in Server Core 2008 R2 you can also launch menu type utilities such as **SCONFIG,** which will be extensively used in this section of the manual. Tulloch (2009, p.5), outlines the GUI applications which were available in the original release of Server Core 2008:

1. Command prompt executable by running **cmd.exe**
2. Notepad, executable by running **notepad.exe**
3. Registry Editor, executable by running **regedt32.exe**
4. System Information, executable by running **Msinfo32.exe**
5. Task Manager, executable by running **taskmgr.exe**
6. Windows Installer, executable by running **msiexec.exe**
7. Microsoft Support Diagnostic Tool, executable by running **msdt.exe**
   a. This tool requires an internet connection unless you use an **Offline Package**, as discussed by Microsoft (2011).

A1 - Windows Server 2008 R2 Installation

When you boot your system with the installation media, you will be presented with the menu shown in Figure A1.1. Choose the relevant language, time, currency, and keyboard settings and click **Next**.

Figure A1.1 – Region Settings

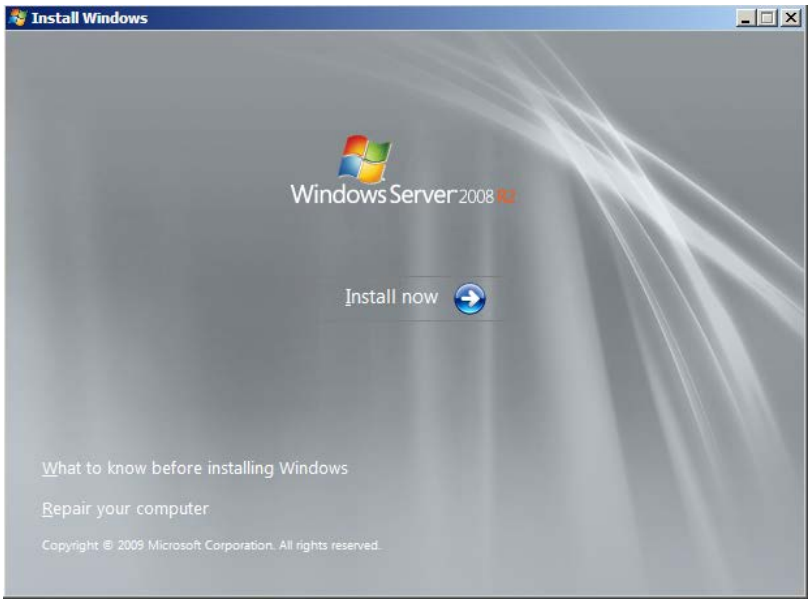
INFORMATION

If you make a mistake on this section, you can remedy it when Windows has been installed.

Click **Start** and in the **Search programs and files** text box type **intl.cpl** and press **Enter**. You can alter all region and language settings at this location.

You will now be presented with the menu shown in Figure A2.1. Select **Install now** to proceed with the installation.

Figure A1.2 – Install Windows



INFORMATION

What to know before installing windows

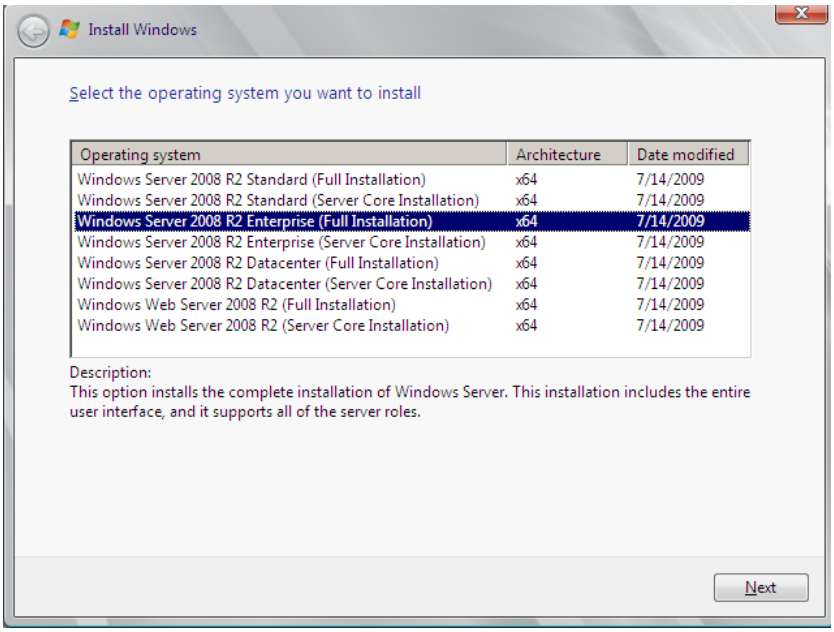
This option displays a document with information on system requirements, guidelines about back-up and pre-preparation of the Active Directory environment.

Repair your computer

This option allows the administrator to use system recovery tools or to restore the computer using a system image, should the system fail to boot up correctly.

At this stage you will be asked which operating system you wish to install. The steps to date will be repeated for the **Server2** and **Server Core** installations. Select the relevant operating system as shown in Figure A1.3 and click **Next** to proceed. The next window contains the license terms. After reading the terms, if you are satisfied with their contents, click the checkbox ***I accept the license terms*** and click **Next** to continue.

Figure A1.3 – Selecting Windows Server 2008 R2 installation



INFORMATION

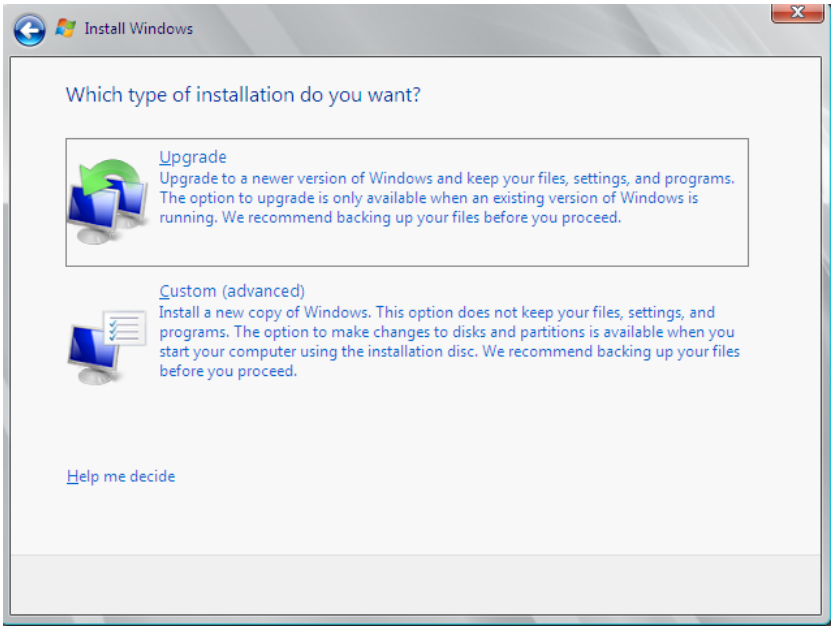
The standard, enterprise, and datacenter edition are all pitched at different licensing costs, with corresponding levels of features.

Recommended Reading:

Morimoto, Noel, Droubi, Mistry, Amaris and Yardeni (2010 , pp.12 – 15) discuss in detail the various versions of Server 2008 R2 available for installation shown in Figure A1.3.

Now, you will be asked which type of installation you want (as shown in Figure A1.4). Select **Custom (advanced)** to install a new copy of windows.

Figure A1.4 – Selecting installation type



INFORMATION

Help me decide

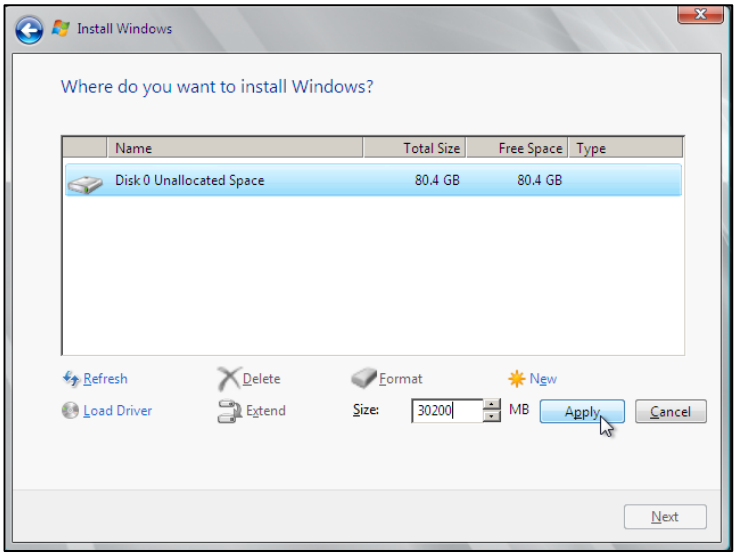
This option gives extensive details regarding the process involved in both the **Upgrade** and the **Custom(advanced)** options.

You will now be asked where you wish to install windows. A separate partition should be created for the installation of the operating system.

Select **Drive options (advanced)** followed by **New.** You will be presented with the options shown in Figure A1.5. Specify the size of the partition for the operating system; for Windows Server 2008, 10GB is the minimum as outlined by Microsoft (n.d.). However, extra disk space will be required for paging, dump files, log files etc. Specify the size as approximately 30GB and select **Apply**. Please note that you must enter the value in megabytes.

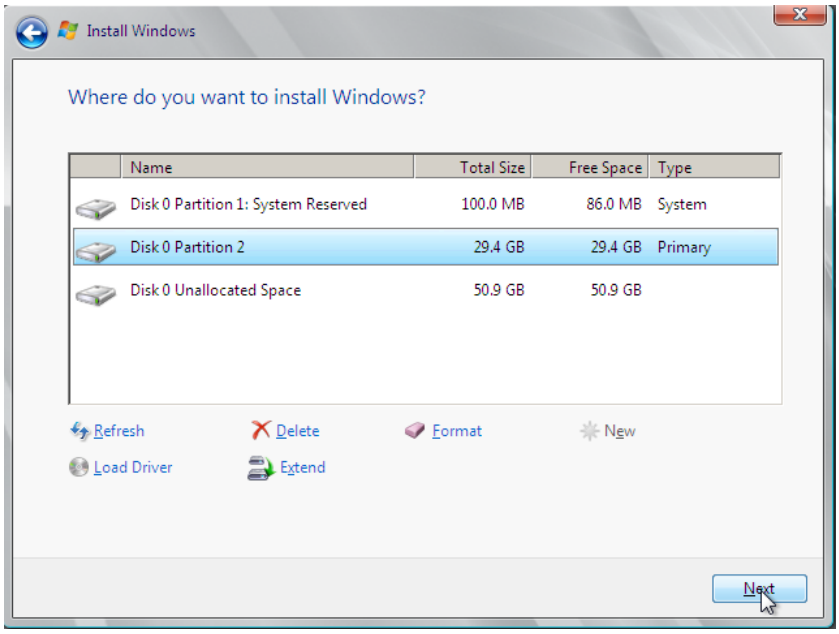
Select **Next** to begin the installation.

Figure A1.5 – Specifying partition size for Windows installation



A warning message will pop up stating that additional partitions may be created for system files. Select **OK** and you will see the results of the disk partitioning as shown in Figure A1.6. Click **Next** to begin the installation.

Figure A1.6 – Selecting partition for operating system install



The length of the installation time will depend on the amount of ram available and the speed of your hard drive or processor. Between four to ten minutes is a reasonable estimate. When the install is completed, you will be notified that ***The user's password must be changed before logging on the first time.*** Select **OK**.

Enter your desired password and select the arrow as shown in Figure A1.7 to continue. Select **OK** when notified that ***Your password has been changed***. Windows Server 2008 R2 has now been installed; you will be greeted by the **Initial Configuration Tasks** menu shown in Figure A1.8.

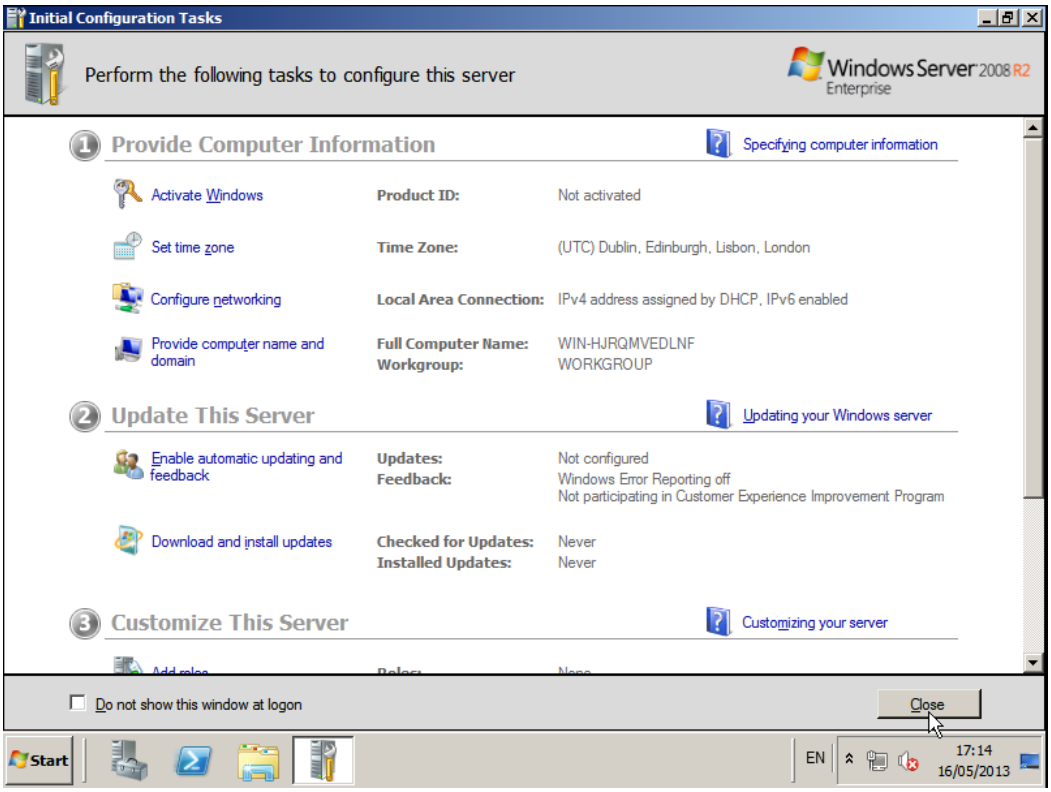
Figure A1.7 – Entering Passwords

INFORMATION

It is important that when choosing a password, that you consider password complexity requirements.

It is also important to note, that whilst the **Administrator** account is used throughout this manual for demonstrative purposes, it is a security best practice recommendation that you rename the Administrator account, as discussed by Microsoft (n.d).

Figure A1.8 – Initial Configuration Tools



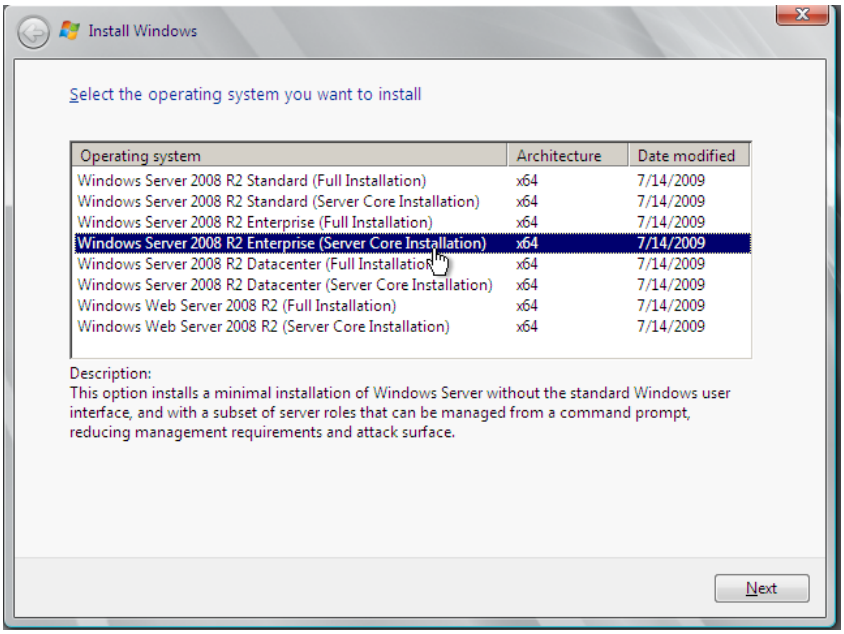
INFORMATION

You may tick the box beside **Do not show this window at logon** if you do not wish to use this utility the next time you reboot your system.

A2 - Windows Server 2008 R2 Core Installation

For the installation of the server core, the steps are exactly the same as Windows Server 2008 R2 Enterprise until you reach the operating system selection screen as shown in Figure A2.1. Choose the Server Core Installation and click **Next** to proceed.

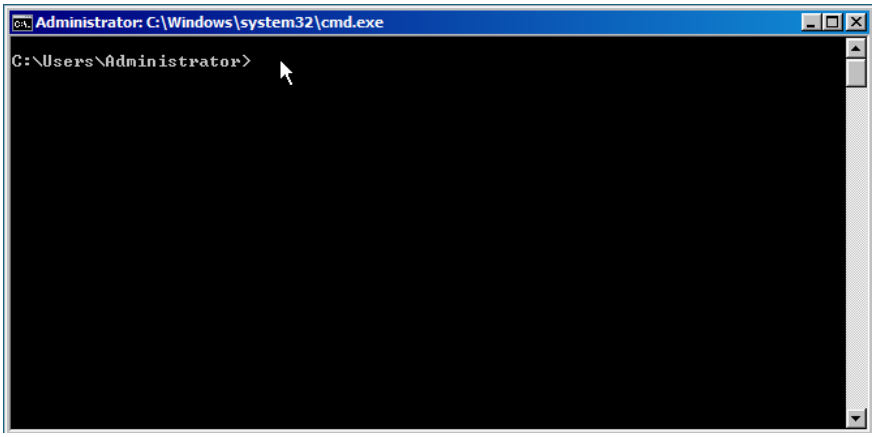
Figure A2.1 – Selecting the Server Core Installation



The next window contains the license terms. After reading the terms, if you are satisfied with their contents, click the checkbox ***I accept the license terms*** and click **Next** to continue. Now, you will be asked which type of installation you want. Select **Custom (advanced)** to install a new copy of windows.

When the install is completed, you will be notified that ***The user's password must be changed before logging on the first time.*** Select **OK**. Enter your desired password and select the right-pointing blue arrow to continue. Windows Server 2008 R2 Core has now been installed; you will be greeted by the server core environment shown in Figure A2.2.

Figure A2.2 – Server Core Environment

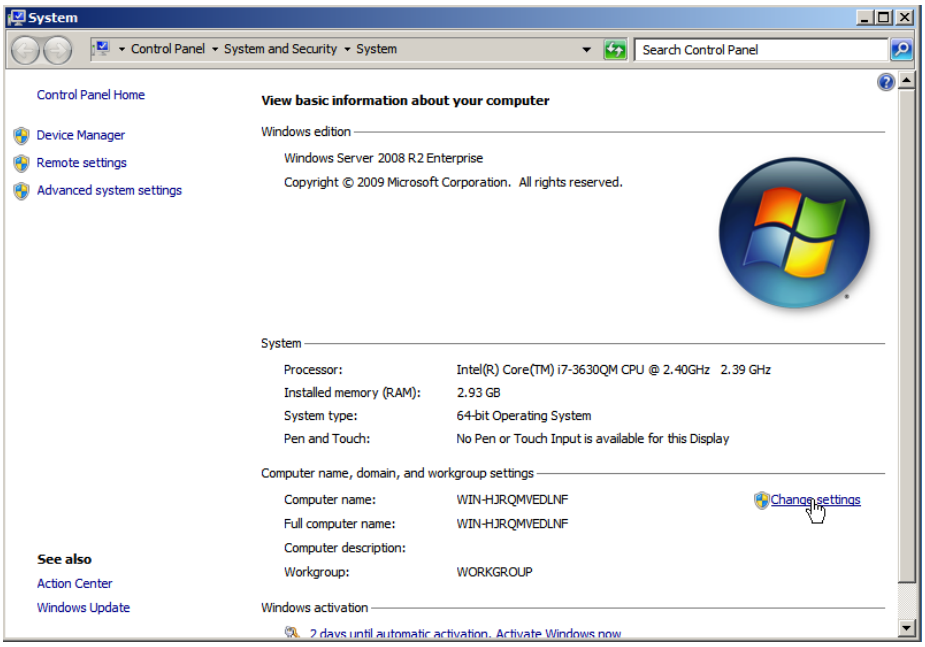


A3 - Renaming the Computers

Rename Server 2008 R2 GUI

To rename the computer in the full Windows Server 2008 R2 environment, click the **start** button, right-click **Computer** and select **Properties**. Select **Change Settings** as shown in Figure A3.1.

Figure A3.1 – System Control Panel Applet



INFORMATION

Entering "Server 1" as the computer name is not permitted as whitespace characters are not permitted (as are many other characters).

When you have changed the computer name, you can verify it has successfully changed in the **Initial Configuration Tasks Menu** (which is set to automatically open on login) as shown in Figure A3.3.

The **System Properties** window will appear with the **Computer Name** tab opened. You will see the current non-descript computer name. Select **Change** and you will enter the **Computer Name/Domain Changes** window as shown in Figure A3.2.

Figure A3.3 – Verifying Computer Name Change

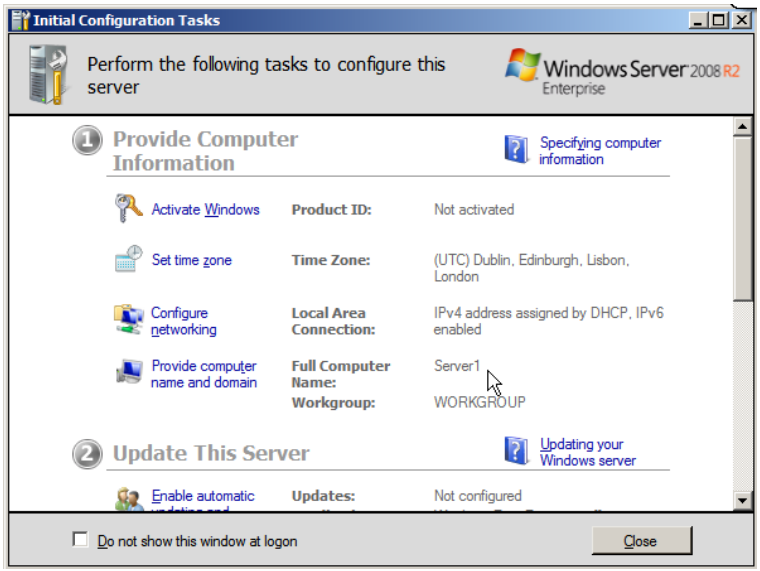
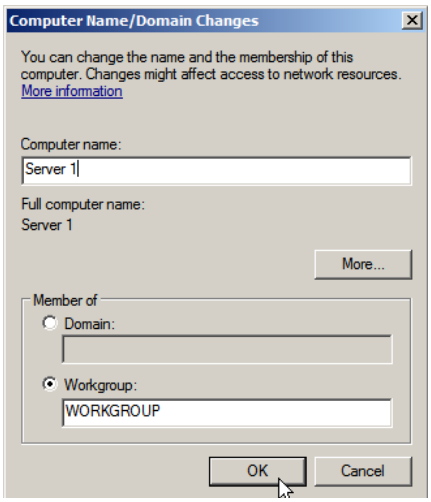


Figure A3.2– Change Computer Name



Change the computer name as shown (Server1 in this instance, Server2 for the other GUI server) and select **OK** to continue. You will be prompted to restart the computer, select **OK** to proceed. Proceed to Attempt any task and you will be prompted to restart again, select **Restart Now** to do so.

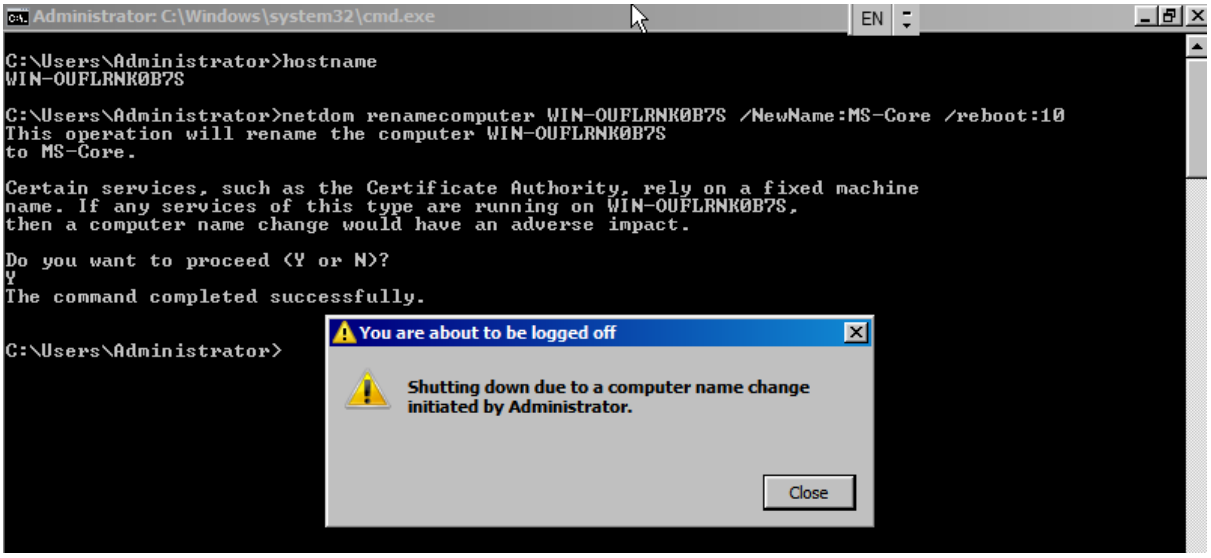
Rename Server Core

In the server core environment, you can check the computer name using the **hostname command**. As shown in Figure A3.4 the initial computer name for the sample system was WIN-OUFLRNK0B7S.
To change the computer name use the following command:

CMD	Netdom renamecomputer <Computer> /NewName:<NewComputerName> /reboot:<Delay>

- <Computer> represents the current computer name.
- <NewComputerName> represents the name you wish to change the computer to
- <Delay> represents the time delay for restarting the computer
    - Renaming the computer requires a reboot, so it is convenient to add reboot to the command

Figure A3.4 – Rename Server Core

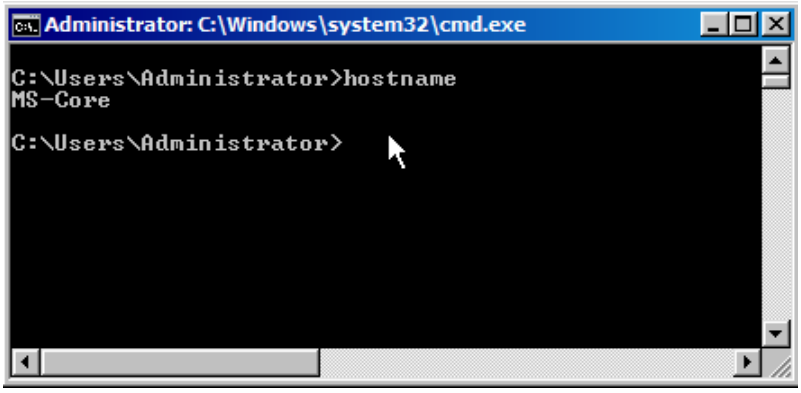


In the above example (Figure A3.4), the command used to rename the computer was:

CMD	Netdom renamecomputer WIN-OUFLRNK0B7S /NewName:MS-Core /reboot:10

To verify the computer name change was successfully implemented, upon restart, run the **hostname** command again; as shown in Figure 3.5.

Figure A3.5 – Verifying Server Core Renaming



A4 - Machine Network Configuration

To ensure that your machines can communicate on the network, you may need to turn the firewall off with the command shown below. The firewall is not required on an internal private network.

CMD	Netsh advfirewall set allprofiles state off

Introduction

The machines are to be statically assigned IP addresses from the range 192.168.0.0/24. This is the Classless Interdomain Routing (CIDR – pronounced *cider*) format of representing IP addresses. /24 means that the first 24 bits of the subnet mask (the first three octets of the IP address) represent the network number i.e. 192.168.0. The final part of the IP address represents the host address. Ross and Kurose (2010, pp.352-355) explain CIDR notation in more detail, and it is a recommended read for enhanced understanding.

The subnet mask is set as 255.255.255.0, which will always be the case when the first 24 bits represent the network. The default gateway is not set; this ensures that the network is private.

IP address assigned

Client	192.168.0.1
Server 1	192.168.0.2
Server 2	192.168.0.3
MS-Core	192.168.0.4

Statically assign Server GUI

The steps undertaken to statically assign the Server GUI system are to be repeated for both servers.

In the **Initial Configuration Tools** menu, under the subheading **Provide Computer Information**, click **Configure networking**. You will be presented with the **Local Area Connections** window shown in Figure A4.1.

Right-click the **Local Area Connection** and select **Internet Protocol Version 4** as highlighted in Figure A4.1. Select **Properties** which will bring to the window shown in Figure A4.2.

Obtain an Ip address automatically will be selected by default. Instead, select **Use the following IP address** and enter in the required values.

The first three nodes in the subnet mask represent the network with the last node representing the host.

Figure A4.1 – Local Area Connection Properties

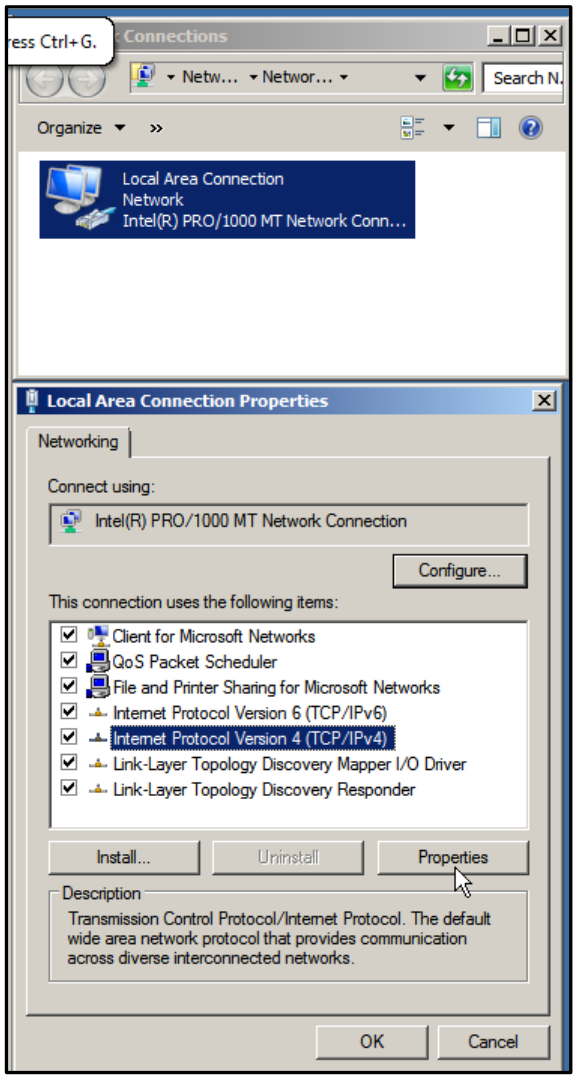
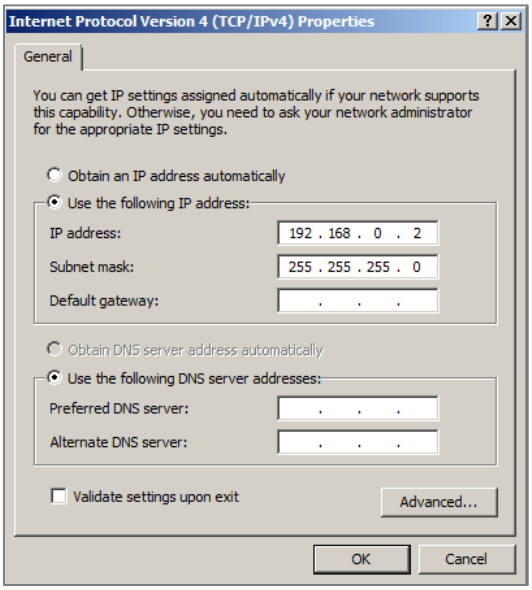


Figure A4.2– IPv4 Properties



When you are satisfied with your entries, select **OK** to continue. You can test that your changes have been successful by running **ipconfig** in the **command prompt**.

Statically Assign Server TUI

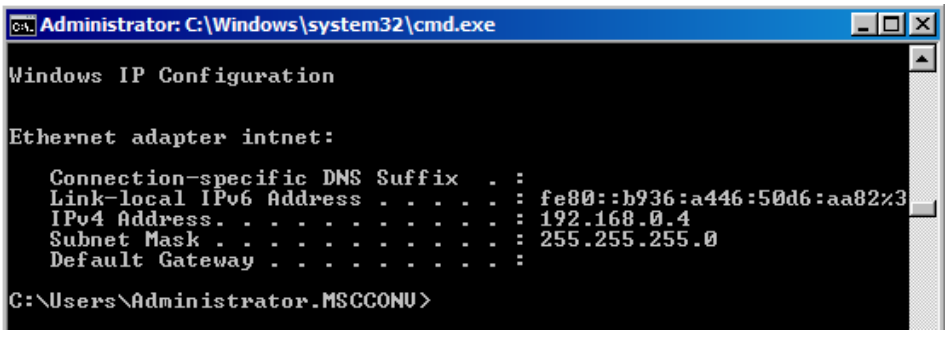
In the TUI environment, run the following command:

CMD

```
netsh interface ipv4 set address name="Local Area Connection" source=static
address=192.168.0.4 mask=255.255.255.0
```

To verify that the changes made have been successful, run **ipconfig;** this will display the new network settings as shown in Figure A4.3. Note that the Ethernet adaptor is named “intnet”; on your machine it is more likely to be named “Local Area Connection”. An exercise on renaming the network can be found later in this manual.

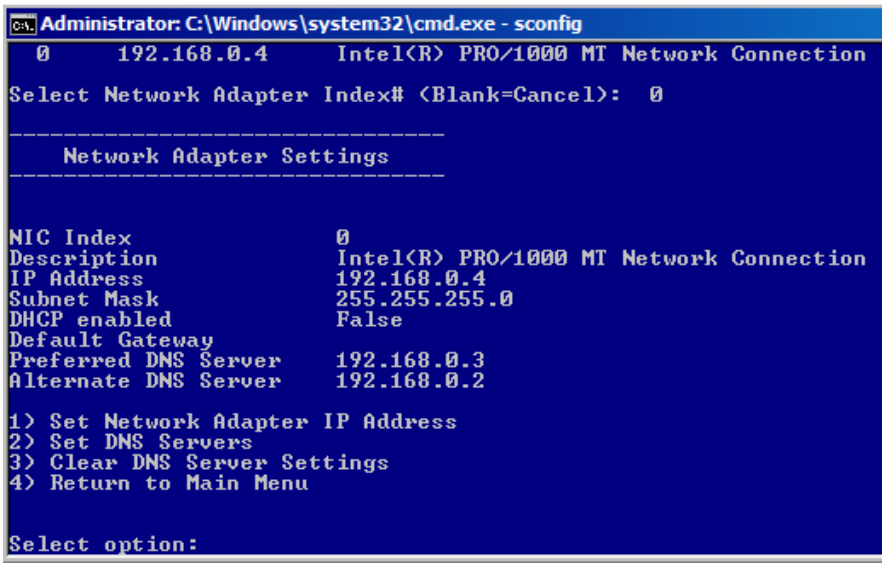
Figure A4.3 - Ipconfig



You can also work with network settings using the **sconfig** utility. Run the **sconfig** command and press **8** to work with network settings. As shown in Figure A4.4, enter the index number of the network adaptor. Your network settings are displayed, and options are available to work with the IP address and DNS settings.

Follow the options given to return to the main command line (4 to return to server configuration followed by 13 to return to the command line).

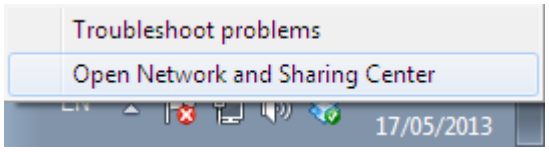
Figure A4.4 - Sconfig



Statically assign Windows 7 Client

At the bottom right-hand corner of your screen, right-click on the mini-computer icon (to the left of the speaker icon) and select **Open Network and Sharing Center** (Figure A4.5).

Figure A4.5 – Network and Sharing Center

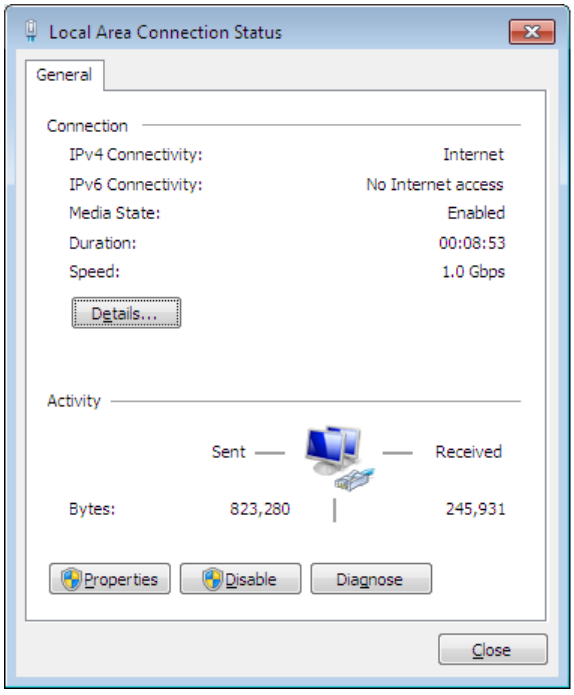


This will bring you to the **Local Area Connection Status** window shown in Figure A4.6.

Select **Properties**. From here, the steps are identical to steps carried out for Windows Server 2008 GUI.

Ensure **Internet Protocol Version 4** is highlighted and click **Properties**. Select **Use the following IP address** and enter the required values, selecting **OK** when finished.

Figure A4.6 – Local Area Connection Status



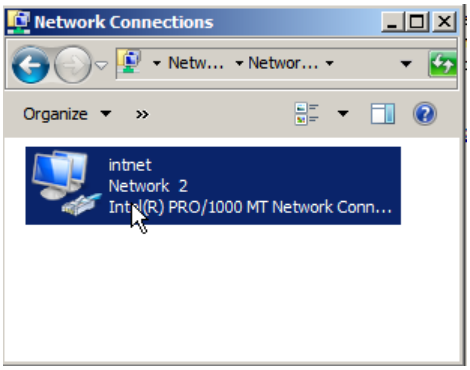
Intnet internal network

Server GUI

In the **Initial Configuration Tools** menu, under the subheading **Provide Computer Information**, click **Configure networking**. You will be presented with the **Local Area Connections** window shown in Figure A4.7

Right-click the **Local Area Connection**, select **Rename** and type **intnet**.

Figure A4.7 – Renamed Network



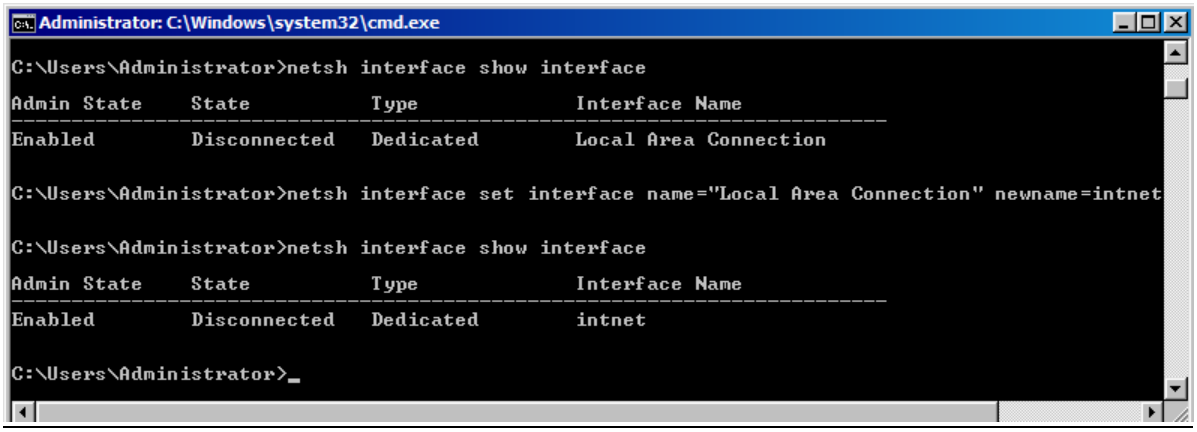
Server Core Environment

As shown in Figure A4.8, to check the current network interface name, run the **netsh interface show interface** command. To change the network name use the following command:

CMD	**Netsh interface set interface name=”Current Network Interface Name” newname=new network name**

An example of implementation of this command is shown in Figure A4.8. Running the **netsh interface show interface** command again allows you to check that the renaming was successful.

Figure A4.8 – Changing the MS-Core network name



Windows 7 Client

Click the **start** globe, and in the search bar type ***networking and sharing center*** and click the aforementioned result. In the left-hand navigation pane click **change adapter settings.** You will be presented with the **Local Area Connections** window shown in Figure A4.7 above. As before, right-click the **Local Area Connection**, select **Rename** and type **intnet**.

Figure A4.9 – Network Diagram

Server 1
IP Address: 192.168.0.2
Subnet Mask: 255.255.255.0
Preferred DNS: 127.0.0.1

Server 2
IP Address: 192.168.0.3
Subnet Mask: 255.255.255.0
Preferred DNS: 192.168.0.2
Alternate DNS: 127.0.0.1

MS-Core
IP Address: 192.168.0.4
Subnet Mask: 255.255.255.0
Preferred DNS: 192.168.0.3
Alternate DNS: 192.168.0.2

Client1
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
Preferred DNS: 192.168.0.2
Alternate DNS: 192.168.0.3

Verification of network interconnectivity

To verify that all machines can communicate with each other, one can use the **ping** command from the command prompt. Figure A4.10 demonstrates four machines operating within virtual environments on a host machine; each instance of VMware Workstation demonstrates one machine successfully pinging another machine. Figures A4.11 to A4.14 show each machine pinging the respective remaining machines.

Figure A4.10 – Verification of network interconnectivity

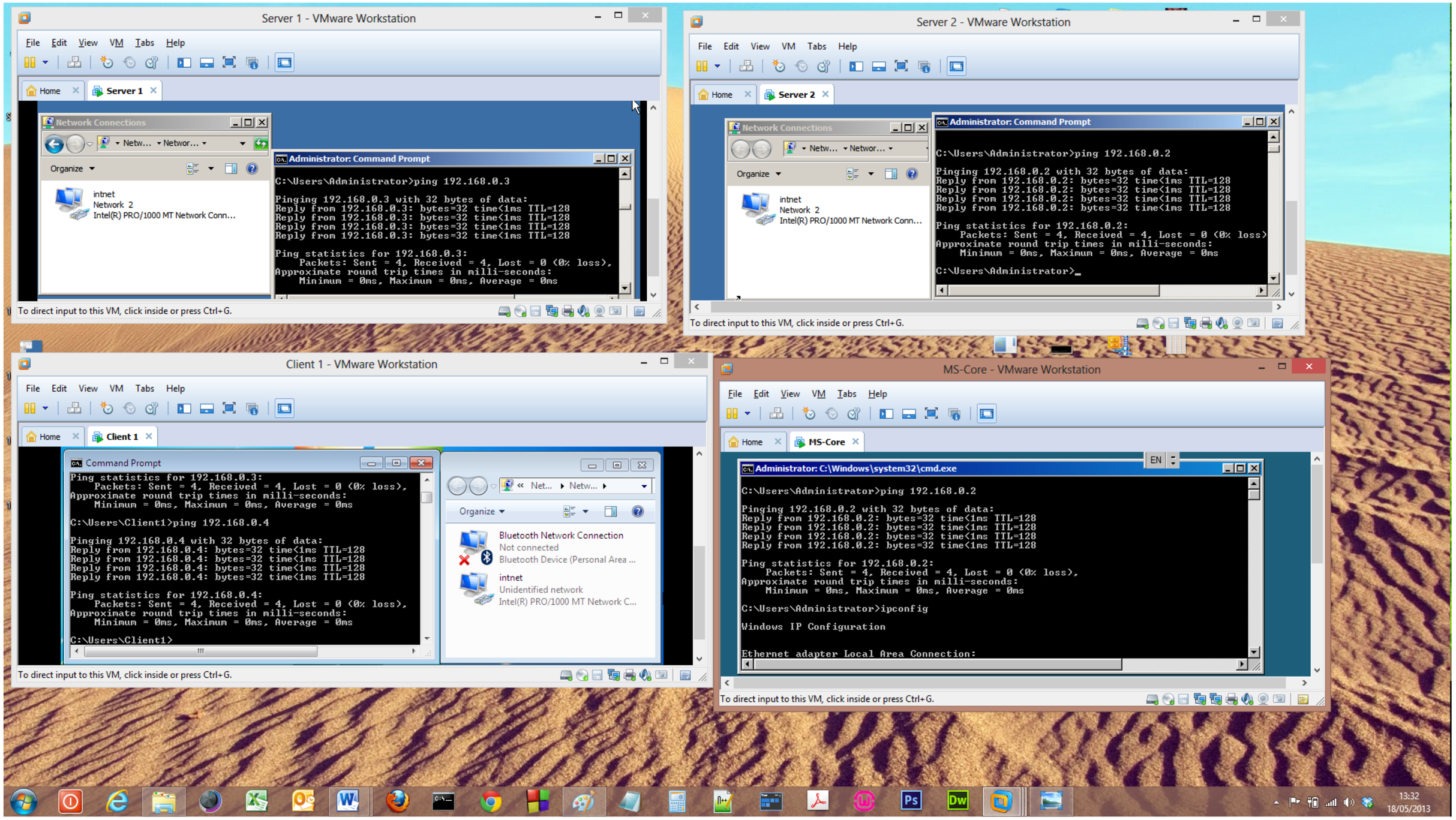


Figure A4.11 – Server 1 pinging all other machines

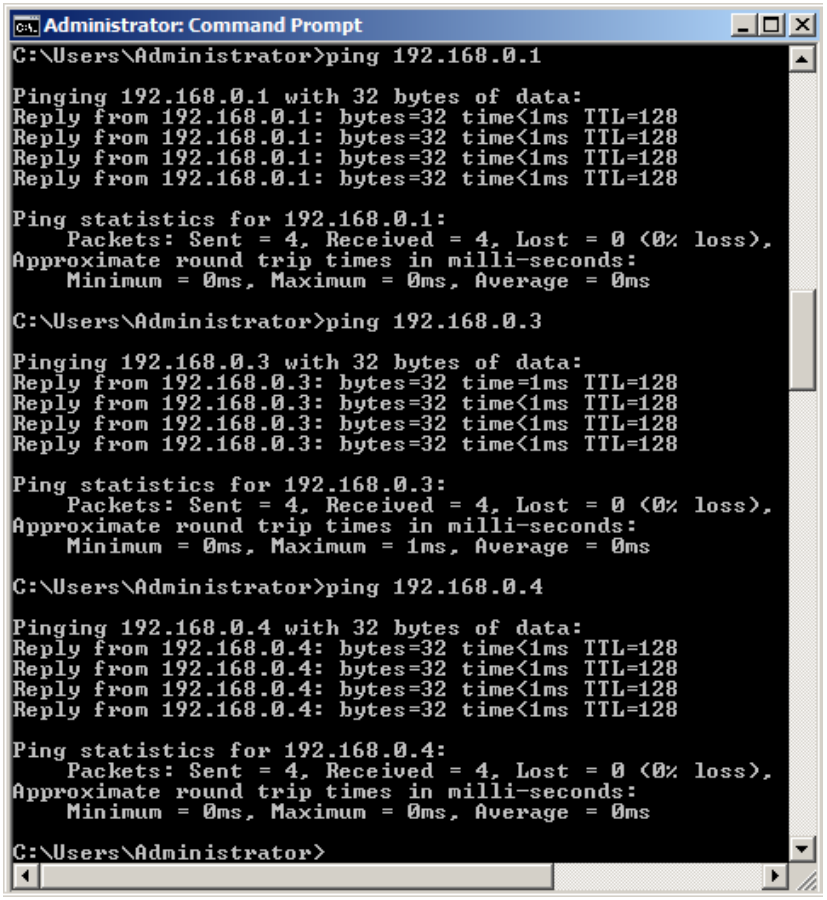


Figure A4.12 – Server 2 pinging all other machines

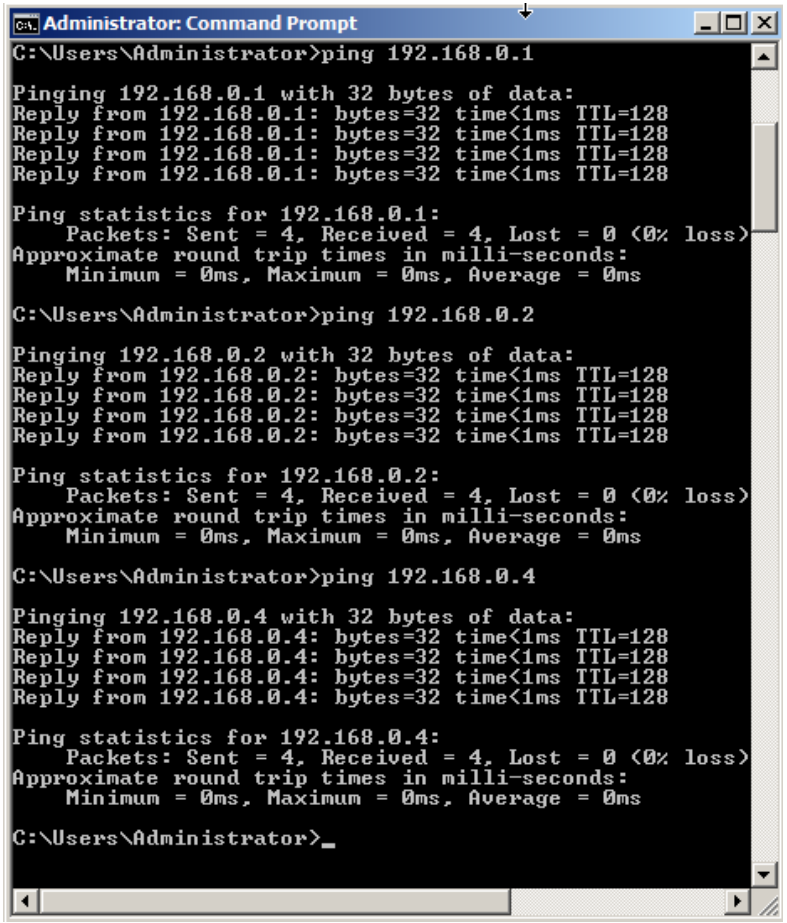


Figure A4.13 – Client 1 pinging all other machines

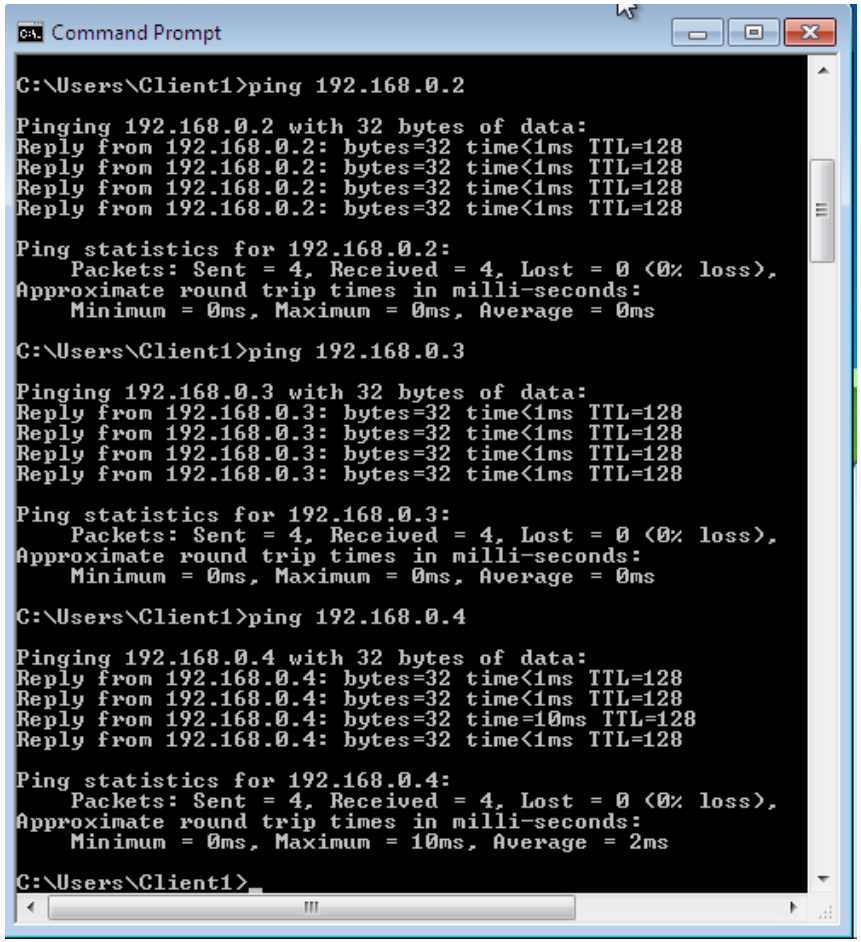
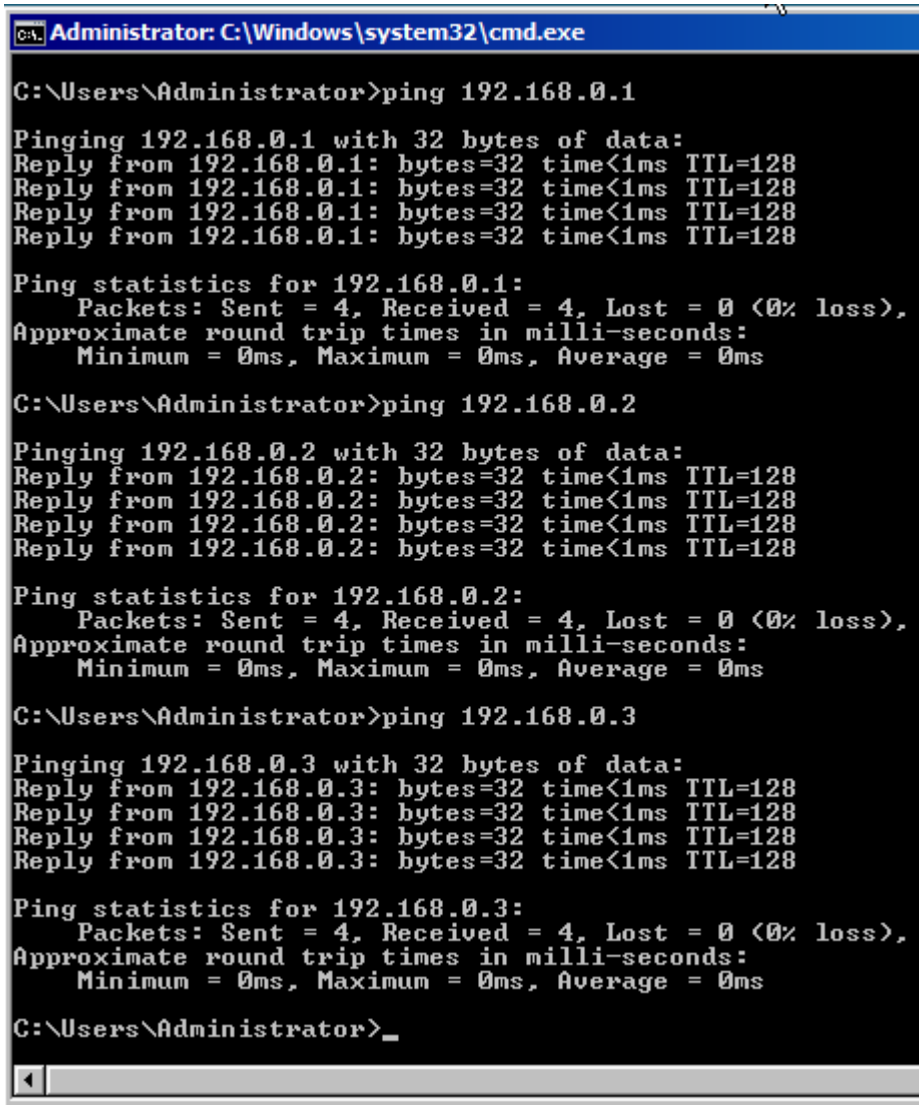


Figure A4.14 – MS-Core pinging all other machines



TASK B – FOREST SETTINGS

B0 - Task Introduction

In this section, you will carry out the following tasks:

1. Create a tree named **MSCCONV.IPA**, and promote **Server1** from a member server to a Domain Controller, using **dcpromo**.
2. Add **Server2** as a second domain controller, DNS settings must be configured before running **dcpromo**.
3. Add **Client1** to the domain, you will also have to configure DNS settings beforehand.
4. Set DNS settings and join the Domain using the **sconfig** utility on MS-**Core.**

Active Directory, Trees and Forests

Active Directory is used for administrative purposes to enable a network to operate as a single entity. Clines and Loughry (2008, pp.7-11) explain Active Directory in detail, and it is a recommended read for further understanding.

As outlined by Minasi, Gibson, Finn, Henry and Hynes (2010, p.230), "A forest is a group of one or more domains that share a common directory". They also define a tree as a "group of domains with a common namespace".

In this task, the tree is called **mscconv.ipa.** A child domain could be created within the tree (domain), for example, named **am.mscconv.ipa**. You could create a separate tree (domain) in the same forest, for example, named **mscnegotiated.ipa**.

Domain Controller

Server1 will be promoted from a member server to a domain controller (DC). A domain controller contains a copy of Active Directory Domain Services (AD DS) and is required to assign and apply security policies upon user and computer objects across the network. The DC is also required to install and update software.

In order for other machines on the network to locate the DC, they must take the IP address of the primary DC as its preferred DNS server.

Second Domain Controller

Server2 will be configured as a second domain controller. The computers on the network will use the second DC`s IP address for their machine`s alternate DNS address.

This means that if **Server1** fails, the network will still run via **Server2**. If **Server1** failed, and **Server2** did not exist, the network would go down. A back up of Active Directory would be required to restore the domain.

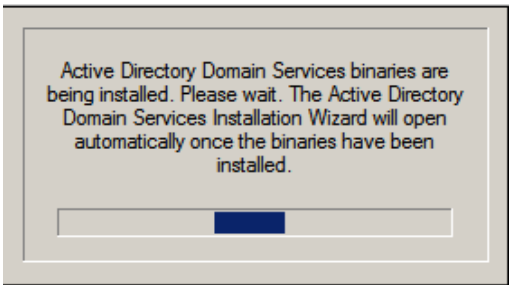
DNS Explained

A Domain Name Server (DNS) is used to translate a Fully Qualified Domain Name (FQDN) into an IP address and Vice Versa. For further reading, Black (2009, pp. 251-252) explains DNS in more detail.

B1 - Server 1

DCPromo is used to configure forest settings. Click the **start** button and type dcpromo in **Search programs and files**. Click the search result, and a message will be displayed as shown in Figure B1.1. You will then be presented with the **Active Directory Installation Wizard.** The option **Use advanced mode installation** allows you to create a new domain tree in an existing forest. This option is not required at this time. Click **Next** to proceed.

Figure B1.1 – Installation of Binaries



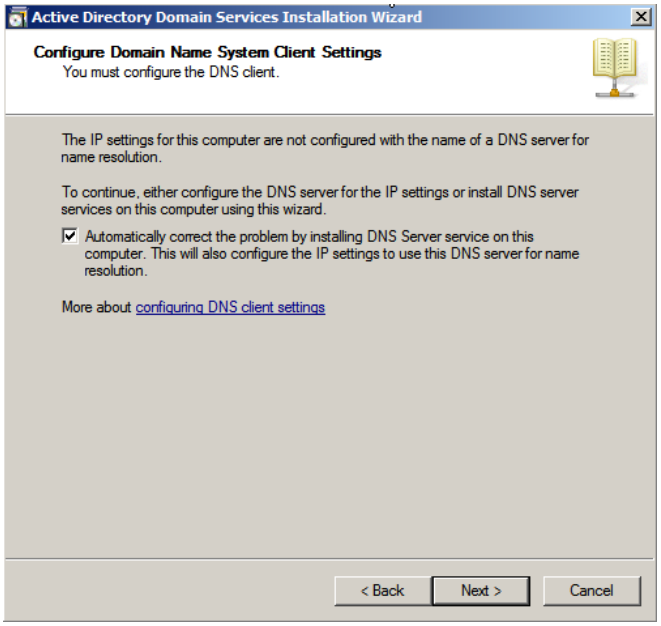
INFORMATION

The binaries are the code necessary for the member server to become a domain controller.

A message will appear regarding operating system compatibility; (this only affects versions of windows earlier than vista service pack 1) click **Next** to continue. A message will appear as shown in Figure B1.2 advising that DNS settings must be configured.

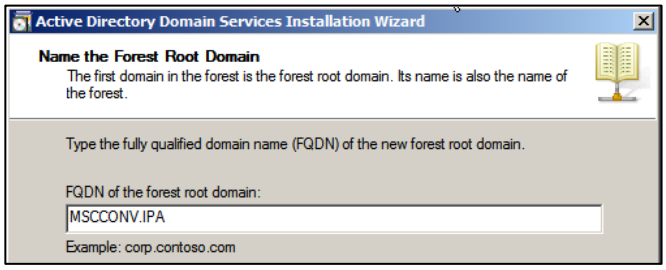
Tick the box that automatically configures DNS settings and choose **Next**. You will be asked whether to create a domain controller for an existing forest or for a new forest.

Figure B1.2 – DNS Configuration Message



Select **Create a new domain in a new forest** and click **Next** to continue. Now, the forest root domain must be named. Enter the fully qualified domain name (FQDN) as shown in Figure B1.3 and click **Next** to continue.

Figure B1.3 – Forest Root Domain



The wizard will check if the forest name already exists and will also verify the NetBIOS name. You will now be prompted to set the forest functional level, as shown in Figure B1.4.

Choosing **Windows Server 2008 R2** provides the most features, however, if your company has an older server in the network, it cannot be added as a domain controller to the forest using this functional level. You can always raise, but you can never lower, the forest functional level.

You should set the forest functional level to the highest that your environment can support provided you are confident that you will never need to add an older server to the domain. When you are happy with the level, select **Next** to continue.

The **additional domain controller options** window will appear. Click **Next** to proceed.

Figure B1.4 – Set Forest Functional Level

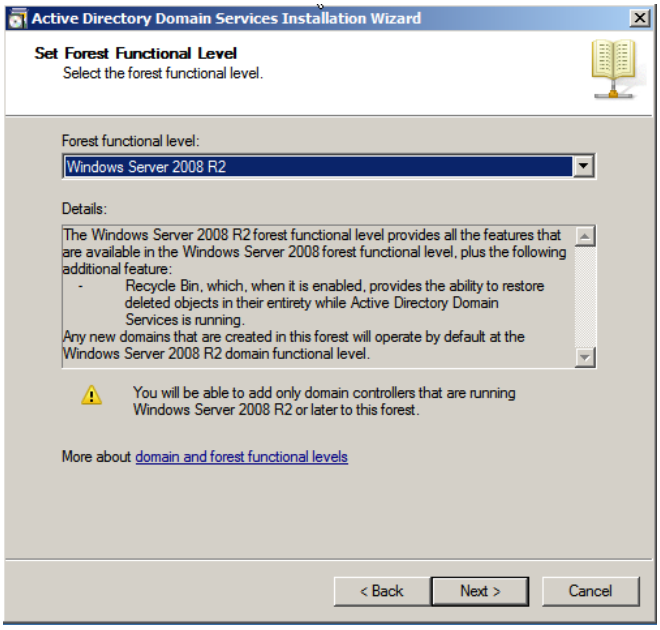
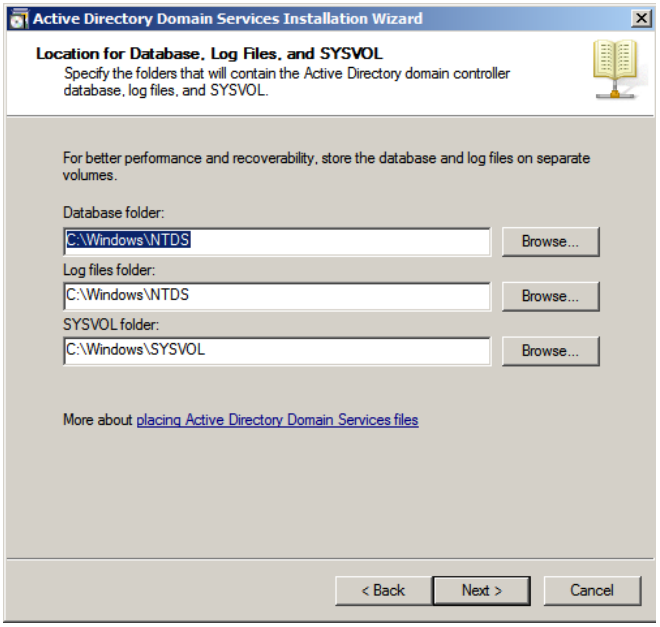


Figure B1.5 – No existing DNS entry

A warning regarding DNS delegation will be displayed as shown in Figure B1.5. This warning simply means that DCPromo has recognized that there is no existing DNS entry. It asks you should to create a DNS entry. Click **Yes** to continue. Now you will be prompted for the location of files as shown in Figure B1.6.

Figure B1.6 – Location for Files



INFORMATION

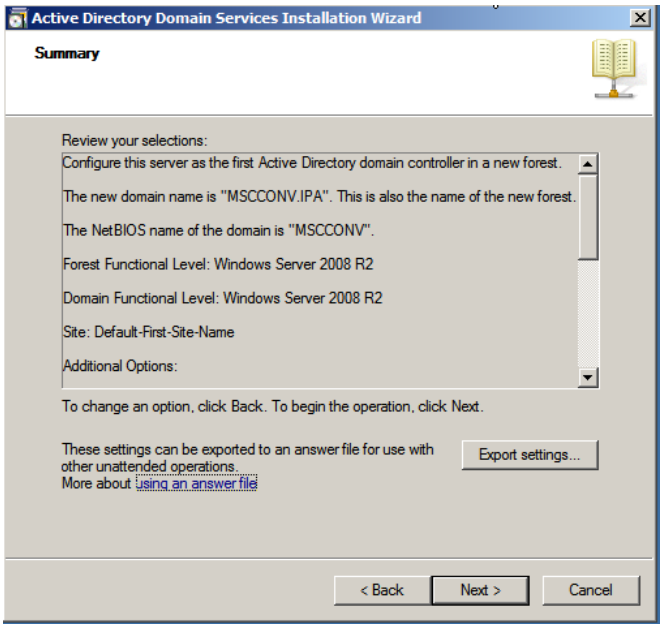
The database and log files can be stored on separate volumes to increase performance.

Also note that the **SYSVOL** folder must be located on an NTFS drive.

Click **Next** to continue when you are satisfied with the file locations. You will be asked to create a password for Directory Services Restore Mode (DSRM). DSRM is used to perform maintenance to or a restoration of Active Directory. A special administrator account is a requirement for DSRM. Enter the desired password and click **Next**.

The summary window as shown in Figure B1.7 reviews the options selected to date. There is also an option to export settings; this is useful to automate subsequent installations of Active Directory Domain Services.

Figure B1.7 – Summary

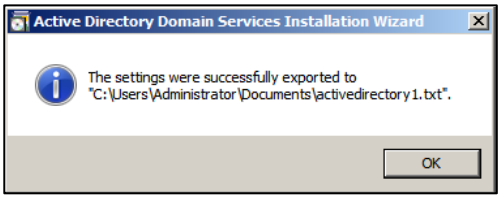


INFORMATION

If you wish to export the settings entered thus far as a template for further AD DS installations, click **Export Settings**, choose a file-name and directory and click **Save**. You should receive a message as per Figure B8.

Minasi, Gibson, Finn, Henry and Hynes (2010, p.244) discuss how to run this text file for future installations.

Figure B1.8 – Settings Exported



To proceed with the installation, click **Next**. The wizard will spend some time configuring settings as shown in Figure B1.9. The computer will need to be rebooted; therefore it is convenient to select the **Reboot on completion** option.

Figure B1.9 – Configuration of AD DS

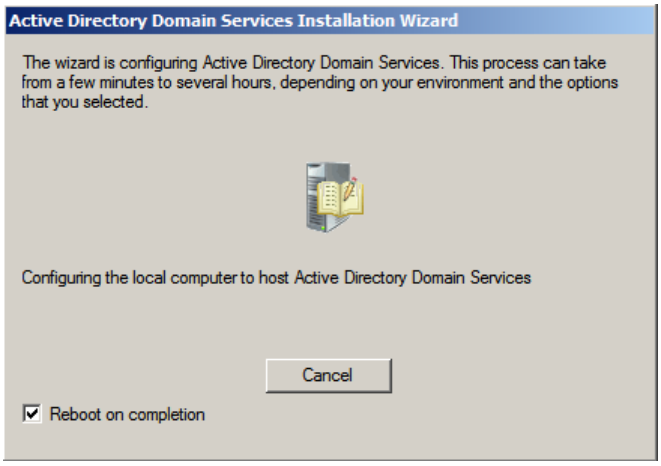
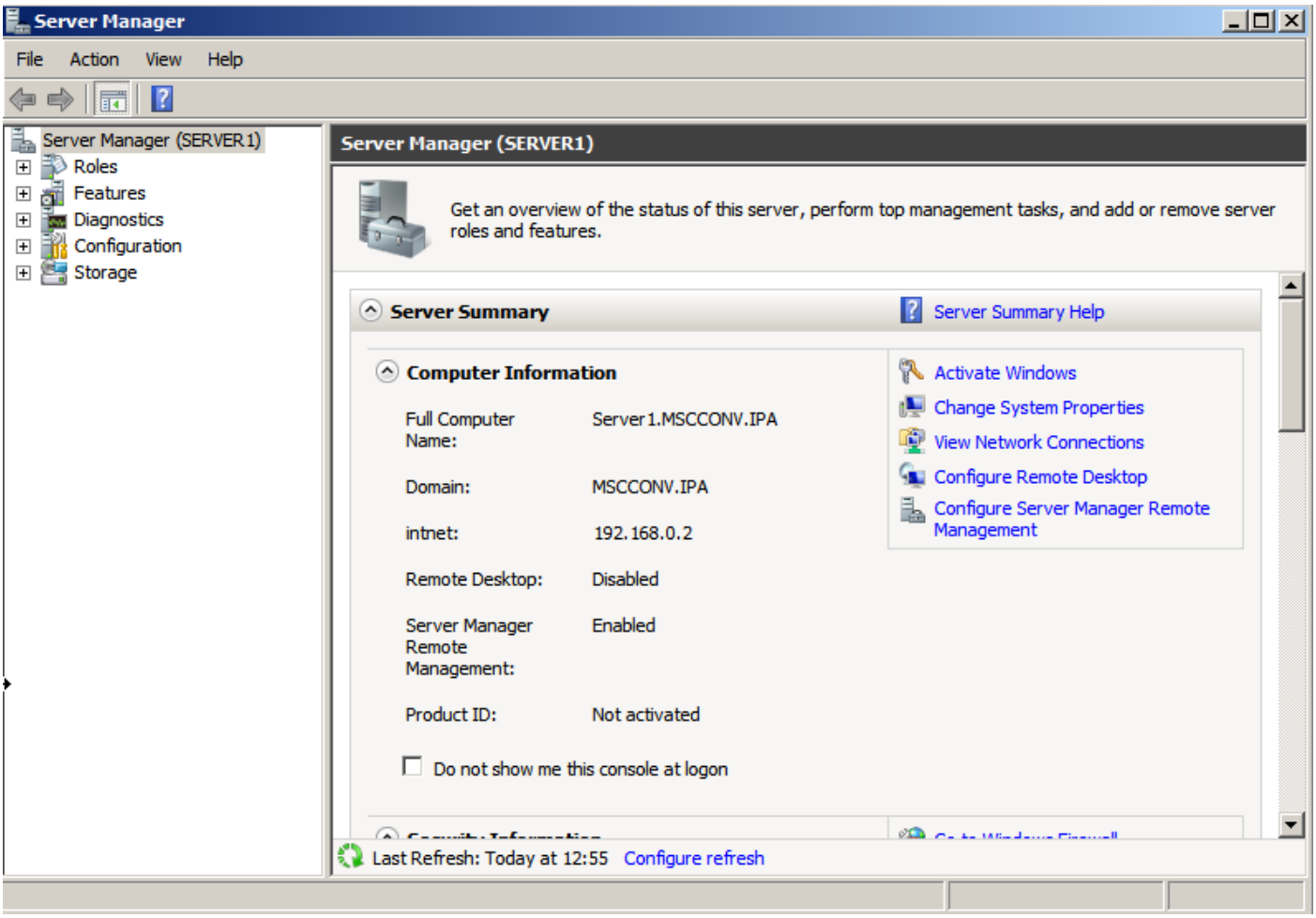


Figure B1.10 – upon reboot

Upon reboot, after Windows has configured some settings, you can see the result of the wizard by noting the prefix to the username (MSCCONV as shown in Figure B1.10).

After logging in, you will be presented with the **Server Manager** utility as shown in Figure B1.11. Note how the computer name has been appended with the forest root domain.

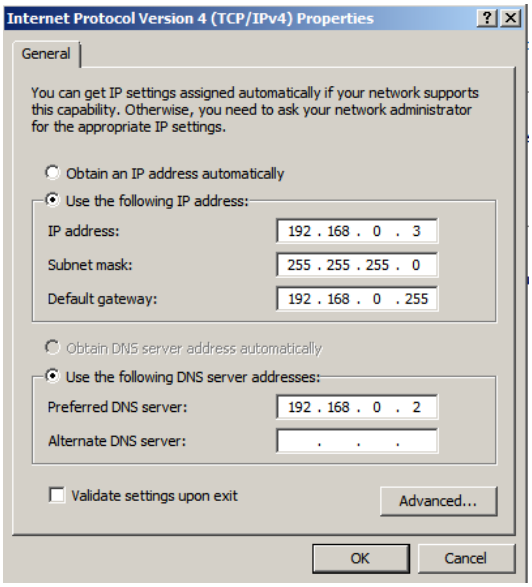
Figure B1.11 – Server Manager



B2 – Server 2

DNS settings must be configured before adding a new domain controller to the second server.

Figure B2.1 – Ipv4 Settings



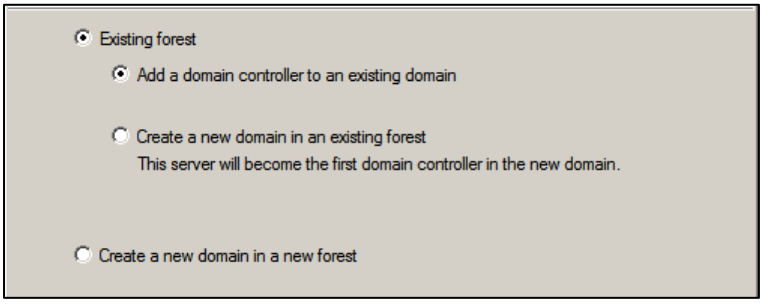
From the **Initial Configuration tools** menu select **Configure networking.** Right-click the **intnet** connection and select **Properties**. Ensure **Internet Protocol Version 4** is selected and click **Properties**.

This will bring you to the **IPv4 Properties** menu shown in Figure B2.1. Ensure that the preferred DNS server address is the same as the IP address of **Server1** (the first GUI Server configured in this manual).

Select **OK** to implement your changes.

Follow the **dcpromo** settings outlined for Server1 until the window where you are asked whether to create a domain controller for an existing forest or for a new forest (shown in Figure B2.2). On this occasion, instead of creating a new domain, select **Existing forest** and also select **Add a domain controller to an existing domain.** Click **Next** to continue.

Figure B2.2 – Existing Forest



You will be presented with the **Network Credentials** menu shown in Figure B2.3. As shown, you are to enter the name of the domain in the forest where you plan to install a domain controller; in this manual the domain used to illustrate is **MSCCONV.IPA**.

Since you are connecting to another machine, you cannot use the current user's credentials to perform this installation. Instead **Alternate credentials** will be selected by default and you must select **Set** to enter in the domain administrator credentials as shown in Figure B2.4.

Back in the **Network Credentials** window select **Next** to continue. A message will be displayed as shown in Figure B2.5.

Figure B2.3 – Network Credentials

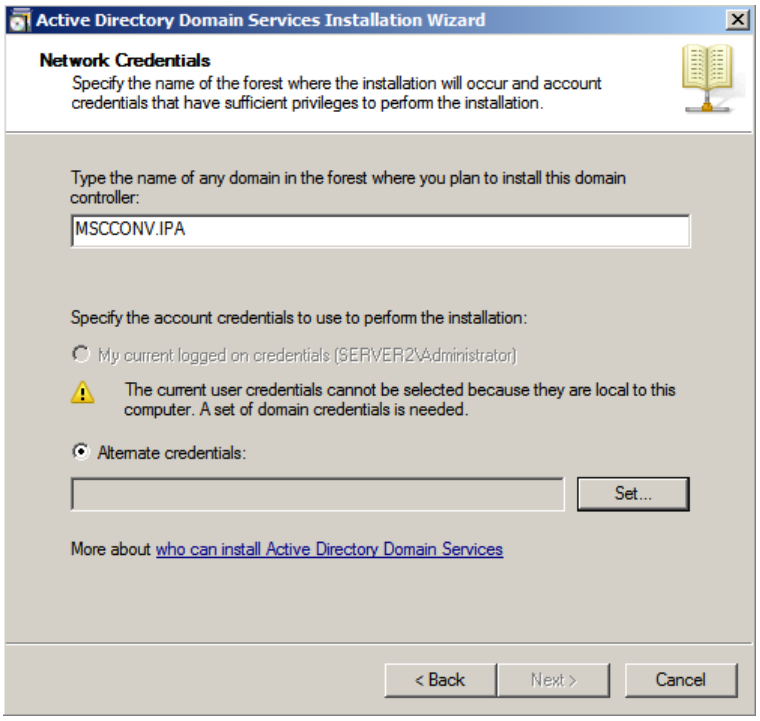


Figure B2.4 – Domain Administrator Credentials

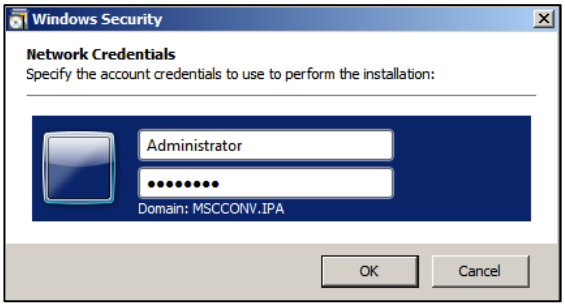
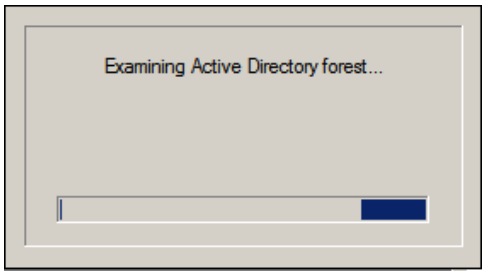


Figure B2.5 – Examining Forest



The **Select a Domain** step will appear as shown in Figure B2.6. Ensure the relevant domain is selected and click **Next**. The next step is the **Select a Site** window; ensure the **Default-First-Site-Name** is selected and click **Next**. You will enter the **Additional Controller Options** window shown in Figure B2.7. **DNS server** and **Global** catalog should both be selected; click **Next** to continue.

Figure B2.6 – Select a Domain

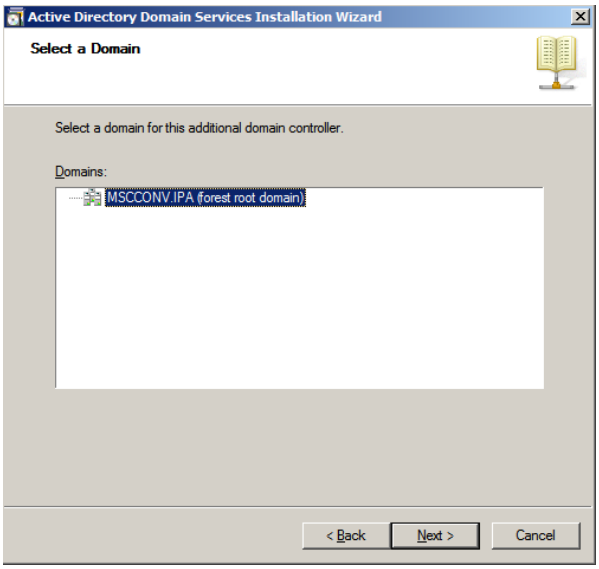
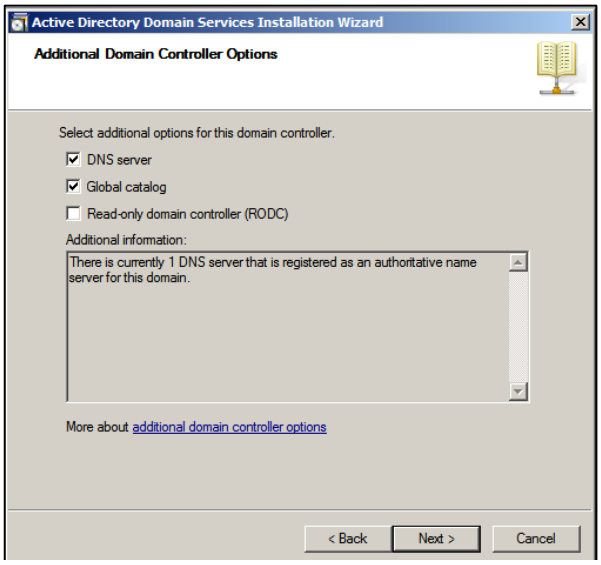


Figure B2.7 – Additional Domain Controller Options



The rest of the steps are the same as illustrated for Server1 from Figure B1.6 onwards. Should a warning for DNS delegation appear, select **Yes** to proceed.

Now you will be prompted for the location of files. Click **Next** to continue when you are satisfied with the file locations. You will be asked to create a password for directory services restore mode. Enter the desired password and click **Next**.

The summary window as shown in Figure B2.8 reviews the options selected to date. As previously discussed, there is an option to export settings; this is useful to automate subsequent installations of Active Directory Domain Services.

Figure B2.8 - Summary

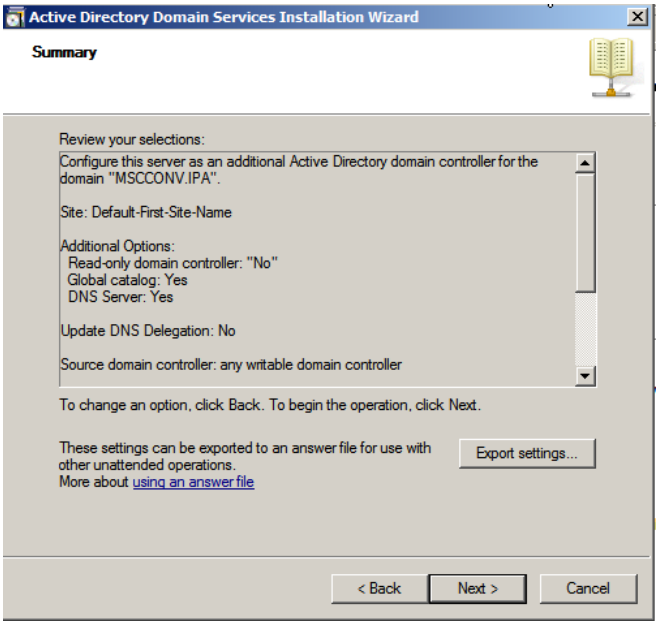
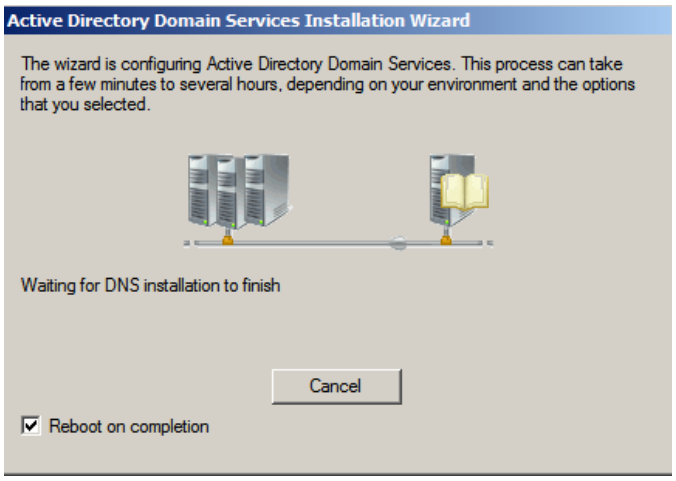


Figure B2.9 – Configuration of AD DS



The wizard will spend some configuring settings as shown in Figure B2.9. The computer will need to be rebooted; therefore it is convenient to select the **Reboot on completion** option.

Upon reboot, after Windows has configured some settings, you can see the result of the wizard by noting the prefix to the username.

After logging in, you will be presented with the **Server Manager** utility as shown in Figure B2.10. Note how the computer name has been appended with the forest root domain.

Figure B2.10 – Server Manager

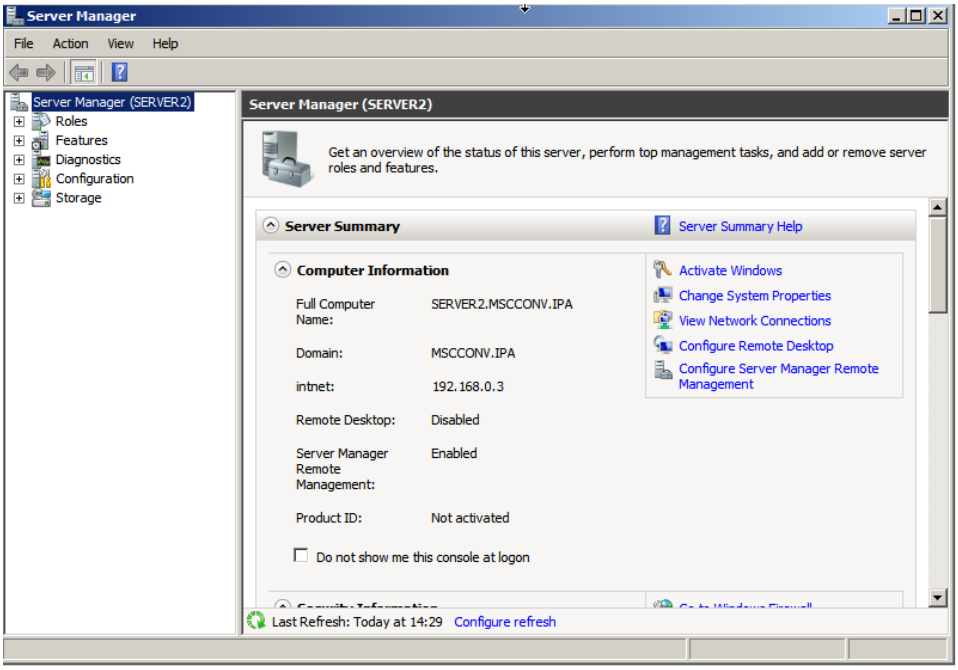


Figure B2.11– Pinging Server1 from Server2

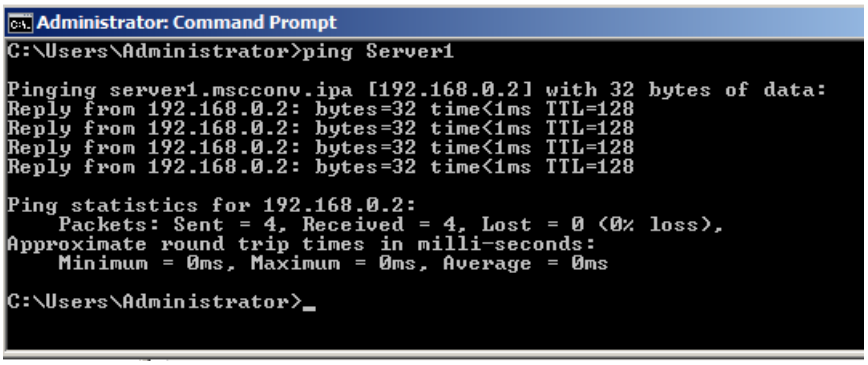
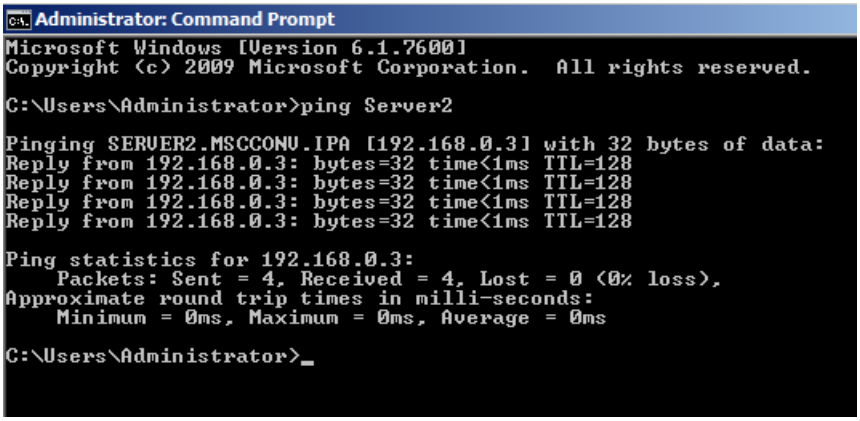


Figure B2.12 – Pinging Server2 from Server1



INFORMATION

To test the machine interconnectivity and domain implementation, you can ping between the servers by pinging the computer name rather than the IP address; as shown in Figures B2.11 and B2.12.

Note the domain name appended to the computer name.

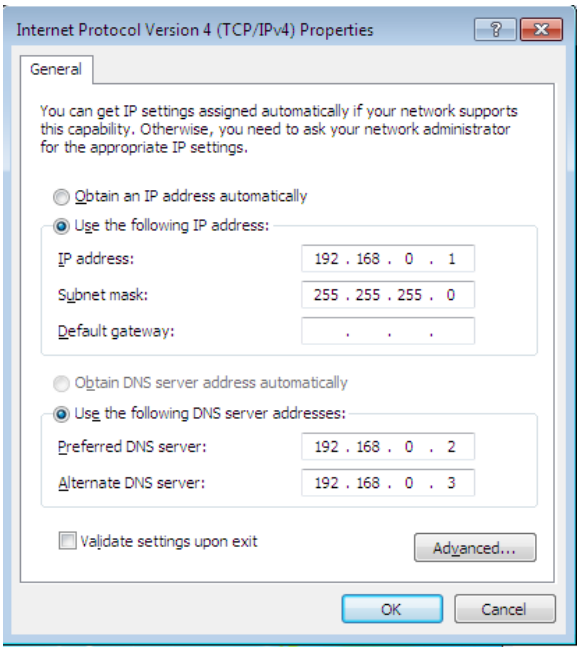
B3 - Windows 7 Client Machine

As with **Server2** machine, you must configure DNS settings before joining the domain. Type **networking and sharing center** into the search bar, and click the result under the **Control Panel** heading. Click the **intnet** network and then click **Properties** in the window that popped up. In **intnet Properties** ensure **Internet Protocol Version 4** is selected and click **Properties**.

This will bring you to the**IPv4 Properties** menu shown in Figure B3.1. Ensure that the preferred DNS server address is the same as the IP address of Server1 (the first GUI Server configured in this manual).

Select **OK** to implement your changes.

Figure B3.1 – Configuring Client 1 DNS



To join the Active Directory Domain, click the **start globe**, right-click **Computer** and select **Properties** as illustrated in Figure B3.2. This brings you to the **System** menu. Under **Computer name, domain, and workgroup settings** click **Change settings**. Now, in **System Properties**, under the **Computer Name** tab, click **Change** (Figure B3.3).

Figure B3.2 – Access the System Menu

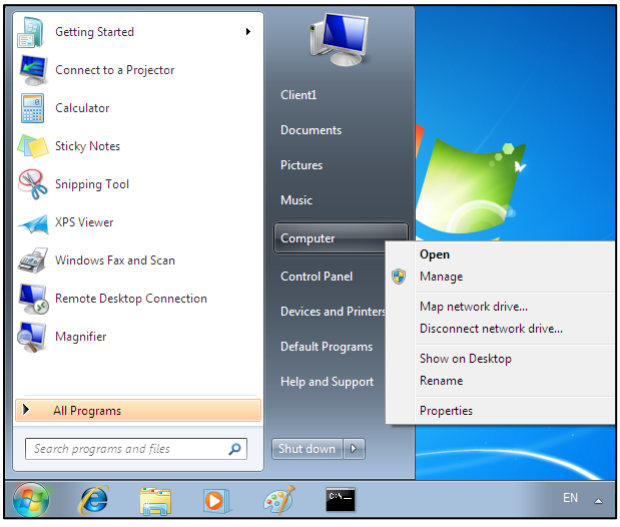
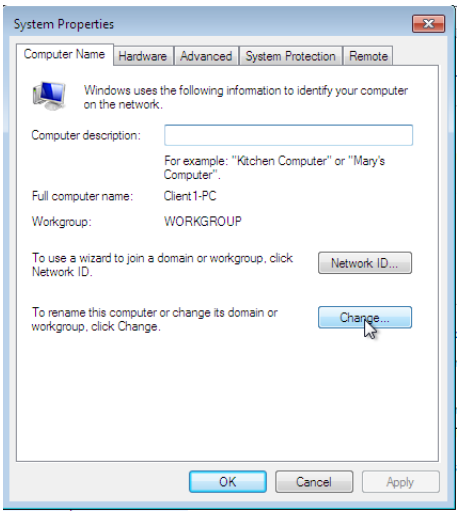


Figure B3.3 – System Properties



As shown in Figure B3.4, under **Member of**, select **Domain** and enter the domain name. If successful, you will be asked to enter login credentials to access the domain as per Figure B3.5 (the login credentials must be a domain administrator`s account). You should receive a welcome to the domain message as shown in Figure B3.6.

Figure B3.4 – Computer Domain Changes

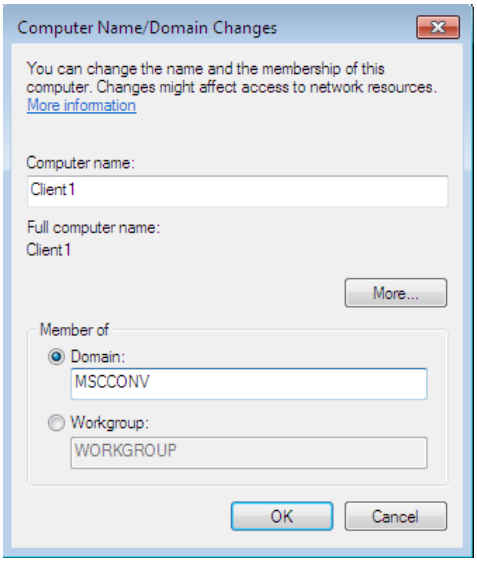


Figure B3.5 – Login Credentials

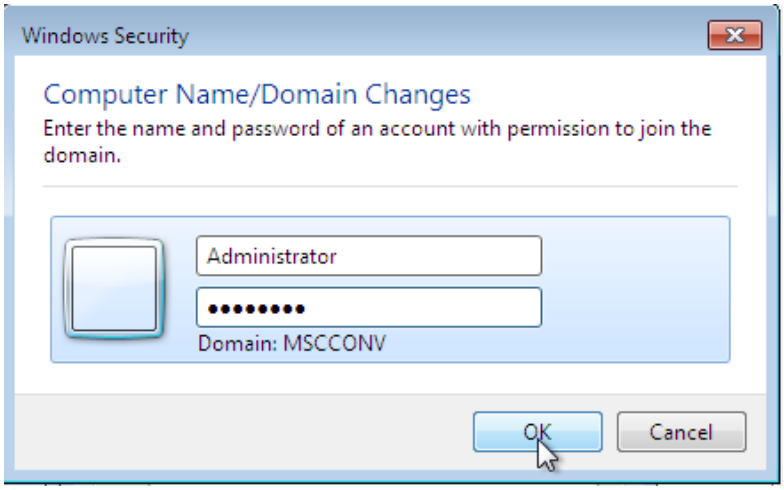
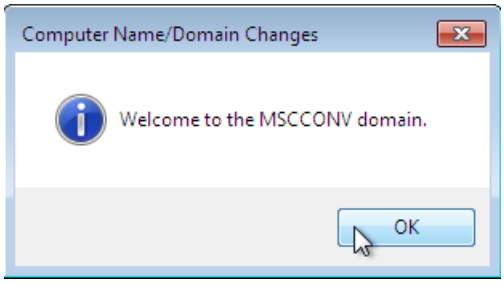


Figure B3.6 – Welcome to the domain



You will be notified regarding the need to restart the computer to apply changes. Click **OK.**

Another notification will ask you whether to **Restart Now** or **Restart Later**. Click **Restart Now** to continue.

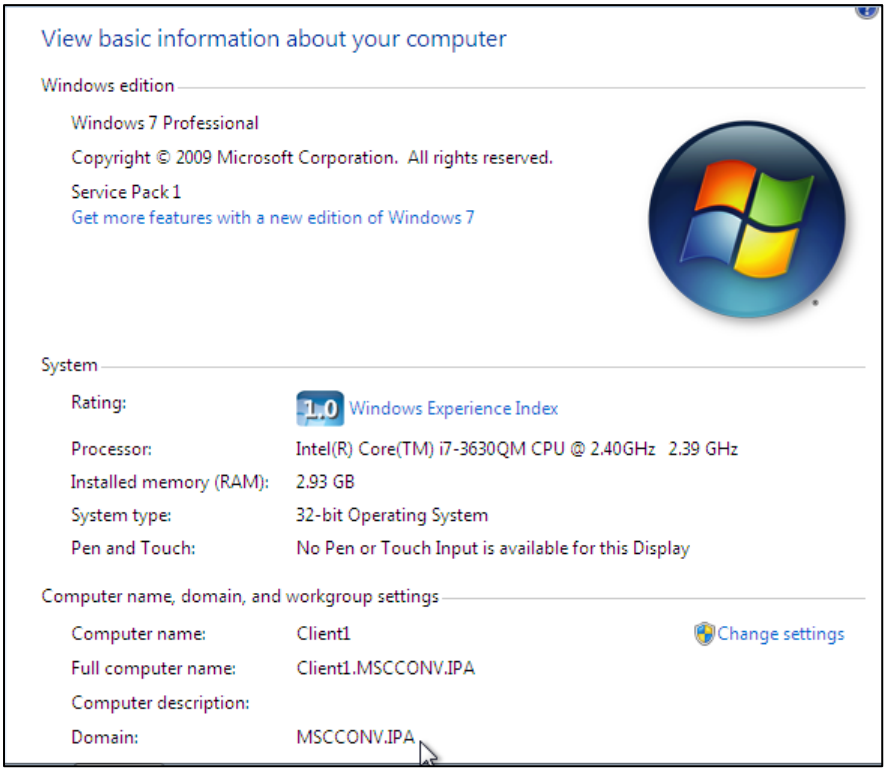
Upon reboot you may notice that the login options display the computer name as the login option (Figure B3.7). Instead, click **Switch User** to login using the active directory domain. Login as domain-name\username as shown in Figure B3.8.

Figure B3.7 – Initial Logon Option

Figure B3.8 – Domain Logon Option

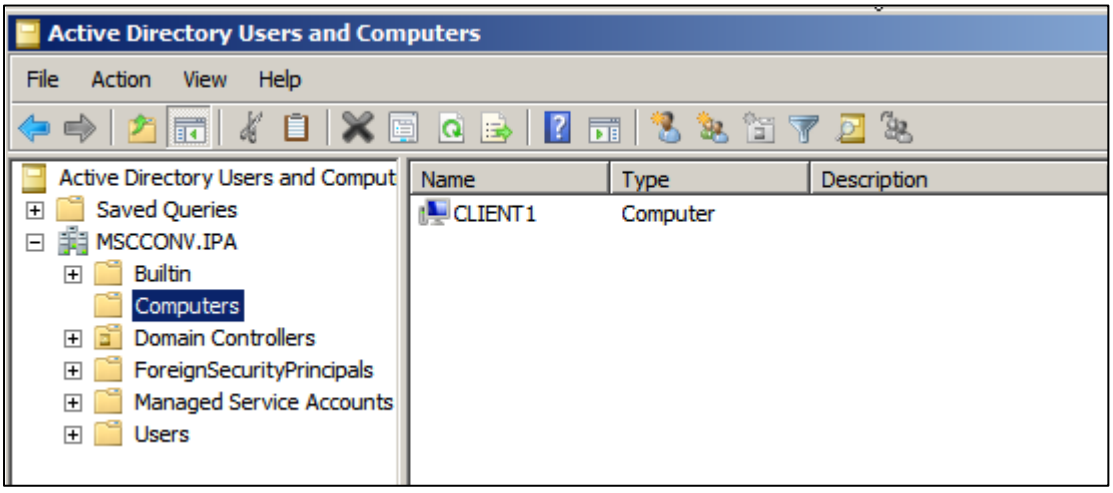
To verify that the computer has changed the domain you can check the **System Properties** on the client machine; noting the domain name under **Computer name, domain, and workgroup settings** as shown in Figure B3.9.

Figure B3.9 – System Properties domain changes



On the **Server1** machine, click **Start**, **All Programs**, **Administrative Tools**, **Active Directory Users and Computers**. In the left-hand navigation pane, expand **MSCCONV.IPA** (the domain tree) and click on **Computers**. You should see that the client computer is listed (as in Figure B3.10).

Figure B3.10 – Active Directory Users and Computers



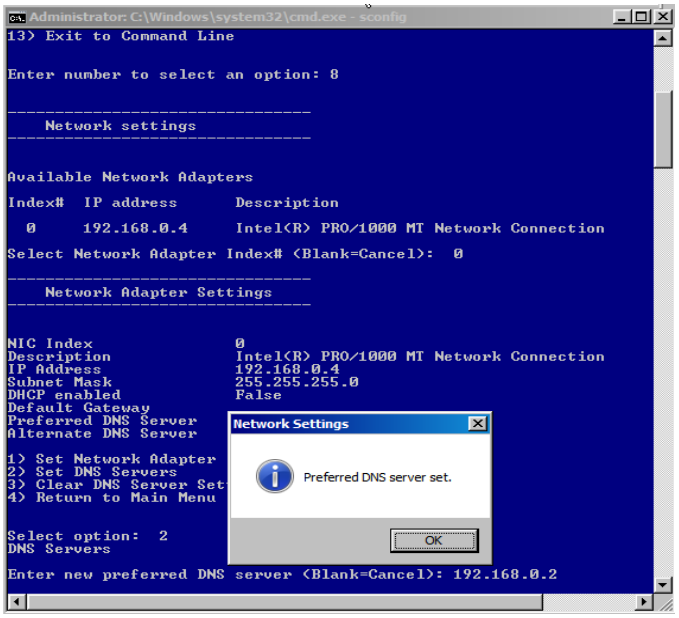
B4 - MS-Core Machine

As before, you need to set the DNS settings before joining the domain. Type **sconfig** in the command line and press **enter**. Type **8** and press **Enter** to proceed to the network settings.

You will then be asked to choose the network adapter you wish to modify.

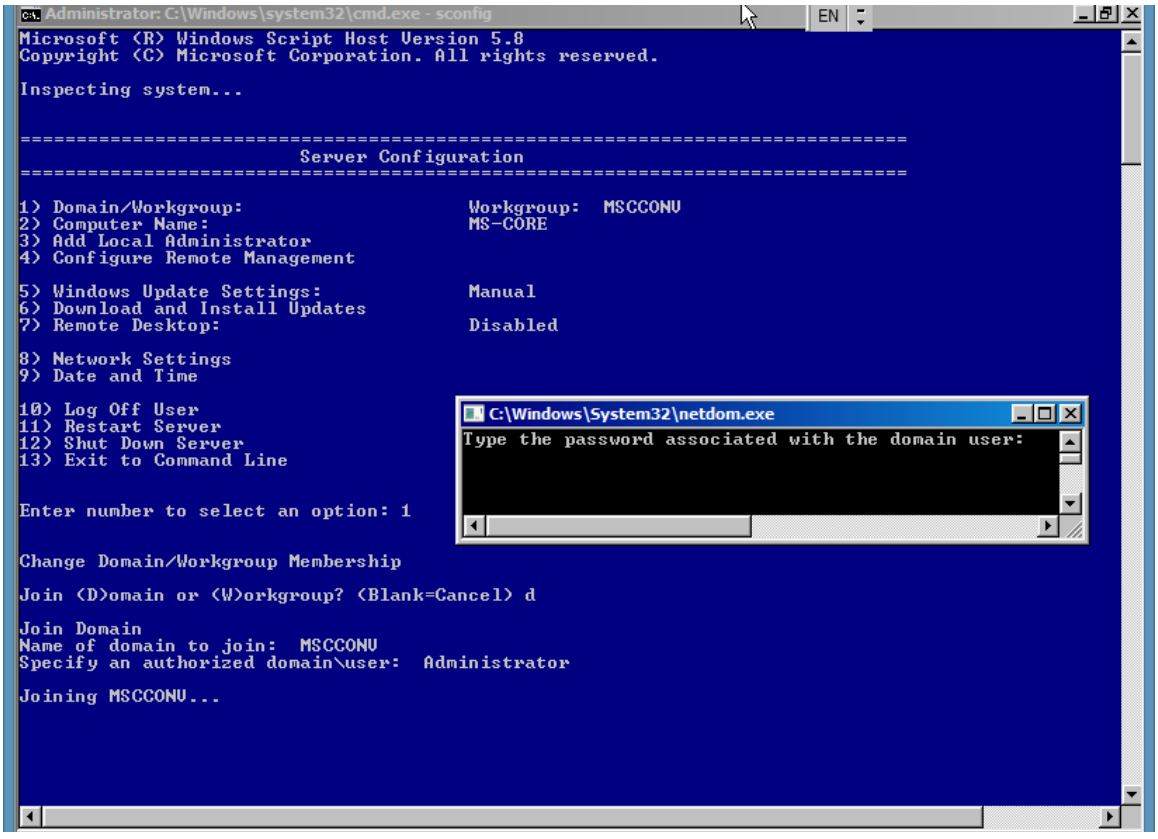
Type the index number of the relevant network adapter which will bring you to the **Network Adapter Settings** shown in Figure B4.1. Type **2** to set the DNS settings and enter the IP address of the main domain controller (**Server1**). A message should appear stating "***Preferred DNS server set***".

Figure B4.1 – Network Adapter Settings



To configure the domain, in the **Server Configuration** menu (Figure B4.1) type **1** and press **Enter**. You will be prompted to either change the domain or workgroup membership. Type **d** and press **Enter** to work with the domain. As illustrated in Figure B4.2, type the domain name and press **Enter**. You will be asked to specify a password associated with the domain user as shown. You will be prompted to restart the computer, press **Enter** to proceed.

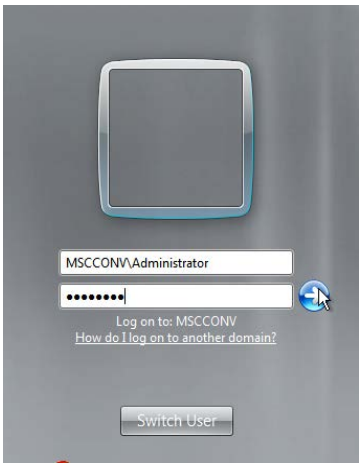
Figure B4.2 – Server Configuration



Upon reboot, the login screen will be similar to that shown in Figure B4.3, with the username preceded by the computer name. To login to the active directory domain click **Switch User**; this will bring you to the logon screen shown in Figure B4.4. In the username box type **domainname\username**; (i.e. MSCCONV\Administrator as shown), and also enter the user`s password credentials.

Figure B4.3 – Computer Logon

Figure B4.4 – Domain Logon



When logging on, you will notice in the command line that the domain name is appended to the username as shown in Figure B4.6.

Also, if you run **sconfig**, you will notice that the domain is listed opposite the first option, **Domain/Workgroup** (as shown in Figure B4.5).

Furthermore, on the server machine, click **Start**, **All Programs**, A**dministrative Tools**, **Active Directory Users and Computers**.

In the left-hand navigation pane, expand **MSCCONV.IPA** (the domain tree) and click on **Computers**. You should see that the MS-Core computer is listed (as in Figure B4.7).

Figure B4.5 – Domain Listed in Sconfig

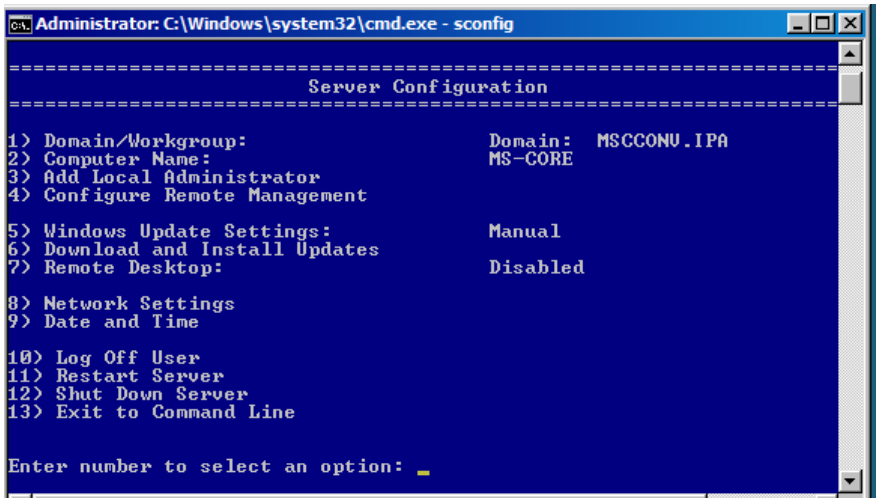


Figure B4.6 – Command Prompt

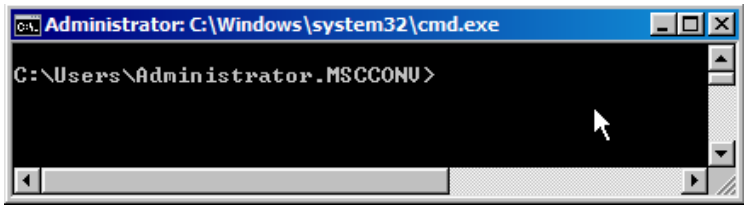
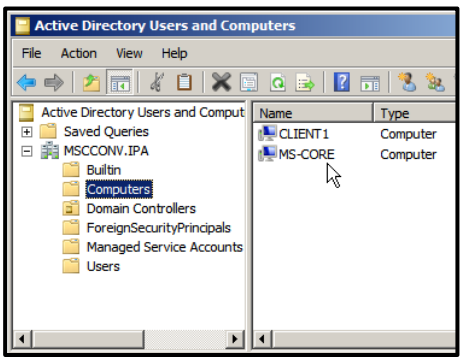


Figure B4.7 - ADUC



TASK C – HARD DRIVE CONFIGURATION

C0 - Task Introduction

In this section, you will carry out three main tasks:

1. **Install 2 additional 40GB hard disks on Server1**

The hard drive will be auto detected by the operating system. For further reading, Meyers (2012, pp.449-450) discusses auto detection in more detail.

---

2. **Mirror the operating system to Disk 1**

As outlined by Meyers, M. & Jernigan, S. (2013, p.935) disk mirroring is a "process by which data is written simultaneously to two or more disk drives". Read and write speed is consequently reduced. However, if one disk fails, the operating system still exists on the other disk. This is known as data redundancy, which is fundamental to keeping companies operating in the event of disk failure.

For further reading, a research paper by Google (2007) discusses in detail the various factors that lead to drive failure, such as age, workload and temperature.

After installing the drives, they will appear in the **Disk Management** console as offline, and with read-only attributes. Using the command prompt, the disks will be set online, and read-only attributes will be removed. Disk 1 will be converted from a basic disk to a dynamic disk as part of the mirroring process. Myers, M. & Jernigan, S. (2013, pp.195-197) discuss basic disk and dynamic disks in more detail.

---

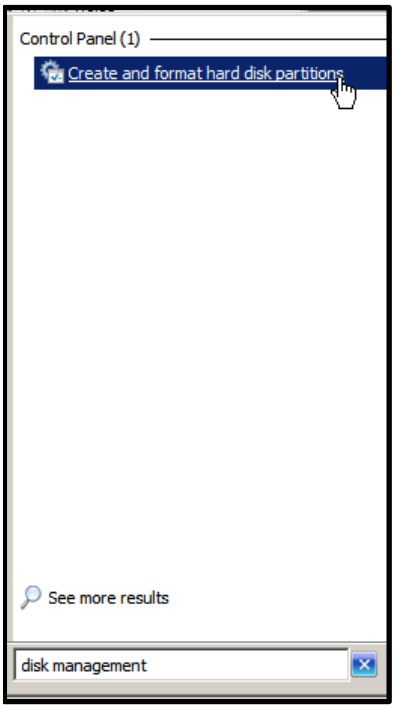
3. **Create a spanned volume across the three disks on Server1**

A spanned volume will be created using the remainder of the disk space on **Server1**. A spanned volume is a dynamic volume that incorporates free space from two or more dynamic hard disk drives. In Windows, you can create a single volume encompassing up to 32 different physical drives.

C1 - Mirror the operating system

To mirror the operating system onto the first of your newly installed drives, you can use the disk management console. Navigate here by typing **disk management** in the search bar and clicking the result as shown in Figure C1.1.

Figure C1.1 – Search Bar

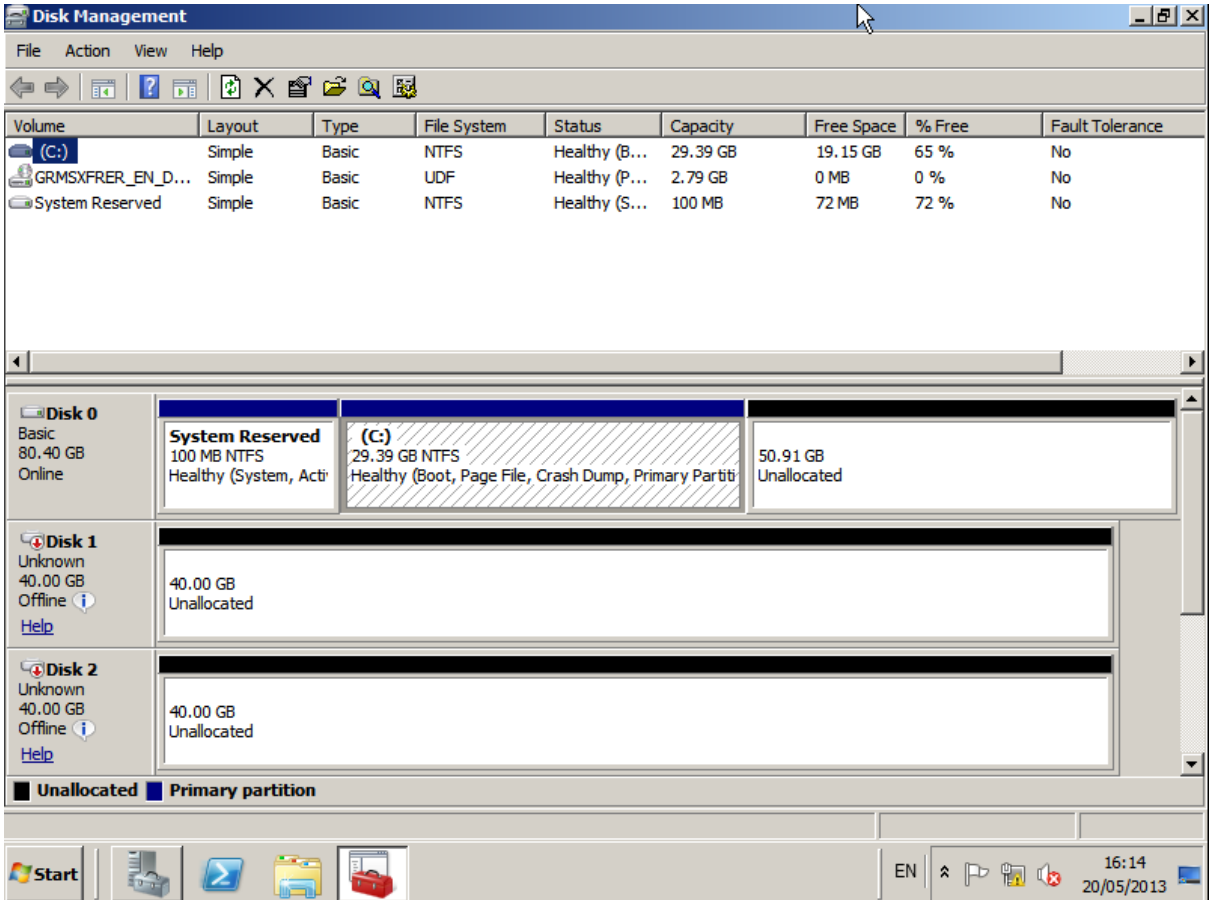


As shown in Figure C1.2, the disks are noted as being offline. You must set the disk(s) as online and you must also remove read-only attributes before the disks can be initialized and used for mirroring the operating system drive.

To do this, open your command prompt and type **diskpart** to access the disk management utility in the command prompt. You may use the **list disk** command as shown in Figure C1.3 to see the status of the currently installed disks. To work with a specific drive, use the **select disk number** command, where **number** represents the disk number; as illustrated in Figure C1.3 where disk 2 is worked on.

Use the command **online disk** to set the disk online. You may run **list disk** again to verify that the disk is now online as required. To remove read-only attributes from the disk, run the command **attributes disk clear readonly** as shown in Figure C1.4.

Figure C1.2 – Disk Management Console

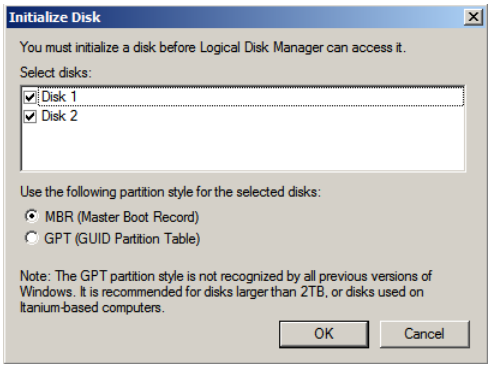


After the attributes have been cleared, restart the disk management console and a message will prompt you to initialize the disks, as shown in Figure C1.5. Click **OK** to proceed.

The differences between Master Boot Record (MBR) and GPT (GUID Partition Table) are useful to understand.

An article by Mackenzie-Low (2011) discusses the differences.

Figure C1.5 – Initialize Disk



Back in the GUI **disk management** utility right-click the drive with your operating system and click **Add Mirror** as shown in Figure C1.6.

You will be presented with the add mirror window shown in Figure C1.7; select **Disk 1** and click **Add Mirror** to proceed.

You may be warned that this operation converts the basic disk to a dynamic disk as shown in Figure C1.8; click **Yes** to continue.

Figure C1.3 – Setting Drives Online

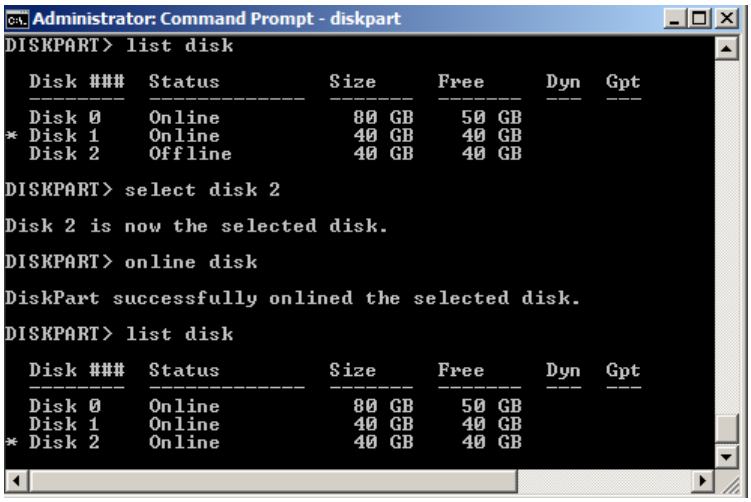


Figure C1.4 – Clear read-only attributes from drive

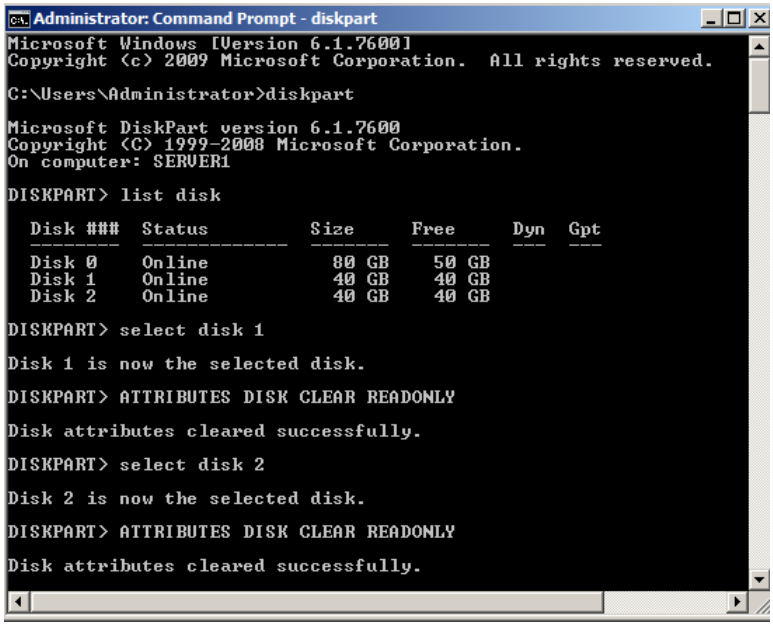


Figure C1.6 – Mirror your operating system drive

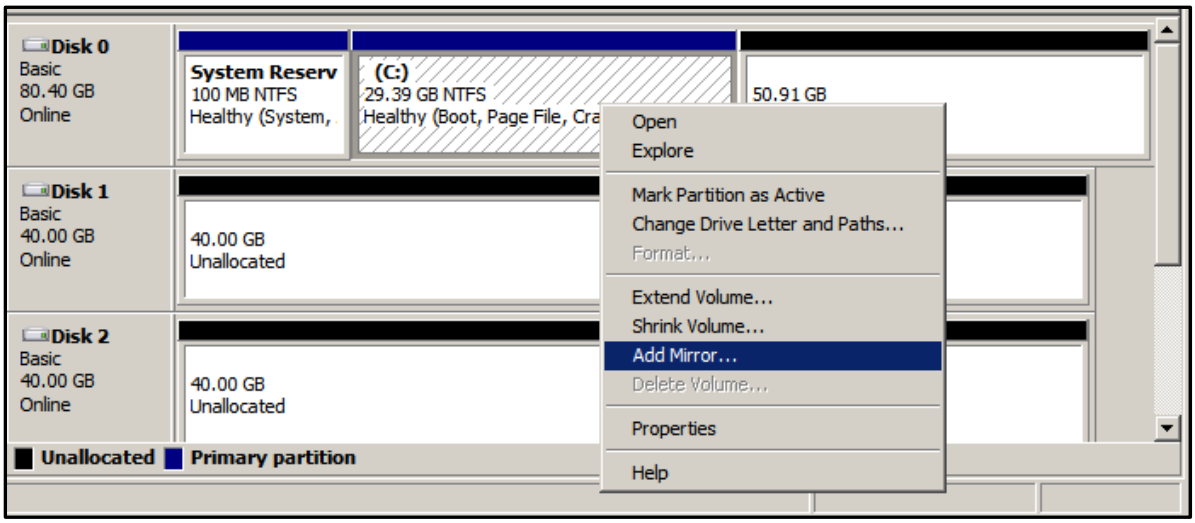


Figure C1.7 – Add Mirror

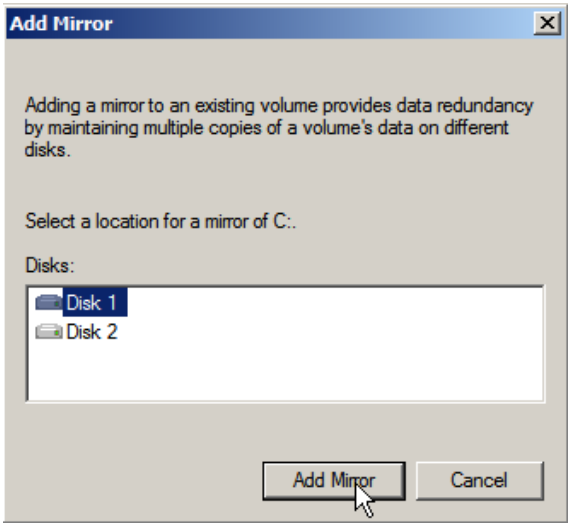
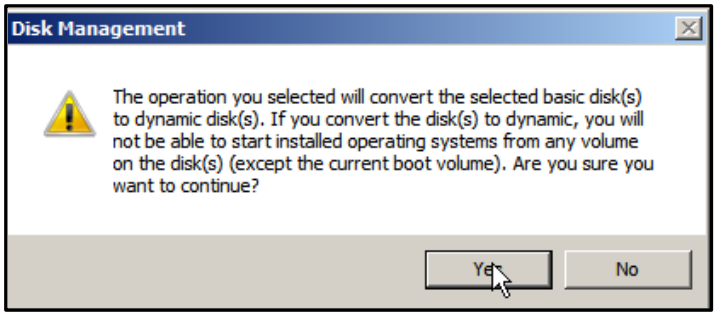


Figure C1.8 – Dynamic disk conversion warning



After the drive is finished "***Resynching***" (Figure C1.9) you will note that that the mirrored drive is marked as being healthy.

Figure C1.9 – Drive Resynching

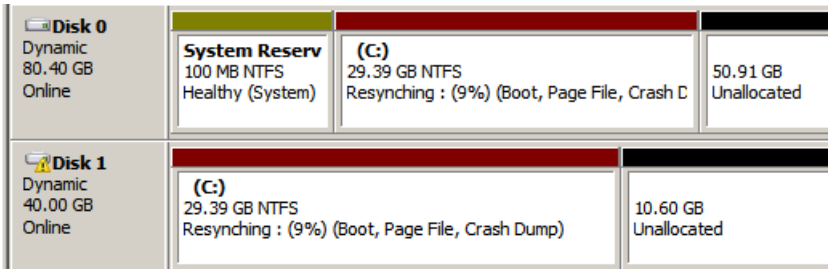
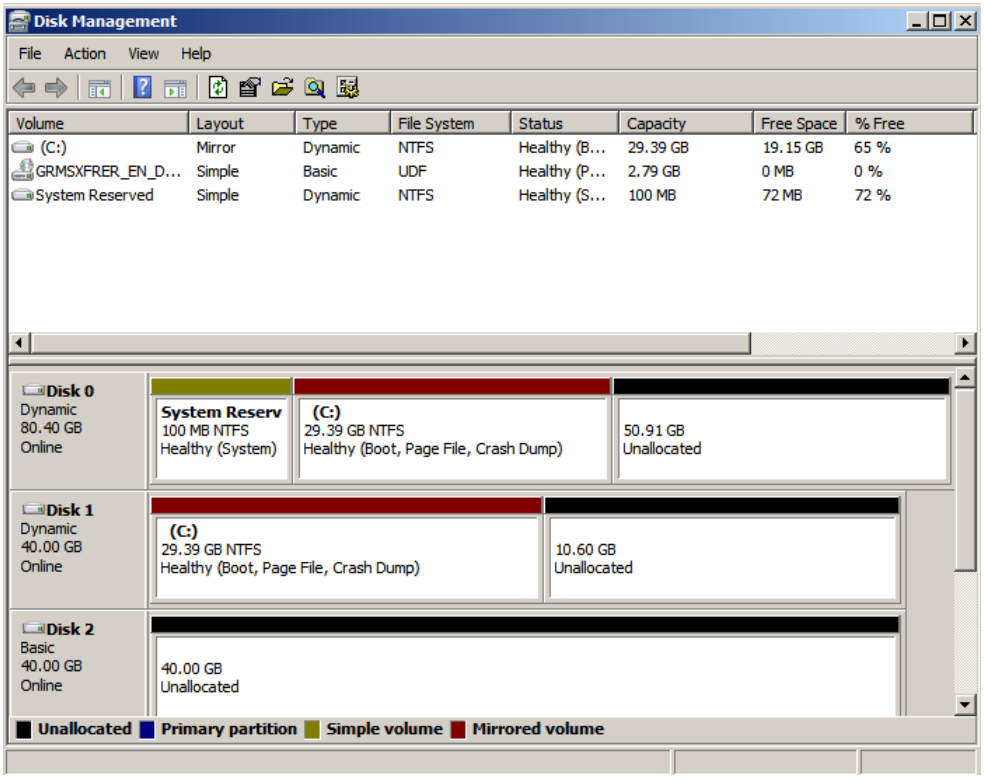


Figure C10 – Drive Mirroring Complete



INFORMATION

When restarting the machine, **Windows Boot Manager** will ask you to choose an operation to start:

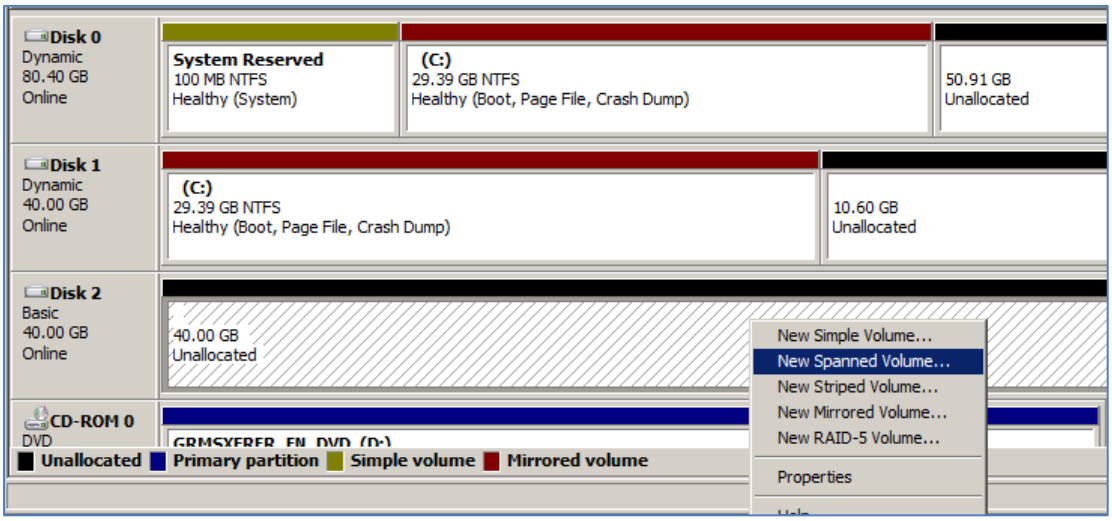
- Windows Server 2008 R2
- Windows Server 2008 R2 – secondary plex

The highlighted choice will be automatically selected after 30 seconds, or you may press **Enter** to proceed immediately.

C2 - Create a Spanned Volume

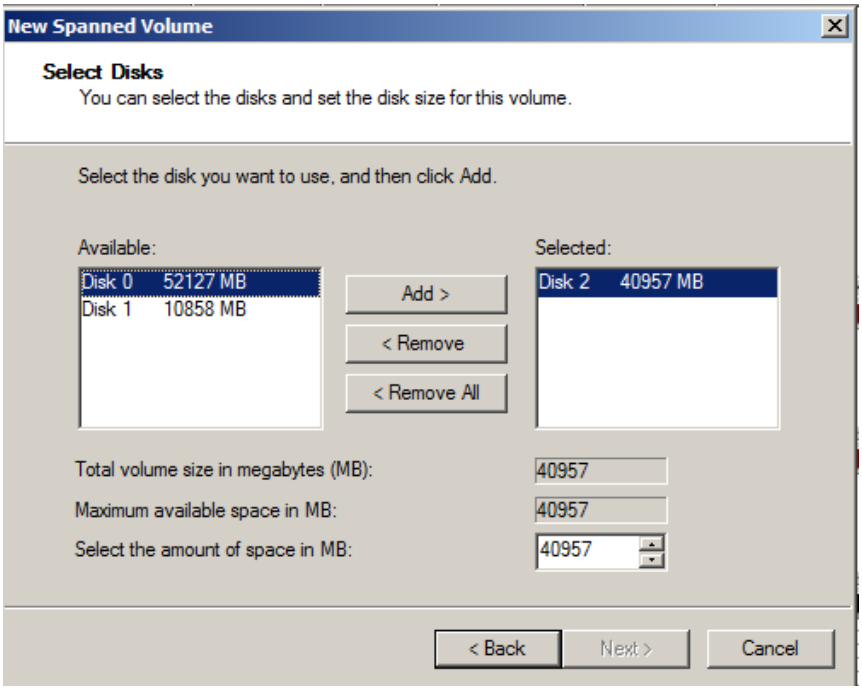
Navigate to the disk management utility by searching for "disk management" in the search bar. As illustrated in Figure C2.1 right click on the fully unallocated drive (disk 2) and click ***New Spanned Volume***. If you had attempted this on Disk 0 the option to click ***New Spanned Volume*** would not be available to you. You will be brought to the first screen for the **New Spanned Volume Wizard**. Click **Next** to proceed.

Figure C11 – New Spanned Volume



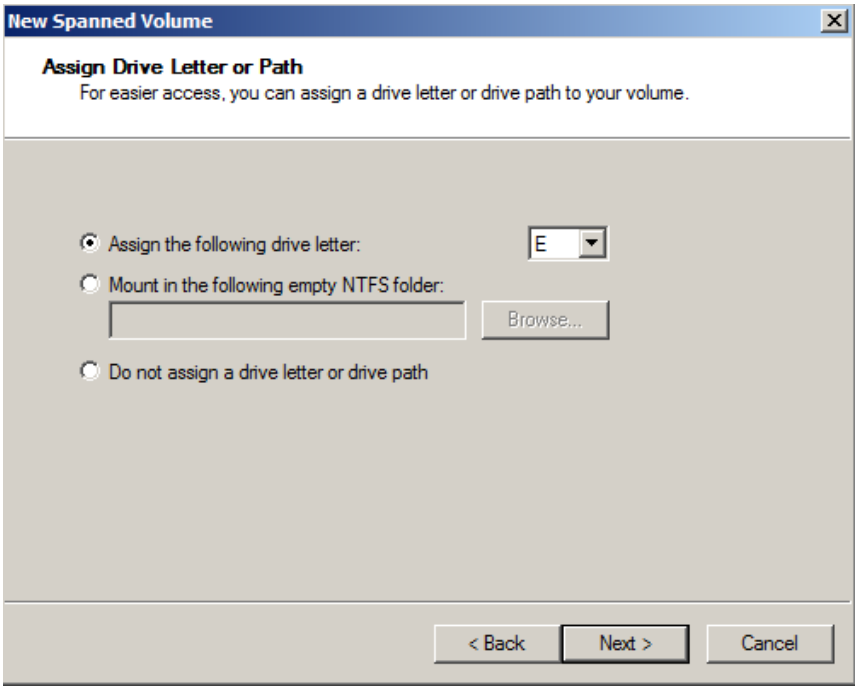
You will be asked to select the disks you wish to include in the spanned volume as shown in Figure C2.2. To using the remainder of the disks add each drive from the ***Available*** list to the ***Selected*** list. To do this, click and ensure the available disk is highlighted, and click **Add** which transfers that disk to the selected list. When your list is complete, click **Next** to continue.

Figure C2.2 – Select Disks



You will now be asked to assign a drive letter or path. In Figure C2.3 the default next available letter, E, is chosen. You can choose another letter if you wish by clicking the drop down list. Click **Next** when you are happy with the drive letter.

Figure C2.3 – Assign Drive Letter or Path



INFORMATION

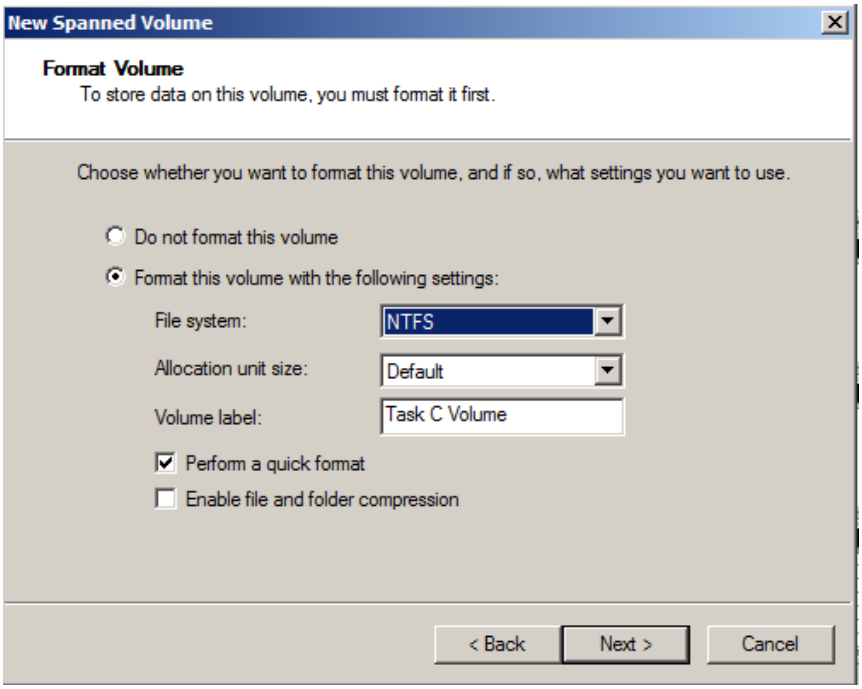
If your machine had numerous drives, you may wish to mount a drive in a folder to avoid confusion in the **Computer** window.

Or you may require the installation of more than 26 drives (There is a 26 drive letter limitation).

The folder will be located on another drive, and is assigned a drive path to the actual hard drive.

The next window in the wizard is the **Format Volume** wizard. In Figure C2.4, the default options are selected, with the exception of the **Volume Label** which has been renamed. Click **Next** and you will be brought to summary window of the wizard as shown in Figure C2.5.

Figure C2.4 – Format Volume



INFORMATION

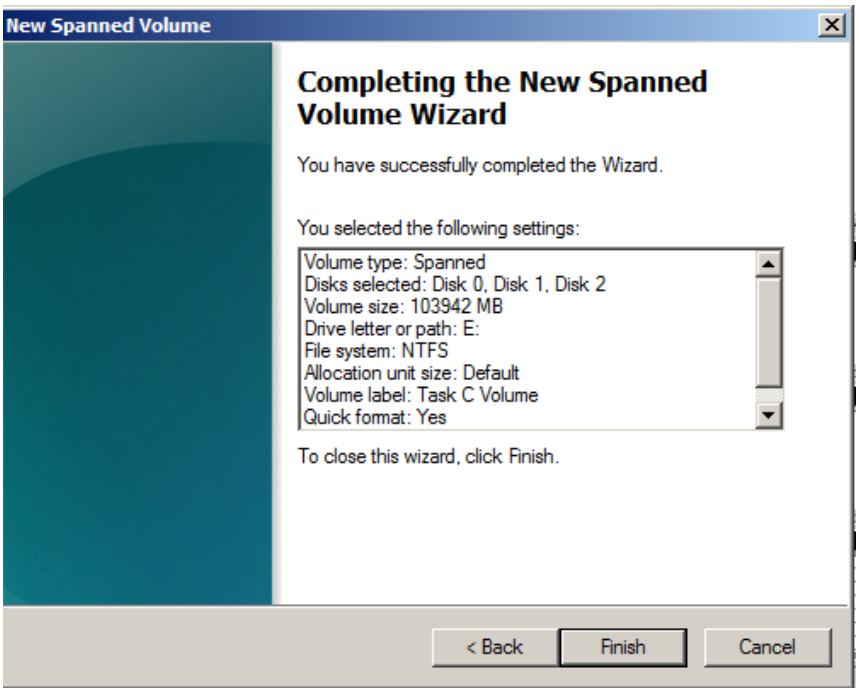
The **Volume Label** text box allows you to give a meaningful label to a drive.

It is displayed in **Computer** as a prefix to the drive letter instead of the default **"Local Disk"**.

In this scenario, it is fine to leave the **Allocation Unit Size** as **Default.** However, as discussed by Vanover (2010), the unit size is more important when dealing with large volumes.

You could enable file and folder compression if disk space is low, however this may impact on performance.

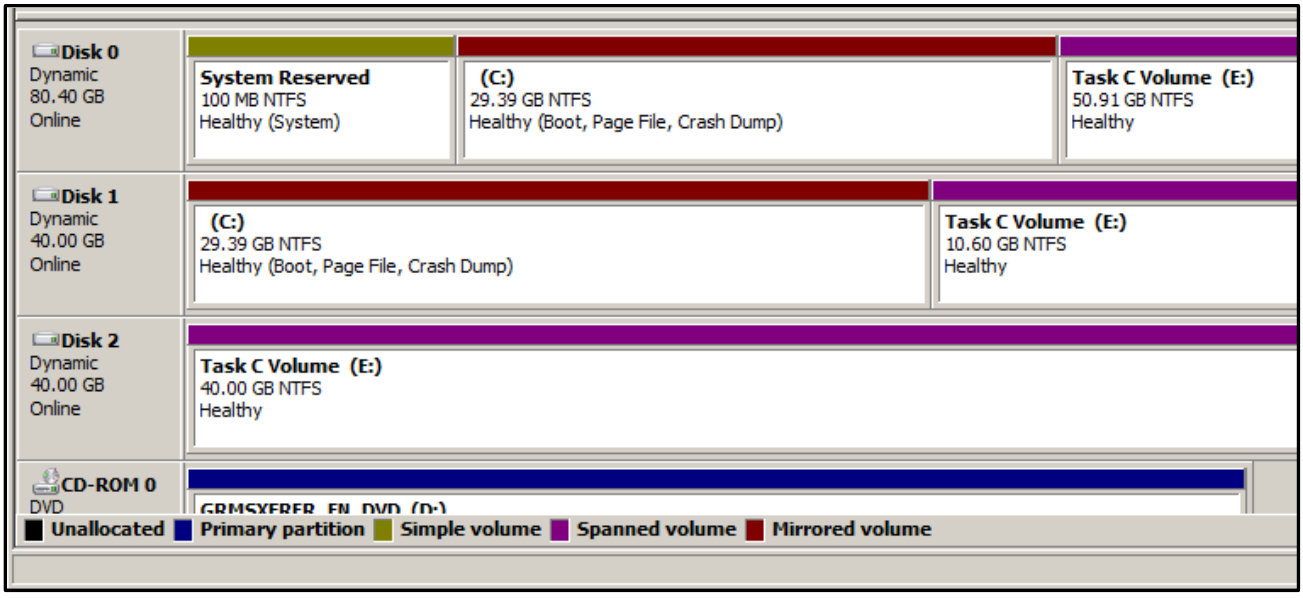
Figure C2.5 – Wizard Summary



If you are satisfied with the wizard`s summary of drive implementation options, click **Finish** to proceed. You may receive a warning that a basic disk will be converted to a dynamic disk, this is normal; click **Yes** to proceed.

In disk management, you should notice a healthy drive noted, and colour coordinated, as shown in Figure C2.6.

Figure C2.6 – Disk Management – Spanned Drives Implemented



TASK D – ORGANIZATIONAL UNIT STRUCTURE

D0 - Task Introduction

In this task users are created within Organizational Units (OUs). The purpose of an OU is to consolidate objects (users, computers, groups etc.) in Active Directory. Any objects can be located in an OU to make them simpler to manage. OUs are typically created to match the departmental structure of on organization, or to group users with analogous responsibilities.

In this task, in Section D2, it is demonstrated how to create users using Active Directory Users and Computers (ADUC). This method is fine for a relatively low number of users.

If you must create a large number of users, you will require a more productive method. In Section D2a, it is demonstrated how to create users using a PowerShell command in conjunction with a comma-separate value (CSV) file created in Microsoft Excel.

The logon hours for users are also restricted, with users being able to log on from Monday to Friday only (24 hours per day).

D1 - Creating Organisation Unit

To create an organisational unit (OU), navigate to the **Active Directory Users and Computers** utility. As shown in Figure D1.1, right-click the root domain you wish to work with, select **New** and **Organizational Unit**. You will be asked to name the OU as shown in Figure D1.2. Click **OK** when you have named the OU.

Figure D1.1 – Create New OU

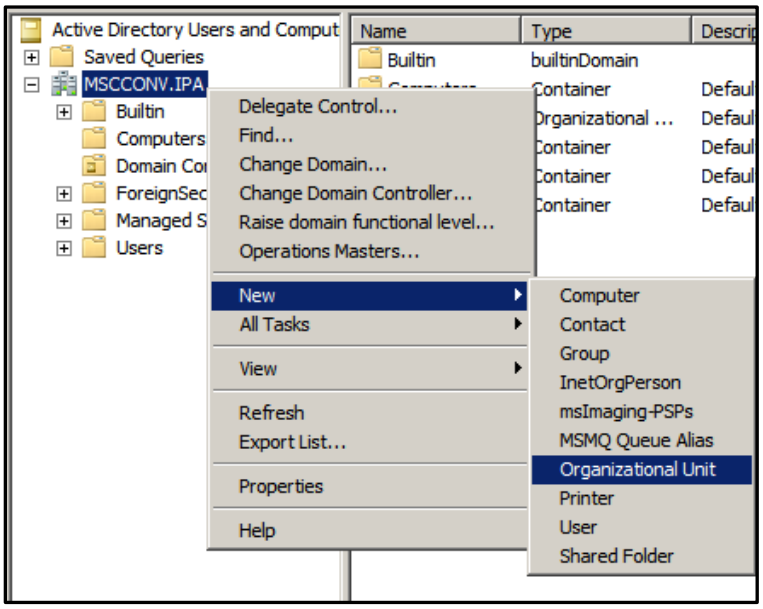
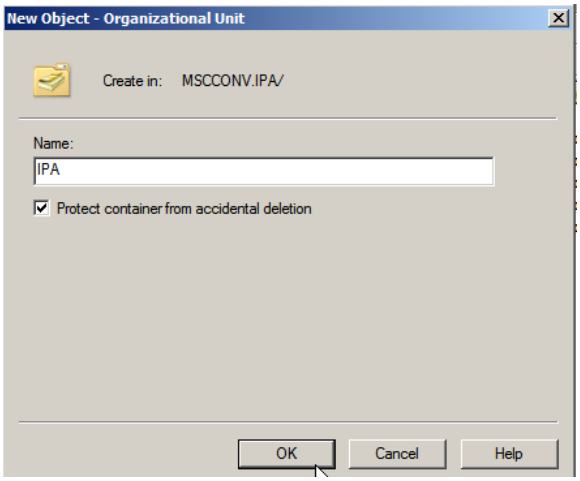


Figure D1.2 – Name the OU



The option "***Prevent container from accidental deletion***" ensures that if the administrator wishes to delete the OU, they must first remove the protection from accidental deletion and then complete the removal.

As shown in Figure D1.3, under the root domain you will notice the newly created OU, namely ***IPA*** in this example. This is a parent OU; to create a child OU right-click ***IPA*** select **New** and **Organizational Unit**.

Repeat this process until you have the desired organisational unit structure, as shown in Figure D1.4.

Figure D1.3 – OU Created

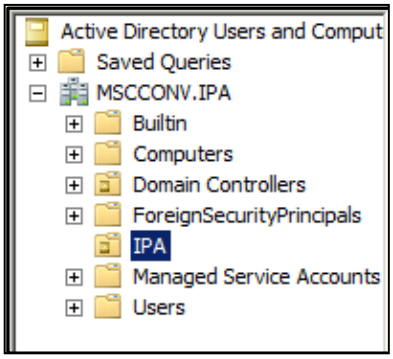
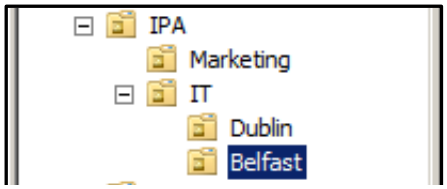


Figure D1.4 – Sub OUs Created



INFORMATION

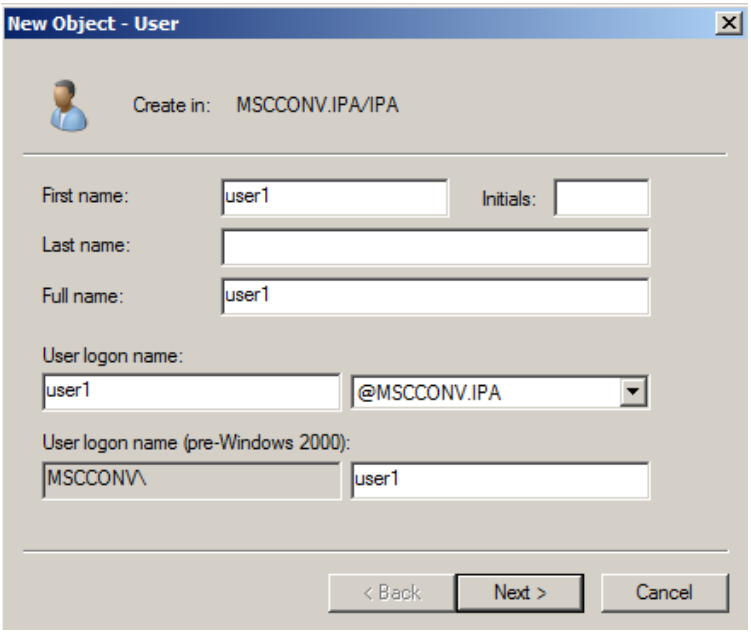
If you wished to delete an OU, you first need to disable the protection from accidental deletion. Right-click the OU, select **Properties** and click the **Object** tab. Ensure the box beside **Protect object from accidental deletion** is unchecked. Click **Apply** and **OK**.

For further information on the prevention of accidental deletion, an article by O Neill (2007) is comprehensive.

D2 - Creating New Users

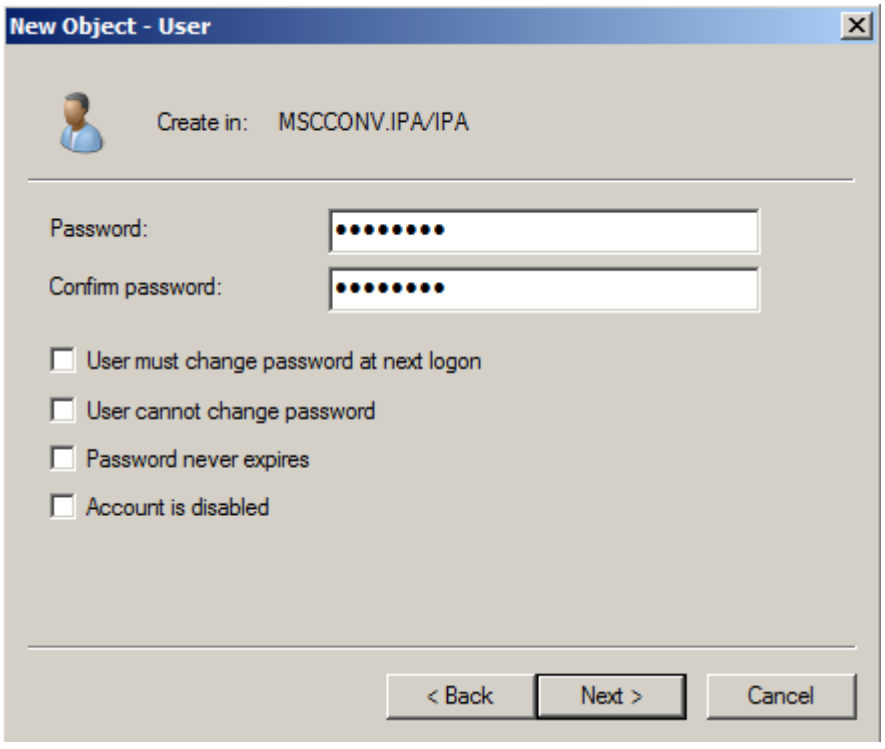
To create a new user, right-click on the OU you wish to create users within, and click **New User**. You will be brought to the **New Object – User** wizard shown in Figure D2.1. Enter the required details and click **Next** to proceed.

Figure D2.1 – New User



You will now be asked to enter password credentials as shown in Figure D2.2. Click **Next** to proceed.

Figure D2.2 – Password



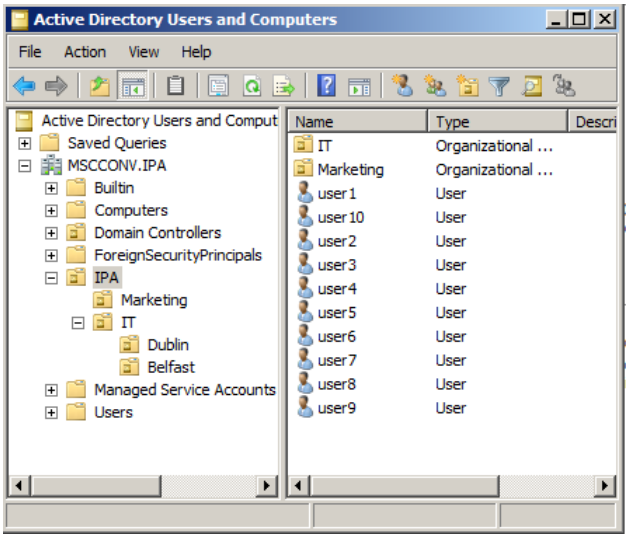
INFORMATION

Basic password settings are available as shown in Figure D2.2.

In Task E, fine grained password policies (PSO) will be implemented. A PSO allows you to assign multiple password policies on different OUs, and is more powerful that the options provided in Figure D2.2.

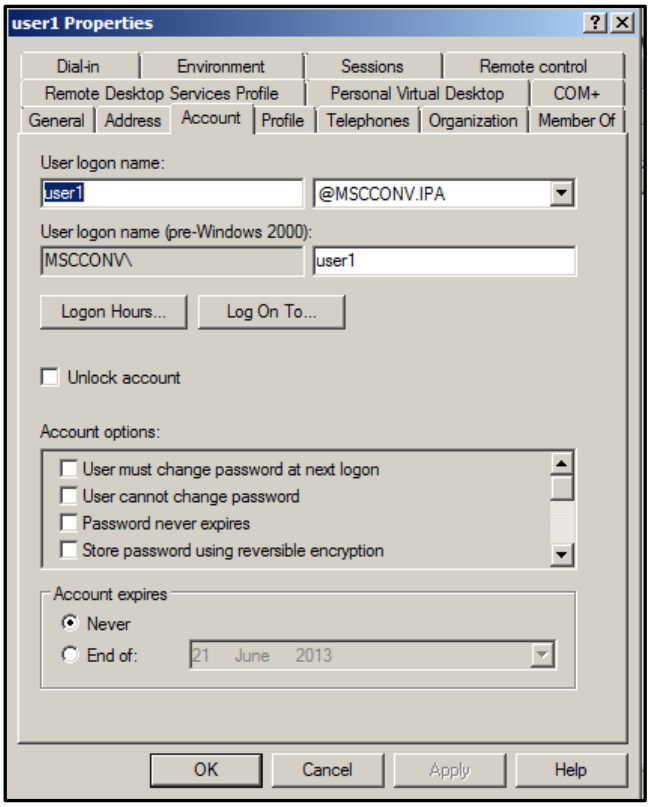
The next screen will provide you with a summary of the users to be created. If you are satisfied with the summary, click **Finish** to create the user. Upon creating the users they will be listed within the OU as shown in Figure D2.3.

Figure D2.3 – Users Created



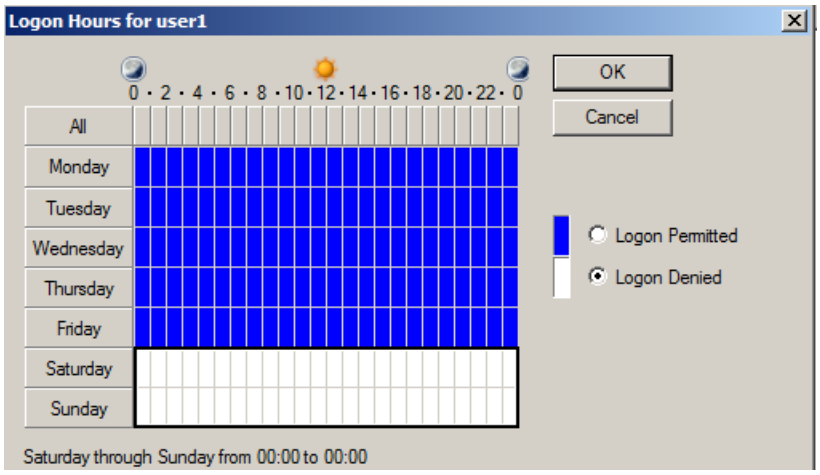
By right-clicking the user and selecting **Properties**, you can specify a wide range of properties for each user. To specify user login hours, select the **Account** tab and select **Logon Hours** as shown in Figure D2.4.

Figure D2.4 – User Properties



You will be brought to the **Logon Hours** utility shown in Figure D2.5. Click and drag across the days/hours you wish to alter and click **Logon** denied to disable access for those time periods.

Figure D2.5 – Logon Hours



Click **OK** to implement the changes. You also must ensure you click **Apply** in the main **Properties** menu.

Figure D2.6 – Ensure you click Apply

When creating users, it is productive to specify the logon hours after creating the first user if all the users have the same logon time restrictions.

When creating the second user, right-click the first user and click **Copy**. This means that you do not have to specify the particular logon hours for each user. You can always alter a particular users properties at any time.

D2a – Alternative Method of creating users

If your company had a significant amount of users, it would be tedious and unproductive to use **Active Directory Users and Computers** to create each user. A better solution would be to create a comma-separated value (CSV) file using Microsoft Excel. As shown below in Figure D2a.1, the first row contains value descriptions and the following rows contain the values that describe the user.

To demonstrate the exercise, a full clone was taken of the **Server1** virtual machine used when creating this manual. Using this clone, the users 1 - 10 were created in the IPA OU, with an "a" appended i.e. user1a, user2a etc.

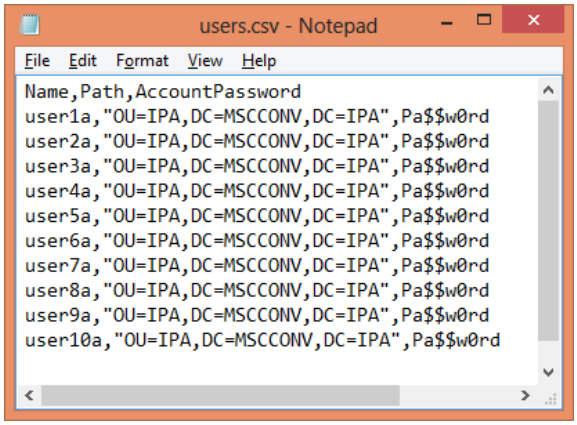
Create an Excel file named **users.csv** on a machine that has Excel installed. Transfer the file to the root of the C Drive on **Server1**. When saving the file, you have to choose **CSV (Comma delimited) (*.csv)** in the drop down list beside **Save as Type**. After clicking **Save**, you may be notified that the file type does not support workbooks that contain multiple sheets, click **OK** to proceed. You will also be notified that some features are not compatible with CSV (such as formatting), click **Yes** to continue.

Figure D2a.1 shows the information created in this CSV file. Figure D2a.2 shows the file opened with Notepad.

Figure D2a.1 – Users.csv

	A	B	C
1	**Name**	**Path**	**AccountPassword**
2	user1a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd
3	user2a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd
4	user3a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd
5	user4a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd
6	user5a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd
7	user6a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd
8	user7a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd
9	user8a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd
10	user9a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd
11	user10a	OU=IPA,DC=MSCCONV,DC=IPA	Pa$$w0rd

Figure D2a.2 – Users.csv in Notepad



Open the **Active Directory Module for Windows PowerShell** (ADMWP) by searching for it as shown in Figure D2a.3. Enter the command below into the ADMWP utility as shown in Figure D2a.4. The resulting users created are shown in Figure D2a.5 in Active Directory Users and Computers.

CMD

```
Import-CSV c:\users.csv | foreach {New-ADUser –Name $_.Name –Path $_.Path –AccountPassword
(ConvertTo-SecureString –AsPlainText $_.AccountPassword –Force) -Enabled $true –
ChangePasswordAtlogon 0}
```

- **IMPORT-CSV:** This lightweight command (cmdlet) reads in the users.csv file. The **|** symbol is known as the pipe, the vertical bar on the keyboard which feeds the CSV file into the next portion of the command.
- **FOREACH:** This cmdlet runs a task using each of the rows (10 users) as a parameter.
- **NEW-ADUser:** This cmdlet creates a new user. **$_.Path** refers to the **Path** header created in the CSV file. The values in the rows under the **Path** header will be substituted for **$_.Path**.
- The password is converted to a secure string and is enabled. The password does not have to be set at logon as **ChangePasswordAtlogon** is given the Boolean value of 0 (false).

Minasi, Gibson, Finn, Henry and Hynes (2010, pp.346-348), discuss the details of this PowerShell command in more detail.

Figure D2a.4 – PowerShell Command

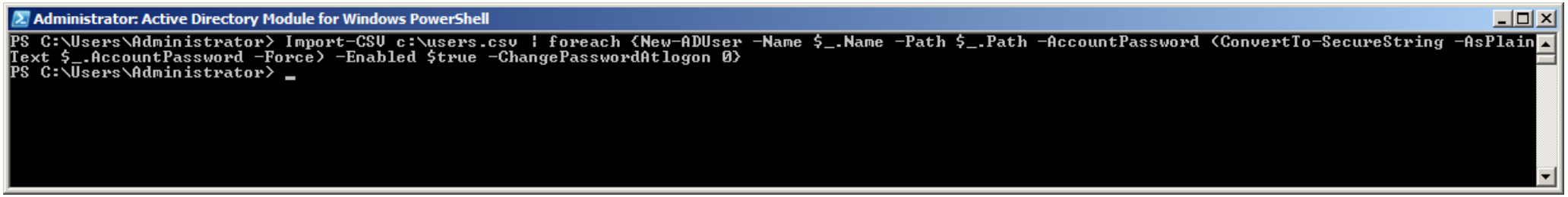


Figure D2a.5 – Users Created after PowerShell Command

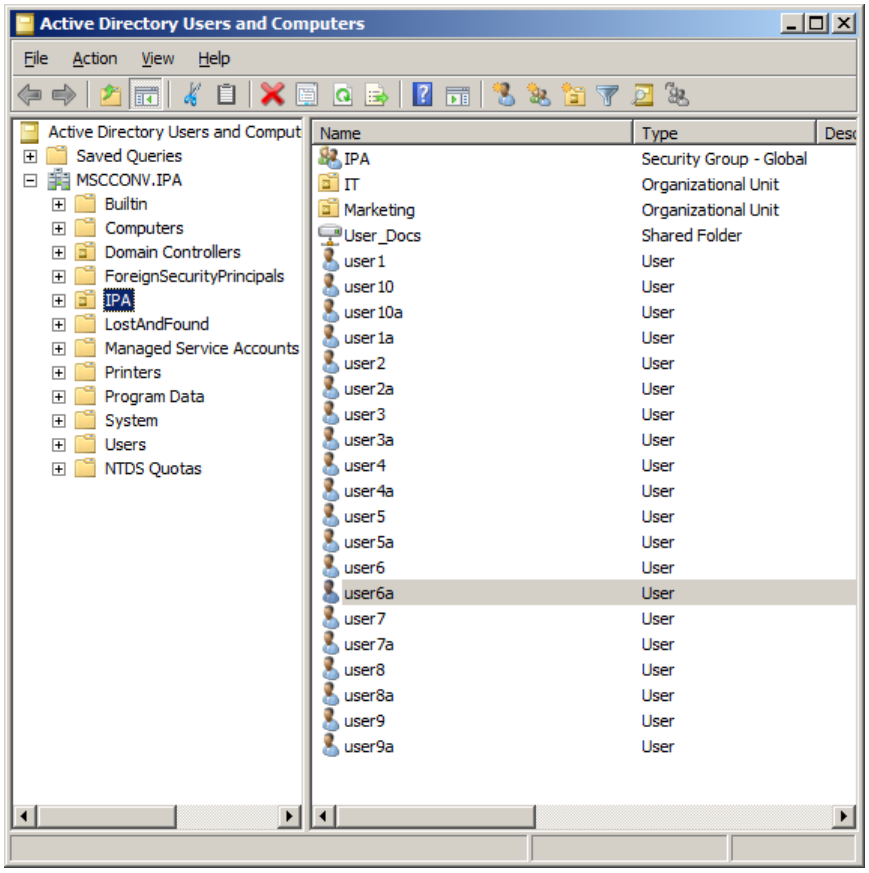
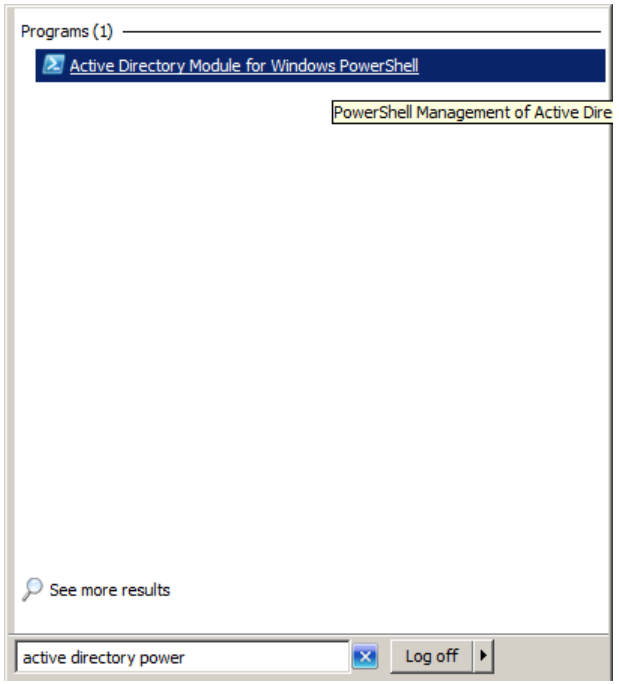


Figure D2a.3 – Searching for ADMWP



TASK E – GROUPING, PERMISSIONS AND GROUP POLICES

E0 - Task Introduction

In this section, you will carry out the following tasks:

1. **Group the users in each Organizational Unit (OU) according to the recommended Microsoft security requirements and hierarchy.**

In Task D, users were created and organized into Organizational Units (OUs). In order to apply permissions to objects within the OU in a productive manner, the objects must be organized into groups. Otherwise you would have to deal with each object at a time, which is highly unproductive. Permissions and Group Policy Objects will be applied to groups later in this section.

Password Settings Objects (PSOs) will also be introduced in this section.

---

2. **Prevent the users in the Marketing OU from having the ability of seeing the IT OU in Active Directory**

This task will be carried out by applying NTFS permissions to the IT Organizational Unit. The Marketing group will be added and denied Full control. Users in the Marketing group will not be able to see the IT OU in **Active Directory Users and Computers** whilst logged onto their account on the Windows 7 Client machine.

---

3. **Group Policy Object (GPO) to forward documents**

A folder is created on the root of the C drive on **Server1.** This folder is shared on the network. A shared folder is created in the IPA OU in Active Directory Users and Computer (ADUC). A group policy object (GPO) is created and edited in the Group Policy Management Editor (GPME) where documents are set to be redirected (to the folder previously created).

Using the **Security Filtering** option, the **Client1** machine is included in the GPO.

---

4. **GPO to prevent access to the Control Panel**

Using the **Prohibit access to the Control Panel** setting in GPME, access is blocked by adding the Belfast group and the **Client1** machine to the security filtering. Using the **Delegation** tab in the setting allows you to add a deny permission for user20, which means that user20 will still be able to access the Control Panel. User19 will not be able to access the panel, nor will any new users created within the Belfast group.

---

5. **GPO to publish a MSI (Windows Installation) file.**

An MSI file is an installation package consisting of installation information and the actual installation files. Publishing an MSI file across the server streamlines the process of providing the ability to install software in a desktop environment.

As completed for the first task in this section, the MSI installation file is located in a folder which is shared on the network. A shared folder is created with ADUC in the Dublin OU.

A GPO is created, linked to the Dublin OU and edited in GPME where a **Software Installation** setting allows you to create a **Package** whereby you specify the path to the installation file. When logging on as a user in the Dublin OU you will have the option of installation the file from the Control Panel. Other users will not have this option.

E1 - Grouping Users

In **Active Directory Users and Computers**, right-click the OU that you wish to group users in, select **New** and **Group** as shown in Figure E1.1.

Give the group a name, assign it a ***Global*** scope and a ***Security*** Group type as shown in Figure E1.2.

Figure E1.1 – Create a Group

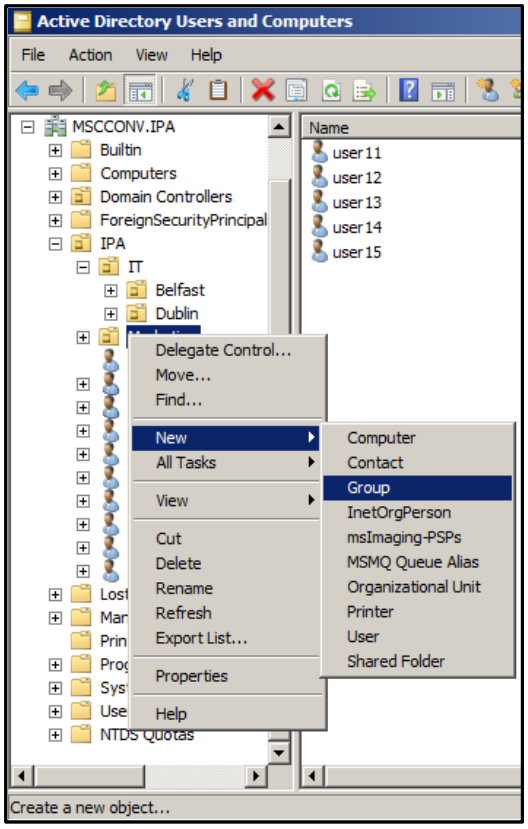
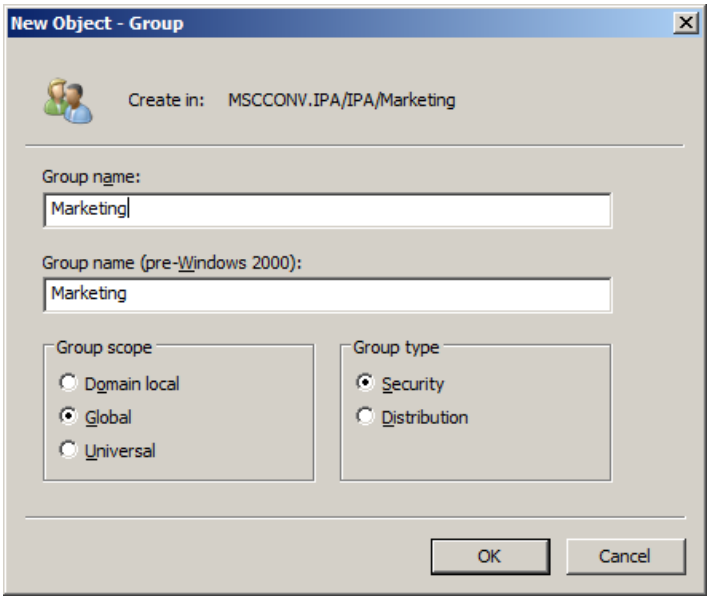
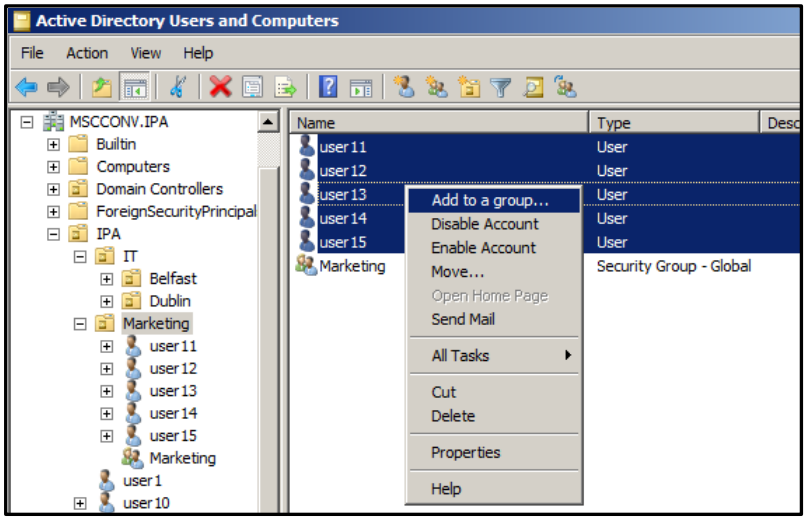


Figure E1.2 – Group Properties



To add users to the group that you created, highlight the relevant users, right-click and select **Add to a group** as shown in Figure E1.3.

Figure E1.3 – Adding users to group created



The **Select Groups** window will appear as shown in Figure E1.4. Under **Enter the object names to select** click in the whitespace and type the name of the group you wish to add the users to. Click **Check Names**.

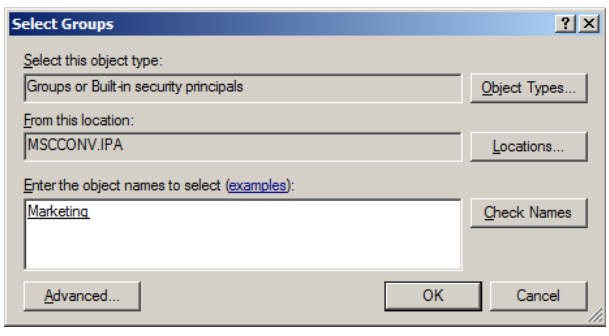
If you have entered the group name correctly it will appear underlined; click **OK** to continue.

When this is complete, check that all users have been added to the group successfully. Right-click the relevant group and click **Properties**.

Select the **Members** tab and note the name of the users listed as being part of the group (as shown in Figure E1.5).

Note that you can also add or remove users from this location. The numerous tabs also provide many group configuration options.

Figure E1.4 – Select Groups



Repeat the aforementioned steps to assign users to their groups. You can also assign groups to a group, as shown in Figure E7.

Simply right-click the group and click **Add to a group**; the steps are the same as adding a user to a group.

Figure E1.7 – IT Properties

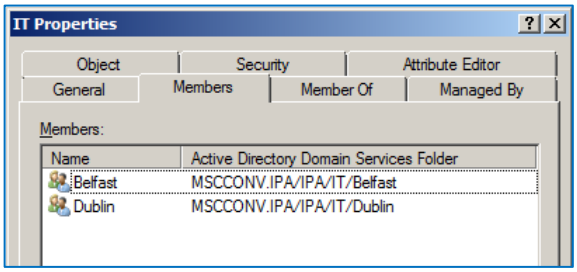


Figure E1.6 shows the initial OU,users, and groups structure, whereby a group was created within each OU. The groups created (security groups) allow the assignment of permissions to objects within that group.

A salient point is made by Holme, Ruest, Ruest & Kellington (2011, p.68) when they argue that "*It is best practice to manage objects in groups rather than to manage each object individually*".

Furthermore, McLean & Thomas (2008, p.145) discuss how "*Microsoft applies GPOs to groups rather than OUs because groups offer better flexibility for managing various sets of users*".

Figure E1.7 shows the final users and groups structure. This includes additional groups to match a more complex organizational structure. The group structure is shown in Figure E1.8 overleaf.

Subgroups are created. For example, within the IPA, groups are created for Accounting, Administration, and Human Resources.

Figure E1.5 – Checking users listed in Group

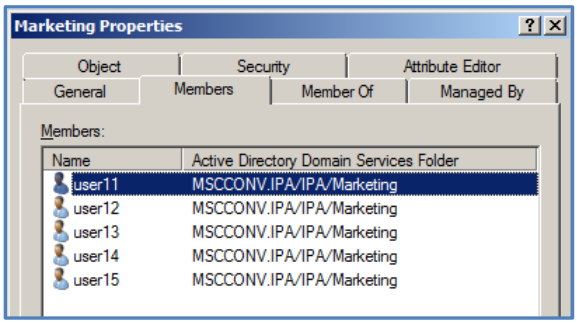


Figure E1.6 – Users and Groups

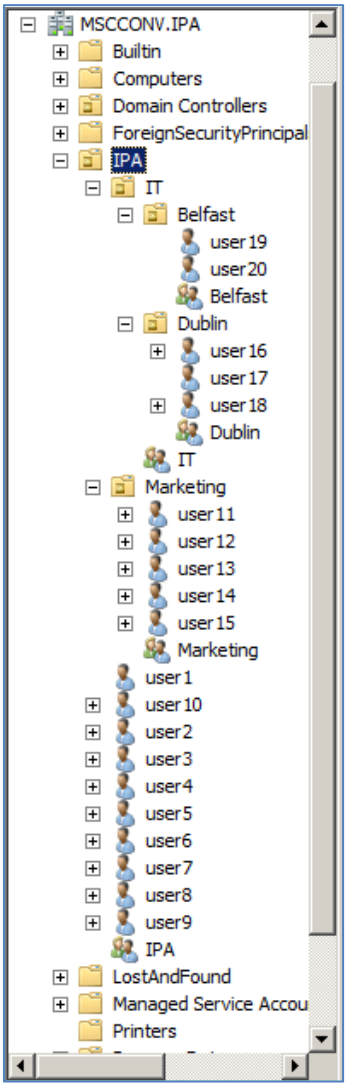
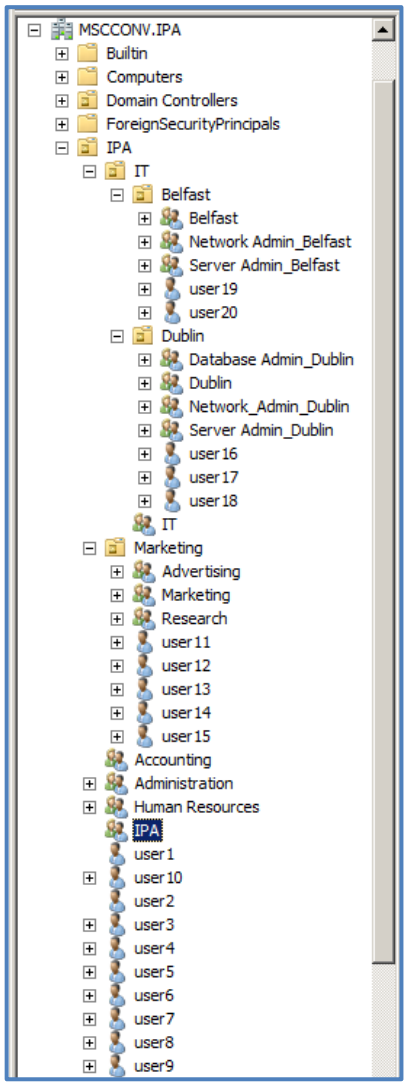


Figure E1.7 – Users and Groups

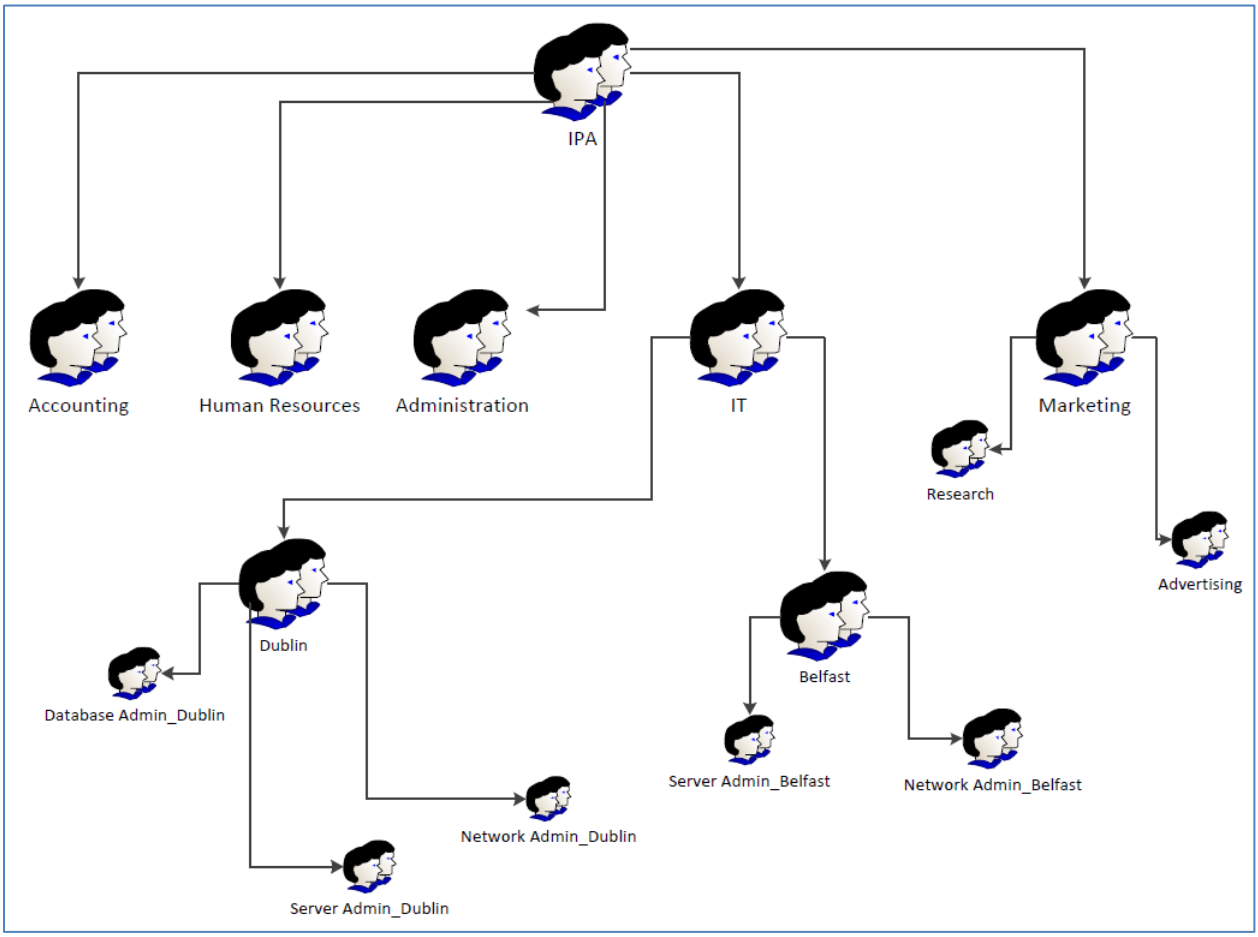


This means that different permissions can be applied to each group, as it is unlikely that the Accounting department require access to the same resources as the Human Resources department, and vice-versa.

If you wished to apply security settings to users across the domain, irrespective of which OU/Group/Department they are a member of, you could apply a principle known as Group Nesting. Imagine that you want permissions to be applied to a printer. A global group (GG) is created in the domain and users are added to this domain. A domain local group (DLG) is created for the printer and the GG is added to this DLG.

The users in the GG receive the permissions assigned to the DLG as the GG is a member of the DLG.

Figure E1.8 – Groups Structure

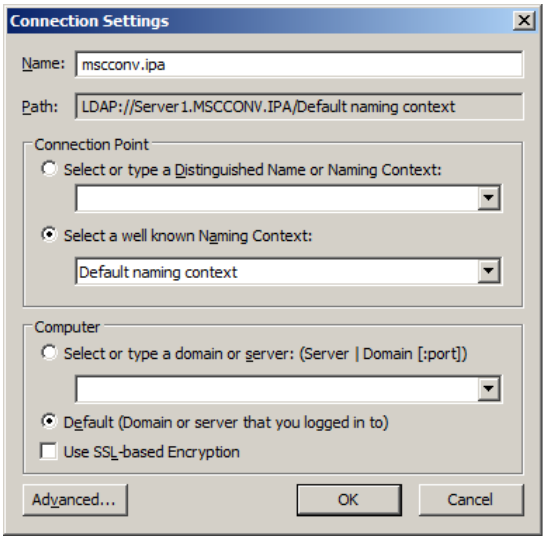


Password policies (PSO) should also be put in place as recommended by security principles. These can be implemented by using ***fine-grained password policies*** using Active Directory® Service Interfaces Editor (ADSI Edit).

ADSI Edit can be launched by typing ***ADSI*** in the search bar and pressing **Enter**. Right-click ***ADSI Edit*** in the left-hand pane and click **Connect to**. As shown in Figure E1.9 enter the fully qualified domain name in the ***Names*** box. Click **OK** to return to the main ***ADSI EDIT*** screen.

As shown in Figure E1.10, expand the list and right-click **CN=Password Settings Container**. Click **New**, and **Object.** You will be asked to select a class, **msDSPasswordSettings** will be the only available option. Click **Next** to proceed. On the next screen give the object a meaningful name (IPA_PSO), and click **Next** to proceed, as shown in Figure E1.11.

Figure E1.9 – PSO connection settings



Stanek (2008, p.1177) discusses PSO precedence in detail, and is a recommended read for a full understanding on how objects with multiple PSOs assigned to them are dealt with.

Figure E1.10 – ADSI EDIT, Create new POS Object

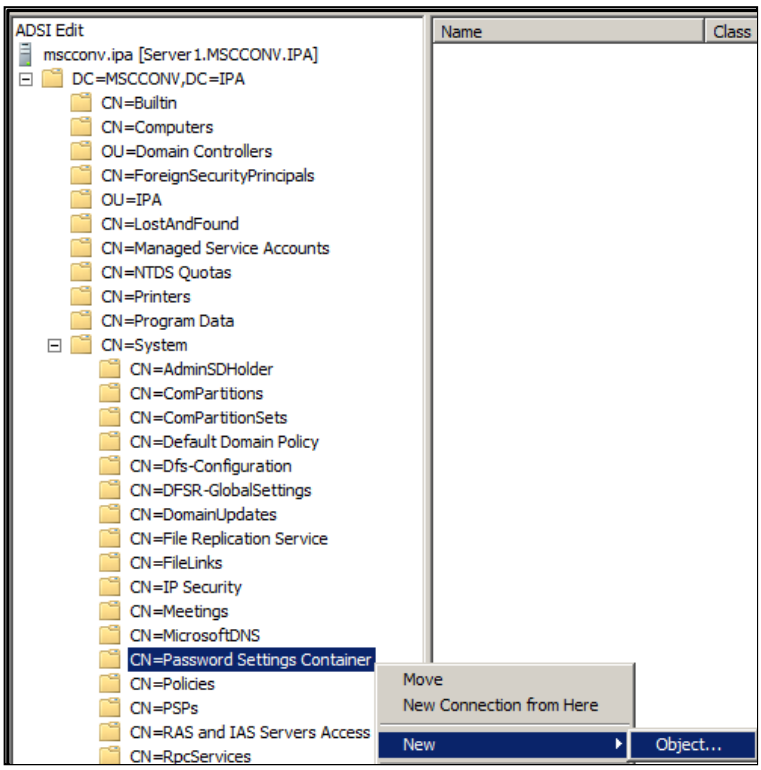


Figure E1.11 – PSO Common-Name

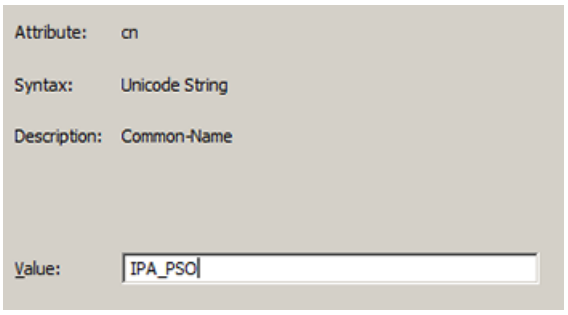
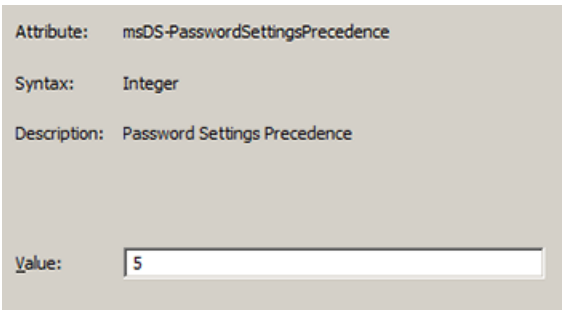


Figure E1.12 – PSO Password Settings Precedence



As shown in Figure E1.12, assign a precedence value to the object; a lower value results in a higher precedence. As per Figure E1.13 you have the option of enabling reversible encryption; this goes against all security recommendations therefore enter **false**.

The next option (Figure E1.14) configures the password history length. This identifies the number of new passwords that must be used before you may use the first password again.

Figure E1.13 – PSO Reversible Encryption

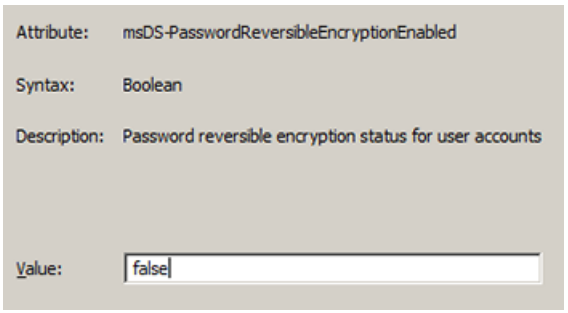
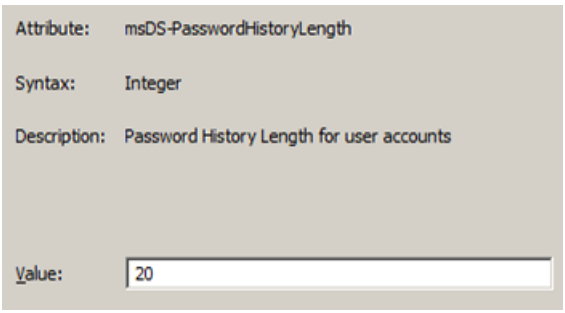


Figure E1.14 – PSO Password History Length



Next, you must state whether passwords should meet complexity requirements (Figure E1.15). Enter **True** to enable this requirement. The next setting is the minimum password length (Figure E1.16); the maximum length being 255.

Figure E1.15 – PSO Password Complexity

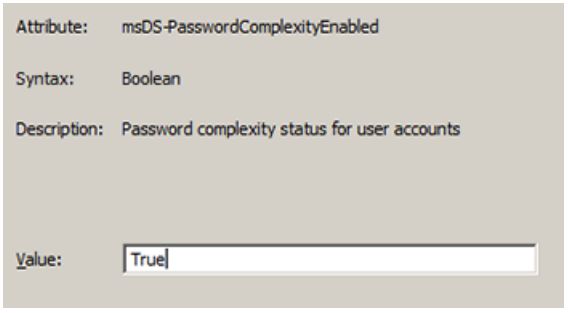
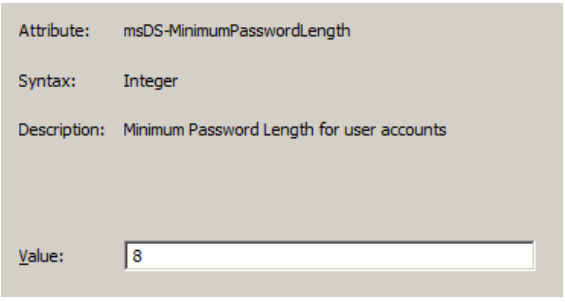


Figure E1.16 – PSO Minimum Password Length



The minimum password age must now be specified, the time specified is the earliest time that a password can be modified after creation; in Figure E1.17 the minimum password age is specified as being 1 day.

The next window specifies the maximum password age i.e. the time after which users must change their passwords. As per Figure E1.18, 31 days is specified as the maximum password age.

Figure E1.17 – PSO Minimum Password Age

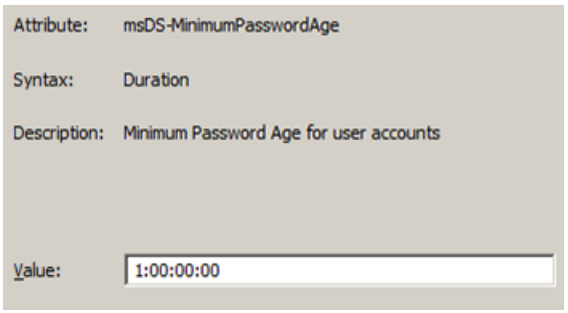
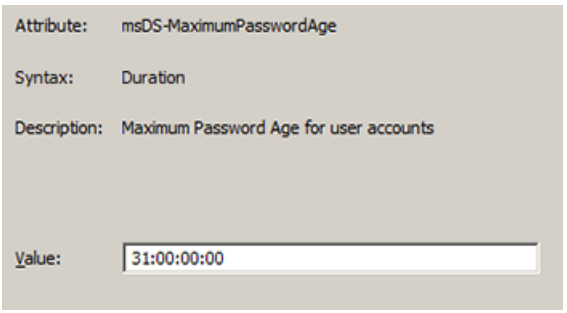


Figure E1.18 – PSO Maximum Password Age



The ***lockout threshold*** is specified as 6 in Figure E1.19; this means that 6 bad password attempts are accepted before the account is locked out. In Figure E1.20, the ***lockout observation window*** is set at 40 minutes. Therefore, in the given scenario the user could specify 5 incorrect passwords, leave the computer for 41 minutes, and then attempt more passwords since the counter would be reset to zero.

Figure E1.19 – PSO Lockout Threshold

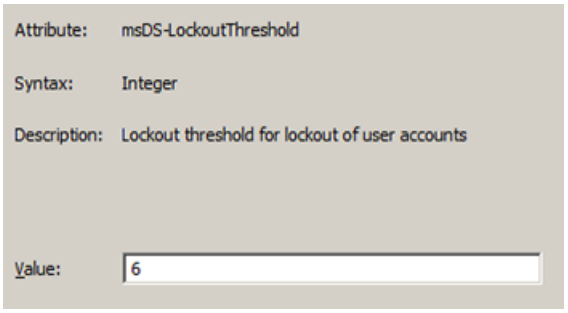
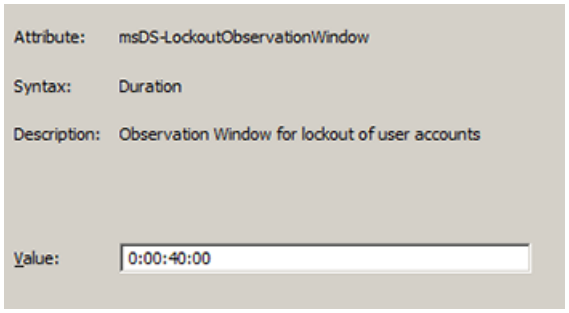


Figure E1.20 – PSO Lockout Observation Window



The lockout duration is specified as 40 minutes as illustrated in Figure E1.21. The user will be locked out of the account for 40 minutes if the lockout threshold is exceeded. In the Final **Create Object** window, as shown in Figure E1.22, click **More Attributes**. **Do Not** click Finish.

Figure E1.21 – PSO Lockout Duration

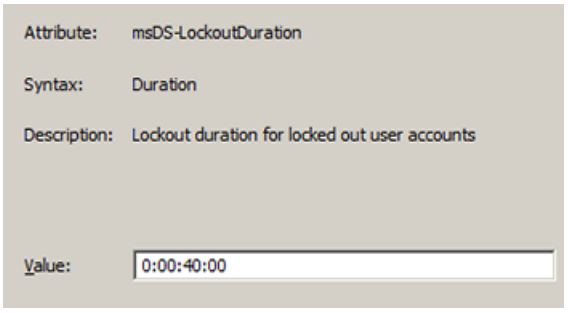
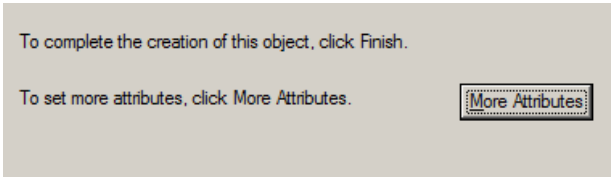


Figure E1.22 – PSO Specify More Attributes

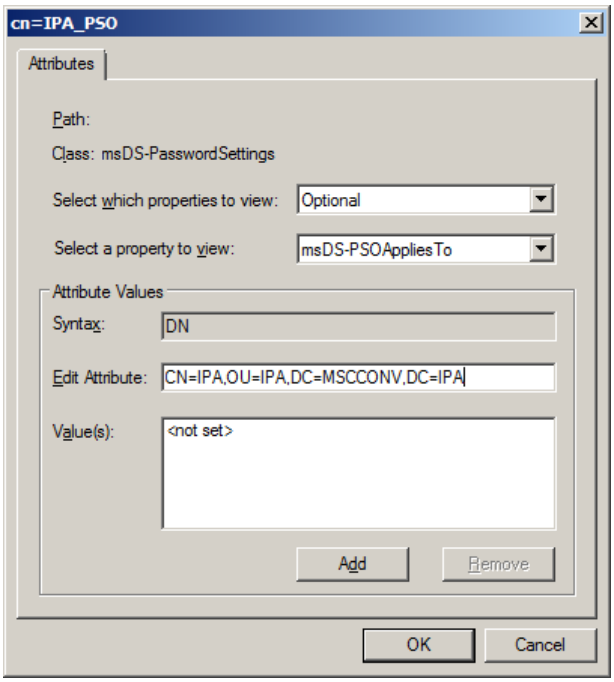


As shown in Figure E1.23, ensure that **msDS-PSOAppliesTo** is selected in the drop down list beside **Select a property to view**.

Enter the distinguished name (DN) of the group that the PSO is to apply to. In this case the DN is as follows:

1. CN (Common Name) = IPA. [This is the IPA Group that the PSO applies to.]
2. OU (Organizational Unit) = IPA. [This is the OU that the IPA Group is contained within.]
3. DC (Domain Component) = MSCCONV. [The first part of the forest root domain i.e. MSCCONV.IPA]
4. DC = IPA

Figure E1.23 – Specifying Distinguished Name



INFORMATION

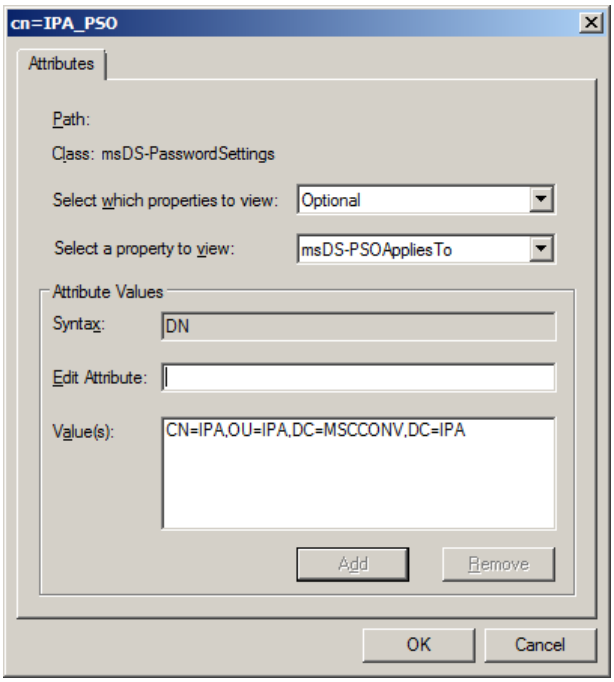
The distinguished name (DN) entered in the **Attribute Values** section is an example of Lightweight Directory Access Protocol (LDAP).

As discussed by Tittel, E. & Korelc, J. (2008 ,p.117), "LDAP is designed specifically to retrieve and access directory data".

It is a communication protocol which enables the management of the directory system by Microsoft and non-Microsoft clients. The DN references the hierarchical path of the object in the Active Directory Database.

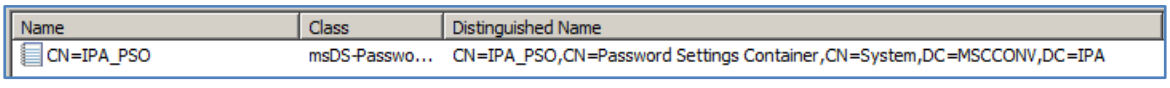
When you have entered the distinguished name, click **Add**, and it will appear in the **Value(s)** box as shown in Figure E1.24. Click **OK**, and then **Finish** (when you return to the final **Create Object** window).

Figure E1.24 – Distinguished name specified.



As shown in Figure E1.25, the PSO will now be listed in the password settings container.

Figure E1.25 – Password Settings Container

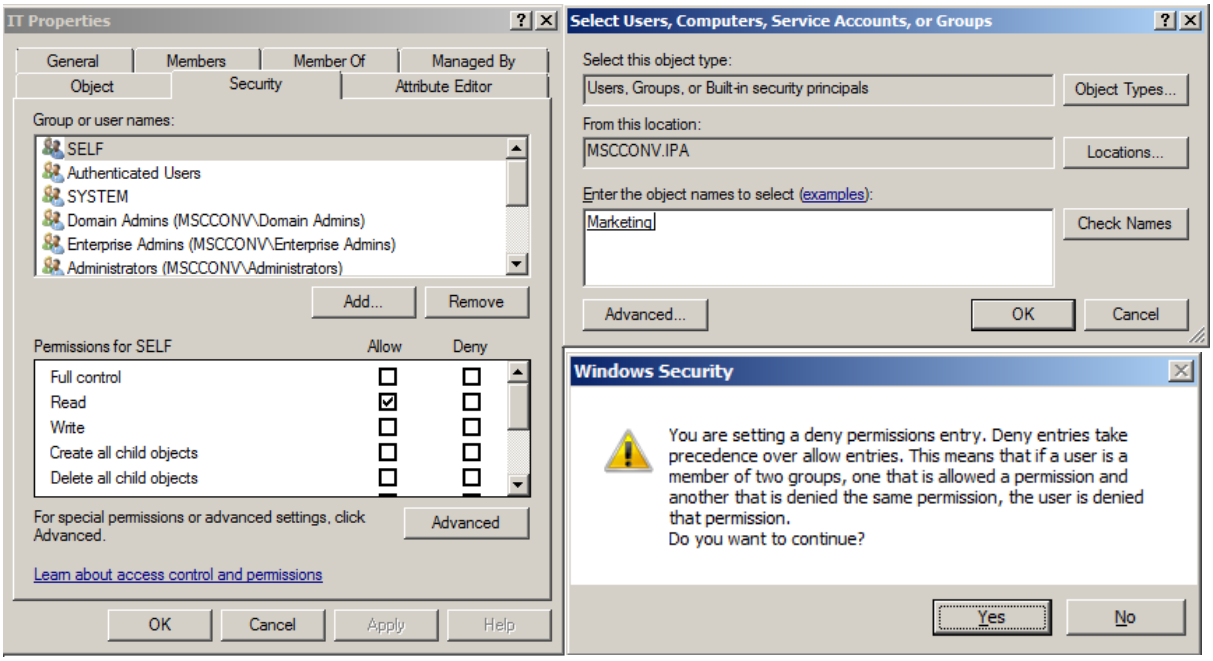


E2 - Prevent Marketing from viewing IT OU in Active Directory

From a domain controller, in the **Active Directory Users and Computers** utility, right-click the OU (IT) that you wish to block users from viewing in Active Directory and click **Properties**. In the **Security** tab click **Add** under the list of **Group or user names**. This brings up the window where you are to enter the group/users that you wish to prevent from viewing the IT OU. As shown in Figure E2.2 type *marketing* and click **Check Names**.

It should appear underlined as shown, click **OK** to proceed. You will be greeted with the standard security warning regarding precedence; click **Yes** to proceed.

Figure E2.1 –OU NTFS Permissions



Back in the **IT Properties** window you will see that the marketing group appears in the list of groups/user names. As shown in Figure E2.2, click the box under **Deny** beside **Full control** and ensure that you click **Apply** to confirm your changes.

Figure E2.3 shows **user5** (member of the IPA OU) logged on with the ability to see the IT OU.

To test that **Sales OU** users cannot see **IT OU** users, login as an IT user and navigate to the **Active Directory Users and Computers** utility.

If the changes have been successful you should not be able to view the IT OU, as shown in Figure E2.4 where **user14** (member of marketing) is logged in and cannot view the IT OU.

Figure E2.2 – Remove Rights from Marketing

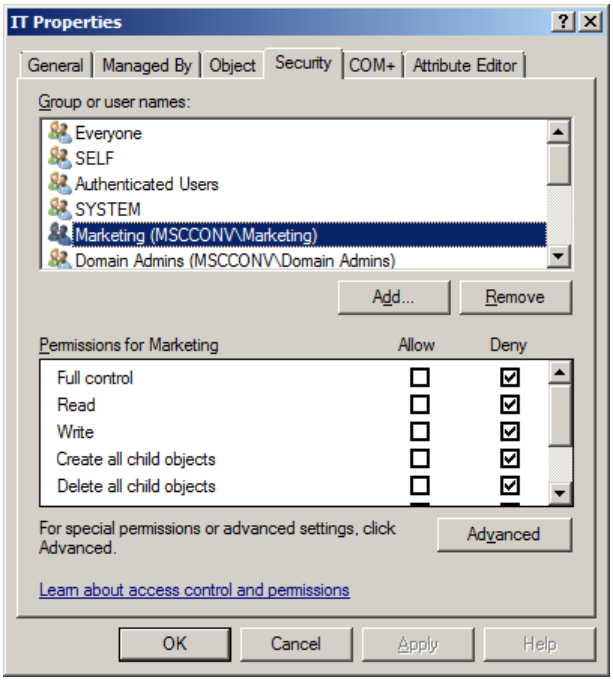


Figure E2.3 – IPA OU user Viewing IT OU

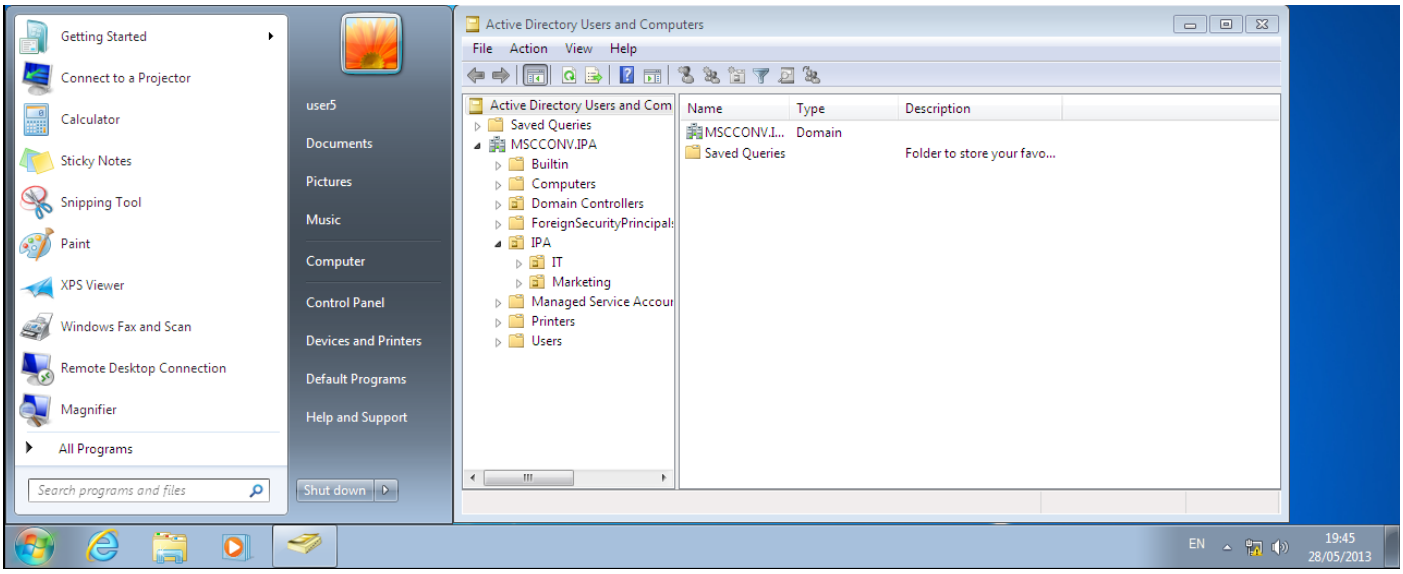
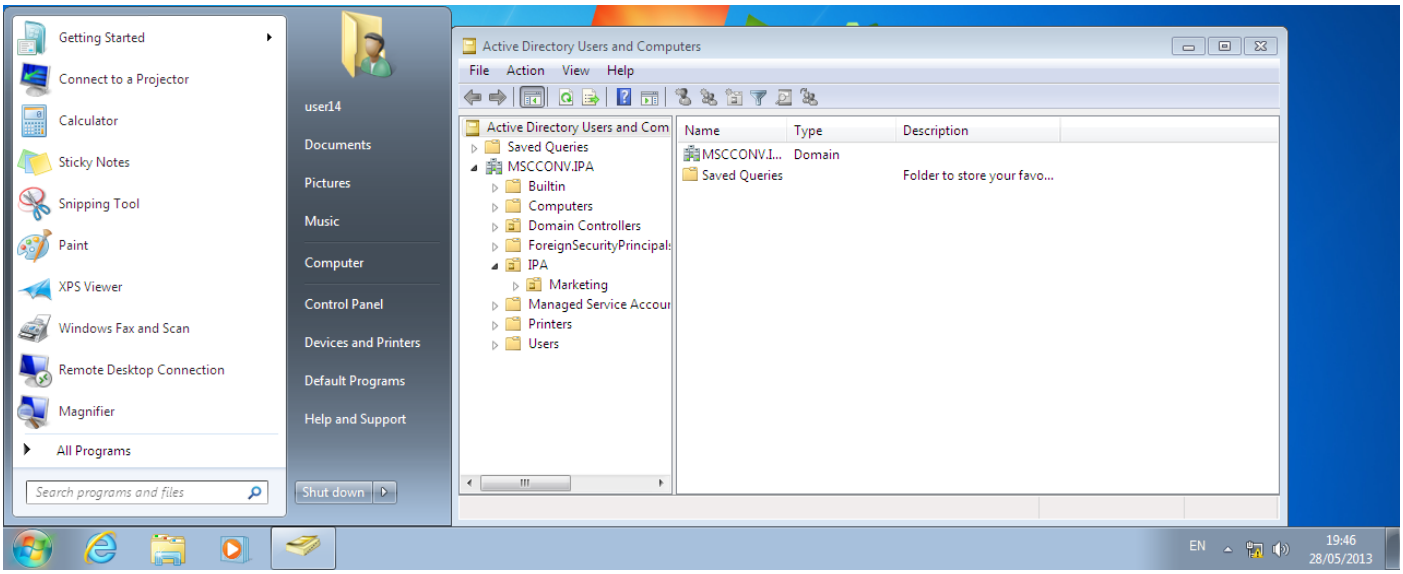


Figure E2.4 – Marketing User unable to view IT OU



E3 - Group Policies

Forwarding Documents

As shown in Figure E3.1, create a folder on the Server2 machine called ***User_Docs*** located on the root of the C Drive. Right-click the folder and select **Properties**. Under the **Sharing** tab click **Share** which will bring you to the **File Sharing** window. Click **Share** and you will be notified that the folder is shared (Figure E3.2). Click **Done** to proceed.

Figure E3.1 –Creating and Sharing Folder

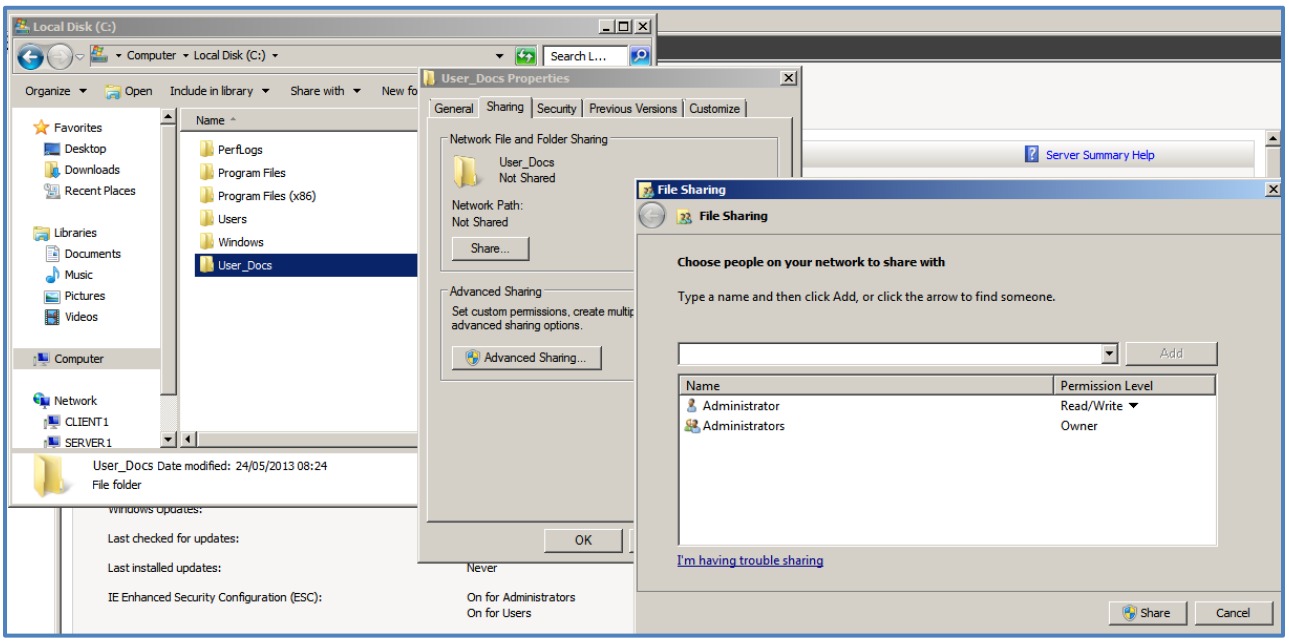
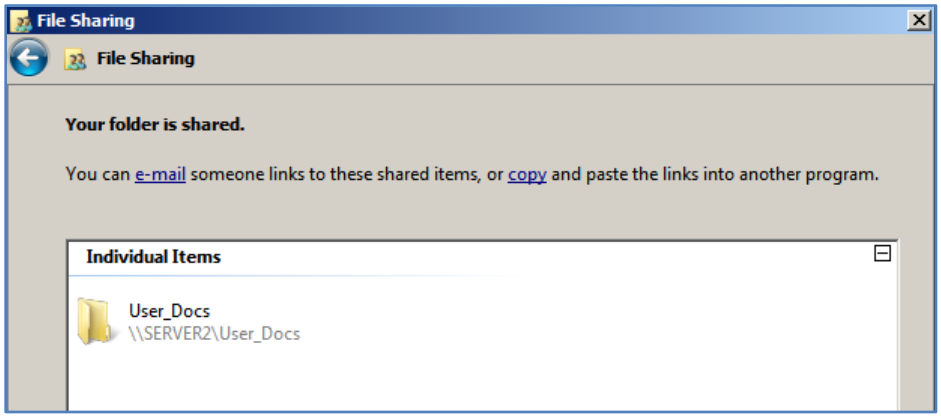


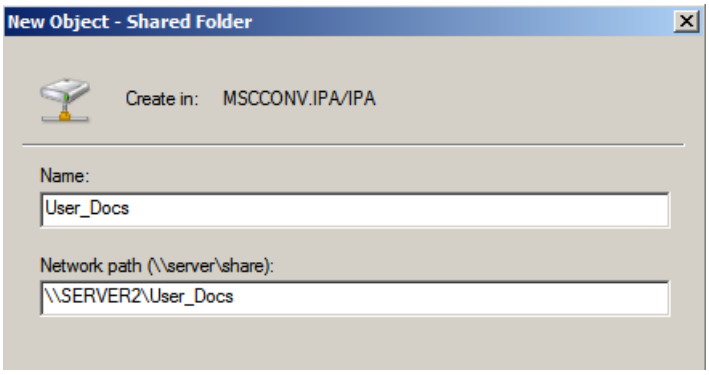
Figure E3.2 – Folder Shared



On the server machine, in **AD UC**, right-click the IPA OU and click **New**, and **Shared Folder**. Give the shared folder a name, and root path as shown in Figure E3.3. Click **OK** to confirm.

TechNet (n.d) discuss how the overall advantage of folder redirection is that "*Users can work with documents on a server as if the documents were based on a local drive. The documents in the folder are available to the user from any computer on the network.*" The aforementioned article can be found by clicking this link (eBook users only), whereby the various folders in Windows 7 that can be redirected are outlined.

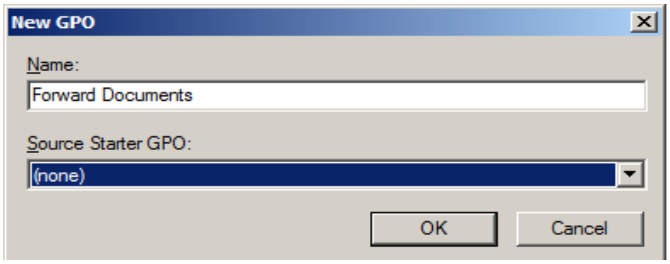
Figure E3.3 – Sharing Folder in AD DS



Now you can create a group policy object to forward the documents as required. In the windows search bar type ***group policy management*** and press **Enter**. As shown in Figure E3.4, right-click **Group Policy Objects** and click **New**.

Give the GPO (Group Policy Object) a name, and leave **Source Starter GPO** as **(none)** as shown in Figure E3.5. Click **OK** to proceed.

Figure E3.5 – New GPO



Right-click the object as shown in Figure E3.6 and click **Edit.** This brings up the **Group Policy Management Editor.** Expand the list as shown in Figure E3.7. Expand **User Configuration – Policies – Windows Settings – Folder Redirection**. Right-click **Documents** and click **Properties.**

In the **Target** tab ensure the ***Setting*** is set at ***Basic – Redirect everyone`s folder to the same location***.

Under ***Target folder location*** choose ***Create a folder for each user under the root path***. You may specify the root path or search for it by clicking **Browse** as shown in Figure E3.8.

Click the **Settings** tab and ensure that ***Grant the user exclusive rights to Documents*** is unticked.

Figure E3.10 shows the root patch correctly specified. Click the **Settings** tab as shown in Figure E3.9, and ensure ***Grant the user exclusive rights to Documents*** is not ticked. Click **Apply** followed by **OK** before exiting.

Figure E3.4 – Create Object

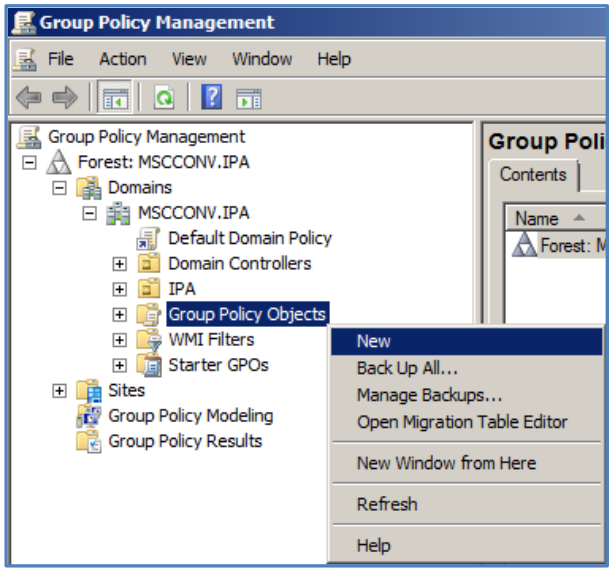


Figure E3.6 – Edit the GPO

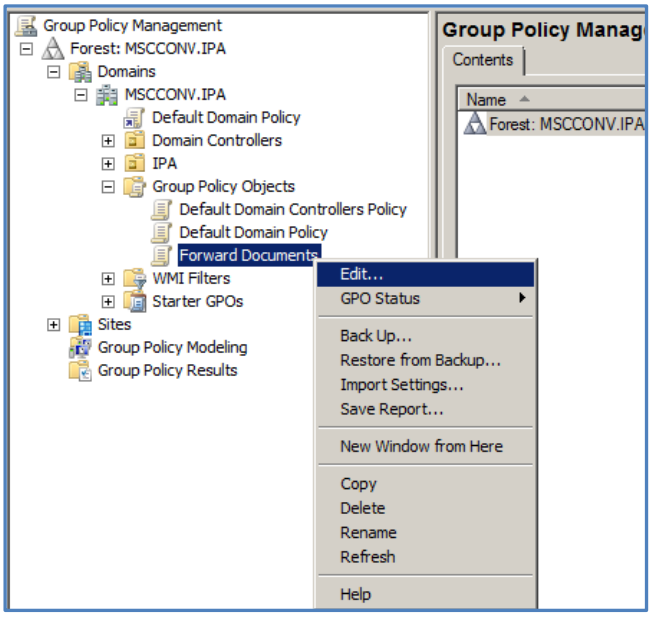


Figure E3.7 – Group Policy Management Editor

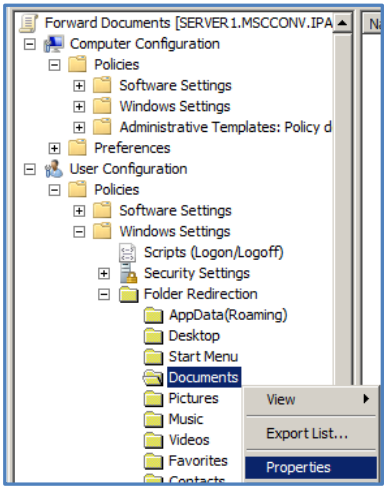


Figure E3.8 – Specifying the Root Path

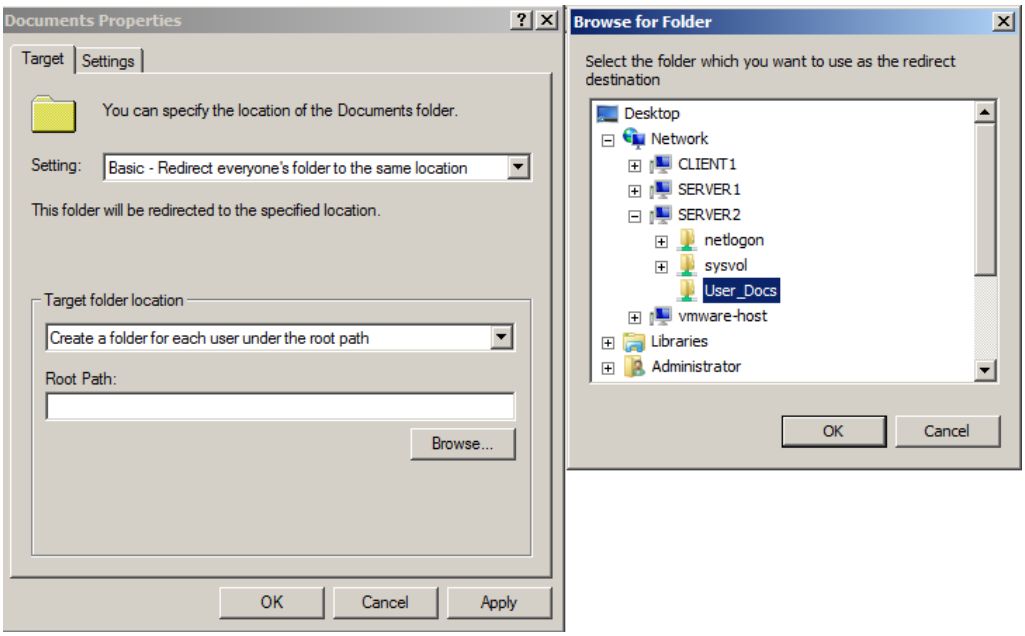


Figure E3.9 – Uncheck exclusive rights

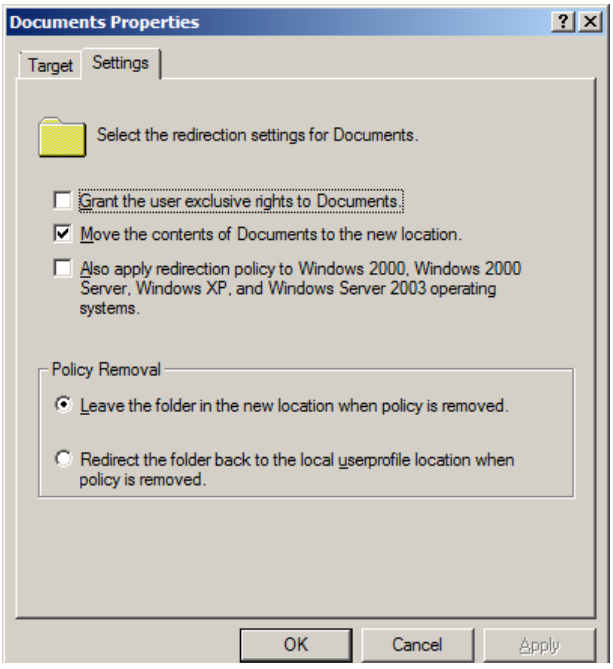
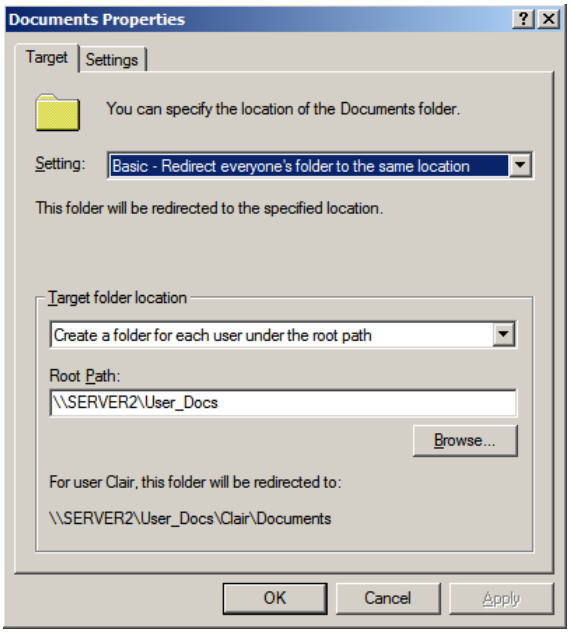
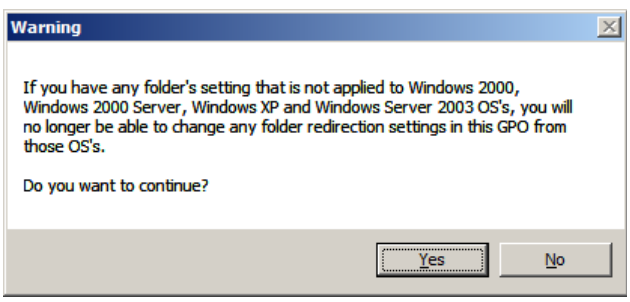


Figure E3.10 – Root Path specified



As shown in Figure E3.11, you will receive a warning regarding redirection settings for older Windows operating systems. Click **Yes** to proceed.

Figure E3.11 – Warning regarding older OS



You will now need to link the GPO you created with the IPA OU. To do this, in the **Group Policy Management** window, right-click the IPA OU and click **Link an Existing GPO** as shown in Figure E3.12.

As shown in Figure E3.13, you will be asked to select a GPO, click **Forward Documents** and **OK** to proceed.

Figure E3.12 – Linking an Existing GPO

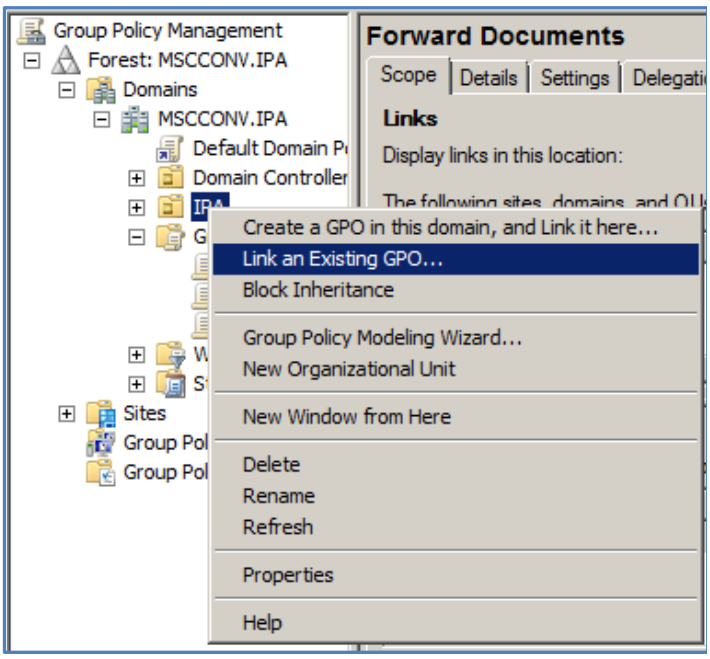
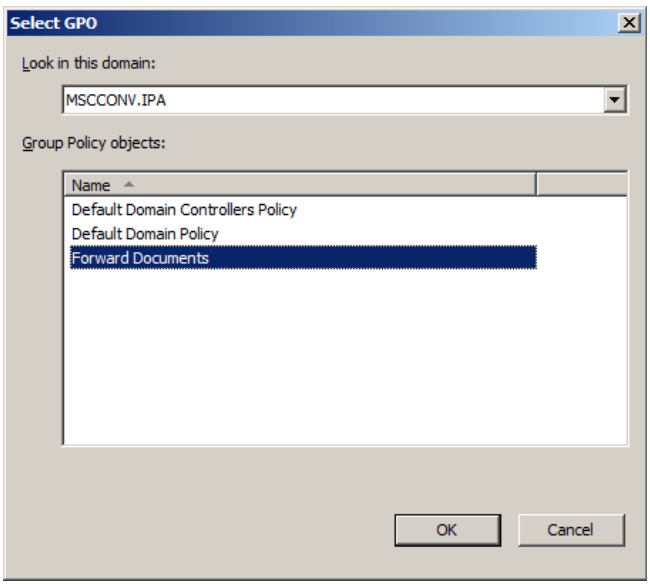


Figure E3.13 – Selecting the GPO to link



Note the security filtering section as shown in Figure E3.14. Client1 will not be listed here. Click **Add** underneath the white box which will bring up the **Select User, Computer, or Group** box as shown in Figure E3.15.

By default computers will not be available for selection, you must click **Object Types** and ensure ***Computers*** is ticked in the list shown in Figure E3.16. Click **OK** and you will be able to select client1 as shown in Figure E3.15.

To test that the implementation has been successful, log on to the client machine with a user. Create or save a document in the documents folder. Once you do this, a folder for the user will appear in the User_Docs folder created on the server machine, as shown in Figure E3.17.

Figure E3.14 – Security Filtering.

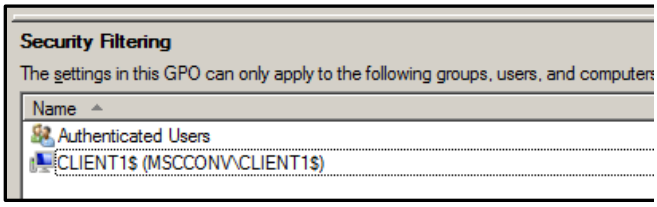


Figure E3.15 – Select Users, Computers, or Groups

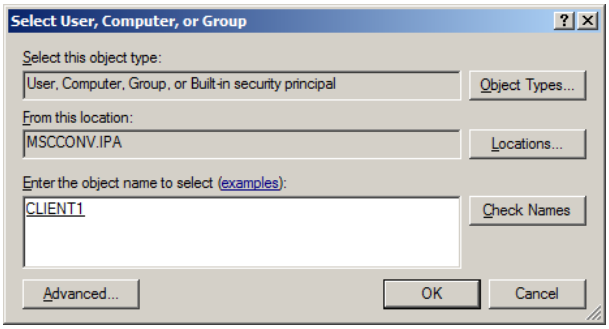


Figure E3.16 – Object Types

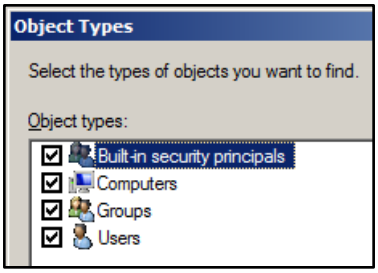
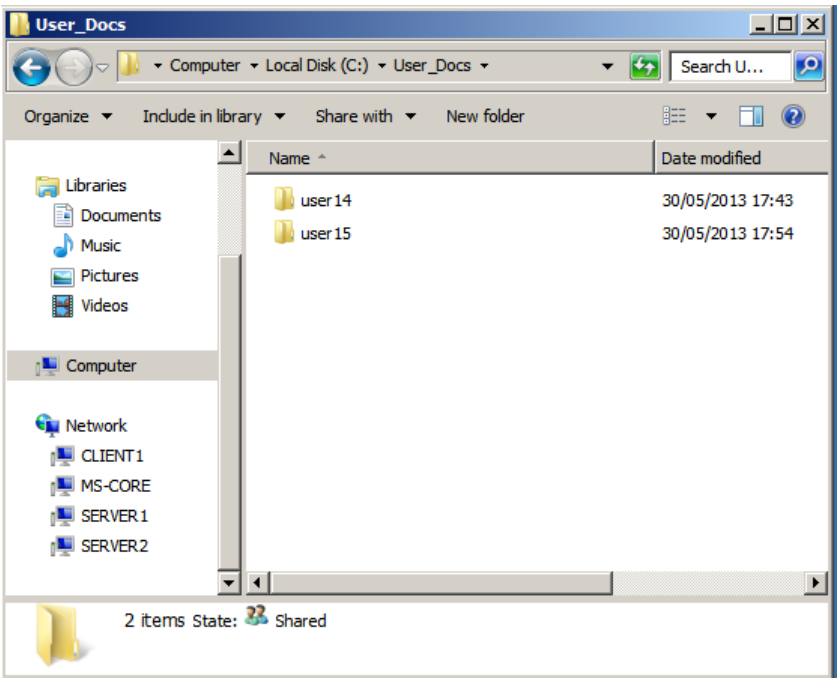


Figure E3.17 – Folders redirected to Server2 machine



Preventing Access to the Control Panel

In the **Group Policy Management** utility expand the domain, right-click **Group Policy Objects** and select **New**. Give it a meaningful name (Block Control Panel) as shown in Figure E4.1.

The object will be created and listed under **Group Policy Objects**. Right-click ***Block Control Panel*** and select **Edit** as shown in Figure E4.2. You will be brought to the **Group Policy Management Editor**.

Expand ***User Configuration, Policies, Administrative Templates*** and click ***Control Panel***. Double-click ***Prohibit access to the Control Panel*** as shown in Figure E4.3.

Figure E4.1 – Naming the GPO

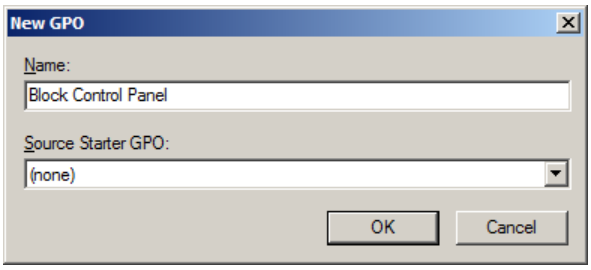


Figure E4.2 – Edit Object

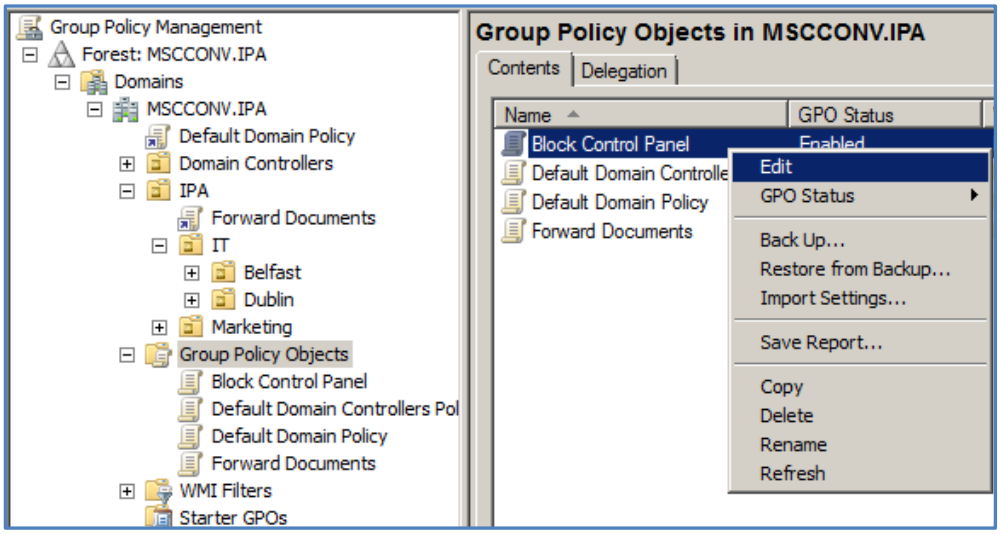
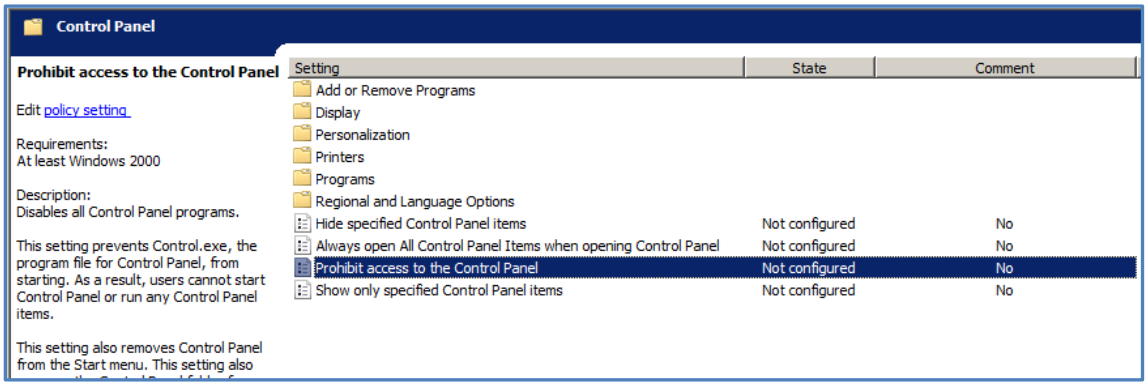


Figure E4.3 – Prohibit access to the Control Panel



Ensure that **Enabled** is selected as shown in Figure E4.4, and click **OK** to continue. Back in the ***Group Policy Management*** utility, notice the **Security Filtering** section as shown in Figure E4.5. This needs to be configured to have the **Belfast** group and **Client1** listed as having the object applied.

Click **Add** and type ***Belfast*** and click **Check Names**. Belfast should appear underlined as shown in Figure E4.5. Click **OK** to apply the group to the group policy object.

Figure E4.4 – Enabling the Setting

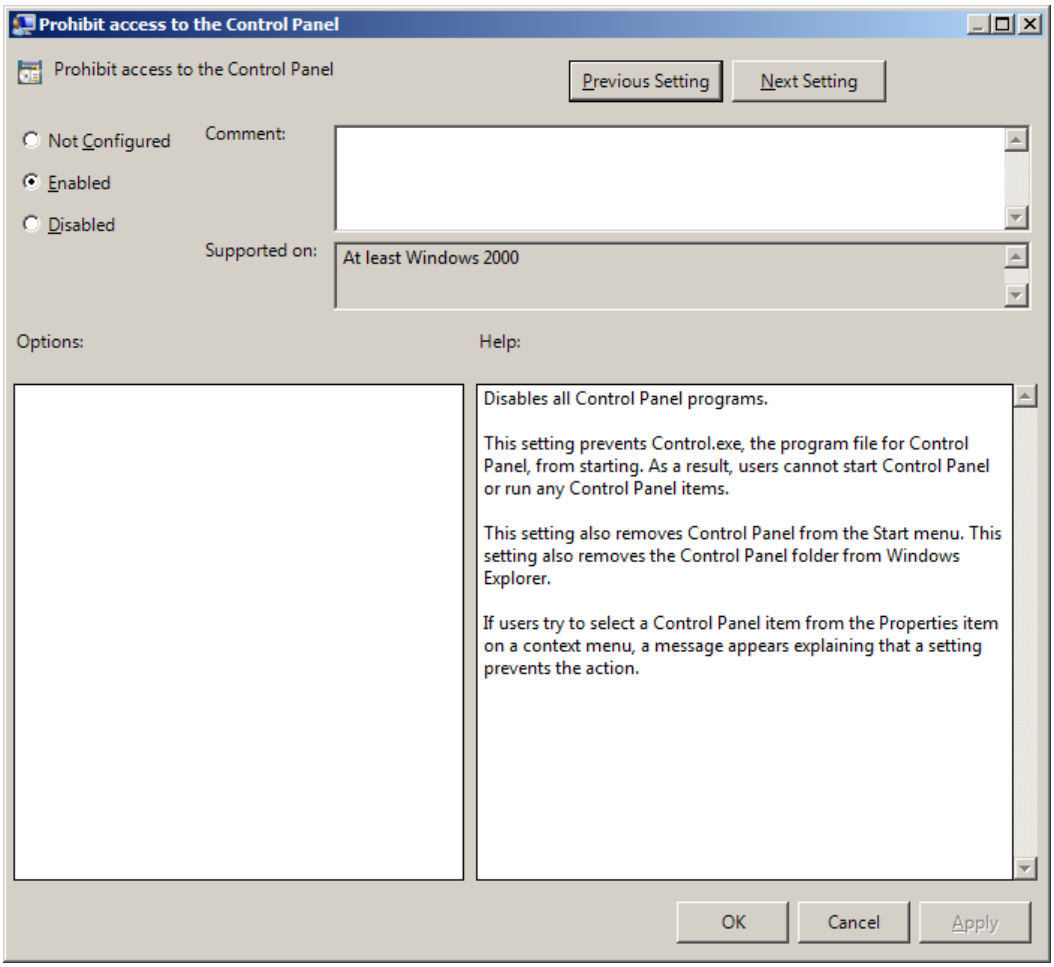
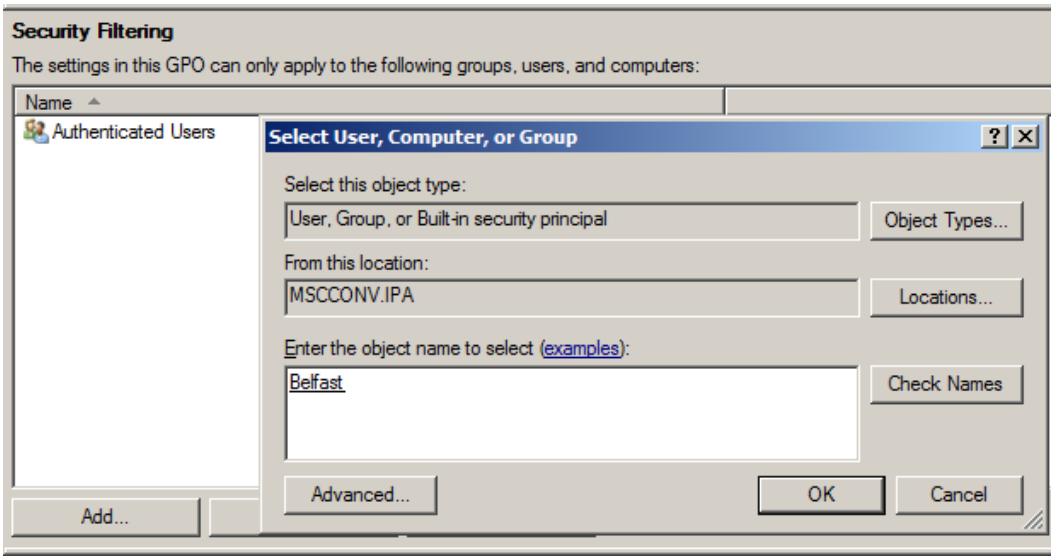


Figure E4.5 – Security Filtering

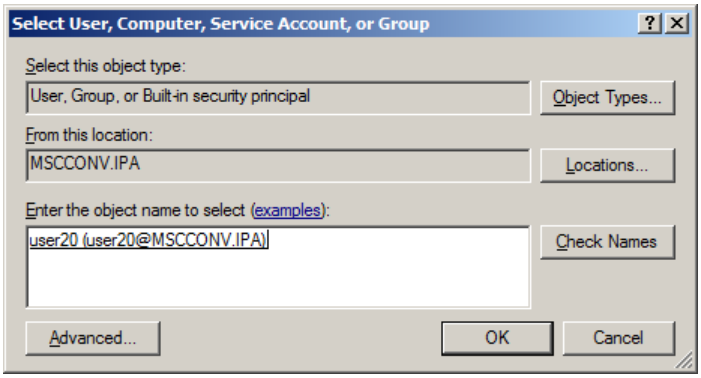


Under Security Filtering, highlight **Authenticated Users** and select **Remove**. Click **Add** once again. In **Select User, Computer, or Group** select **Object Types** and tick the box beside **Computers**. Click **OK**. Type ***Client1*** and click **Check Names**; **Client1** should appear underlined. Click **OK** to apply the **Client1** Windows 7 machine to this group policy.

Above **Security Filtering**, under **Block Control Panel**, click the **Delegation** tab. Click **Advanced** which is in the bottom-right-hand corner. In the resultant **Block Control Panel Security Settings** window, click **Advanced.**

This will display the **Advanced Security Settings** window for the policy. In order to exclude user20 from this policy you must add a deny permission for the user. Click **Add** and type user20 as shown in Figure E4.6.

Figure E4.6 – Choosing user20



Click **OK** and the **Permission Entry** window will appear as shown in Figure E4.7. Click the **Deny** box beside **Full control** and click **OK** to proceed.

You will be notified that you are setting a deny permission as shown in Figure E4.8. Click **Yes**. Ensure that you then click **Apply** back in the **Advanced Security Settings** window.

Note how user20 Is now listed under permission entries as shown in Figure E4.9. Now that the policy object is in place, link it to the Belfast OU by right-clicking it and selecting **Link an Existing GPO** as shown in Figure E4.10.

You will then be asked to select a GPO as shown in Figure E4.11. Select **Block Control Panel** and click **OK**.

Figure E4.8 – Deny precedence

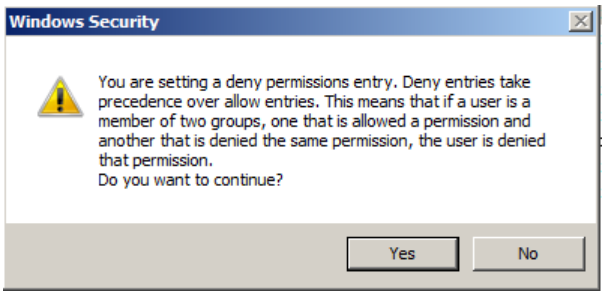


Figure E4.9 – Deny Full Control updated

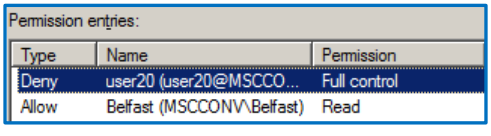


Figure E4.7 – Deny user20 Full Control

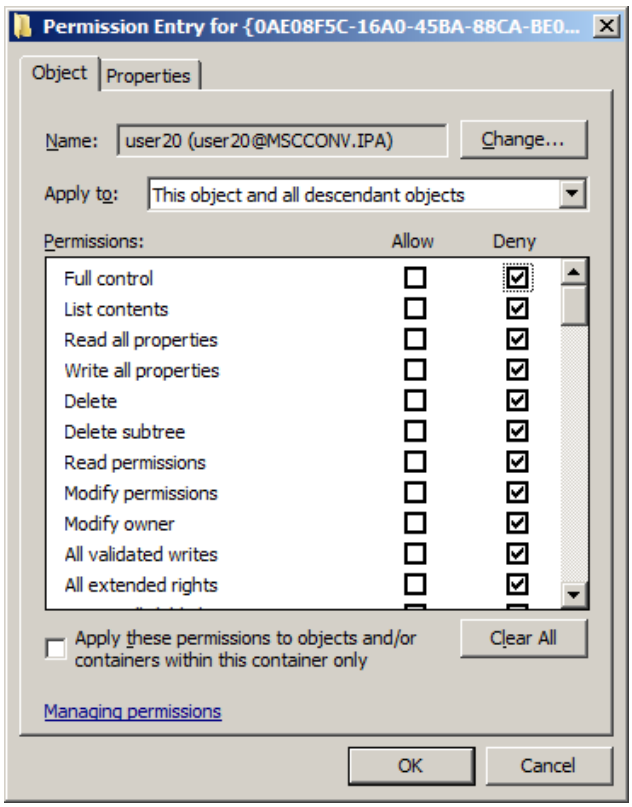


Figure 4.10 – Linking the GPO

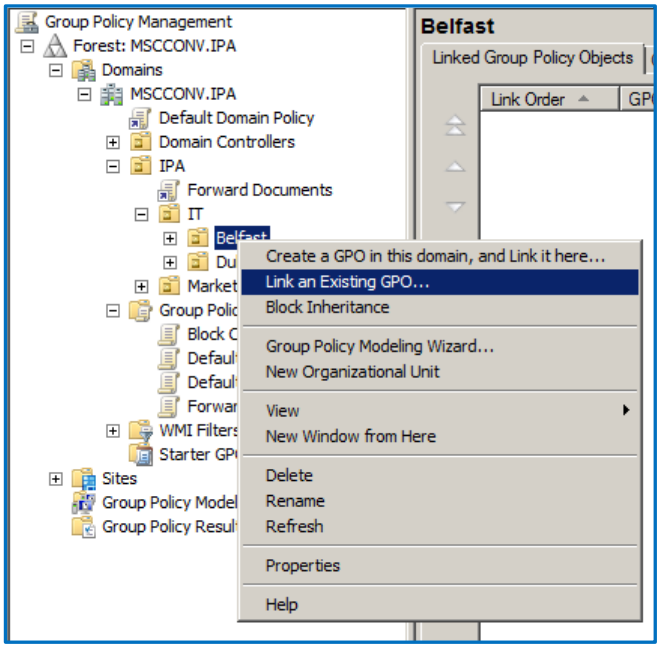


Figure E4.11 – Select GPO

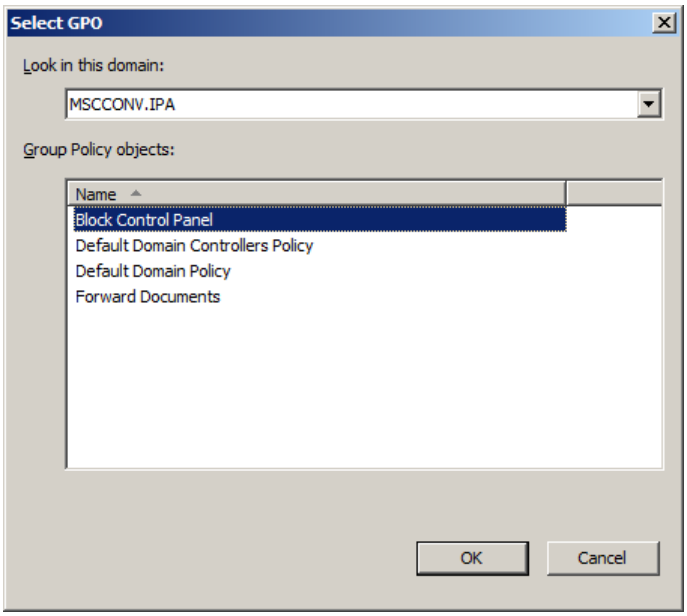
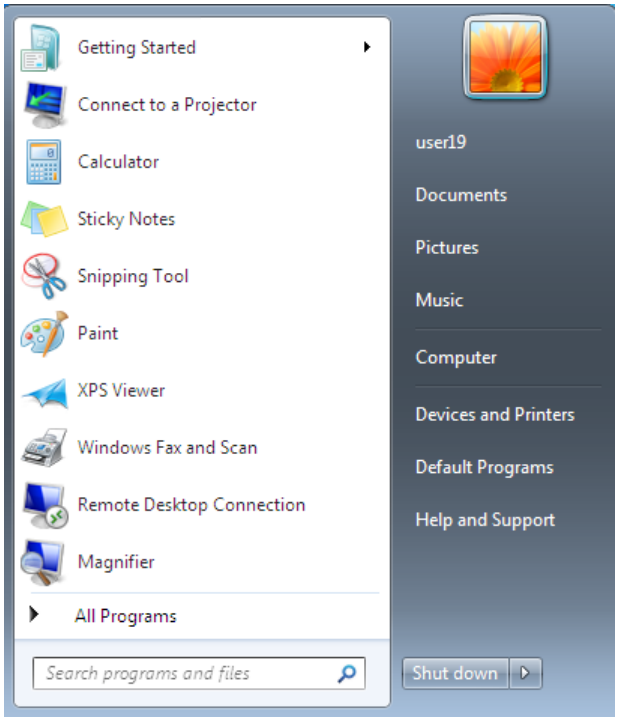


Figure E4.12 – Control Panel not available



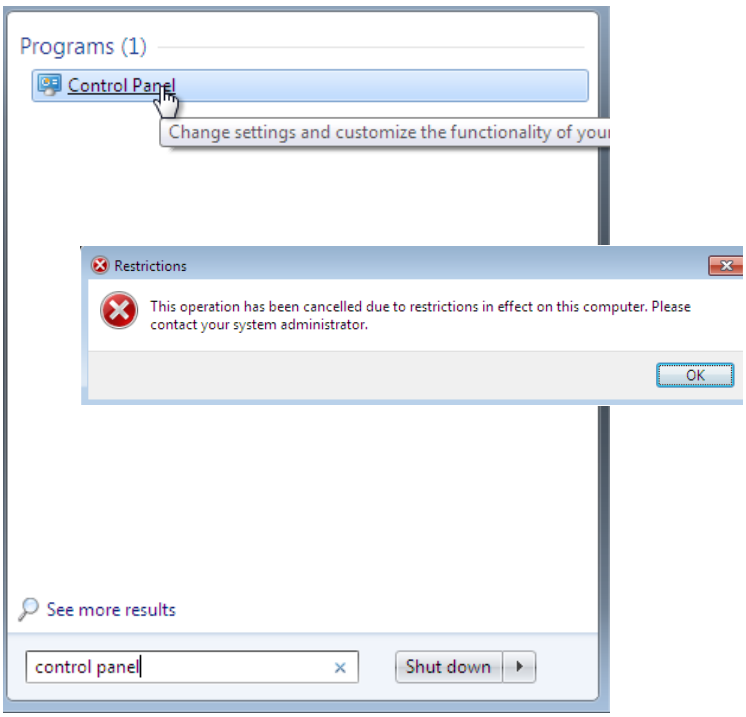
To test the successful implementation of this group policy, login as user19 (Belfast member) and click the **start** globe.

You will notice that the control panel is unavailable for selection as it normally would be as illustrated by Figure E4.12.

Furthermore, if you attempt to run the control panel via the search bar as shown in Figure E4.13 you will be notified of restrictions. Click **OK** and click **OK** again when the ***Unspecified error*** message appears.

The user will also be blocked from running a Control Panel command from the command prompt. Blocking access to the Control Panel prevents users from viewing and changing numerous system settings.

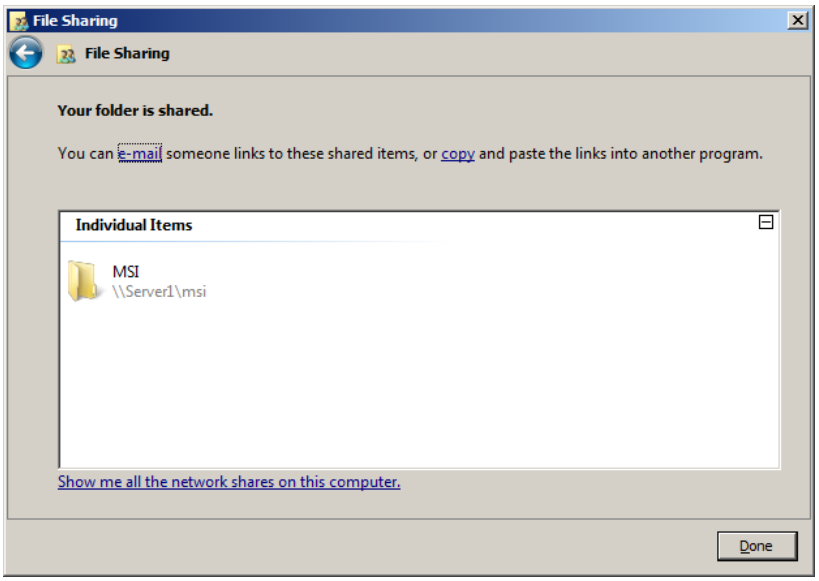
Figure E4.13 – Attempting to run Control Panel



Publish MSI file from C Drive to Dublin Users

Create a folder on the root of the **Server1** machine called ***MSI*** and insert the msi file inside this folder. Right-click the folder and select **Properties**. In the **Sharing** tab click **Share** and then click **Share** in the **File Sharing** window that will appear. A message will notify you that the folder has been shared, as shown in Figure E5.1.

Figure E5.1 – Sharing Folder with MSI File



Click **Done** to proceed. In the **Active Directory Users and Computers** utility right-click the Dublin OU and select **New** and **Shared Folder**. Give the shared folder a meaningful name as shown in Figure E5.2 and click **OK**. Note how the shared folder will be listed in the Dublin OU as shown in Figure E5.3.

Figure E5.2 – Creating Shared Folder in ADUC

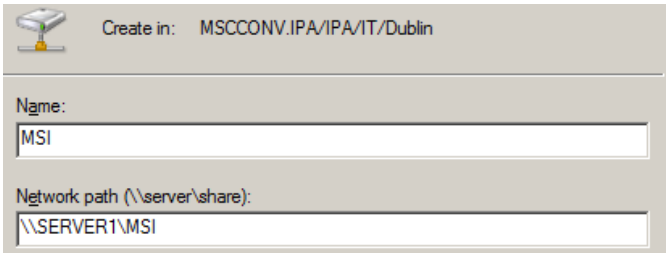
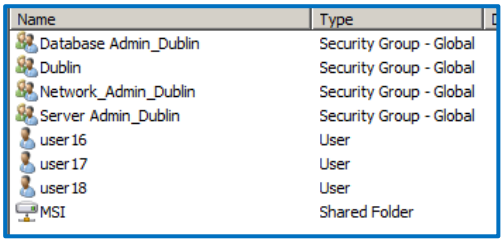


Figure E5.3 – Shared Folder Created



In the **Group Policy Management** utility right-click **Group Policy Objects** and select **New**. Call it **Publish_MSI** and click **OK**. Right-click the Dublin OU and click **Link an Existing GPO**.

Select **Publish_MSI** from the list and click **OK**. Under **Group Policy Objects** right-click **Publish_MSI** and select **Edit**. This will bring you to the Group Policy Management Editor.

As shown in Figure E5.4, expand **User Configuration, Policies, and Software Settings**, right-click on **Software Installation** and select **New**, then **Package**.

You will be brought to the window shown in Figure E5.5. Ensure that you manually type the path to the installation file.

Figure E5.4 – Creating Package in GPME

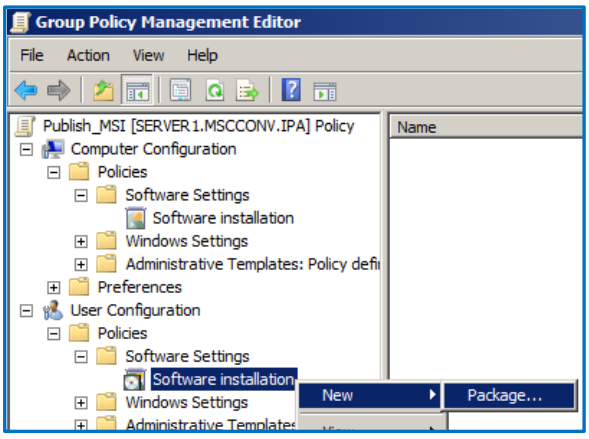
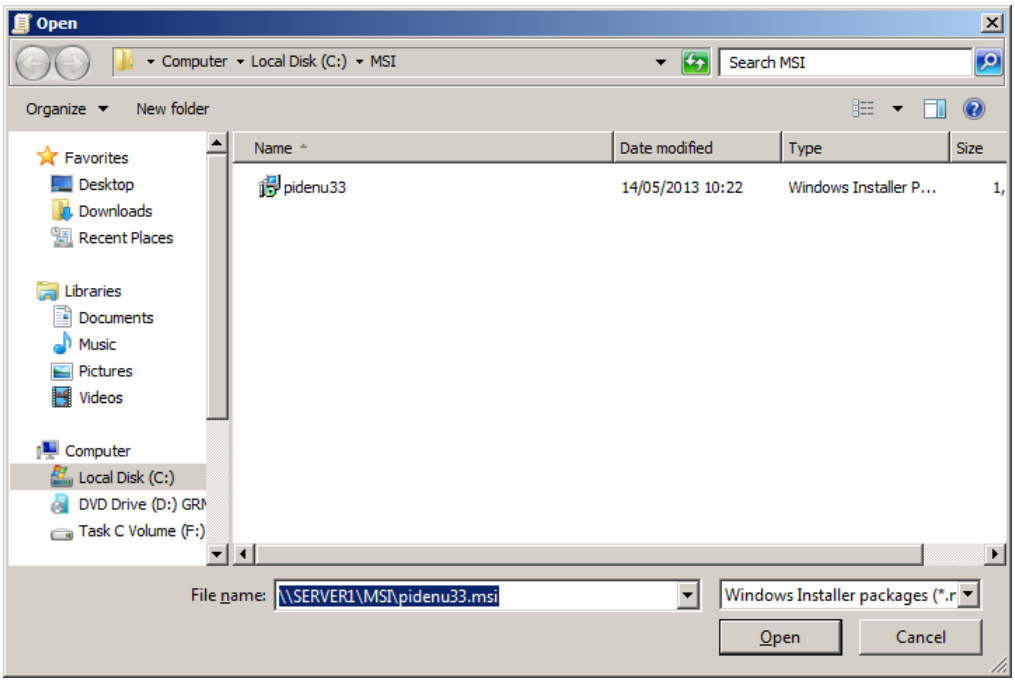


Figure E5.5 – Selecting path to msi file



NOTE

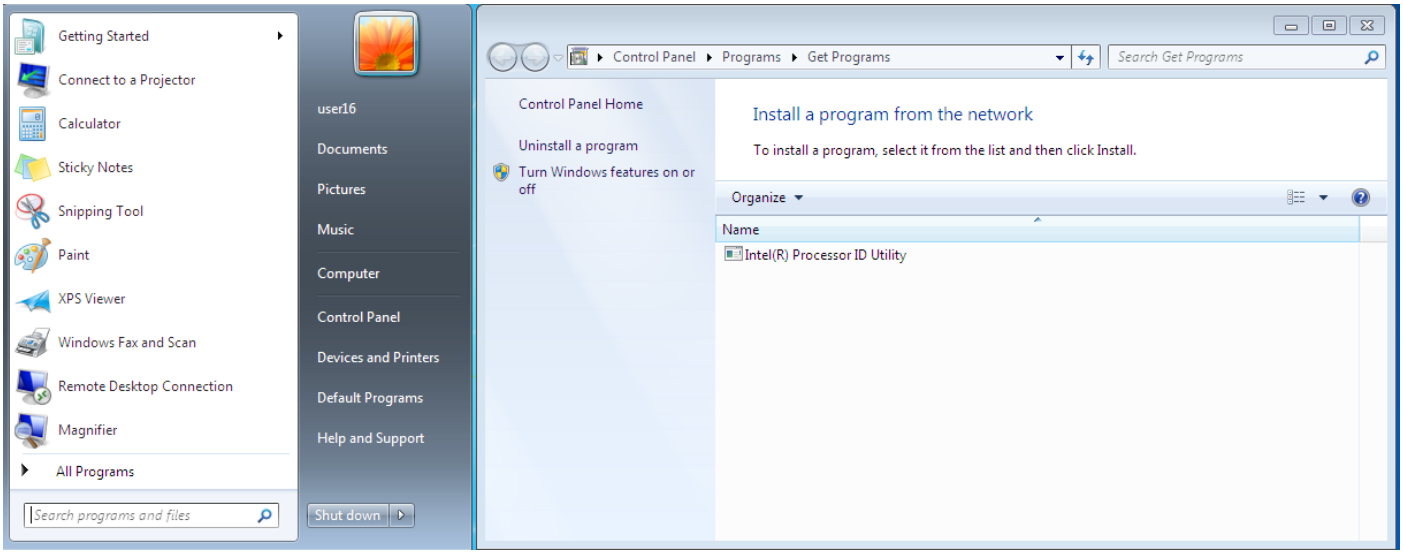
You must manually enter the path to the msi file as shown highlighted in blue.

Pointing and clicking to the file will result in an error.

Click **Open** and you will be asked to specify a deployment method. Select **Published** and click **OK**.

To test if the Group Policy has successfully implemented, login as a user from the Dublin group. Type **install a program from the network** into the search bar and press **Enter**. The MSI file will be listed and ready to install as shown in Figure E5.7.

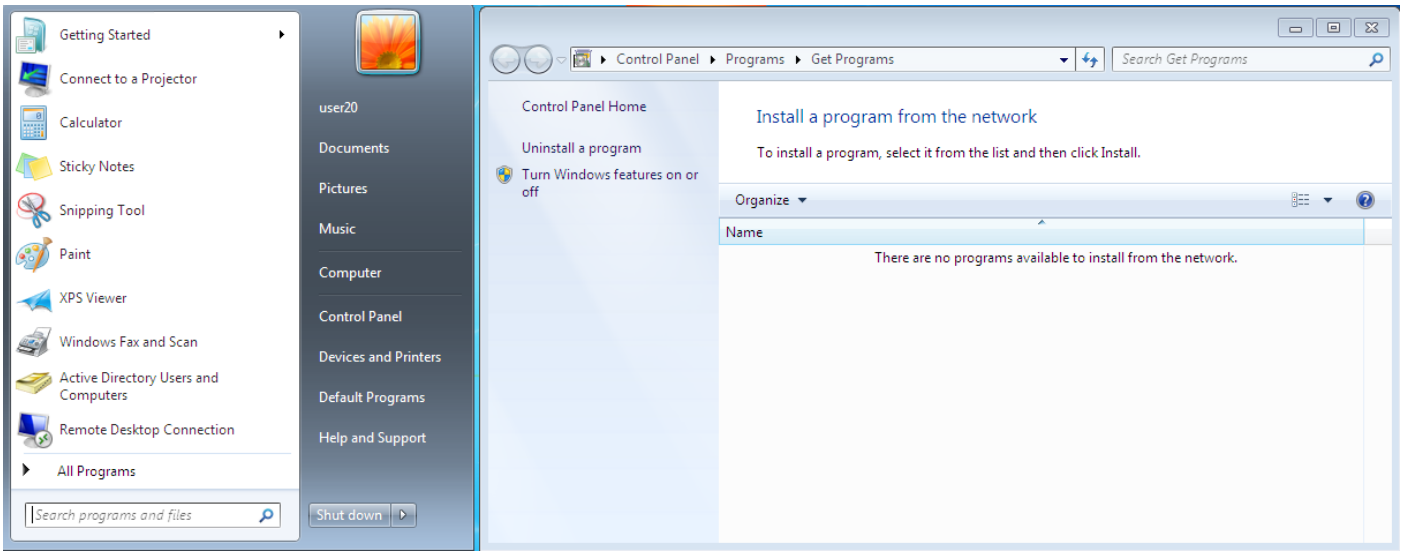
Figure E5.7 – MSI package available for installation from user16 account (Dublin Group)



To test that the policy has been successfully isolated to the Dublin Group, login as a user outside of that group, and attempt to install a program from the network.

As shown in Figure E5.8, there will be no file available for installation.

Figure E5.8 – MSI package unavailable for installation from user20 account (Belfast Group)



Group Policy Modeling Tool

As discussed by Habraken, J. (2008, p.218):

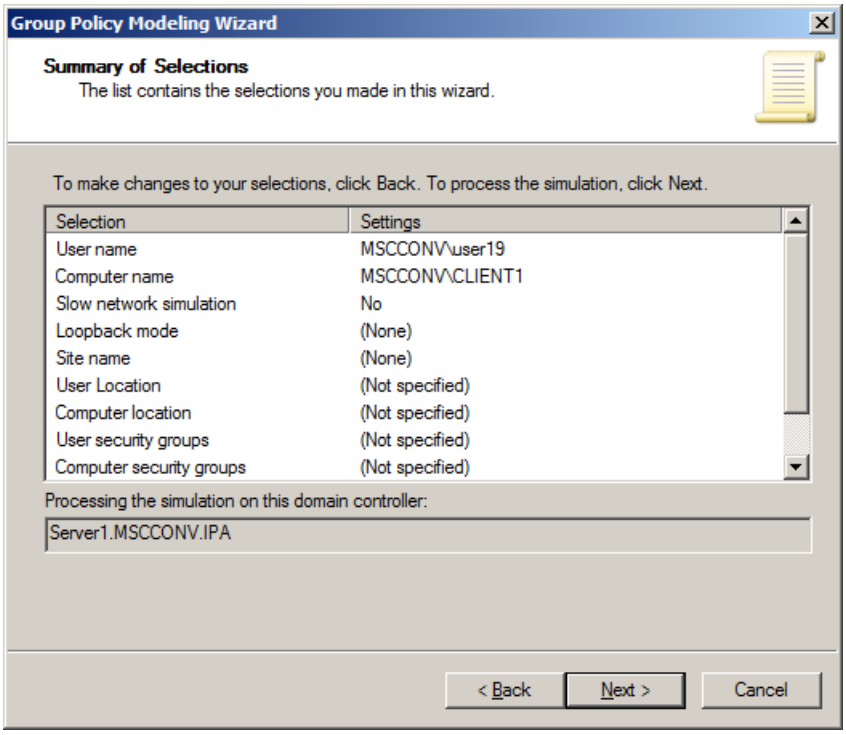
> *The Group Policy Modeling tool enables you to determine how a set of GPOs will affect a particular object in the Active Directory tree such as a user or computer. The Group Policy Results tool enables you to take a look at the resultant set of policies, meaning how both direct and inherited policies actually affect an object in the Active Directory.*

Without this tool, you would be forced to examine the properties of every site, domain and OU to see how policies and containers are linked. You would also have to examine the access control lists (ACLs) and the Windows Management Instrumentation (WMI) to see if there is any filtering. You would also have to check the disabled, block inheritance, and enforce options.

To work with this tool, open **Group Policy Management**, right-click **Group Policy Modeling** (in the left-hand navigation pane at the bottom of the list) and click **Group Policy Modeling Wizard**. Click **Next** at the welcome screen. At the **Domain Controller Selection** window ensure the correct domain and domain controller are selected and click **Next**.

At the **User and Computer Selection** screen, select the user and computer you wish to simulate (by choosing **Browse**). At this stage you can check the option box beside **Skip to the final page of this wizard without collecting additional data**. You will be brought to the **Summary of Selections** window shown in Figure E6.1.

Figure E6.1 – Summary of Selections.



Click **Next** once you are happy with the selections shown. Click **Finish** to be displayed with the results of the wizard.

Figures E6.2 and E6.3 shows the results of user19`s Group Policy Modeling which demonstrates the implementation of the Documents Redirection and Control Panel Blocking GPOs. Figures E6.4 and E6.4 deal with user16 and demonstrate the Publish MSI GPO.

Figure E6.2 – Group Policy Modeling Wizard for User19 (Summary Tab)

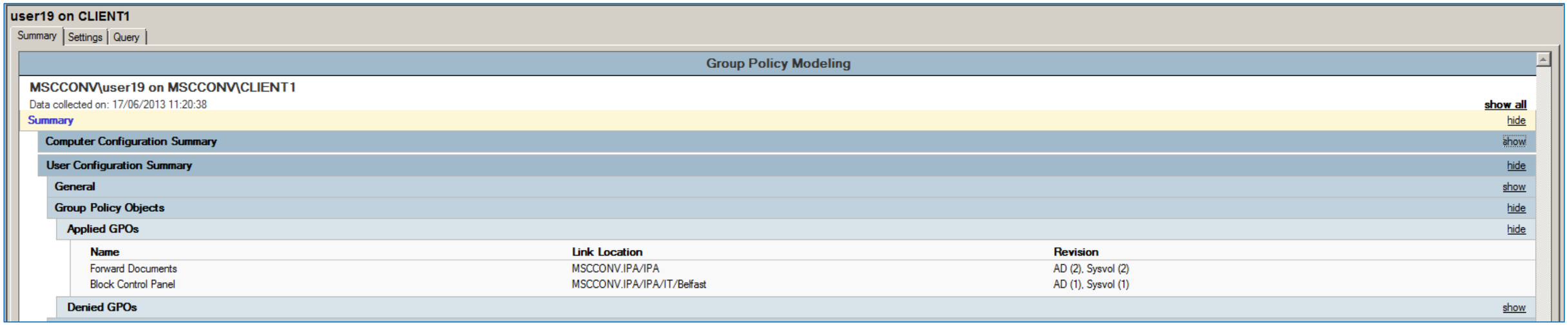


Figure E6.3 – Group Policy Modeling Wizard for User19 (Settings Tab)

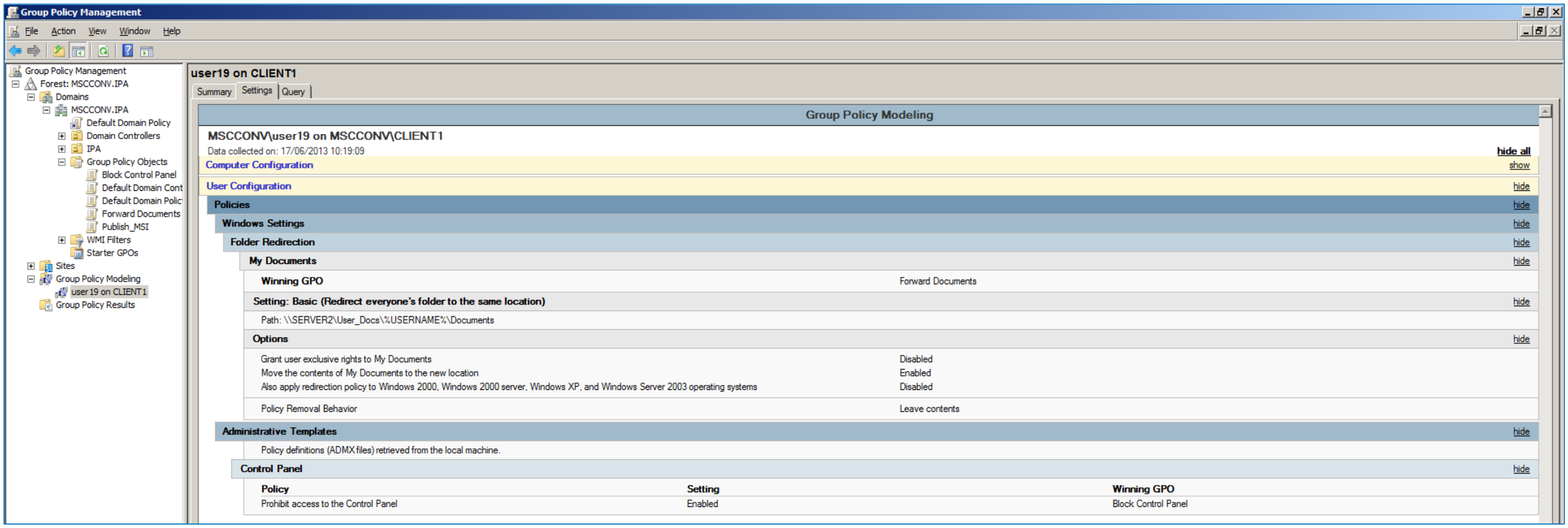
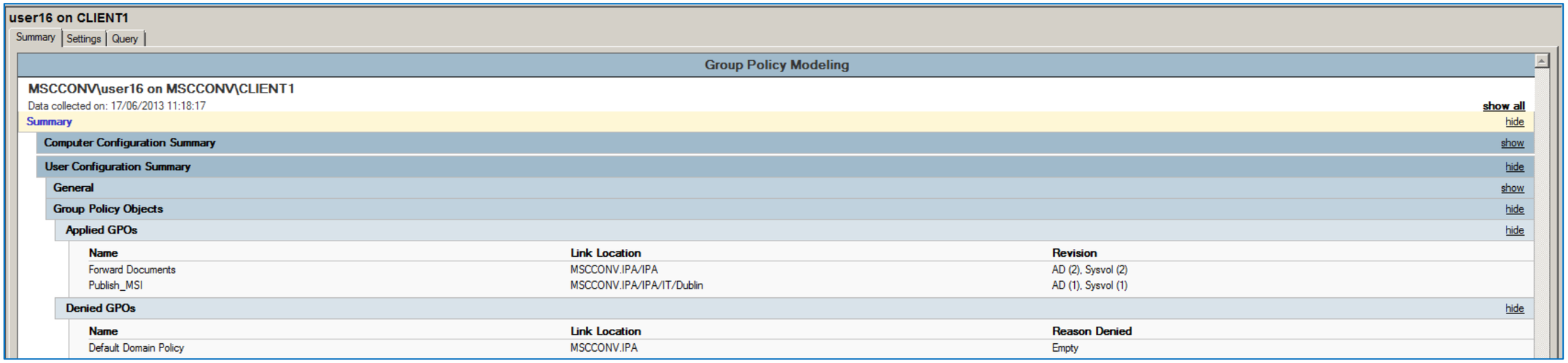


Figure E6.4 – Group Policy Modeling Wizard for User16 (Summary Tab)



user16 on CLIENT1

Summary | Settings | Query

Group Policy Modeling

MSCCONV\user16 on MSCCONV\CLIENT1

Data collected on: 17/06/2013 11:18:17 — show all

Summary — hide

Computer Configuration Summary — show

User Configuration Summary — hide

General — show

Group Policy Objects — hide

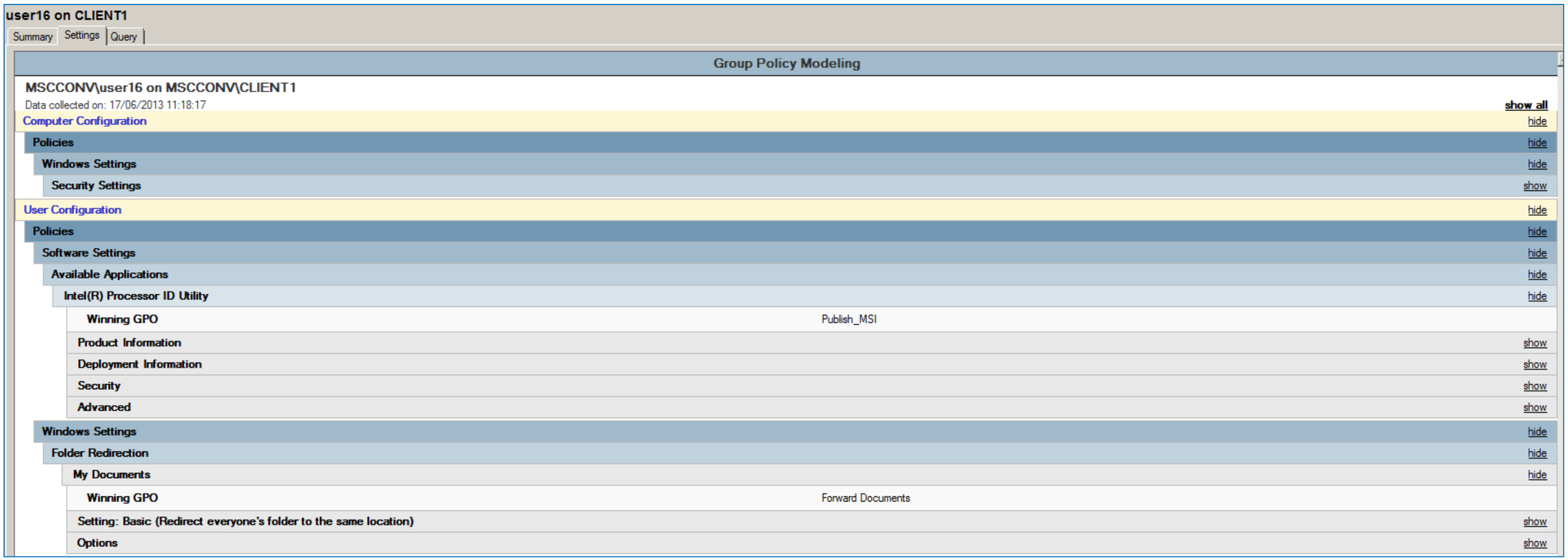
Applied GPOs — hide

Name	Link Location	Revision
Forward Documents	MSCCONV.IPA/IPA	AD (2), Sysvol (2)
Publish_MSI	MSCCONV.IPA/IPA/IT/Dublin	AD (1), Sysvol (1)

Denied GPOs — hide

Name	Link Location	Reason Denied
Default Domain Policy	MSCCONV.IPA	Empty

Figure E6.5 – Group Policy Modeling Wizard for User16 (Settings Tab)



user16 on CLIENT1

Summary | Settings | Query

Group Policy Modeling

MSCCONV\user16 on MSCCONV\CLIENT1

Data collected on: 17/06/2013 11:18:17 — show all

Computer Configuration — hide

Policies — hide

Windows Settings — hide

Security Settings — show

User Configuration — hide

Policies — hide

Software Settings — hide

Available Applications — hide

Intel(R) Processor ID Utility — hide

Winning GPO: Publish_MSI

Product Information — show

Deployment Information — show

Security — show

Advanced — show

Windows Settings — hide

Folder Redirection — hide

My Documents — hide

Winning GPO: Forward Documents

Setting: Basic (Redirect everyone's folder to the same location) — show

Options — show

TASK F – PRINT SERVER

F0 - Task Introduction

In this section **Server1** will be configured as a print server. This will ultimately mean that the printers can be accessed and used by all computers on the network. The steps carried out in this section can be summarised as follows:

1. **Configure Server1 as a print server**

This task is completed by adding the **Print and Document Services** role via the **Server Manager** utility.

2. **Install two printers on Server1**

This task is completed via the **Print Management** utility which will be available after the installation of **Print and Document Services** role.

3. **Publish the printers in Active Directory**

This is a very quick and simple task, completed in the **Print Management** utility.

4. **Add the printers to machines on the network**

This task is completed in the **Add a Printer** utility.

F1 - Configuring Server as Print Server

You can configure a server as a print server through **Server Manager**. In the left-hand navigation pane, right-click **Roles** and click **Add Roles** as shown in Figure F1.1. You can also click **Add Roles** underneath **Roles Summary Help** in the right-hand pane.

Figure F1.1 – Server Manager

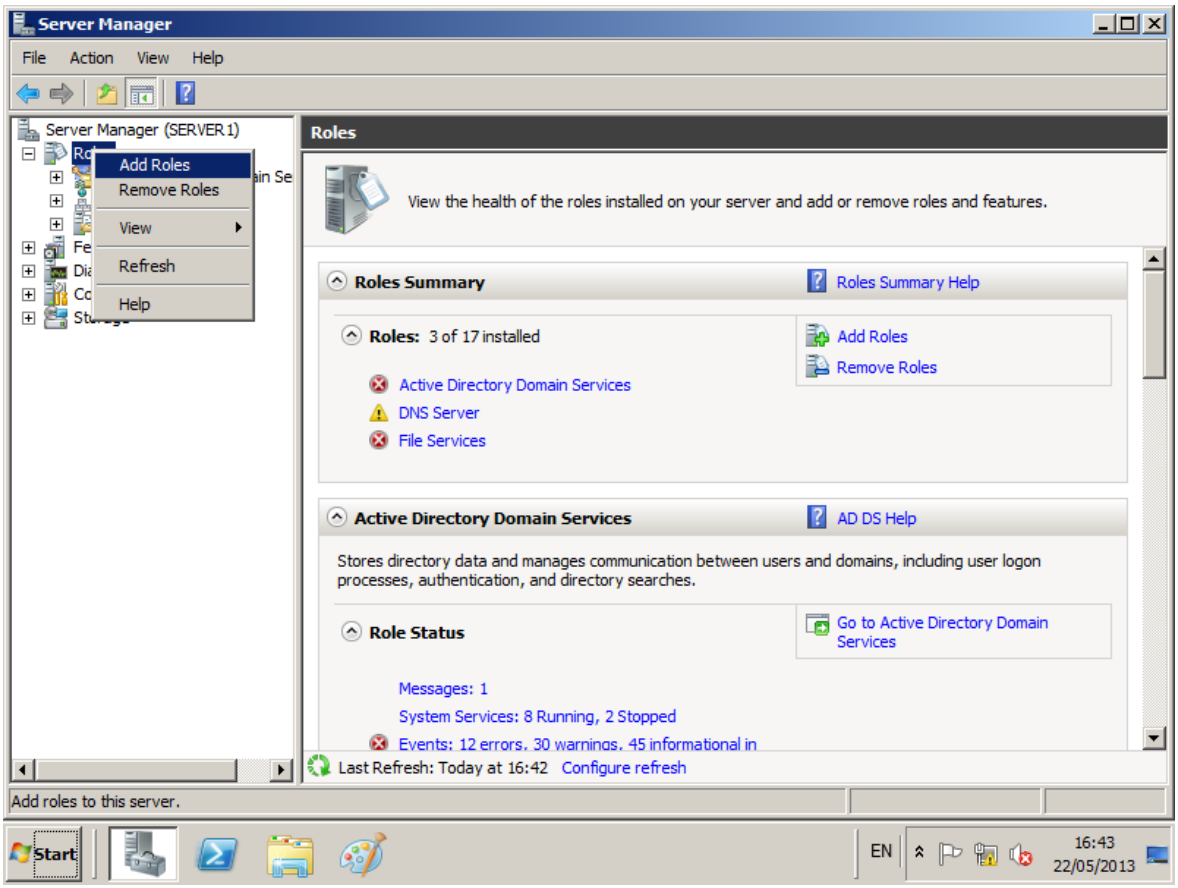
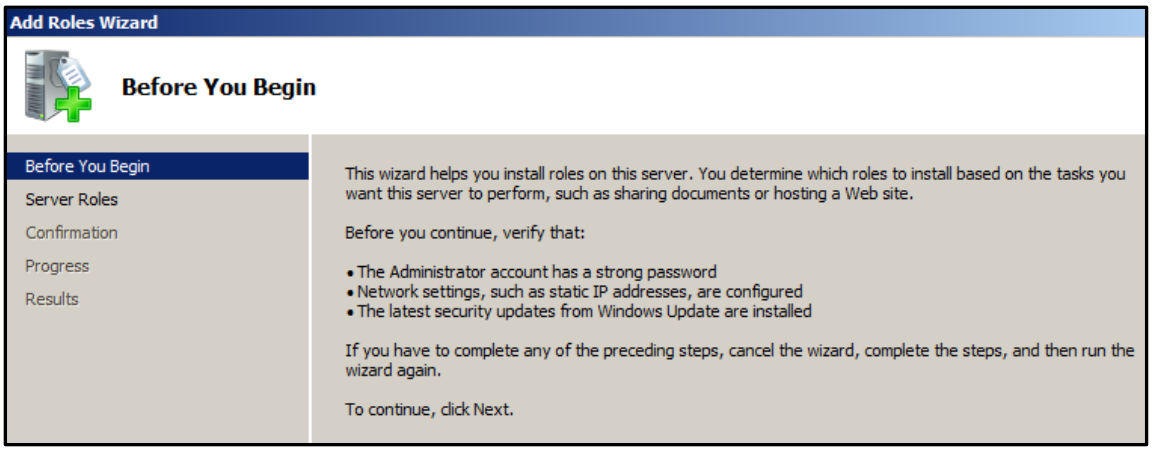
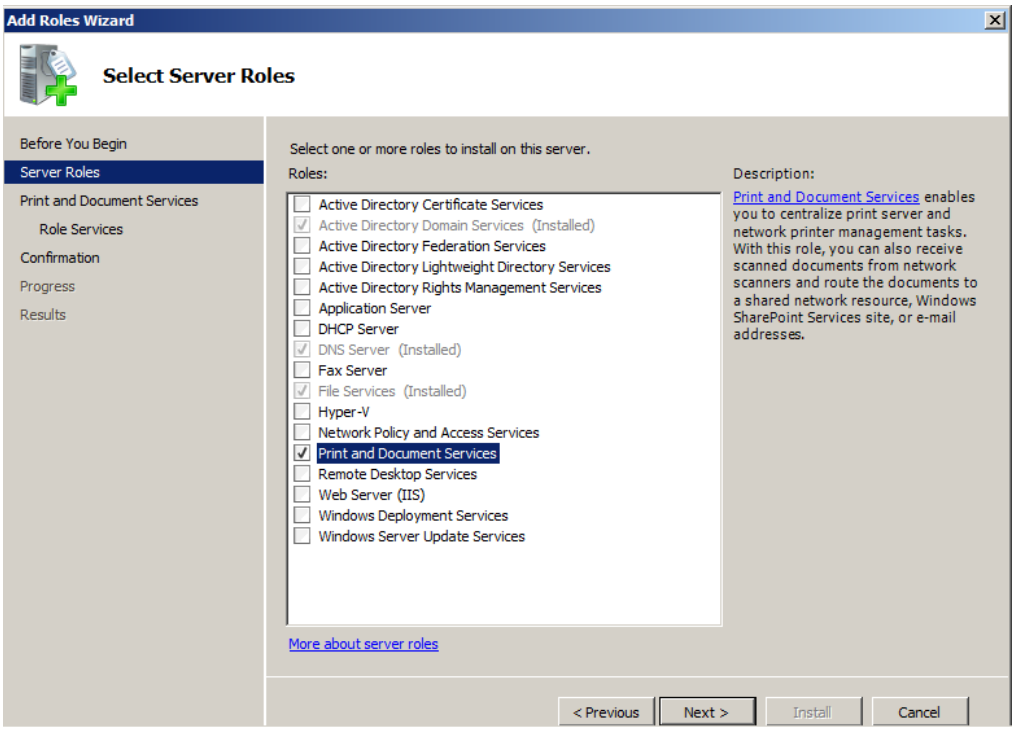


Figure F1.2 – Before You Begin



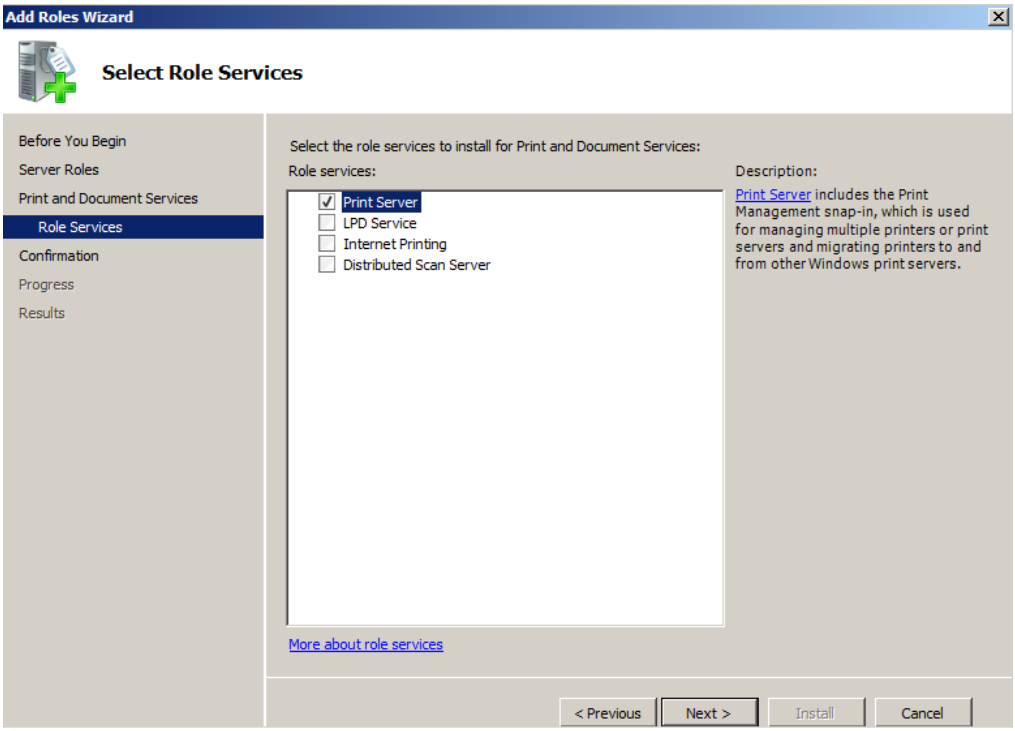
You will receive the above message in Figure F1.2 which will remind you of steps which must be in place prior to adding roles. Click **Next** to proceed. At the **Server Roles** window, tick the **Printer and Document Services** box as shown in Figure F1.3.

Figure F1.3 – Select Server Roles



Click **Next** to proceed. The next step is the **Print and Document Services** window which provides information about printer management tools. Click **Next** to continue. In **Select Role Services** ensure **Print Server** is selected as shown in Figure F1.4 and click **Next** to proceed.

Figure F1.4 – Select Role Services

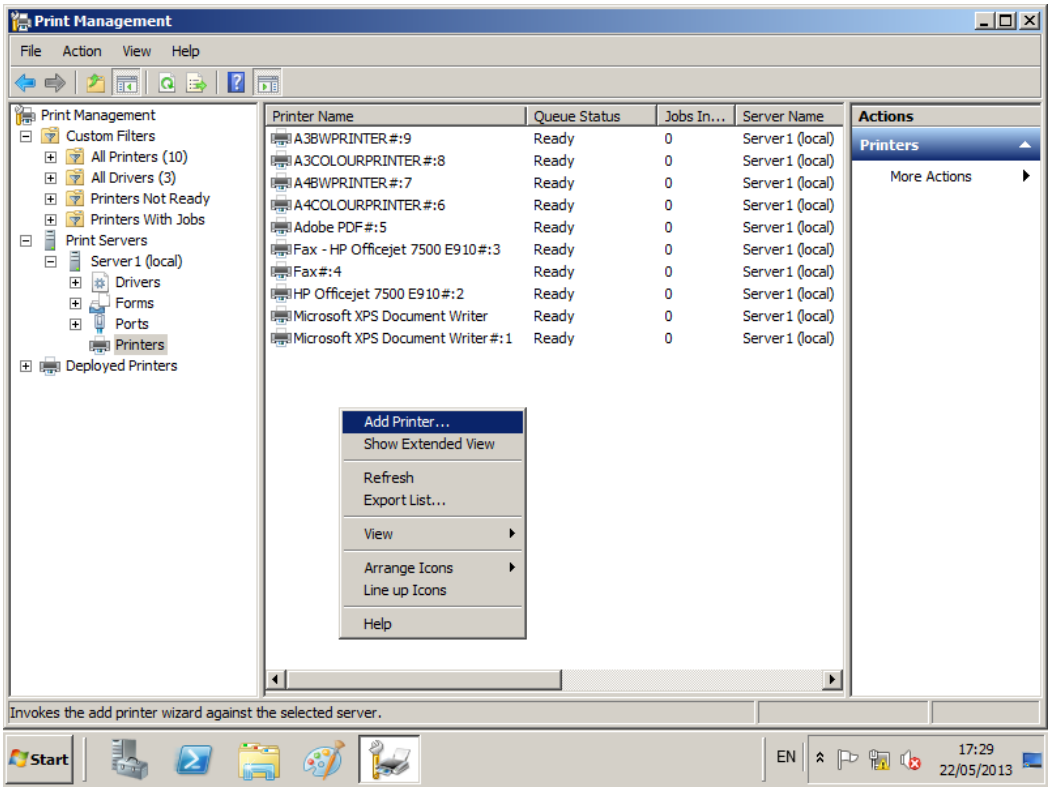


You will be asked to confirm the installation, click **Install** to confirm. After the installation, you should receive a message stating that the **Print Server** role services were installed. Click **Close** to exit the wizard.

F2 - Installing a printer on Server

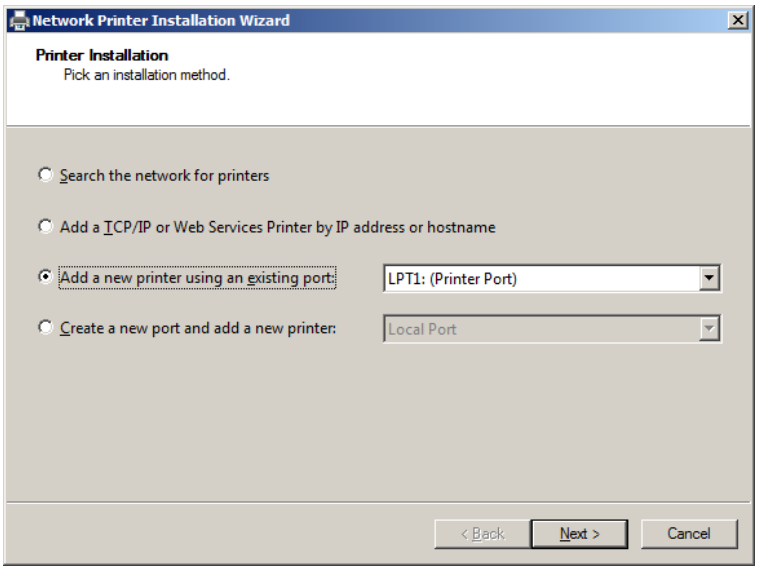
Now that the server is configured as a print server, the **Print Management** utility shown in Figure F2.1 will be available to you. Click **Start**, **Administrative Tools**, and **Print Management** to navigate to this utility. Expand **Print Servers** in the left-hand navigation pane, right-click **Printers** and click **Add Printer**. This brings you to the **Network Printer Installation Wizard** shown in Figure F2.2.

Figure F2.1 – Print Management



Click **Add a new printer using an existing port** and click **Next** to proceed.

Figure F2.2 – Network Installation Wizard



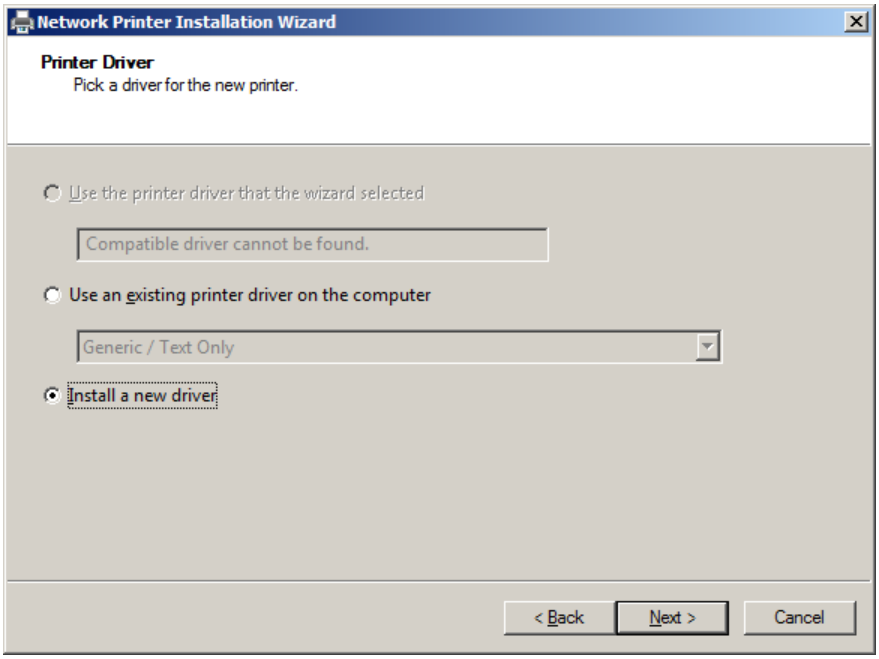
INFORMATION

At this stage, you could also add a printer by its IP address should it be a wirelessly enabled printer.

You could also search the network for printers if they were already installed.

At the **Printer Driver** stage, ensure **Install a new driver** is selected as shown in Figure F2.3. The wizard will attempt to detect the TCP/IP port.

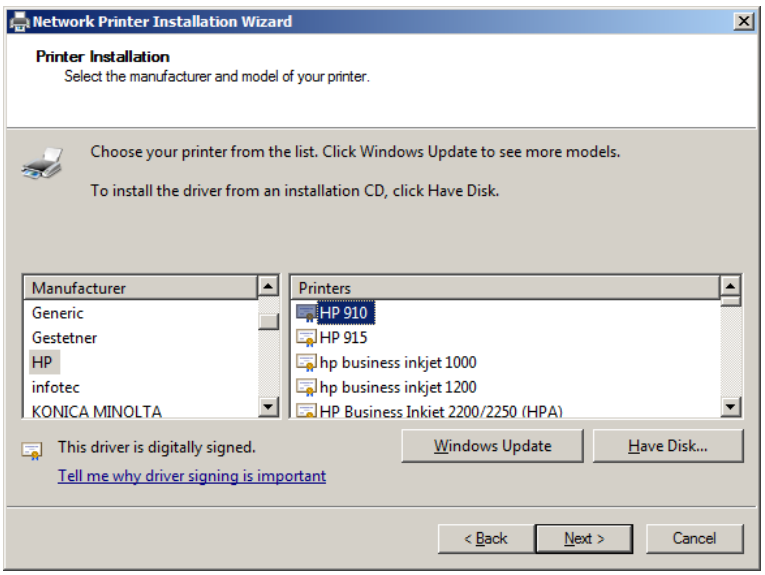
Figure F2.3 – Printer Address



You will be asked to select the manufacturer and model of your printer, as shown in Figure F2.4. Select the relevant details and click **Next** to proceed.

The **Printer Name and Sharing Settings** are specified next. As shown in Figure F2.5, you can specify a printer name, whether to share the printer, along with optional additional information such as location and general comments. Click **Next** when you are ready to proceed.

Figure F2.4 – Printer Installation



INFORMATION

This driver is digitally signed

Since device drivers become part of the operating system, they can cause problems if poorly designed. Microsoft assigns a digital signature to each drive. Meyers (2012, pp.746-748) explain driver signing in more detail.

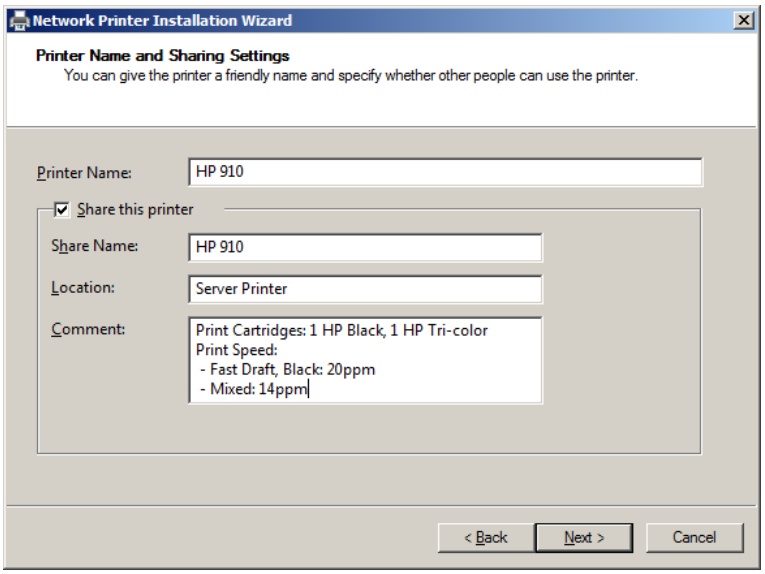
Windows Update

If the printer is not listed, the driver could potentially be found by running Windows Update.

Have Disk

This option is suitable should you have an installation disc with the printer driver included.

Figure F2.5 – Printer Name and Sharing Settings



INFORMATION

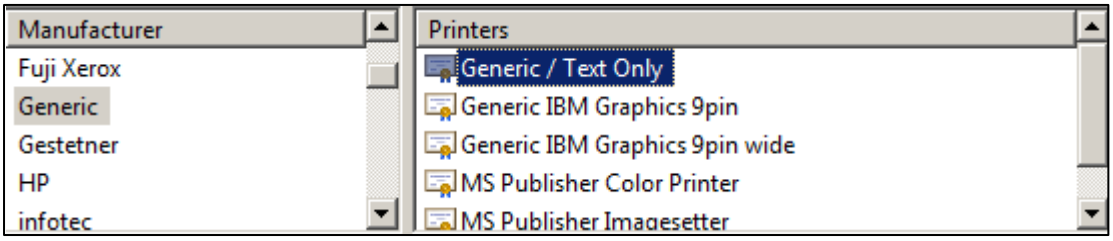
It is useful to enter additional printer information at this stage.

You can often find printer specifications on the manufacturer`s website. For example, HP(n.d) outline the product specifications for the HP910.

The **Printer Found** section outlines the printer settings specified, clicking **Next** will install the printer. After installation, you will have the option to add another printer. Ensure the **Add another printer** box is ticked and click **Finish**.

Follow the steps outlined once more for each printer. The ***Generic/text only*** printer is listed under the manufacturer ***Generic*** as shown in Figure F2.5.

Figure F2.5 – Generic Printer



F3 - Publish Printers in Directory

To publish a printer in the Active Directory, simply right-click the relevant printer in **Printer Management**, and select **List in Directory** (as shown in Figure F3.1). In **Active Directory Users and Computers** you can find the printer in the directory by right-clicking the domain and clicking **Find**, which brings up the **Find Printers** step shown in Figure F3.2.

Figure F3.1 – List Printers in Directory

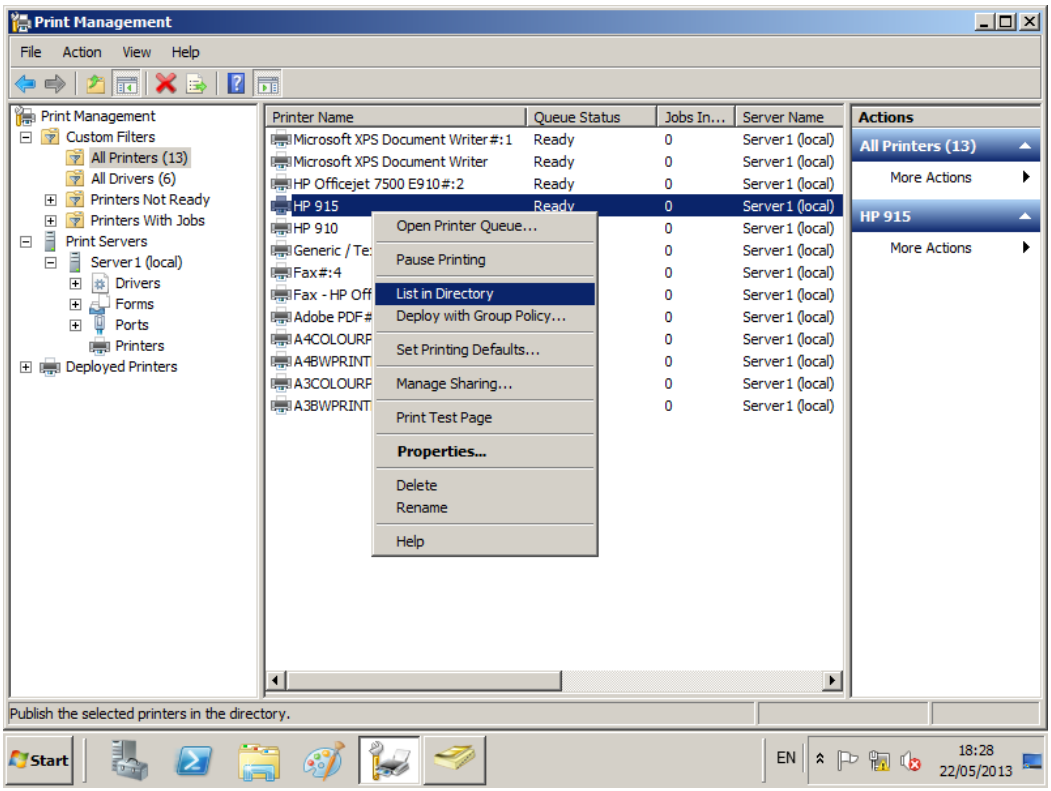
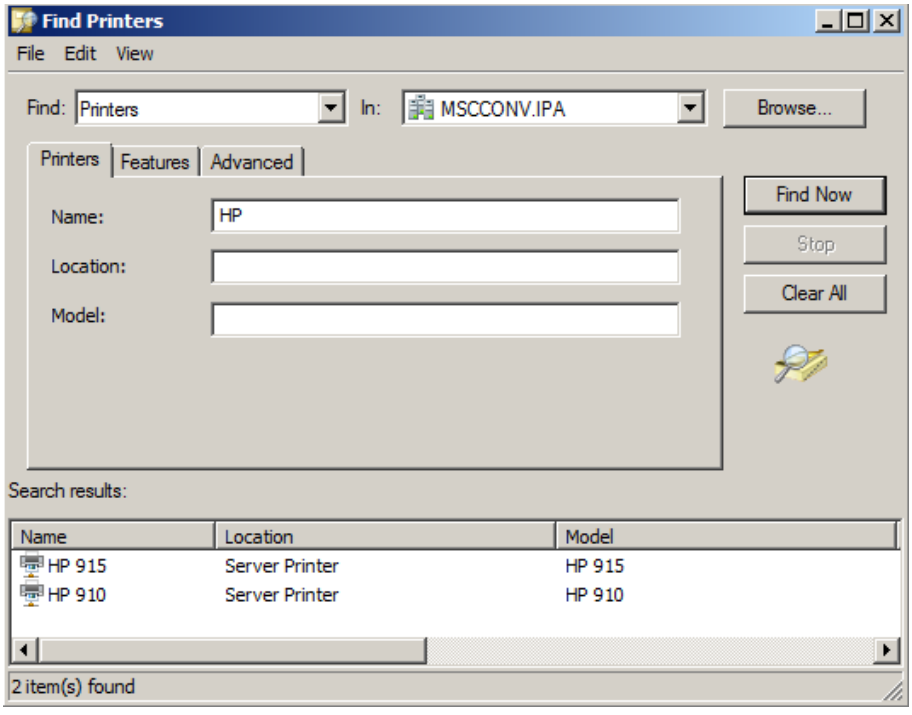


Figure F3.2 – Find Printer in Directory

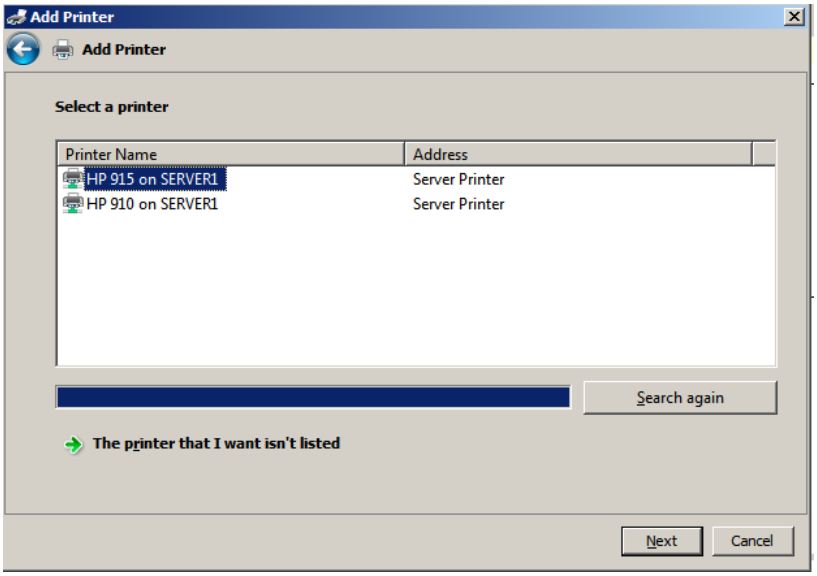


F4 - Adding printers to other machines

To add a printer to your second server, click **Start**, **Devices and Printers** and then click **Add a Printer**. You will then be asked ***What type of printer do you want to install?*** Click **Add a network, wireless or Bluetooth printer** and select **Next** to proceed. You will be brought to the **Select a printer** step as shown in Figure F4.1 which will list the printers found on the network.

Select the printer that you wish to add and click **Next** to continue. You will receive a message that the printer was successfully installed. Upon exiting this window, the printer should be listed in **Devices and Printers**, as shown in Figure F4.2. Repeat the aforementioned steps for each printer that you wish to add. The procedure for the Windows 7 Client machine is also identical.

Figure F4.1 – Adding a printer



INFORMATION

If the printer is not listed you can click **The printer I want isn`t listed**.

You will then be given options to find a printer:

1. In the directory
2. By name i.e. server path
3. By TCP/IP address or hostname
4. Via Bluetooth

Figure F4.2 – Printer Added on Server 2

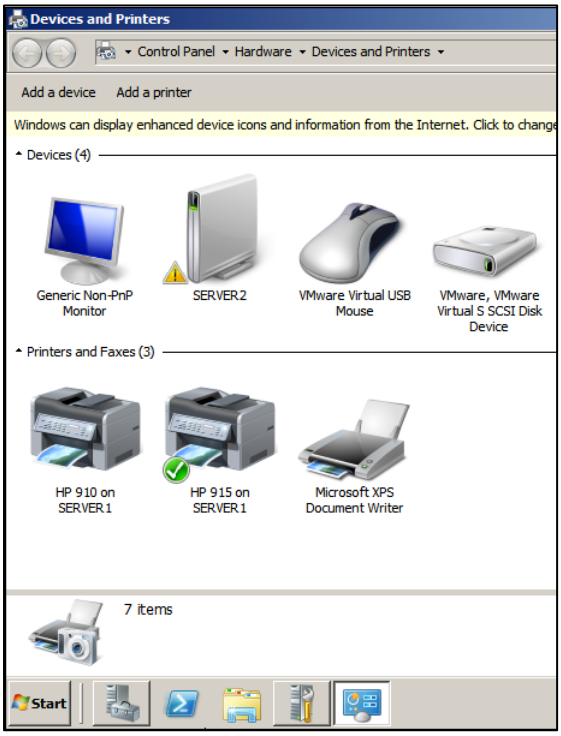
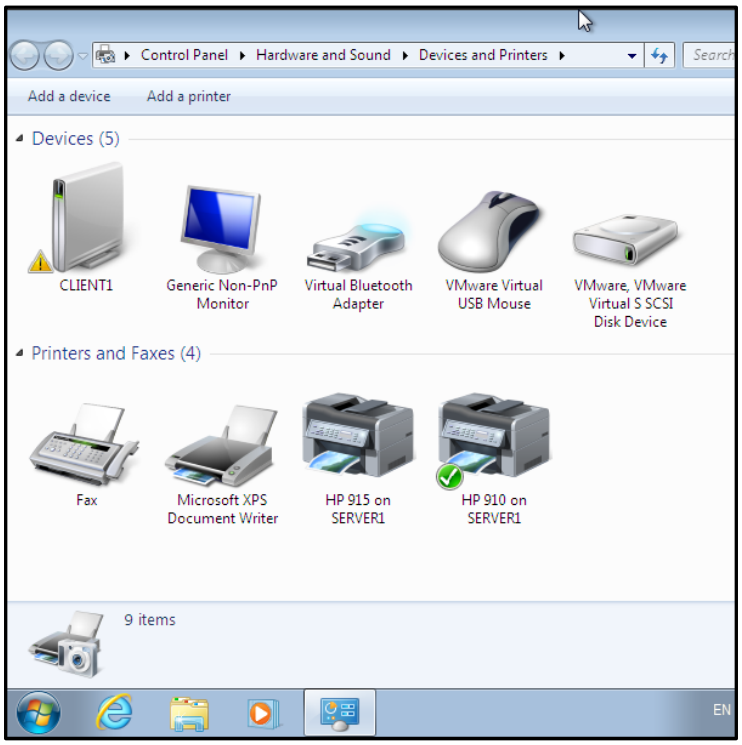


Figure F4.3 – Printers Added to Windows 7 Client Machine



TASK G – FILE SERVER AND REMOTE ADMINISTRATION

G0 - Task Introduction

In this section you will carry out the following tasks:

1. Setup MS-Core as a file server

The Server Core (MS-Core) is enabled as a file server by default, however it is demonstrated in this task how to enable additional file services roles. Furthermore, to test that the file server is working, a text file will be created and saved in **MS-Core**, and accessed on **Client1** after adding the shared folder Snap-in in the Microsoft Management Console (MMC).

Benefits of a File Server

A file server provides a location for the storage of files that can be accessed by any computer on the network. It exists for the storage and retrieval of data – the machines on the network actually work with the data.

---

2. Configure MS-Core for Windows Remote Administration

In order to work with remote administration, the **Remote Server Administration Tools** utility (RSAT) is downloaded and all features are enabled.

Using **sconfig**, the Server Core machine is configured to enable **Remote Server Management** and **MMC Remote Management**. Using **Computer Management** and **Server Manager**, the MS-Core machine is connected which enables the ability for Windows Remote Administration.

Benefits of Windows Remote Administration

It allows the configuration of settings, administration, troubleshooting etc. on a machine from a remote location i.e. without actually having to be at the machine.

---

3. Access MS-Core from Client1 using remote desktop

In the Server Core machine remote desktop is enable using **sconfig**. The firewall is set to allow communication. On the Windows 7 machine, MS-Core is connected to using **Remote Desktop Connection**.

Benefits of Remote Desktop

You can also configure settings etc. from a remote location as per Remote Administration. The difference is that with Remote Desktop, you see and work with the environment as if you were on the machine.

The environment will be displayed in a window, which can be maximized. All key presses and mouse movements are visualised and acted upon as if you were actually using the machine.

G1 - Setup Server Core as a file server

You can run the following command to check what server roles are enabled or disabled:

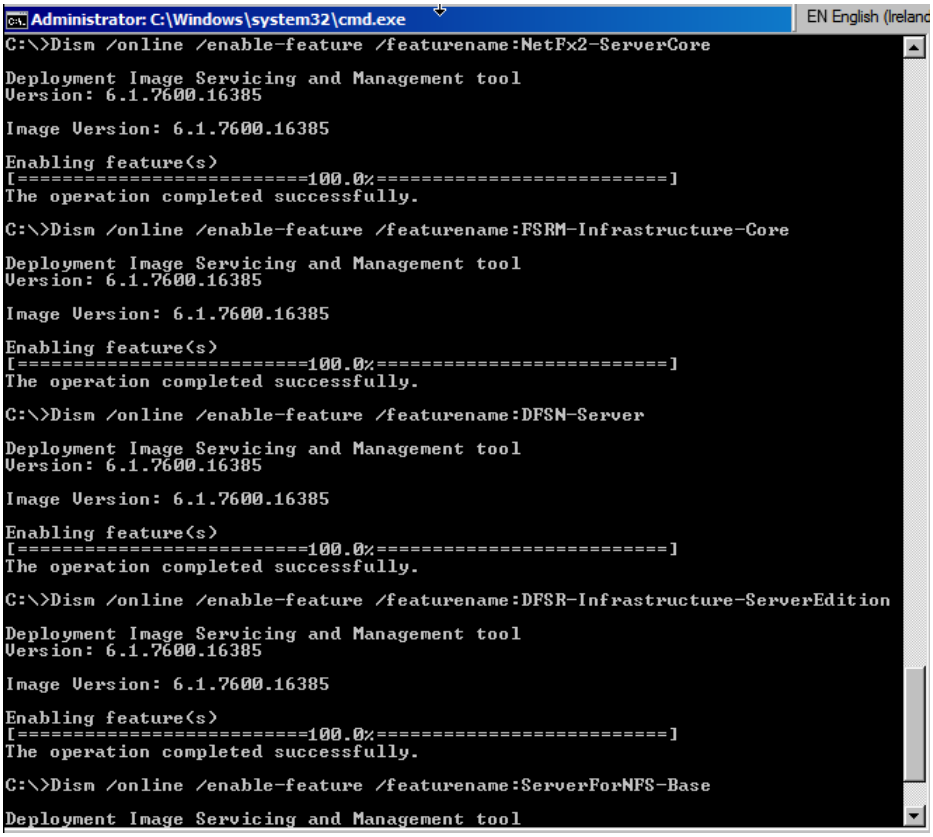
CMD	*Dism /online /get-features /format:table*

Ensure netfx 2 is enabled first as shown in Figure G1.1. The following command is used to enable features:

CMD	*Dism /online / enable-feature /featurename:*

The above command is used in conjunction with the feature names listed in the information box alongside Figure G1.1.

Figure G1.1 – Enabling File Services Roles



INFORMATION

FILE SERVICES ROLES

File Replication Service

FRS-Infrastructure-Core

Distributed File System

DFSN-Server

Distributed File System Replication

DFSR-Infrastructure-ServerEdition

Servers for Network File System

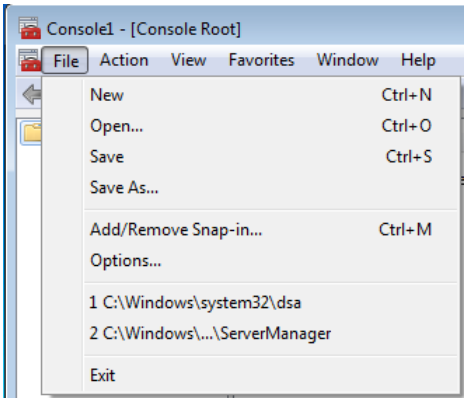
ServerForNFS-Base

Sharing a file from Server Core

To access a file from the Windows 7 Client machine, you may install the Shared Folders snap-in in MMC (Microsoft Management Console). Type **mmc** in the search bar and press **Enter**. You will be brought to the MMC **Console Root**. Click **File** and select **Add/Remove Snap-in** as shown in Figure G1.2.

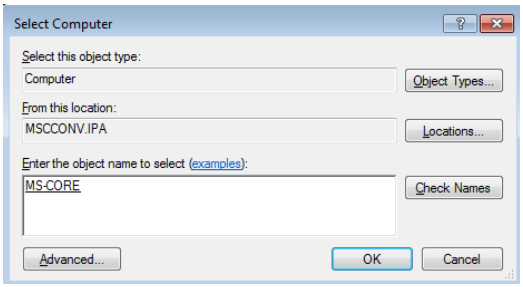
In the **Add or Remove Snap-ins** window, in the left-hand navigation pane highlight **Shared Folders** and click **Add** (Figure G1.3). The **Shared Folders** window will appear. Select **Another computer** and either type the path to the machine or click **Browse**. If you select **Browse** you will be brought to the **Select Computer** window.

Figure G1.2 – MMC Snap-in



In the **Select Computer** window, type ms-core and click **Check Names**. MS-Core should appear underlined as shown in Figure G1.4; click **OK** to continue.

Figure G1.4 – Select Computer



You will be returned to the **Shared Folders** window as shown in Figure G1.5 where the path to the Server Core machine will have been automatically entered in the **Another computer** text box.

Click **Finish** to proceed. To test the implementation has been successful, create a text file on the Server Core machine named ***sharetest.txt***.

To do this, navigate to the **Documents** folder by typing ***cd Documents*** as shown in Figure G1.6. Open Notepad by typing ***notepad.exe***.

Save the text file by clicking **File** and **Save As**, giving it a filename and clicking **OK** as shown in Figure G1.6.

Back in the MMC **Console Root**, right-click **C$** under **Share Name** and click **Open**. You will be displayed with a window to access files on the Server Core.

As shown in Figure G1.7, navigate to the **My Documents** folder and open the ***sharetest*** text document that you create on the Server Core machine.

The path from the shared C Drive is: Users – Administrator.MSCCONV – My Documents.

Figure G1.3 – Add or Remove Snap-ins

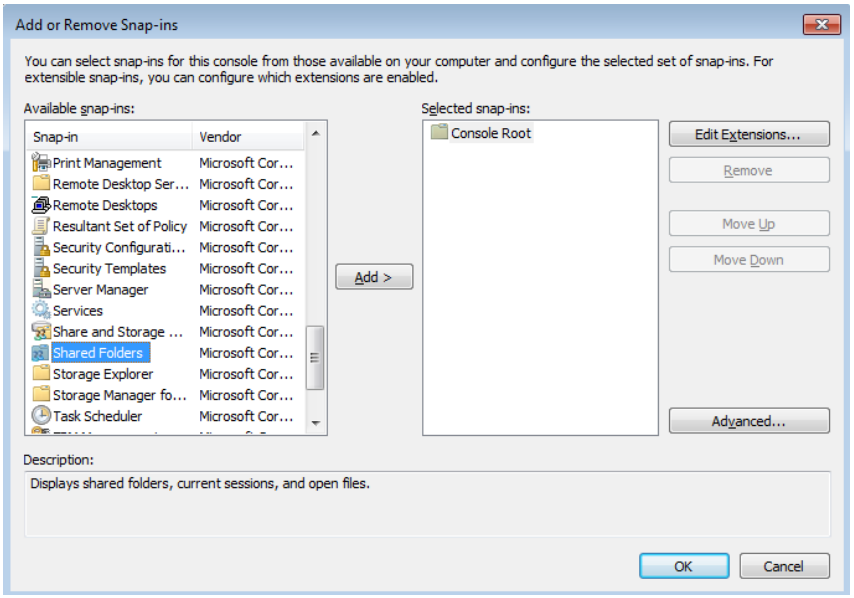


Figure G1.5 – Shared Folders

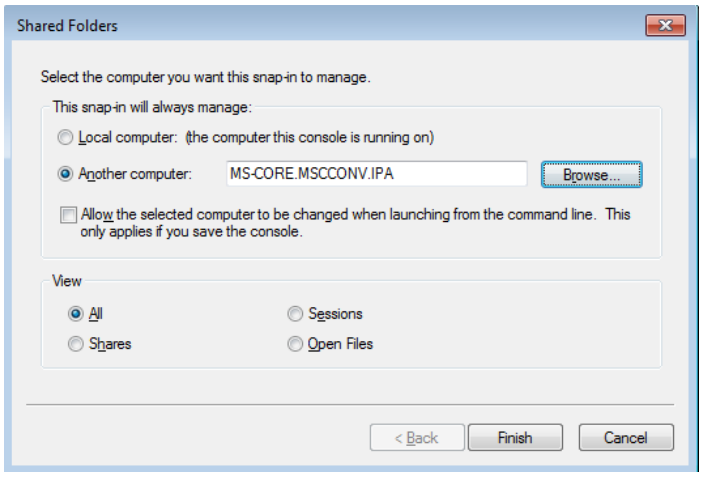


Figure G1.6 – Creating a file to share in Server Core

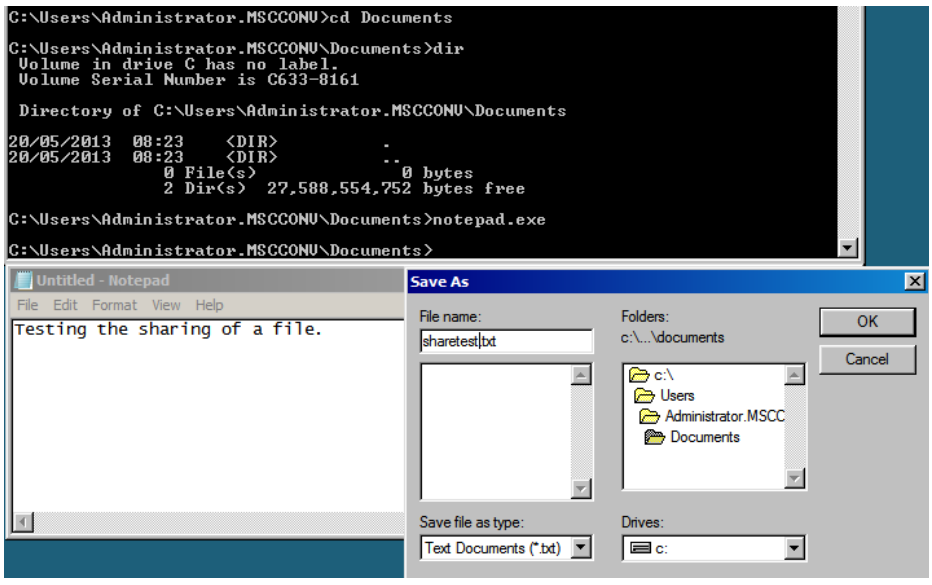
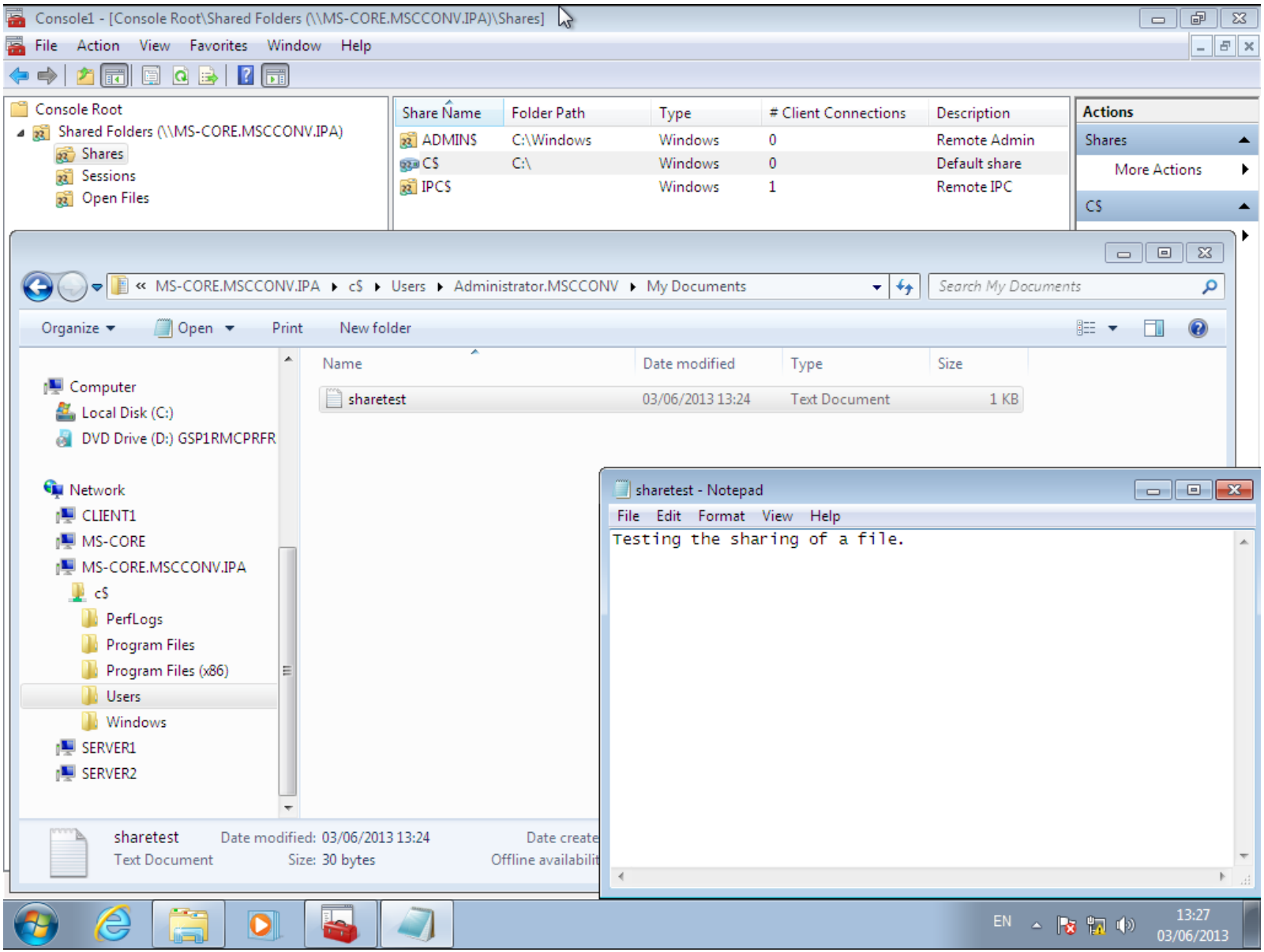


Figure G1.7 – Accessing File from Client 1 Machine

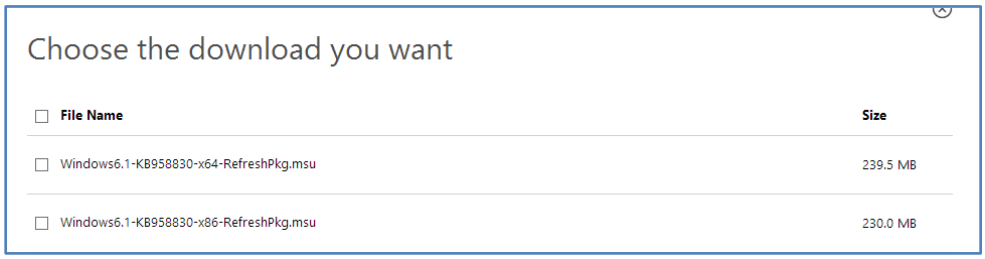


G2 - Configure Server Core for Windows Remote Administration

Download **Remote Server Administration Tools(RSAT)** at http://www.microsoft.com/en-us/download/details.aspx?id=7887.

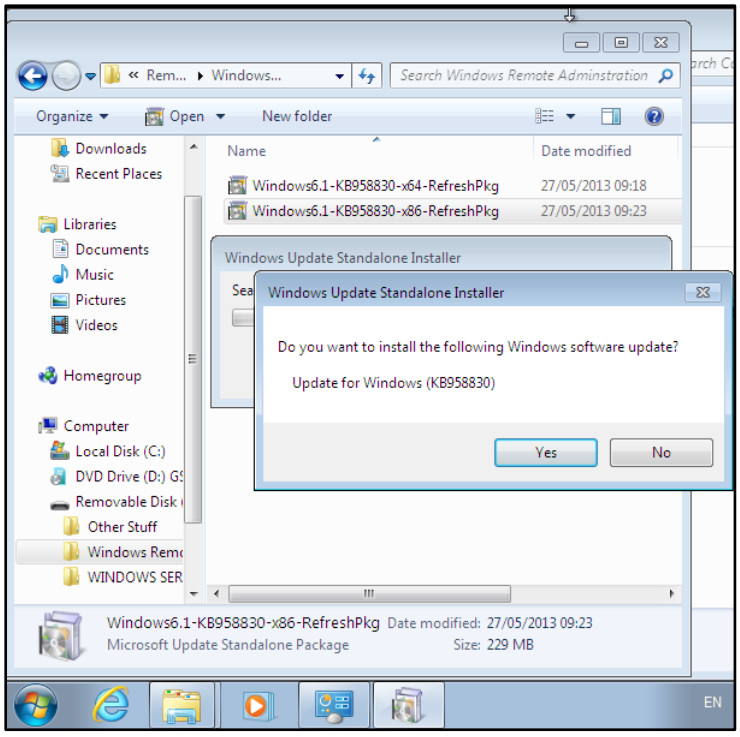
Navigate to the aforementioned link and click the large **download** icon. You will be asked whether to download the 32bit or 64bit version as shown in Figure G2.1 (x64 signifies 64-bit whilst x86 signifies 32-bit). It may be convenient to download both packages if you intend installing this package on multiple systems. Tick the box beside the relevant files and click **Next** to proceed.

Figure G2.1 – choosing RSAT version



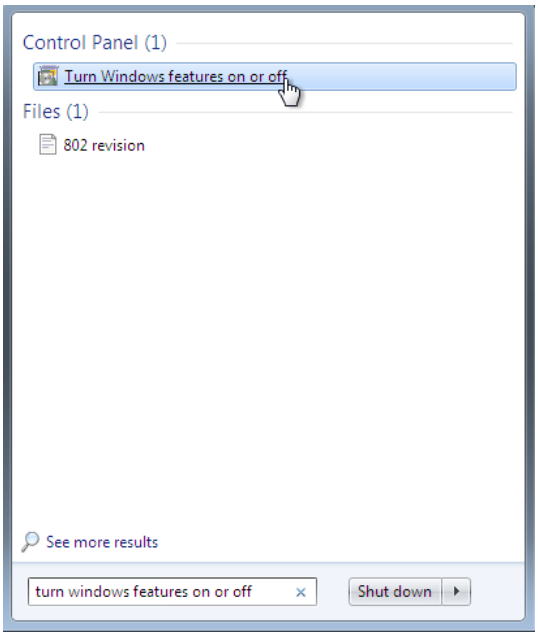
Once the download has completed navigate to the directory to run the relevant installation file. The **Windows Update Standalone Installer** will launch. If you are asked to install a Windows update, as shown in Figure G2.2, click **Yes** to proceed.

Figure G2.2 – Windows Update Standalone Installer



The installation will prepare itself, and you will then arrive at the license terms page. Click **I Accept** to continue. When the installation has completed, click **Close** to exit. The system must be restarted. Upon restart, type "*turn windows features on or off*" in the search bar and click the result under **Control Panel** as shown in Figure G2.3.

Figure G2.3 – Accessing Windows features

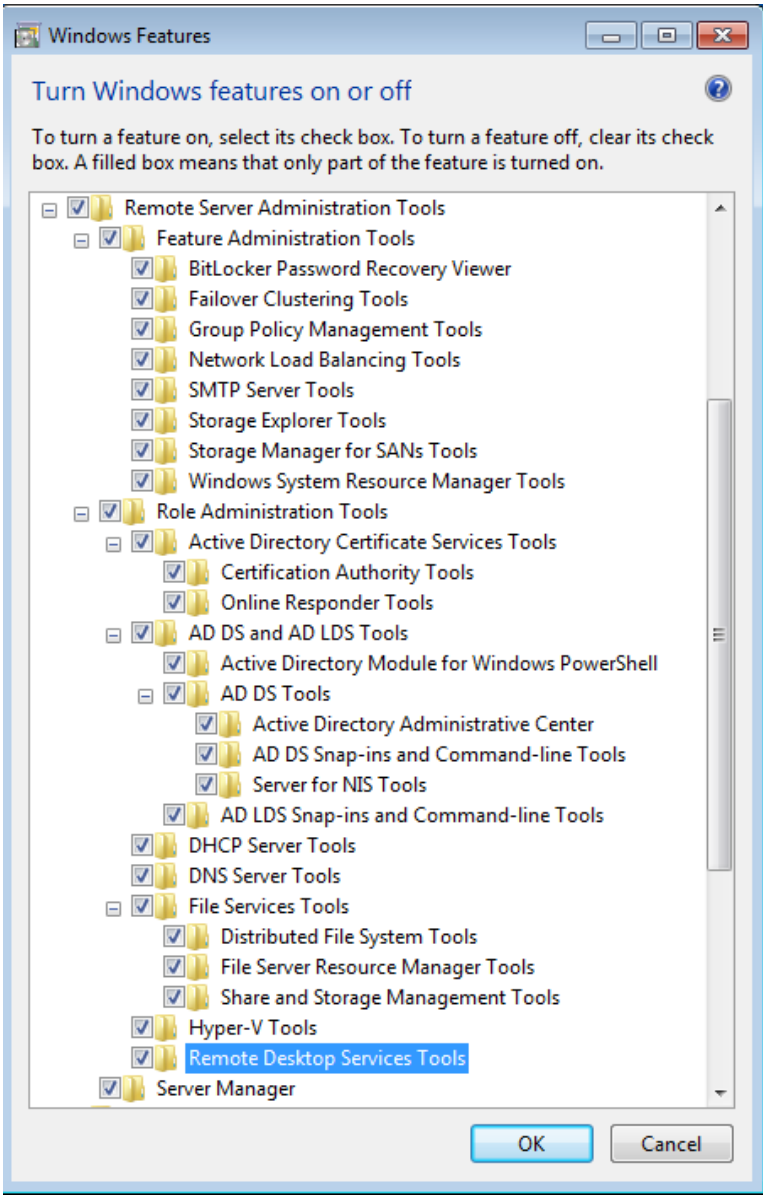


Scroll down until you see **Remote Server Administration Tools(RSAT)**. Expand the list by clicking on the **+** icons until all items are listed as shown in Figure G2.4.

To enable all **RSAT** features, ensure that all the boxes are ticked. After clicking **OK** you will be notified that change may take several minutes to implement.

Now that the **Remote Server Administration Tools** are in place, you must ensure that the firewalls on the server core machine allow remote assistance.

Figure G2.4 – Turn Windows features on or off



On the server core machine, run **sconfig** and type **4** and press **Enter** to work with the **Configure Remote Management** utility. Type **3** and press **Enter** to enable server manager remote management. You may also choose **1** to allow MMC remote management as shown in Figure G2.5 (this allows remote assistance via the **Computer Management** utility).

Figure G2.5 – Sconfig Remote Management Settings

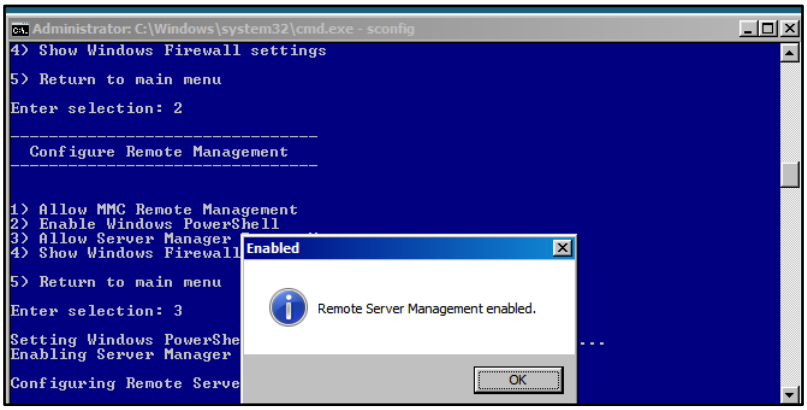
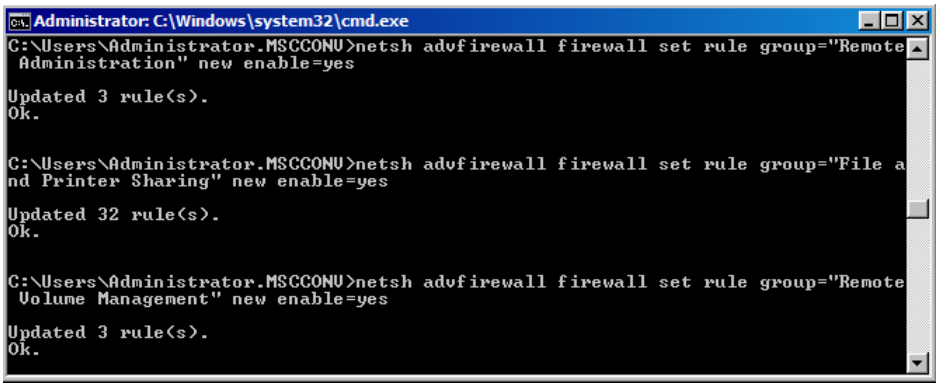


Figure G2.6 – Command Line firewall settings



INFORMATION

You may also use commands at the command line to configure firewall settings; as shown in Figure G2.6.

Computer Management Remote Assistance

In the Windows 7 environment navigate to the computer management utility by searching for **computer management** in the search bar. As shown in Figure G2.7 right-click **Computer Management** and select **Connect to another computer** to proceed. Enter the IP address of the machine that you wish to remote to (MS-Core) beside **Another computer** as shown in Figure G2.8.

Figure G2.7 – Computer Management

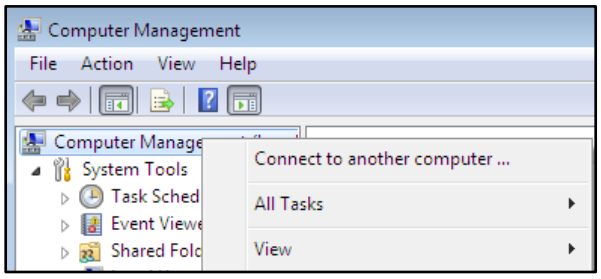


Figure G2.8 – Select Computer

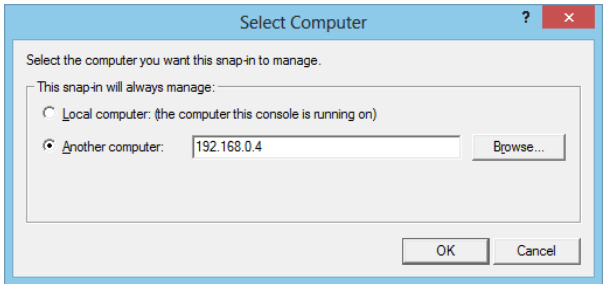


Figure G2.9 – Remote Administration in Computer Management

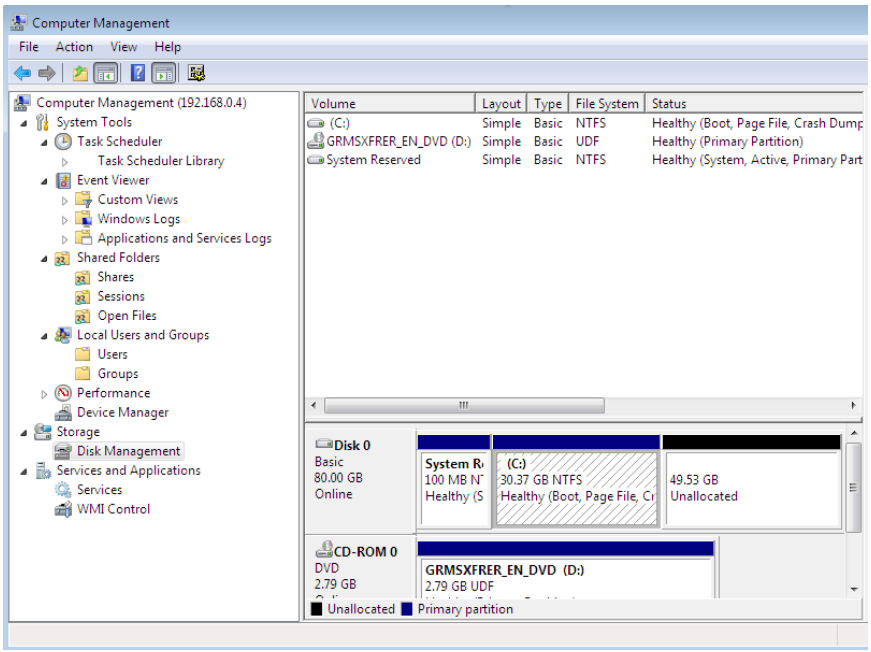


Figure G2.10 - Remote Administration

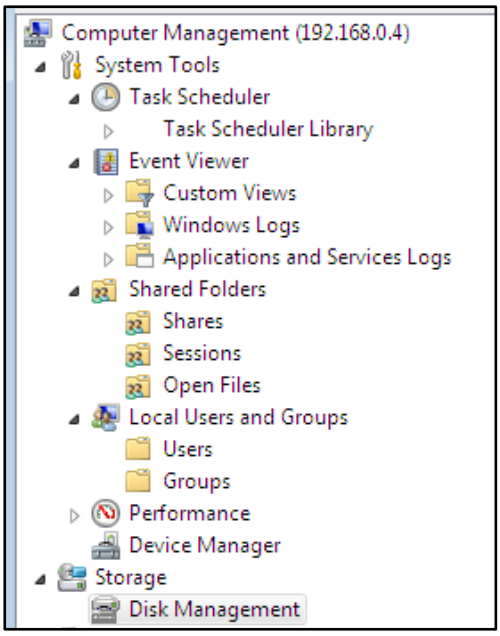


Figure G2.9 and G2.10 above shows the disk management utility pertaining to the Server Core machine accessed via the computer management utility.

Server Manager Remote Assistance

To utilize server manager for remote assistance, search for **server manager** in the search bar. Upon opening you should be prompted to enter the computer name or IP address of the machine that you wish to assist. You can also do this using the **Action** tab or by right-clicking **Server Manager** in the left hand navigation pane. Enter the IP address of the machine that you wish to assist (ensuring that the machine in question is turned on), and click **OK**.

Figure G2.11 – Server Manager

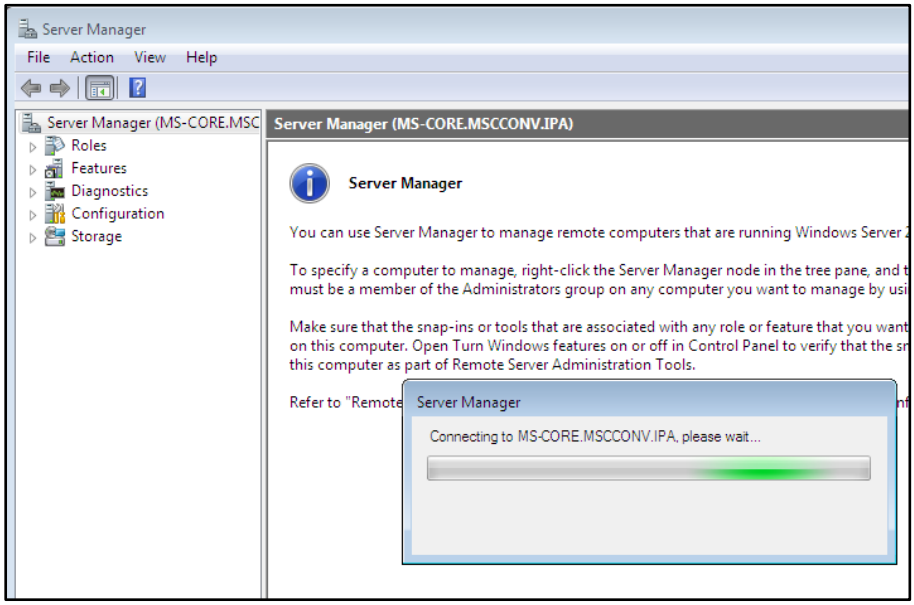
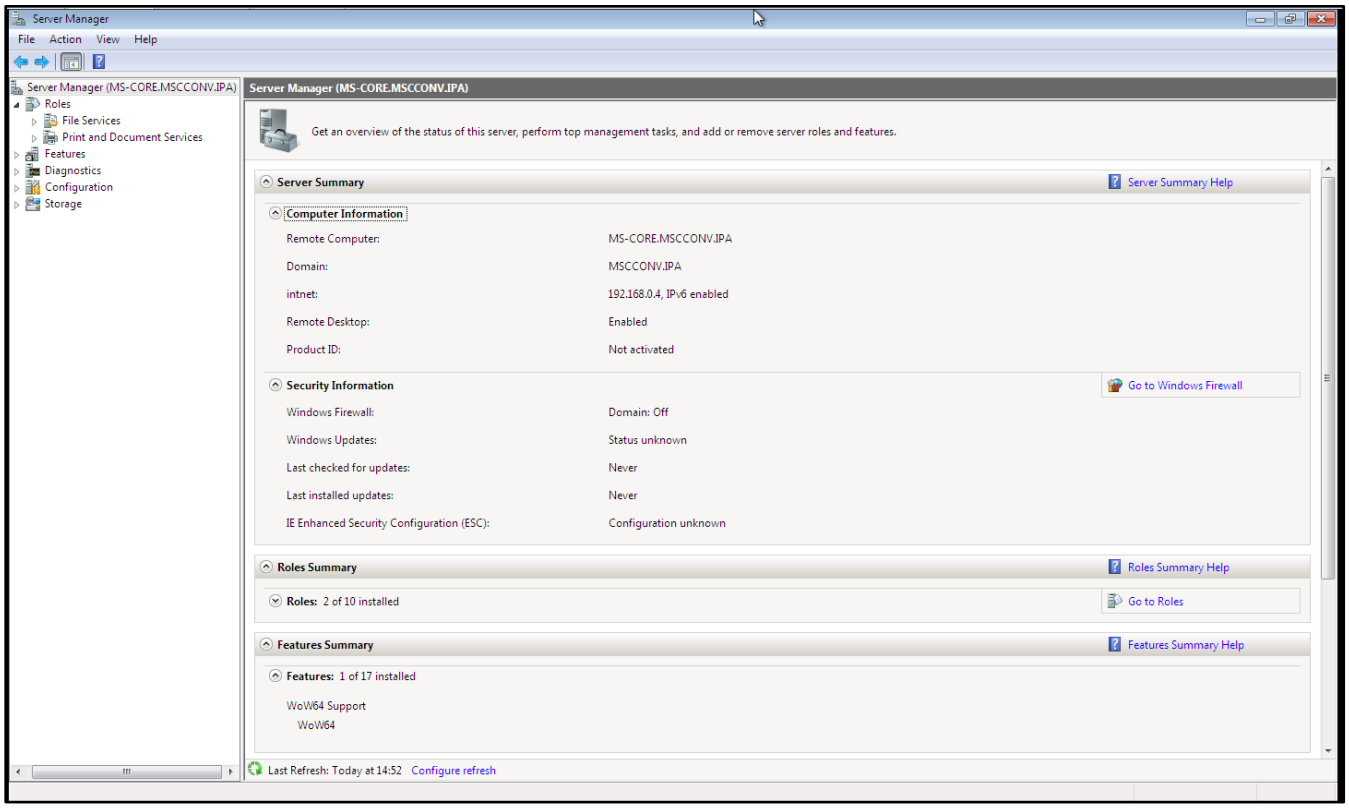


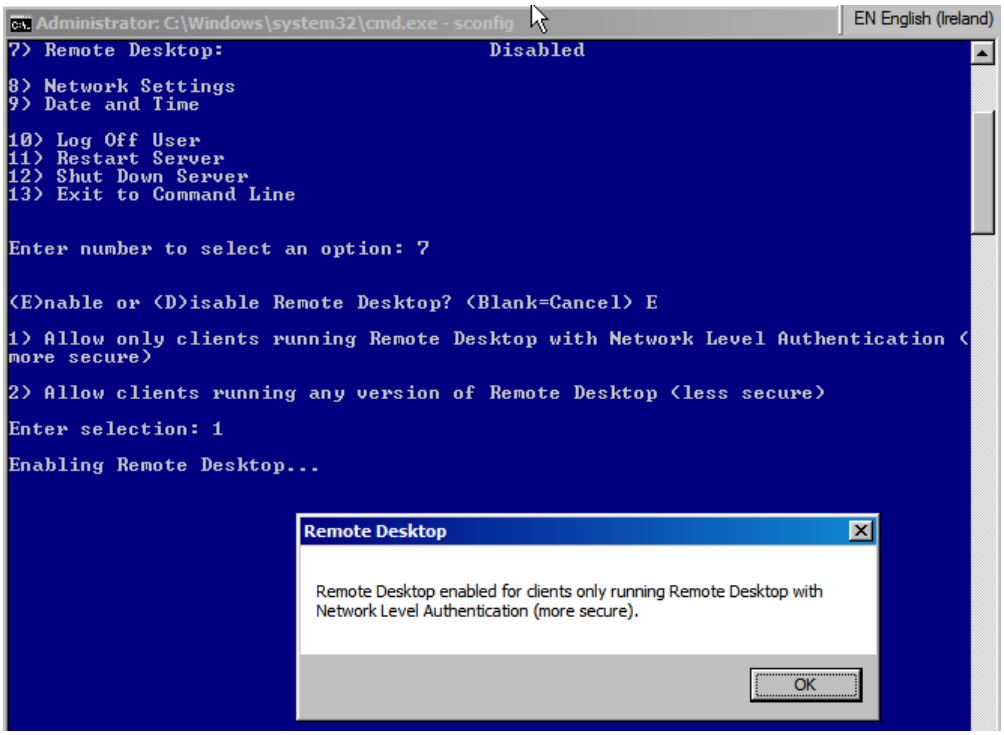
Figure G2.12 – Server Manager connected to Server Core Machine



In Figure G2.12 above, the Server Core is accessed from the Windows 7 Client using remote administration whilst logged on as the Administrator.

G3 - Accessing Server Core from Windows 7 Client using remote desktop

Figure G3.1 – Server Core Remote Desktop Settings



INFORMATION

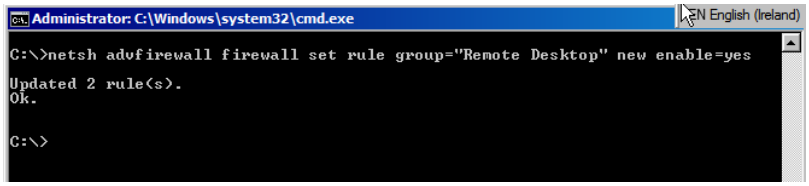
Older machines attempting to connect may require the use of the less secure option 2.

To access the Server Core from the Windows 7 Client machine using remote desktop you must enable remote desktop in Server Core. To do this, run **sconfig** and choose option **7** and press **Enter**.

As shown in Figure G3.1 type E to enable remote desktop and then select 1 as the most secure option. As shown in Figure G3.2, allow the remote desktop to communicate using the following command:

CMD	*netsh advfirewall firewall set rule group="Remote Desktop" new enable=yes*

Figure G3.2 – Remote Desktop Firewall



On the Windows 7 client machine, to initiate the connection type **network** into the search bar. Right-click **MS-Core** as shown in Figure G3.3 and click **Connect with Remote Desktop Connection**.

You can also search for **Remote Desktop Connection** in the search bar and enter in the IP address or computer name of the machine that you wish to connect to.

As shown in Figure G3.4, you will be asked to enter the credentials of the domain administrator in order to remote desktop to the Server Core machine.

Figure G3.3 – Initiating Connection

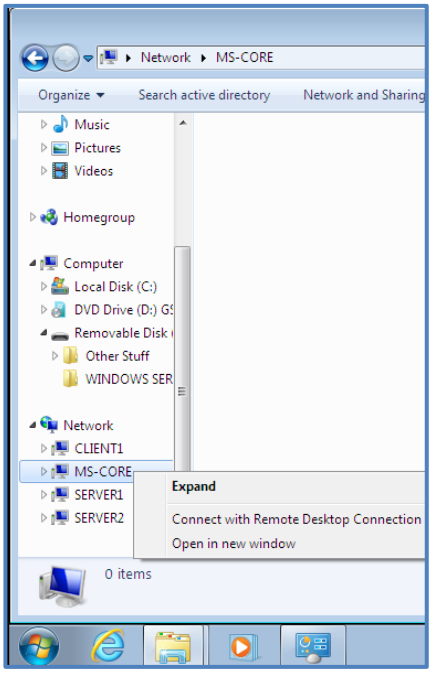


Figure G3.4 – Domain Administrator Credentials

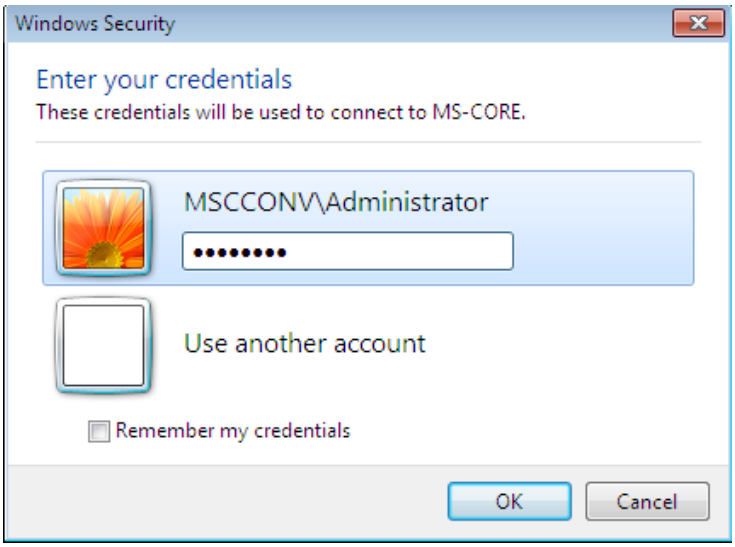
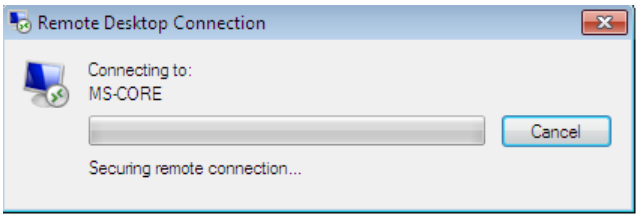
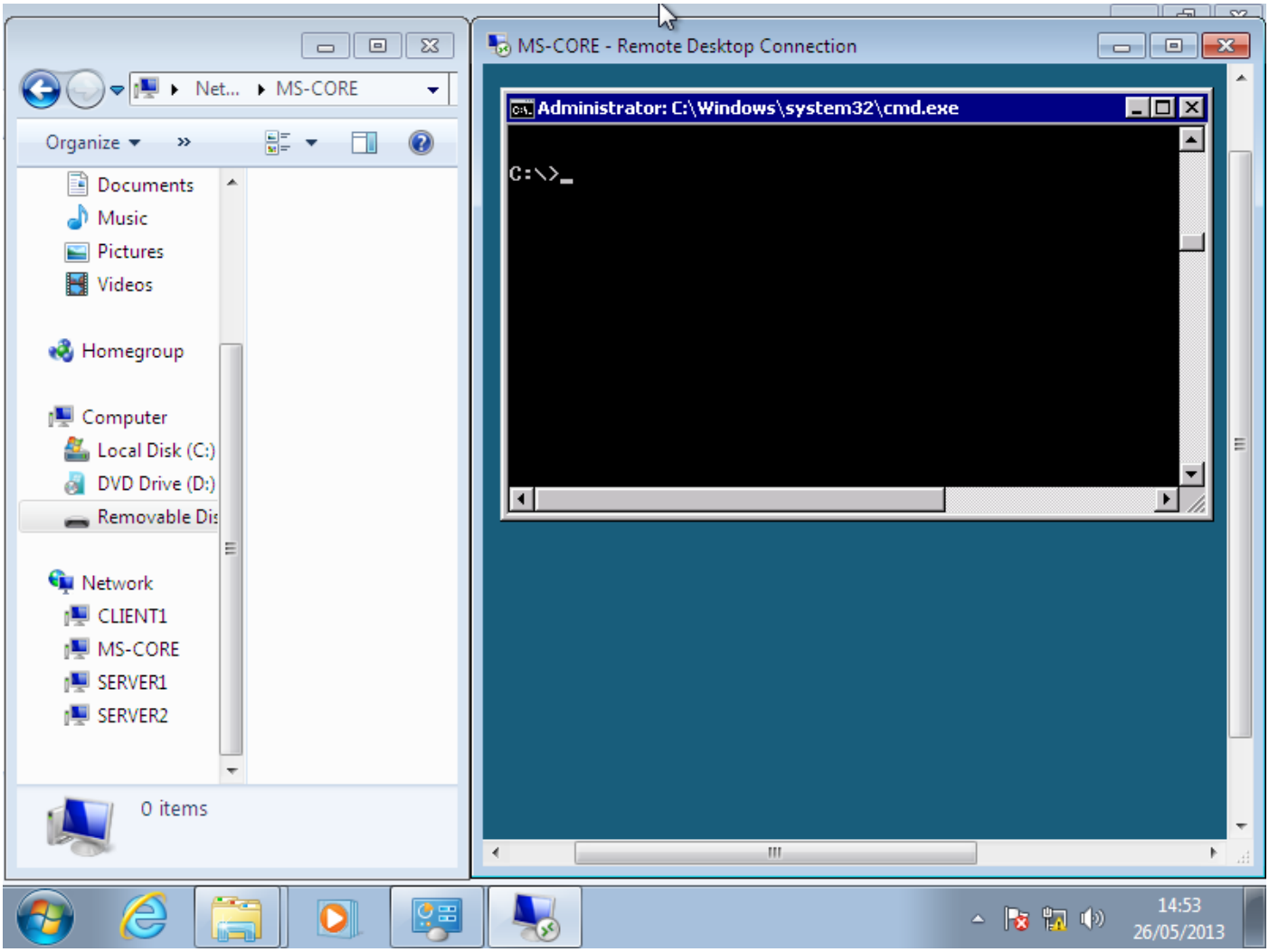


Figure G3.5 – Connection in Progress



Should the connection be successful, you will be presented with an instance of the Server Core machine in a window on the Windows 7 client machine as shown in Figure G3.6. Note that you will be automatically logged out of the Server Core machine. If you log back into this machine, the remote desktop connection will be lost on the Windows 7 client machine.

Figure G3.6 – Connected to Server Core using Remote Desktop



TASK H - DHCP

H0 - Task Introduction

In this section, you will carry out the following tasks:

1. Add the DHCP Server Role

This role is added in the **Server Manager** utility. In the **DHCP Server Wizard**, you will be asked to confirm the parent domain, DNS settings, and to specify a range of IP address for the network (the scope).

Client1 is set to obtain an IP address automatically. It is verified that the IP address is received from DHCP by running **ipconfig** in the command prompt.

---

2. Disable DHCP Services

DHCP Services will be disabled to test what IP address **Client1** receives after the event. The machine will receive an APIPA address, which is short for Automatic Private IP Addressing. As discussed by Webopedia (n.d) "*With APIPA, DHCP clients can automatically self-configure an IP address and subnet mask when a DHCP server isn`t available"*.

The APIPA address range is 169.254.0.1 to 169.254.255.254. APIPA will regularly check for the DHCP server, and if discovered, the DHCP server will take over.

H1 - DHCP Server Role Wizard

Open **Server Manager** and click **Add Roles** in the right-hand pane. Tick the box marked **DHCP Server** from the list of roles and click **Next**.

Click **Next** on the **DHCP Server** stage which introduces and explains what DHCP does. On the ***network connections bindings*** stage you will be asked to select the network connection to work with; highlight the connection and click **Next**.

This will bring you to the ***IPv4 DNS Settings*** stage shown in Figure H1.2. Check that the parent domain and DNS settings are correct and select **Next** to continue.

You will be asked to specify WINS, select ***WINS is not required*** and click **Next** to continue. As outlined by TechNet(n.d),WINS is a naming service required only by older Windows systems.

You will now be required to add a DHCP scope. As shown in Figure H1.3, click **Add** and the ***Add Scope*** window will appear. Give the scope a meaningful name.

Figure H1.1 – Add Roles Wizard

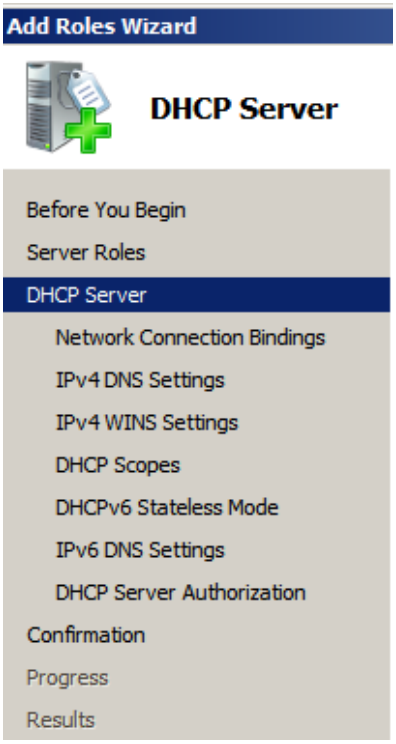


Figure H1.2 – Ipv4 DNS Settings

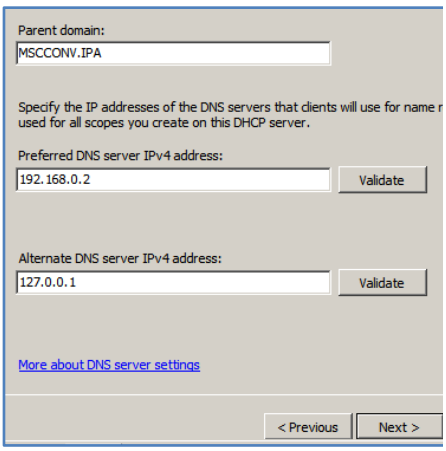
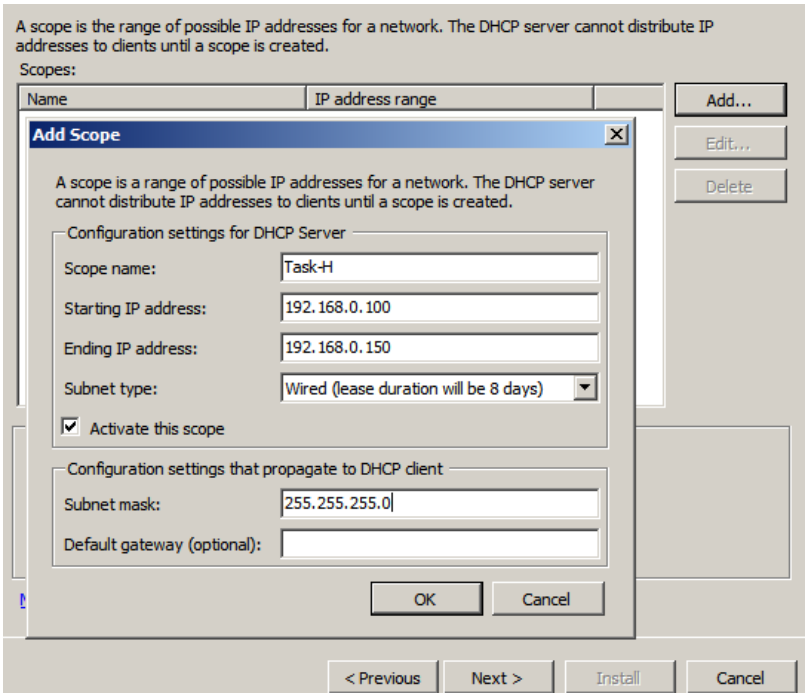


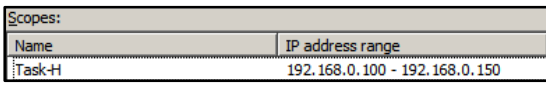
Figure H1.3 – Adding a Scope



Give the scope a starting and ending IP address as shown, and specify that the ***Subnet type*** is to be wired. Ensure that ***Activate this scope*** is ticked and also specify the subnet mask. The default gateway is to be left blank since we are working with a private internal network throughout this manual.

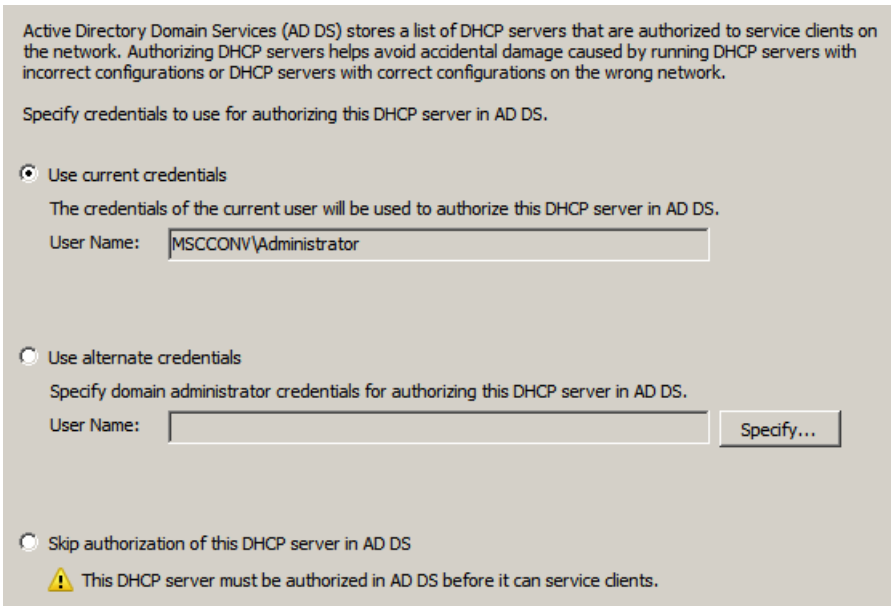
Back in the main scope window the scope should be specified as shown in Figure H1.4. Click **Next** to proceed.

Figure H1.4 – Scope Created



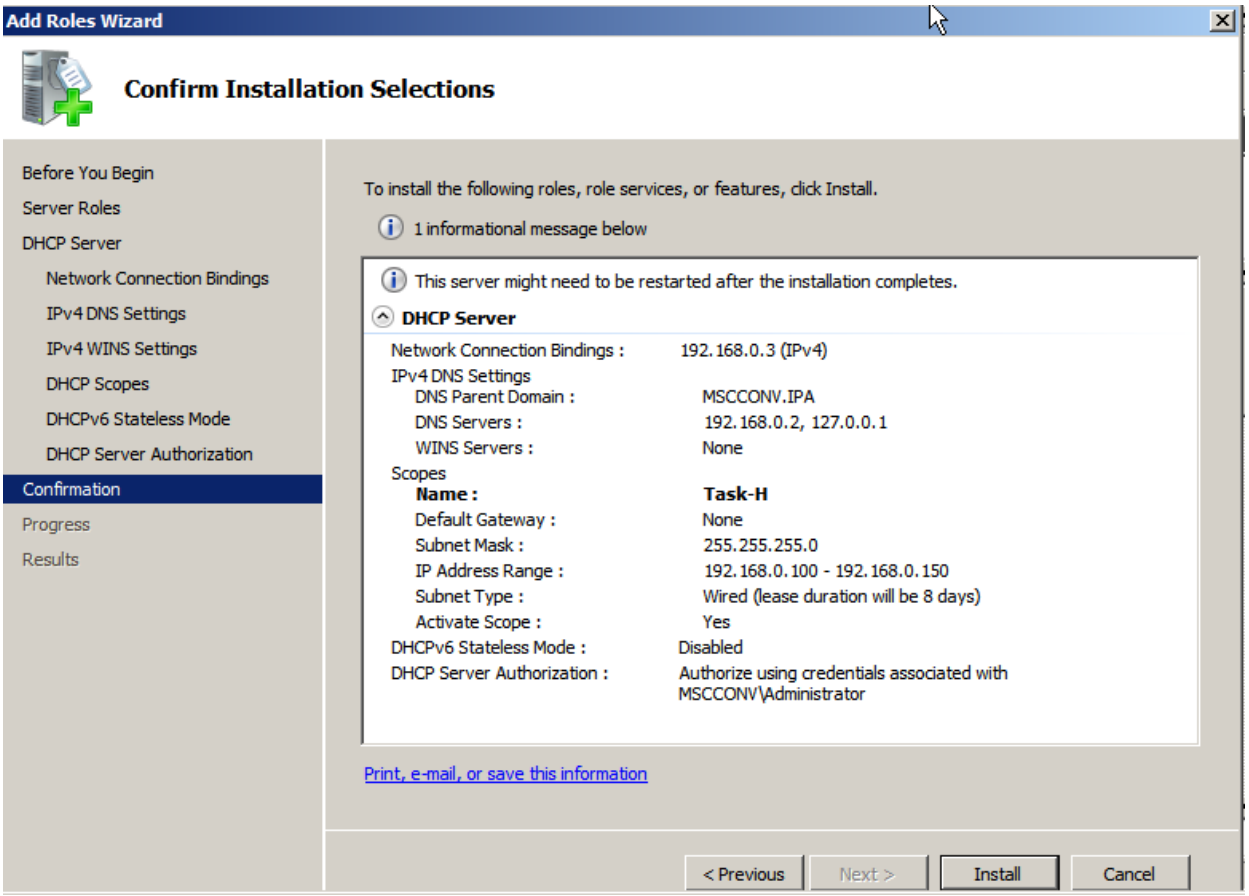
In the next window you will be asked to specify the ***DHCPv6 stateless mode***. Since we do not deal with IPv6 in this manual select ***Disable DHCPv6 stateless mode for this server*** and click **Next.** The next window deals with authorizing the DHCP server in AD DS. Click **Use current credentials** if you are sure the details are correct (as shown in Figure H1.5), and click **Next** to proceed.

Figure H1.5 – Credentials to authorize DHCP Server



You will be presented with the confirmation window which outlines the DHCP settings specified as shown in Figure H1.6. This provides an opportunity for you to review the settings. If you wish to change anything you may click **Previous**, otherwise click **Install** to proceed.

Figure H1.6 – Confirm Installation Selections



You will now be alluded to the progress of the installation. Once the installation has completed, you should receive a message that the DHCP role was successfully installed. Click **Close** to proceed.

H2 - Verify Successful DHCP Implementation

On the Windows 7 client machine navigate to your network IPv4 settings and ensure that settings are obtained

On the server machine, search for **DHCP** in the search bar, open it, and expand the views; selecting **Address Leases** under the scope as shown in Figure H2.1.

In the right-hand pane you should see the IP address and name of the Windows 7 client machine. In Figure H2.2, **ipconfig** verifies that Client1 had received the correct address.

Figure H2.1 – Ipv4 Properties

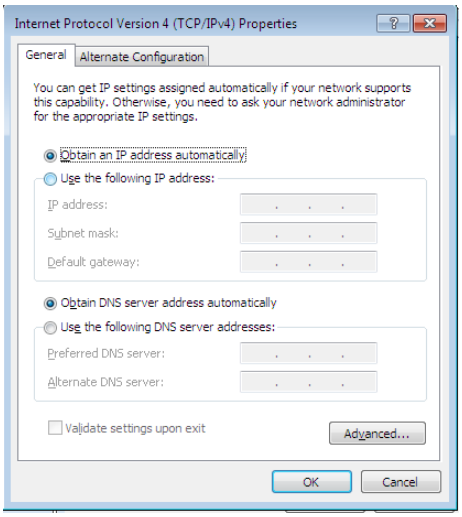


Figure H2.1 – DHCP Utility

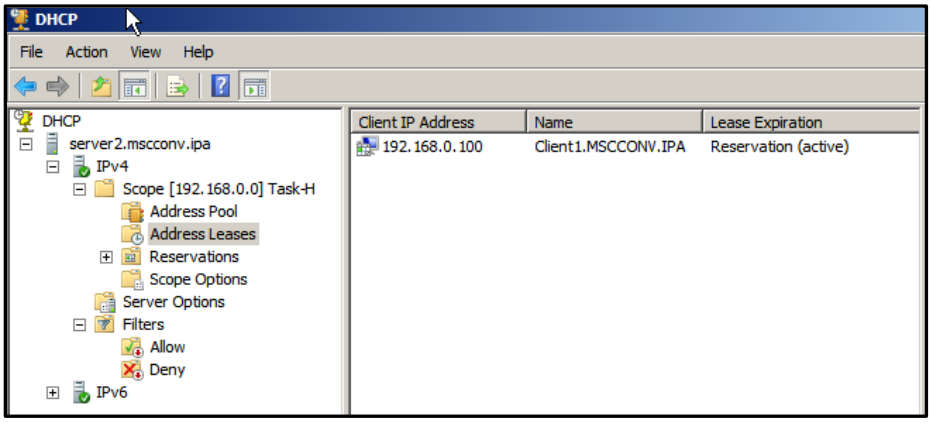
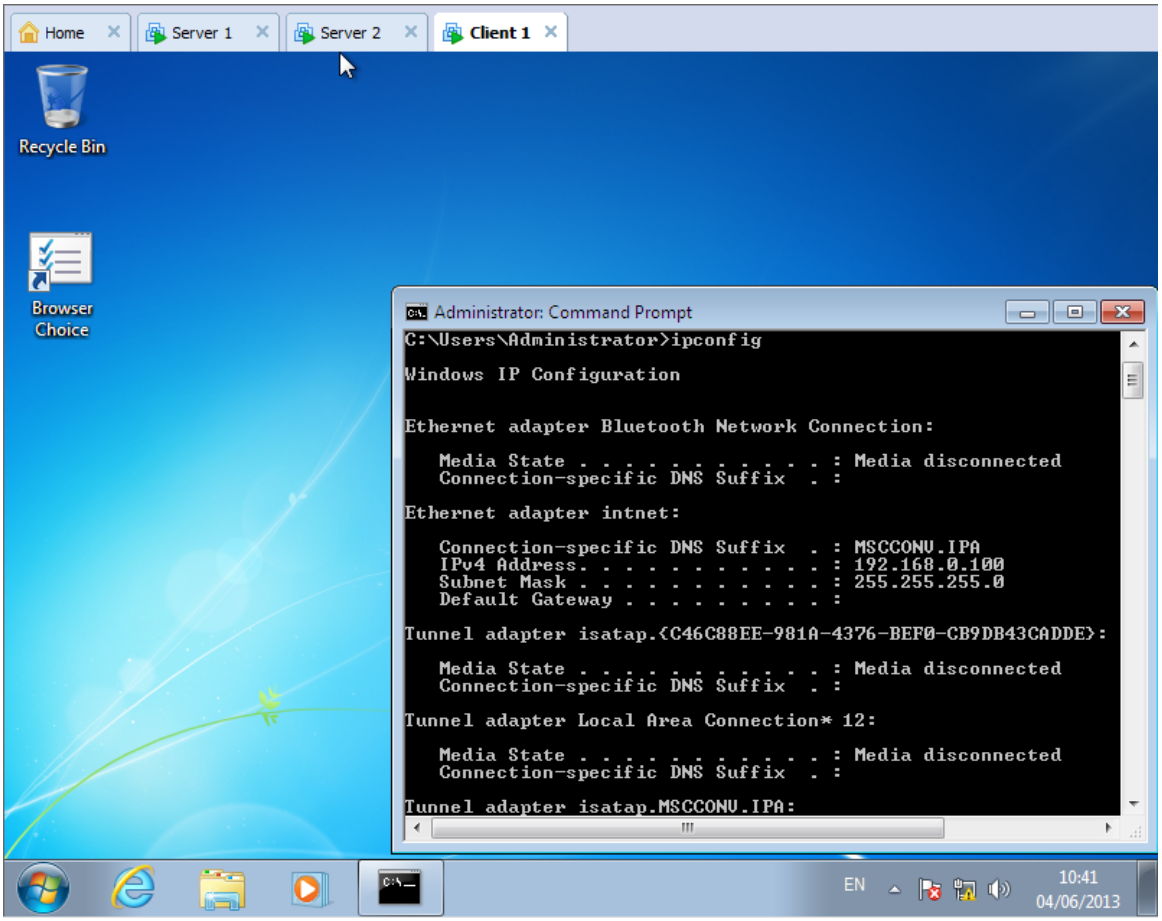


Figure H2.2 – DHCP verified by IPCONFIG on Client1



H3 - Disabling DHCP Services

To disable DHCP services open the DHCP utility, right-click **server2.mscconvipa** (as shown in Figure H3.1), select **All Tasks** and click **Stop**. You will receive the messages shown in Figure H3.2 and Figure H3.3.

Figure H3.1 – Stop DHCP

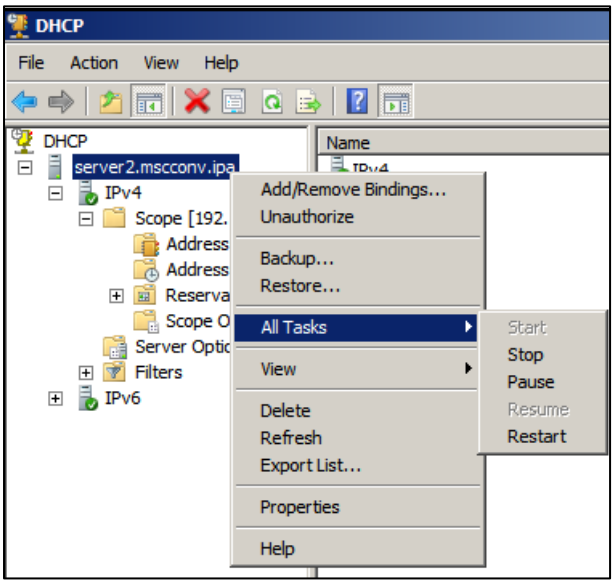


Figure H3.2 – Stopping DHCP

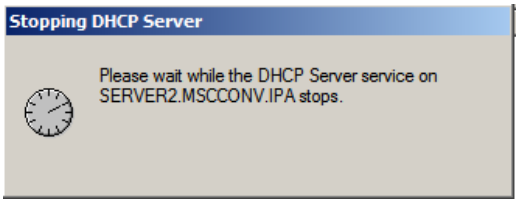
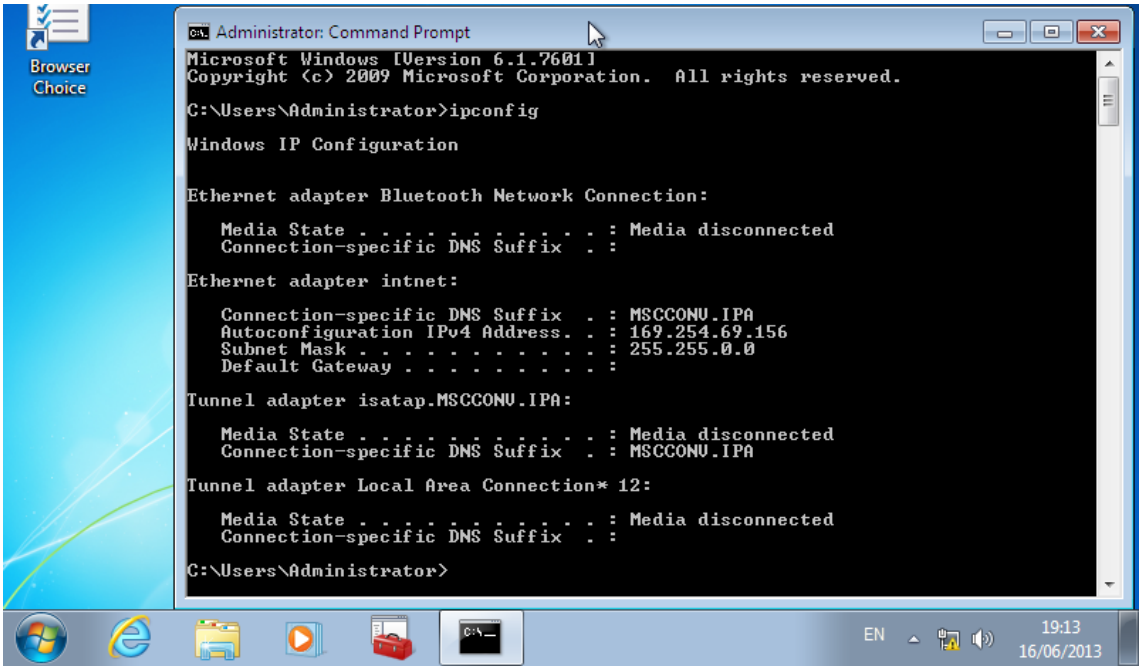


Figure H3.3 – Cannot find the DHCP Server

To check what address **Client1** gets, run **ipconfig** in the command prompt as shown in Figure H3.4. The address **169.254.69.156** is shown. As discussed in the Task Introduction, this is an APIPA address.



APIPA is explained comprehensively by Lowe,D. (2013,p.329):

> If a Windows computer is configured to use DHCP but the computer can't obtain an IP address from a DHCP server, the computer automatically assigns itself a private address by using a feature called Automatic Private IP Addressing (APIPA). APIPA assigns a private address from the 169.254.x.x range and uses a special algorithm to ensure that the address is unique on the network. As soon as the DHCP server becomes available, the computer requests a new address, so the APIPA address is used only while the DHCP server is unavailable.

TASK I –

DECOMMISSION DOMAIN CONTROLLER 2 FROM ACTIVE DIRECTORY

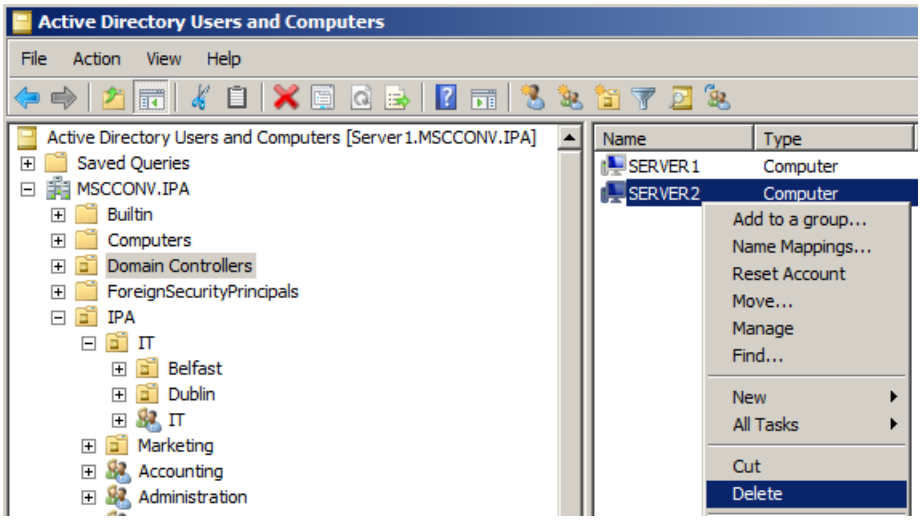
I0 - Task Introduction

Normally, a domain controller (DC) would be decommissioned from the Active Directory system by running DCPromo on the DC itself. However, since the server is unbootable, the Domain Controller object must be deleted in the Domain Controller`s Organization Unit.

I1 – Decommissioning Server2

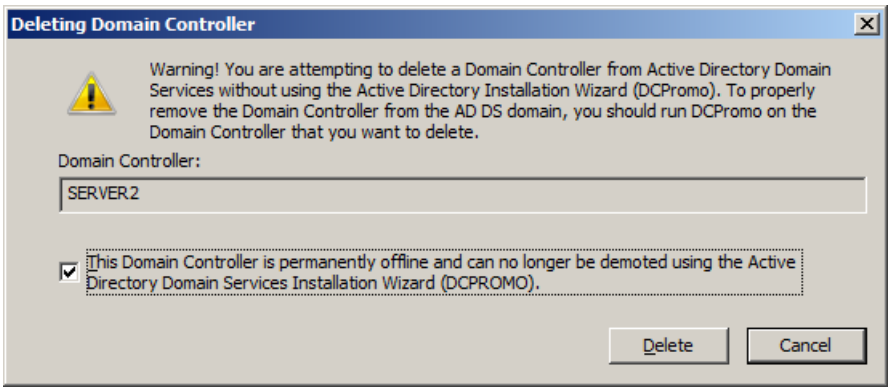
Open **Active Directory Users and Computers** and click on the **Domain Controllers** OU. Right-click **Server2** and click **Delete** as shown in Figure I1.1. You will be asked to confirm that you wish to delete the computer, click **Yes** to proceed.

Figure I1.1 – Delete DC



You will be warned that you are attempting to delete a DC without using DCPromo. Ensure that the box beside **This Domain Controller is permanently offline and can no longer be demoted using the Active Directory Domain Services Installation Wizard (DCPROMO)** is ticked as shown in Figure I1.2 and click **Delete** to continue.

Figure I1.2 - Warning



INFORMATION

As per the network diagram, the MS-Core`s preferred DNS Server is set to be the IP address of the Server2 machine.

It is advisable to change this preferred DNS to Server1`s IP address, as well as Client1`s alternate DNS address.

You will be informed that the DC is a global catalog, click **Yes** to proceed. **Server2** will now no longer be listed in the DC OU and it has been successfully decommissioned.

If the unbootable server becomes bootable at a later stage, you will have to use the **dcpromo/forceremoval** command, as discussed by Minasi, Gibson, Finn, Henry and Hynes (2010, p.264):

> If the failed DC is later recovered, you won't be able to remove Active Directory using DCPromo normally. However, there's a workaround. Instead of just entering dcpromo alone, enter dcpromo /forceremoval. The /forceremoval switch will allow Active Directory to be removed without accessing another DC in the domain.

REFERENCES

1. Black, U. (2009). Sams Teach Yourself Networking in 24 Hours. United States of America: Pearson Education, Inc.

2. Clines, S., Loughry, M. (2008). Active Directory for Dummies, 2nd Edition. Indianapolis, Indiana, United States of America: Wiley Publishing, Inc.

3. Google (2007). Failure Trends in a Large Disk Drive Population. In Usenix (Ed.) *Proceedings of the 5th USENIX Conference on File and Storage Technologies (FAST'07), February 2007*. [Electronic Version]. Retrieved 13th June, 2013, from http://static.googleusercontent.com/external_content/untrusted_dlcp/research.google.com/en//archive/disk_failures.pdf

4. Habraken, J. (2008). Sams Teach Yourself Windows Server 2008 in 24 Hours. United States of America: Sams Publishing.

5. Holme,D., Ruest,N., Ruest,D., Kellington,J.(2011). MCTS Self-Paced Training Kit (exam 70-640): Configuring Windows Server 2008 Active Directory (2nd Edition). Washington, United States of America: Microsoft Press.

6. HP (n.d). HP 910 Series Printers - Product Specifications. *hp.*com. Retrieved 16th June, 2013 from http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01042881&lang=en&cc=us&taskId=110&contentType=SupportFAQ&prodSeriesId=3374057

7. Lowe, D. (2013). Networking All-In-One For Dummies. Hoboken, New Jersey, United States of America: John Wiley & Sons, Inc.

8. Mackenzie-Low,B.(April 28th, 2011). Windows GPT Disks - Is Bigger Really Better?. Petri IT Knowledgebase. Retrieved June 14th, 2013, from http://www.petri.co.il/gpt-vs-mbr-based-disks.htm

9. McLean, I. & Thomas, O. (208). Windows Server 2008 Server Administrator Self-Paced Training Kit. United States of America: Microsoft Press.

10. Meyers, M. (2012). All in one CompTIA A+ Certification Exam Guide Eight Edition. United States of America: McGraw Hill.

11. Meyers, M., Jernigan, S., (2013). Mike Meyers Certification Passport CompTIA A+ Certification Fifth Edition. United States of America: McGraw Hill.

12. Microsoft (2010). Introducing Windows Server 2008 R2. United States of America: Microsoft Press.

13. Microsoft Support (September 15th 2011.). Frequently asked questions about the Microsoft Support Diagnostic Tool (MSDT) when it is used with Windows 7 or Windows Server 2008 R2 - Revision 2.1. *support.microsoft.com*. Retrieved June 12th, 2013, from http://support.microsoft.com/kb/973559

14. Minasi, M., Gibson, D., Finn, A., Henry, W., Hynes, B. (2010). Mastering Microsoft® Windows Server® 2008 R2. Indianapolis, Indiana, United States of America: Wiley Publishing, Inc.

15. Morimoto, R., Noel, M., Droubi, O., Mistry, R., Amaris, C., & Yardeni, G. (2010). Windows Server 2008 R2 Unleashed. United States of America: Pearson Education, Inc.

16. O Neill (2007). Windows Server 2008 Protection from Accidential Deletion. Retrieved June 14th,2013 from http://blogs.technet.com/b/industry_insiders/archive/2007/10/31/windows-server-2008-protection-from-accidental-deletion.aspx

17. Ross, K.W, & Kurose, J.F. (2010). Computer Networking, A Top-Down Approach, Fifth Edition. United States of America: Pearson Education, Inc.

REFERENCES

18. Spears, R.A. (2005). McGraw-Hill`s Dictionary of American Idioms and Phrasal Verbs. United States of America: The McGraw-Hill Companies, Inc.

19. Stanek, W.R. (2008). Windows Server 2008 Inside Out. Washington, United States of America: Microsoft Press.

20. TechNet (n.d). DHCP and WINS. *Technet.microsoft.com.* Retrieved 27th May, 2013 from http://technet.microsoft.com/en-us/library/cc958937.aspx

21. TechNet (n.d.). Folder Redirection Overview. *Technet.microsoft.com.* Retrieved 28th May, 2013 from http://technet.microsoft.com/en-us/library/cc732275.aspx

22. TechNet (n.d.). Renaming the Administrator account. *Technet.microsoft.com*. Retrieved June 12th, 2013, from http://technet.microsoft.com/en-us/library/cc747353(v=ws.10).aspx

23. TechNet (n.d.). Windows Server 2008 System Requirements. *Technet.microsoft.com*. Retrieved June 12th, 2013, from http://technet.microsoft.com/en-us/windowsserver/bb414778

24. Tittel, E., Korelc, J. (2008). Windows Server 2008 for Dummies, 2nd Edition. Indianapolis, Indiana, United States of America: Wiley Publishing, Inc.

25. Tulloch, M. (2009). Windows Server 2008 Server Core Administrator`s Pocket Consultant. United States of America: Microsoft Press.

26. Vanover, R. (2010); NTFS allocation unit sizes for large volumes. TechRepublic. Retrieved June 14th,2013 from http://www.techrepublic.com/blog/datacenter/ntfs-allocation-unit-sizes-for-large-volumes/2678

27. Webopedia (n.d). APIPA. *Webopedia.*com. Retrieved 16th June,2013 from http://www.webopedia.com/TERM/A/APIPA.html

BIBLIOGRAPHY

1. Dulaney, E. & Harwood, M. (2012). CompTIA Network+ N10-005 Authorized Exam Cram. United States of America: Pearson.

2. Lowe, D. (2010). Networking For Dummies, 10th Edition. Hokoben, New Jersey, United States of America: John Wiley & Sons, Inc.

3. Northrup, T. & Mackin, J.C. (2010). Windows 7 Enterprise Desktop Support Technician Self-Paced Training Kit. MCITP Exam 70-685. United States of America: Microsoft Press.

4. Petri, D. (2010). Enable Remote Management of Windows Server 2008 R2 Server Core. *Petri.co.il*. Retrieved 28th May, 2013 from http://www.petri.co.il/2008-r2-server-core-enable-remote-management.htm

5. Petri, D. (2009). Remotely Managing Windows 2008 Server Core Firewall. *Petri.co.il*. Retrieved 28th May, 2013 from http://www.petri.co.il/remotely-managing-windows-2008-server-core-firewall.htm

6. Leiden, C. & Wilensky, M. (2009). TCP/IP For Dummies, 6th Edition. Indianapolis, Indiana, United States of America: Wiley Publishing, Inc.

7. TechNet (n.d). Configuring a Server Core installation: Overview. *Technet.microsoft.com*. Retrieved 20th May, 2013 from http://technet.microsoft.com/en-us/library/ee441257(v=ws.10).aspx

8. TechNet (n.d). Installing a server role on a server running a Server Core installation of Windows Server 2008 R2: Overview. *Technet.microsoft.com*. Retrieved 20th May, 2013 from http://technet.microsoft.com/en-us/library/ee441260(v=ws.10).aspx

APPENDICES

APPENDIX A - LIST OF FIGURES

LIST OF FIGURES