Windows Server 2012 R2
Network Installation Guide

Nicholas Rushton, BA Hons.

Callisto Technology And Consultancy Services

© 2014-2017 CTACS

Updated 17th July 2017

Contents

COMMENTS & REVIEWS FROM OTHER PURCHASERS

You're in good company - thousands of people have used guides from CTACS to help them setup their home and business networks. This is what purchasers of the *Windows Server Network Installation Guide* have written in their reviews:

One of the best entry level guides to server installation – *"As an entry level, step by step, setup guide, Nick Rushton's guides are beautiful. The step by step setup portion of the guide is both very well written, and very informative, and it even covers some extensions of the server technology that are nice to have. For advanced setup, there are more comprehensive guides, both through Kindle, and out on Microsoft's tech sites, but this guide will allow you to get a server up, running, and fully functional."* – Bill L, May 2015

Perfect Intro to Installation and Basic Configuration – *"This is a great, simple introduction to the installation and basic configuration of Windows Server 2012 R2. There's a minimum of introductory / what's new in this release / what's a network kind of filler material - the book pretty much gets straight into step-by-step instructions on how to install and then configure the installation."* – Amazon Customer. August 2015

Great Guide – *"To the point with actual steps for completing an installation"* – JWP, April 2015

Five Stars – *"Really basic instruction for beginners like me. I would buy it again."* – Nancy, August 2015

A very helpful quick reference – *"While I have a fair knowledge of PC operating system setup, I had very little experience with servers. This helped with initial setup."* – Amazon Customer, March 2015

Introduction

What is this guide and who is it for?

The purpose of this guide is to take the reader through a typical installation of a small Windows Server 2012 R2 network and is written for the following audience:

- Someone who is new to Windows Server 2012 R2 and installing it for the first time
- Someone setting up Windows Server 2012 R2 in a small business setting
- Someone wishing to learn the basics of Windows Server 2012 R2 and who wants a succinct, practical guide based on real world scenarios

The approach is very much practical and hands on. It should give you a basic understanding of Windows Server and help you setup a network that should meet the needs of a typical small organization such as a business, charity, church, school and so on. However, it is not intended as a detailed description of all Window Server's many capabilities or as a reference manual. It assumes a reasonable working knowledge of Windows and the basics of networking. It is written in a friendly, "do-it-like-this" style, rather than with undue emphasis on theory and abstract topics.

Editions of Windows Server 2012 R2

Windows Server 2012 R2 comes in four different, general purpose editions (plus there are a further three editions for use in more specialized roles). For the most part, the differences are more to do with licensing and capacity rather than functionality. The table below compares the four editions but in summary: *Standard* is the everyday version for businesses, education and so on; *Foundation* is a lower-cost variant for very small companies; *Datacenter* is for larger organizations with multiple servers and/or locations; *Essentials* is for small businesses without in-house support and features a simplified user interface for configuration and management. The information in this guide is most applicable to Standard and Foundation editions. Users of Essentials would find the CTACS *Windows Server 2012 R2 Essentials Guide for Small Businesses* more relevant than this book.

	Foundation	Essentials	Standard	Datacenter
Maximum number of users	15	25	Based on licenses ("unlimited")	Based on licenses ("unlimited")
CALs (Client Access Licenses)	Not required (included/implied)	Not required (included/implied)	Need to be purchased separately	Need to be purchased separately
Maximum number of SMB connections	30	16,777,216	16,777,216	16,777,216
Maximum number of processors ("64-bit sockets")	1	2	64	64
Maximum RAM	32GB	64GB	4TB	4TB
Hyper V Virtualization	No	No	Yes	Yes
Server can join a Domain	No (for migration only)	No (for migration only)	Yes	Yes
Simplified interface ("Essentials")	No	Yes	No	No
Server Core mode	No	No	Yes	Yes
Windows Server Update Services	No	Yes	Yes	Yes

Help with the Artwork?

Pictures and illustrations can sometimes be problematic with eBooks. If you would like a free printable PDF file containing all the illustrations, just forward a copy of the email confirmation you received from when you bought the book to enquiry@ctacs.co.uk (please make sure there is no personal financial information in your email).

1. HARDWARE AND INFRASTRUCTURE

1.1 File Server

Windows Server requires its own, dedicated file server. A file server is similar to a normal desktop computer but is designed to hold multiple hard disk drives for additional storage and to be more reliable as it is intended to be powered up continuously. The main suppliers of file servers include Dell, HP, Lenovo, Fujitsu and IBM; other brands are available, but you may wish to avoid obscure manufacturers and unbranded machines. File servers are not usually available in retail stores but are obtained from specialist IT dealers or online. If you are learning about Windows Server and do not happen to have a spare server to hand, you can use virtualization software on most modern computers to run a copy in a closed environment (a good, free product that runs both on PCs and Macs is Oracle's *VirtualBox*). If you do not have a copy of the Windows Server software, you can download a fully-functional but time-limited evaluation copy from Microsoft, which is ideal for learning purposes.

Choosing a server can be daunting, particularly as it is not something that an organization or individual is likely to buy very often (the typical replacement cycle for a server being around 5 years). Given the specialist nature of the topic, you may wish to seek professional advice if you are not experienced in such matters. The following suggestions are guidelines only to help get you started:

- Spend as much as you can afford.
- In general, memory contributes more than processor power. So, you would usually be better off spending your money on more RAM rather than a marginally faster processor.
- Multiple disk drives are desirable as they enable increased capacity and performance. If you have at least two drives they can be configured to provide redundancy in the event of problems (referred to as *RAID*, this topic is discussed in the next section).
- Disk drives should be *server grade* or *enterprise grade*, meaning they have higher performance and improved reliability, for instance something from the Western Digital SE or Seagate Constellation series, or SAS drives.
- Most servers have more than one network adapter. This enables them to share the workload, providing better throughput, or provide redundancy in the event of one failing.
- Some servers have the option of redundant power supplies – if one fails then the other one takes over automatically. This is worth having.
- Servers are available in both tower format (similar to desktop PCs) and in horizontal rack format, for mounting in cabinets alongside other equipment (typically communications equipment and network switches).
- Often the given base price for a server is for a bare-bones model and hard disk drives, memory and other features may have to be additionally specified. Costs can add up – be aware that a complete system may be several times the initial headline price and budget accordingly.
- Consider taking out a maintenance agreement at the time of purchase. These vary in service levels and cost and your choice will depend upon your requirements, but generally provide peace of mind and good value. The key decision point is: How long can you do without the server? It is possible to obtain maintenance agreements that provide an onsite presence within 4 hours.

For a very small business or other organization with less than ten staff, a suitable choice may be a *micro-server*. This is still a proper server rather than just a glorified PC, but in a small, low-cost form factor. The genre was largely invented by Hewlett-Packard and their ProLiant MicroServer series is very popular. An equivalent model from Dell is the T20. For a slightly larger organisation – say up to 25 users or so – a standard entry-level file server is more appropriate. Beyond that, increasingly powerful servers are available that can service hundreds of users. The next stage is to use multiple servers, with the workload spread across them. As mentioned above, there are a number of vendors to choose from. Dell are a popular choice as everything can be conveniently ordered from their website.

Note that it is not necessary to purchase a monitor, keyboard and mouse for the server, as it can be operated without them in so-called *headless operation*. Borrow them from another machine for the initial installation, as thereafter they are not required.

1.2 Disk Drives and Storage Options

Most desktop and laptop computers have one physical hard disk, configured as a single volume - commonly referred to as "the C: drive" - upon which everything is stored. However, in a server there is usually a need for a greater amount of storage, plus that storage also has to be very reliable. Performance becomes a consideration too, as many people may be accessing the server simultaneously. The way to address these requirements is by using multiple hard drives and to configure them in special ways. There is no *one-size-fits-all* solution here as it depends upon the size, requirements and budget of the organization. The options are reviewed below.

Single Drive System

A server in a very small business environment may only have a single physical hard drive. In such a case, it should be divided into two volumes: a volume on which the operating system is installed (the C: drive) and a volume on which the organization's data is stored (the D: drive). The rationale here is that if the operating system ever needs to be re-installed or upgraded, then it can be done without directly affecting the data. The C: volume does not need to be huge – 60GB to 100GB is quite adequate and the remainder of the drive should be partitioned as the D: drive. The major downside to a single drive system is that in the event of the drive failing then the server will be out of action until it can be replaced, plus the associated risk of data loss is high.

Twin Disk Drives

A very common approach is to have two hard drives in the server, one for the operating system and one for the data. The first one can be quite small; at the time of writing, the smallest readily available drives are 160GB, which is ideal. The second drive, for the data, can be as large as you need. This arrangement gives some performance benefits, as the drives operate independently, sharing the workload, plus the operating system and data are quite separate, which facilitates re-installations and upgrades. However, it still does not address the issues of reliability and protection.

RAID

RAID is short for *Redundant Array of Independent (or Inexpensive) Disks*. There are various types of RAID, referred to using a numbering system i.e. RAID 0, RAID 1, RAID 5 etc. The basic idea is to improve reliability and performance by using multiple disks to provide redundancy and share the workload. The most common scenarios in small server systems are RAID 0, RAID 1, RAID 5 and RAID 6.

- **RAID 0** consists of two identical drives. When a file is written, some data goes on one drive and some goes on the other. As both drives are being written to or read simultaneously, throughput is maximised. However, as bits of files are scattered across the two drives, if one drive fails then everything may be lost. Also, the speed of disk drives is not necessarily the bottleneck in many servers. For these reasons RAID 0 should be avoided, as it offers no protection at all, but it is described here for reasons of completeness.

- **RAID 1** consists of two identical drives that mirror each other. When a file is saved there are actually two separate but identical copies behind the scenes, one held on each drive, even though you can only see one as the mirroring process itself is invisible. If one of the drives fails, the second one automatically takes over and the system carries on without interruption. At the earliest opportunity the faulty drive should be replaced with a new one; the system is then synced it so it becomes a true copy of the remaining healthy drive in a process known as 'rebuilding the array'. In a RAID 1 system, the total usable storage capacity is half that of the total drive capacity installed. For example, if a server has two 2TB drives installed then the total amount of usable storage capacity is 2TB rather than 4TB.

- **RAID 5** uses at least three but preferably four or more drives. Data is written across all the drives simultaneously, along with what is known as *parity information*. The benefit of this is that the system can cope with the failure of any one single drive. RAID 5 is considered to offer a good combination of price, performance and resilience. Whereas a RAID 1 system loses 50% of the total drive capacity in order to provide resilience, RAID 5 loses only about 25%. For instance, if a server has four 2TB drives installed then the total amount of usable storage capacity is 6TB rather than 8TB.

- **RAID 6** uses at least four but preferably five or more drives. It is similar to RAID 5, but uses two sets of parity information written across the drives. The benefit of this approach is that the system can cope with the simultaneous failure of two drives, thereby making it more resilient than RAID 5, although it loses more capacity

in order to provide that resilience. If a server has five 2TB drives installed in a RAID configuration, then the total amount of usable storage capacity is 6TB rather than 10TB.

What to do? If you have a server with a single drive, then the question of RAID does not arise. If you have a server with two drives, you should consider using RAID 1. If you have a server with three or four drives it should be configured for RAID 5 and if you have five drives, then use RAID 6. The RAID level is usually set using a BIOS option on the server and once set cannot easily be changed.

It is important to note that RAID systems require a special controller and that these come in two types. Low-cost servers may have a so-called built-in RAID controller on the motherboard; these are referred to as 'software RAID' or 'embedded RAID' by manufacturers but are known colloquially as 'fake RAID' and are to be avoided as they can be prone to failures and data loss. Instead, a separate hardware RAID controller card should be purchased as this offers better performance and reliability.

One important thing to note is that a RAID system is not a backup system. It can help prevent data loss in the event of problems but it is still important to make separate provision for backup. For instance, if the server was stolen or the premises went up in flames then the data would be lost regardless of whether and what RAID system was used.

Storage Spaces

Storage Spaces is an alternative to RAID and is a standard feature in Windows Server. It is designed to address three aspects of storage:

Firstly, on a Windows computer each hard drive normally has a separate drive letter to identify it. For instance, the first drive is the C: drive, the second is the D: drive, the third is the E: drive and so on. However, it is more convenient, particularly in a network, if drives can be pooled together to appear as a single large volume. This makes it easier to find things by removing the requirement to know which physical drive a particular file or folder is located upon:
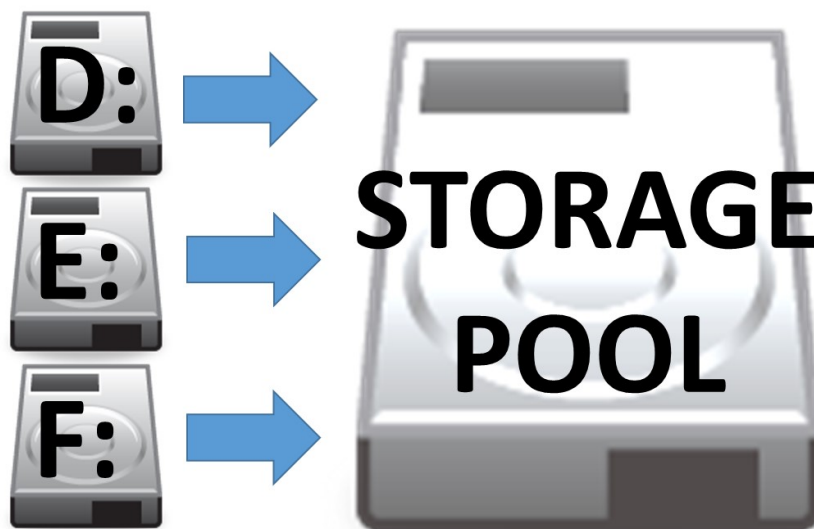

Figure 1: Storage Pool aggregates the hard drives

Secondly, like RAID, Storage Spaces provides a degree of protection against data loss in the event of a drive failing. Multiple copies of files are stored on different drives; if a drive fails then a copy from a different one is automatically used. The failed drive can then be replaced and added back to the storage pool. Finally, the pool can easily be added to in order to provide more storage space, without excessive disruption or reconfiguration. One important thing to note is that the drives can largely be of any type; for instance, external USB hard drives can be connected to the computer and added to the storage pool.

In many respects Storage Spaces is more flexible than RAID, as well as being cheaper to implement. However, overall performance may not be so high, although this is not necessarily an issue in a small setup.

SSD and 2 ½ inch Drives

Solid State Drives or SSDs offer a significant performance boost over conventional mechanical hard drives or HDDs. Having said that, drive performance is not necessarily a big consideration in small systems as there are other potential bottlenecks, such as network and processor performance. SSDs are expensive compared to HDDs, probably too expensive for general purpose storage in most instances. However, there may be some merit in using a SSD for the C: drive that holds the operating system.

Most file servers use 3 ½ inch HDDs as these offer the highest capacities and best price-performance among disk drives. Smaller 2 ½ inch drives ("laptop drives") can be an alternative in some scenarios: they use less power, are quieter and can be more reliable due to reduced vibration levels. The disadvantages of 2 ½ inch drives are that they are not available in such high capacities and are more expensive. Also, they may need to be mounted in caddies to make them fit into the drive bays on the server.

1.3 Internet Connection, Hub, Router

A network has to be connected to the outside world in order to access the internet and provide remote access to the network for staff who are working outside the office or travelling. Many small businesses will have an all-in-one router or wireless router; in turn, this may be connected to one or more switches and wireless access points. Three considerations to follow here are:

- Use wired connections whenever possible as performance is better than wireless
- Wired connections should be at Gigabit speed, wireless connections at 801.11N or better
- Avoid domestic grade equipment. Spending more on professional or prosumer ("professional consumer") routers and switches will give better performance and reliability
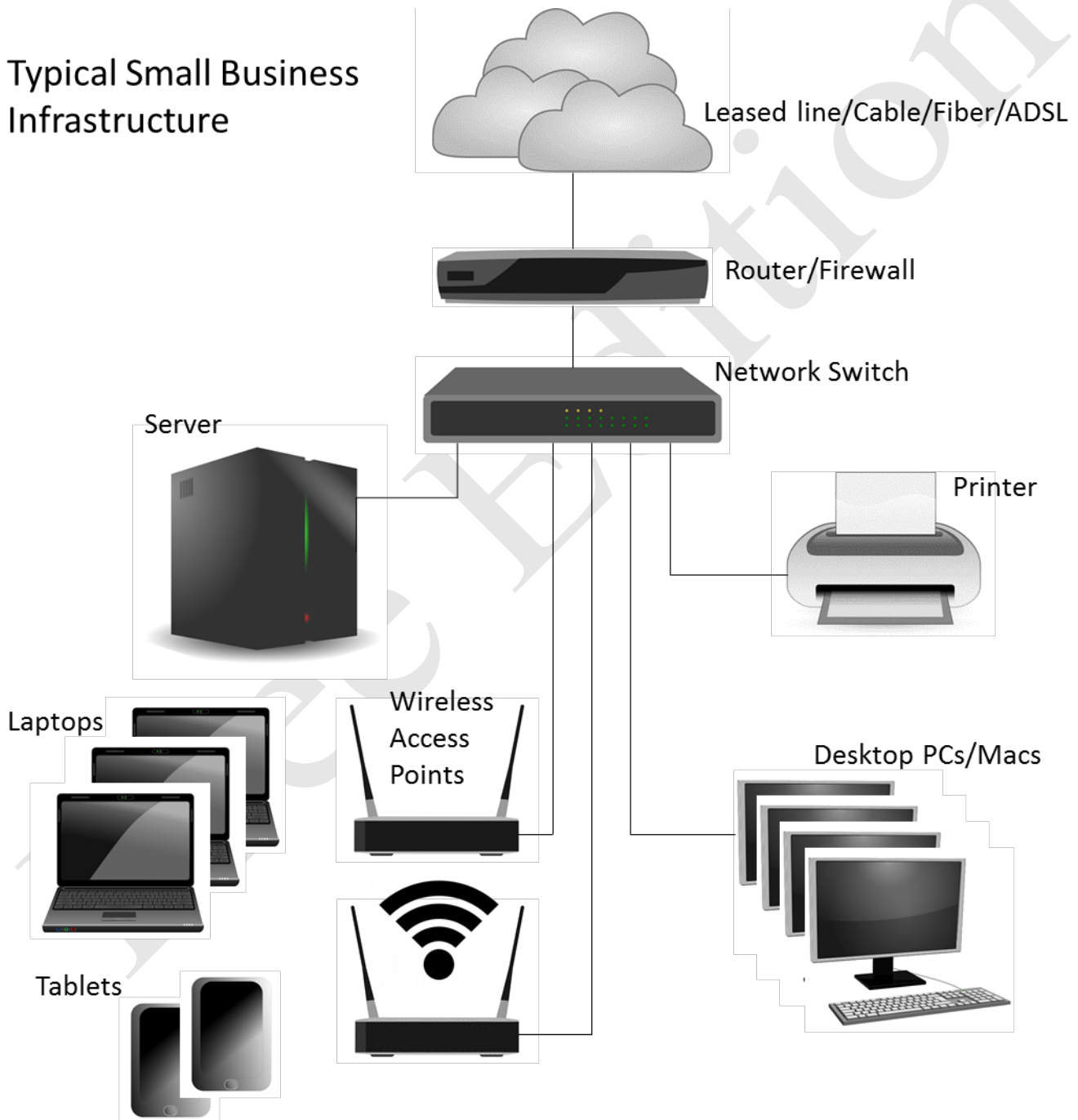

Figure 2: Typical small business infrastructure

1.4 IP Considerations

Every device on a network has a unique number within that network to identify it, known as its *IP address*. These numbers consist of four sets of digits and take the form *nnn.nnn.nnn.nnn*. Nearly all of the possible numbers are allocated to the internet for websites and other purposes and are known as *public IP addresses*. However, a small selection is available for internal or local area networks; these are known as *private IP addresses* and are invisible to the outside world. As these IP addresses are private they can safely be used by anyone and the exact same numbers are used millions of times over. The three number sequences which are available for private use are:

10.0.0.0 to 10.255.255.255
172.16.0.0 to 172.31.255.255
192.168.0.0 to 192.168.255.255

Most equipment intended for use in small businesses tends to be pre-set to use the 192.168.nnn.nnn numbering scheme; for instance, internet routers commonly have an address of 192.168.1.1 or 192.168.1.254 depending on brand. Although these addresses can be changed, there is rarely any need to and it is best not to do so unless one has a good understanding of the topic.

Devices such as computers and printers do not come with an IP address already allocated; instead, they have to be configured with a suitable address. There are two ways of doing so - you can use *static IP addresses* or *dynamic IP addresses*.

With static IP addresses, it is necessary to visit each device and individually configure it. For instance, you might set the first PC to be 192.168.1.101, the second to be 192.168.1.102, the third to be 192.168.1.103 and so on. You have to be careful to keep track of everything and above all make sure that there are no duplicates. If this sounds like hard work then that's because it is – you might get away with it if there are only a handful of computers but beyond that it rapidly becomes unworkable.

With dynamic IP addresses, the numbers are assigned automatically by a DHCP (Dynamic Host Configuration Protocol) server and it keeps track of everything. This is not necessarily a physical server like a file server, rather it is a piece of software. Many all-in-one routers of the sort used in small businesses have DHCP server software built-in. If Windows Server detects one of these during the installation, it will use it. However, if it does not it can provide its own DHCP service, although this has to be separately configured.

Regardless of whether the IP addresses come from a router or are supplied by Windows Server itself, it is a good idea to have a scheme to follow. As mentioned above, routers are commonly set to numbers such as 192.168.1.1 or 192.168.1.254. The server should be set to an adjacent address. Printers and any specialised devices should be close by. The numbers allocated for computers should be a contiguous block of numbers elsewhere. So, for instance, a typical setup might be as follows:

IP Address(es)	Role
192.168.1.1	Internet router/gateway
192.168.1.2	File server
192.168.1.3-192.168.1.20	Use for printers and other special devices
192.168.1.50-192.168.1.250	Use for computers, tablets, smartphones etc.

The above scheme will work for an organization with up to a couple of hundred computing devices. In a larger setup, with multiple servers, dozens of printers and maybe thousands of users, a more sophisticated scheme would be required, necessitating the use of *subnets*. This takes it outside the scope of this guide, but a more detailed explanation can be found online at http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html.

Note: there are two 'flavors' of IP: TCP/IPv4 and TCP/IPv6. In this guide we are using the more common IPv4, as most people find it easier to deal with addresses such as 192.168.1.nnn rather than something like, say, 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

2. INITIAL INSTALLATION OF WINDOWS SERVER 2012 R2

There are three main techniques by which the Windows Server software can be installed onto a server:

- **Method 1:** Windows Server has been supplied on a DVD. Go into the BIOS of the server and set it to boot from CD/DVD (accessing the BIOS varies according to the server brand, but is typically the F2 key on Dell and the F10 key on HP). Insert the DVD, connect an Ethernet cable to the server and restart it. A slight variation on this is where the software has been provided on or copied to a bootable USB drive, in which case substitute USB for DVD.

- **Method 2:** The server manufacturer has supplied a special start-up or management disk. This typically provides driver and RAID support for the server and may do some other configuration work. The usual process is to set the server to boot from CD/DVD as described above. Insert the disk, plug in an Ethernet cable and restart the server. The management software will run – this may take several minutes – after which you will be prompted to eject the disk and insert the Windows Server DVD. The server may then restart.

- **Method 3:** Windows Server has been purchased pre-installed on the server, most commonly in the form of Windows Server Foundation edition. This does not mean that it is ready to use, just that what normally comes on the distribution DVD has already been copied to the server's hard drive so the installation process can run from there. Plug in an Ethernet cable and start the server.

Regardless of which method is being used, after a short while the following screen is displayed. Check the regional settings, make any changes as required and click **Next**:
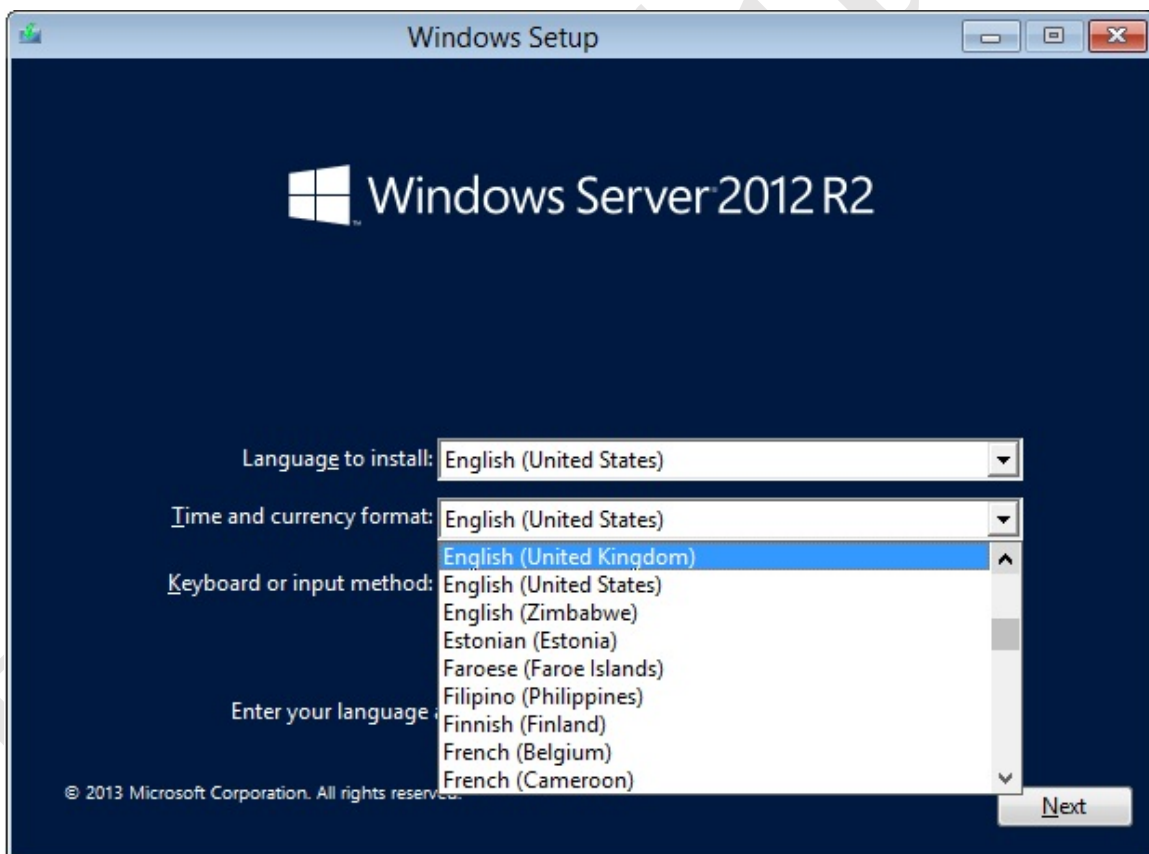

Figure 3: Specify regional settings

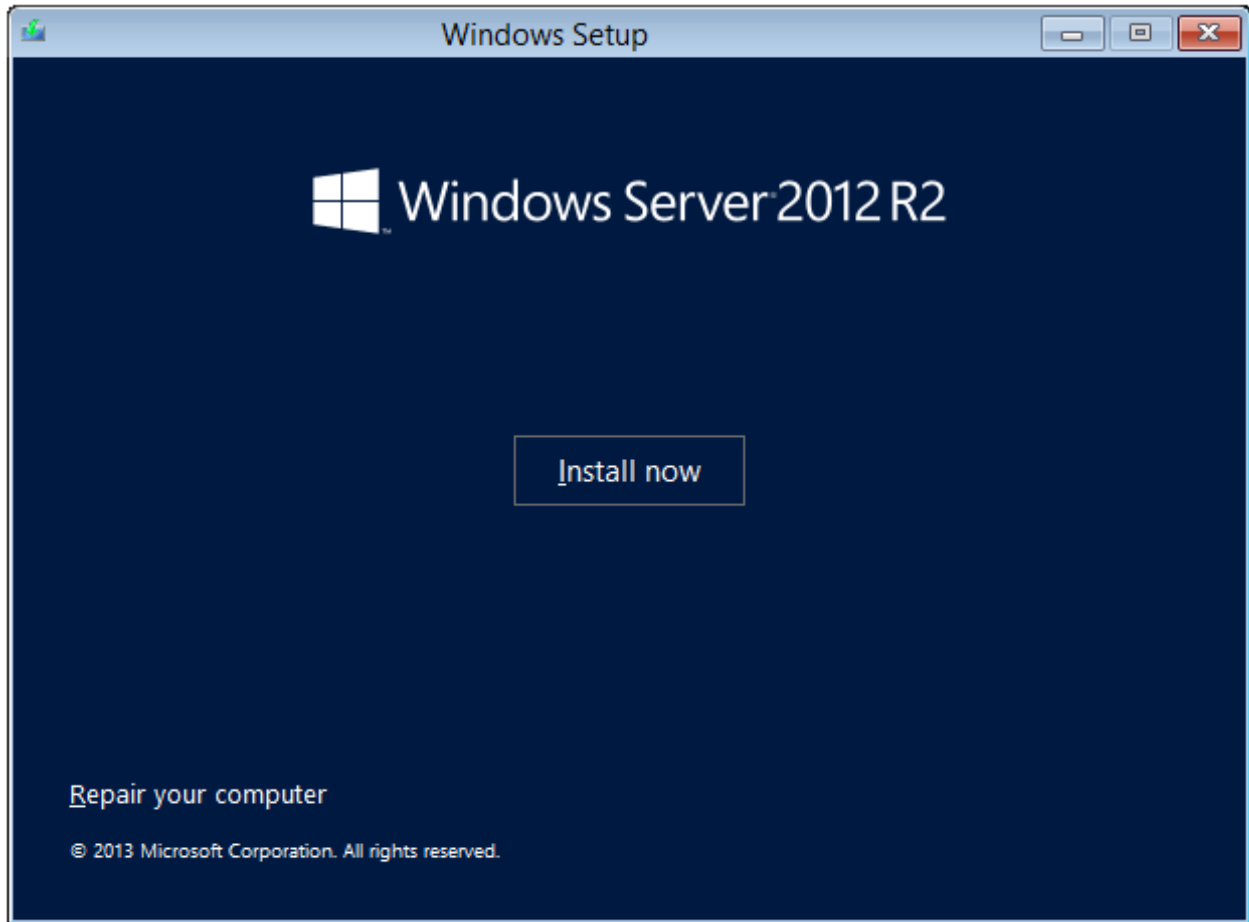On the following screen click the **Install now** button:

Figure 4: Click to begin installation

Depending on the edition, you may receive a choice of what to install. The primary distinction is between *Server with a GUI* and *Server Core Installation*. With the former, Windows Server will look like a regular version of Windows complete with Desktop, icons, Start Screen and so on. With the latter, the Windows interface ('GUI') is not installed and the server is more like an appliance or black box; this mode is more suitable for installations that have many servers. Choose **Windows Server 2012 R2 Standard (Server with a GUI)** and click **Next**:
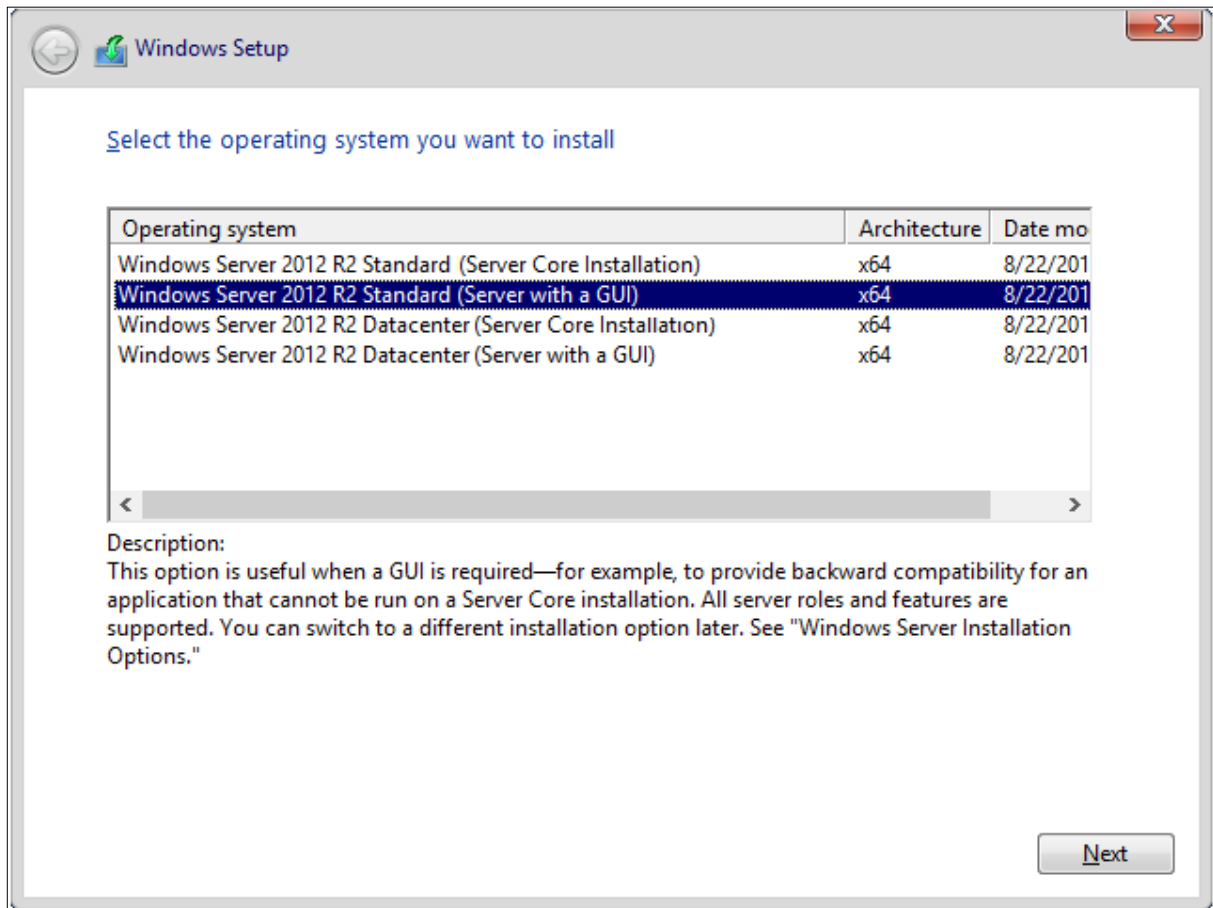
Figure 5: Select the operating system to install

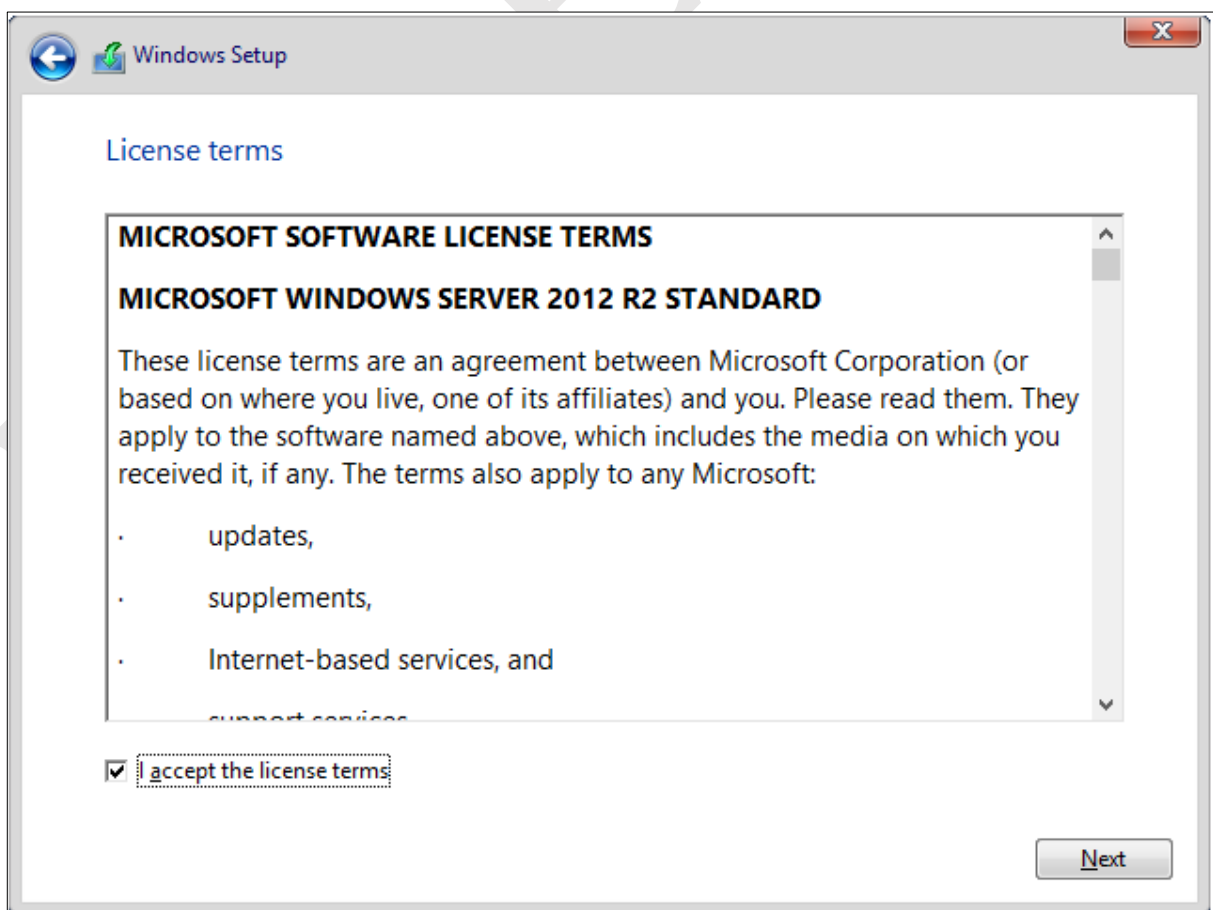Tick the **I accept the license terms** box and click **Next**:

On the subsequent screen choose **Custom: Install Windows only (advanced)**:
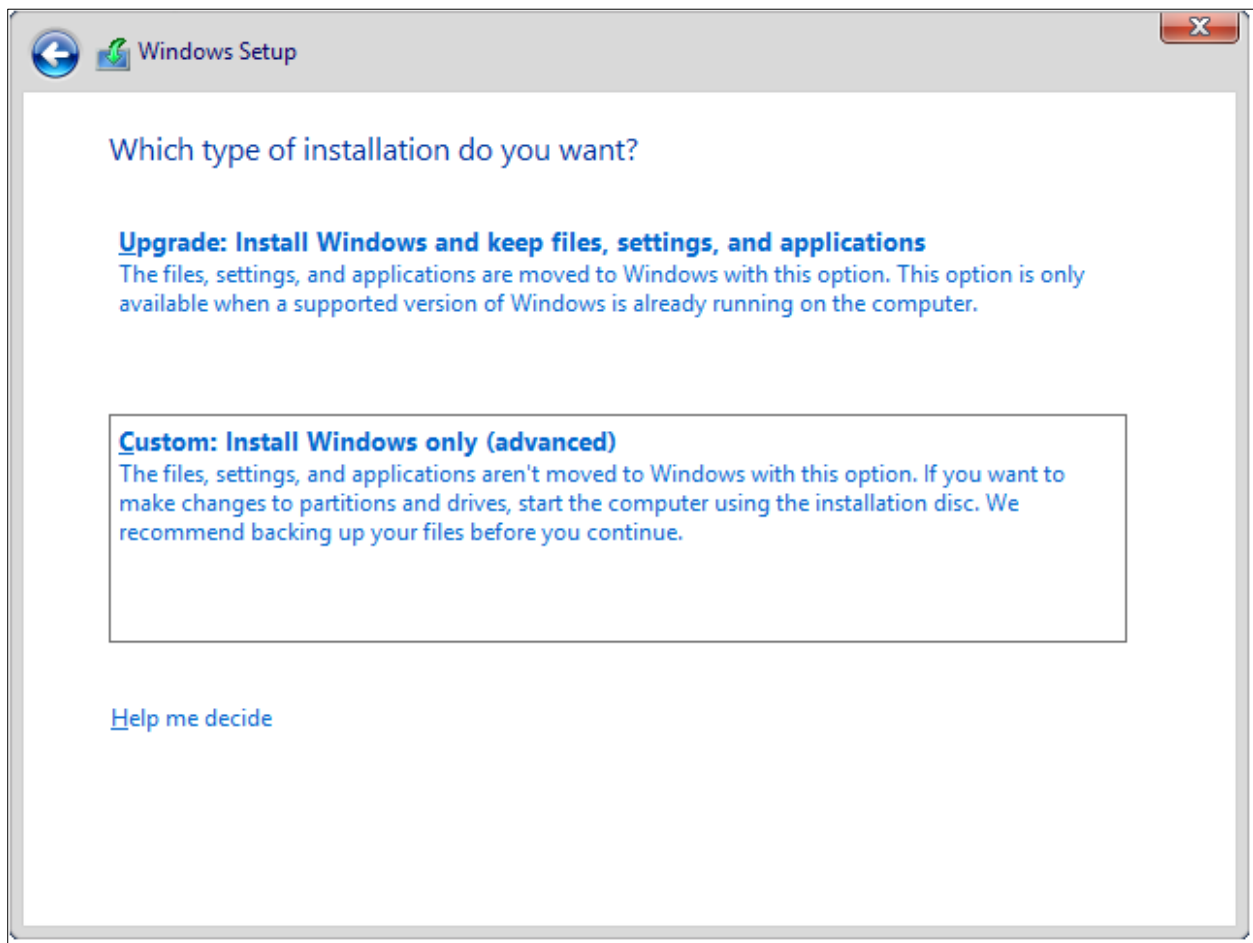

Figure 7: Choose 'Custom Install'

A decision has to be made about where to install Windows Server. What options are available will depend on what drives are in the server and how they are configured. On a very small system there may only be one drive. A larger system might have two drives; typically, Windows would be installed on the smaller one and the larger one would be used for data. On a RAID system the drives will appear as a single volume (unless, perhaps, the installation was started from a manufacturer's management CD/DVD as described at the beginning of this chapter). Do not try to use the 'System Reserved' partition. The Windows drive should be at least 60 GB in size but slightly larger is better. In this example, the server has 1 TB storage, divided into one partition of about 100 GB and one of about 900 GB. We will therefore use the former. **Very important:** make sure the drives/partitions are formatted before proceeding, then click **Next**:
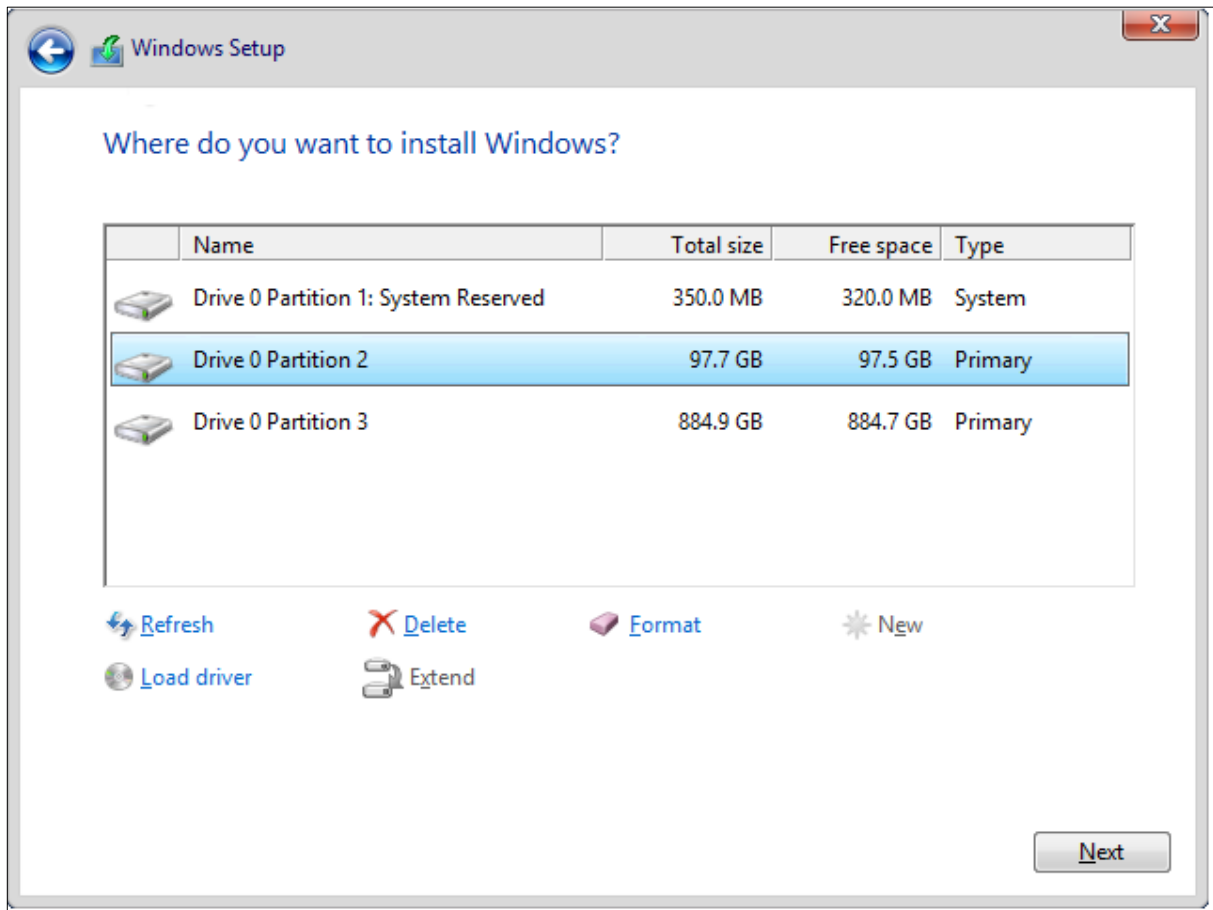
Figure 8: Choose the installation partition

The next phase typically runs for around 10-15 minutes and the server may restart several times during the course of it:
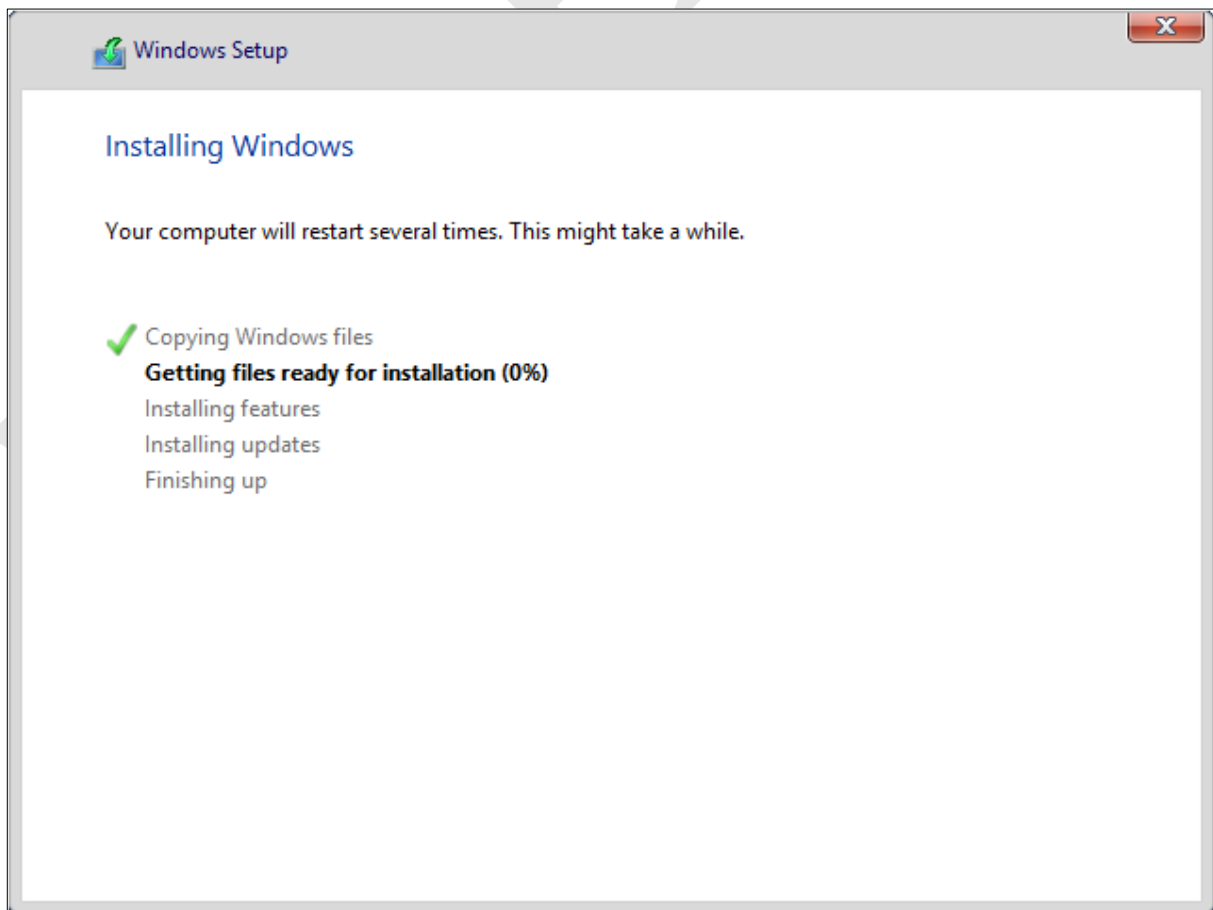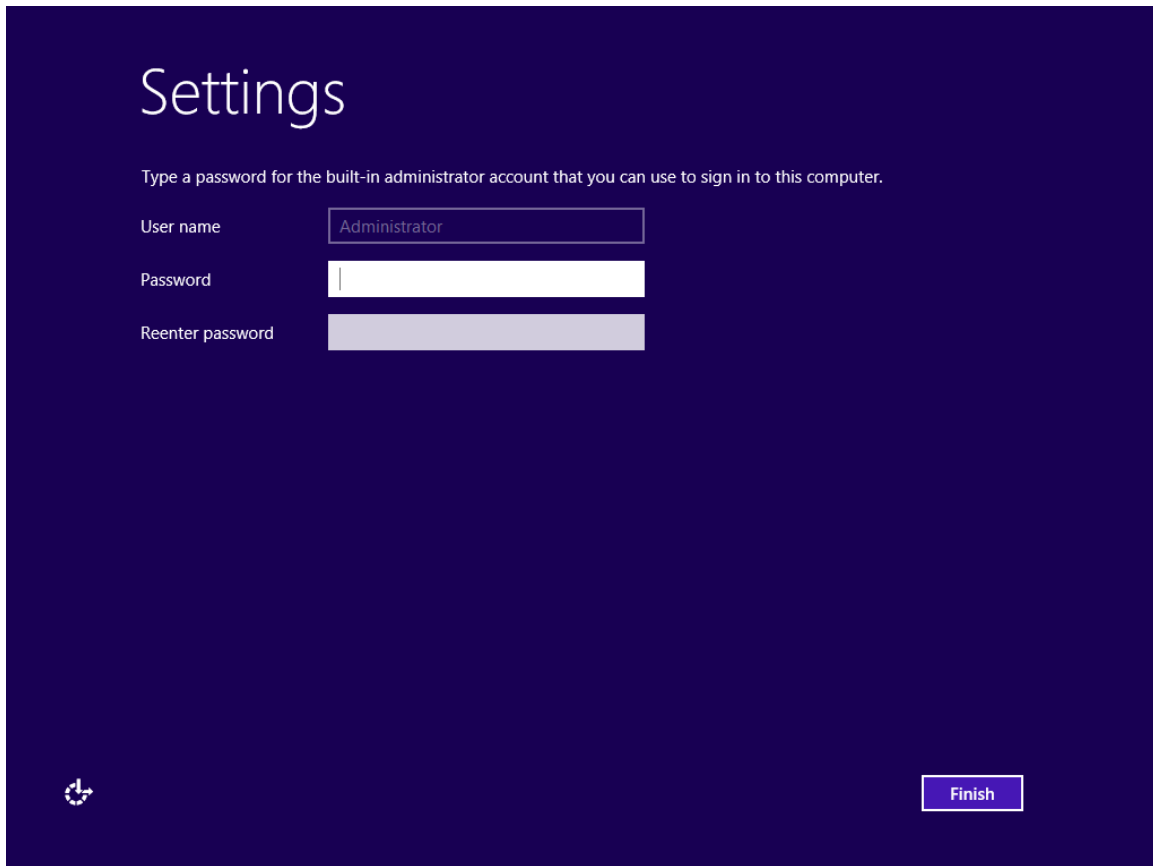
Figure 9: Installation progress screen

Eventually the following screen will appear, prompting you to create a password for the Administrator account. Choose something non-obvious - a mixture of letters, numbers and punctuation is best - and make a note of it. Then click **Finish**:

Figure 10: Specify a password for Administrator

On the subsequent screen press **Ctrl+Alt+Del** simultaneously to login. Do so using the Administrator credentials that you have just defined:
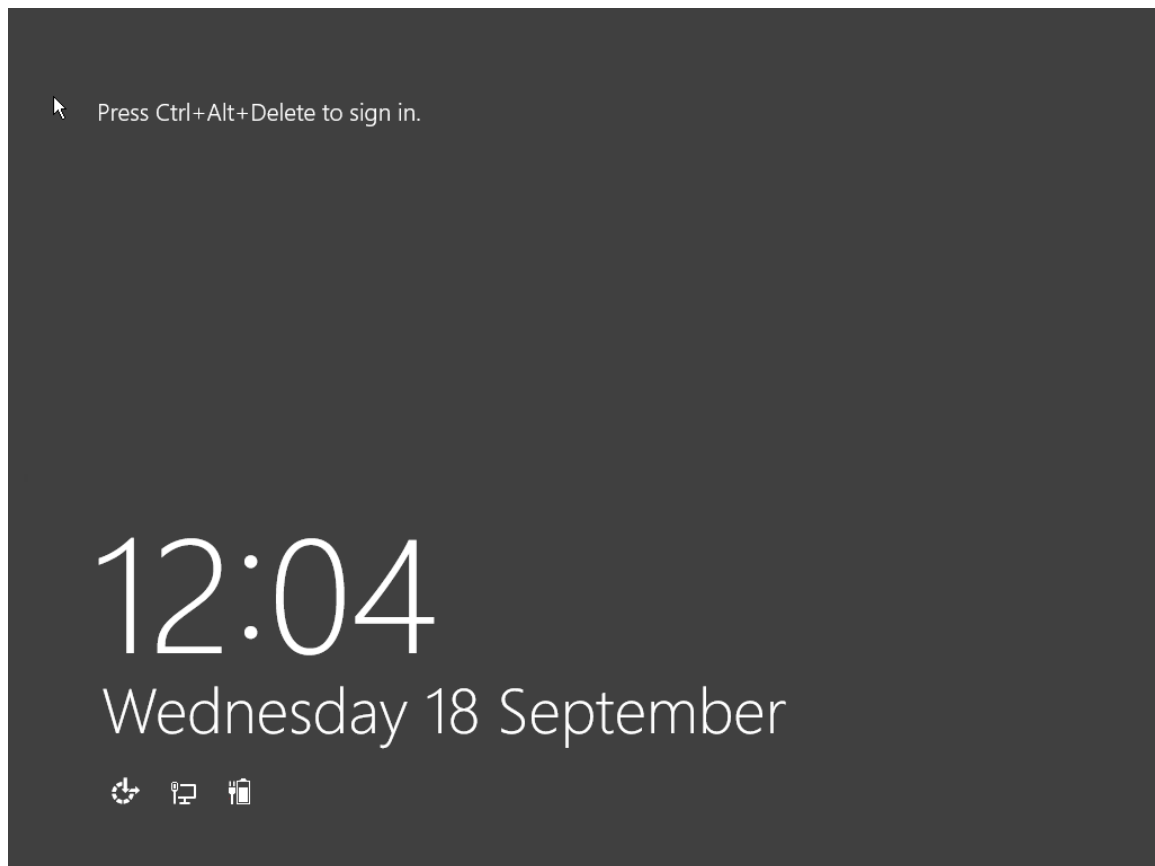
Figure 11:Press Ctrl+Alt+Del to login

Following the first login, a message is displayed on the right-hand side of the screen asking whether Windows Server should look for other devices on the network, including printers. It is important that you choose **Yes**, otherwise Windows will be configured with a public rather than private networking profile and things will not work correctly:
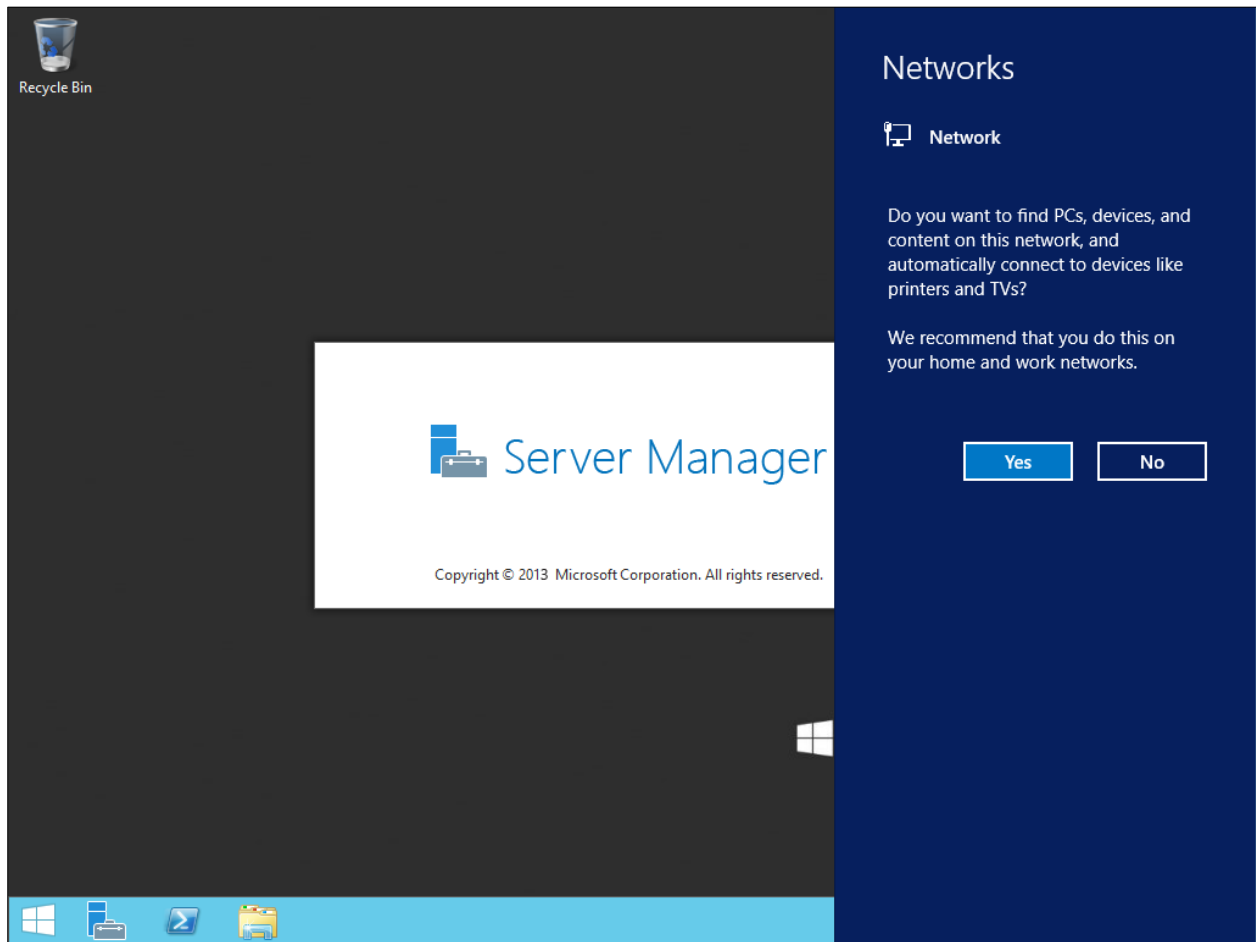
Figure 12: Search screen for other network devices

After a short delay the main *Server Manager* screen will appear. This is used for configuring and managing most aspects of the server's operation. In some respects it operates like a web site – notice the backwards and forwards buttons in the top-left hand corner:
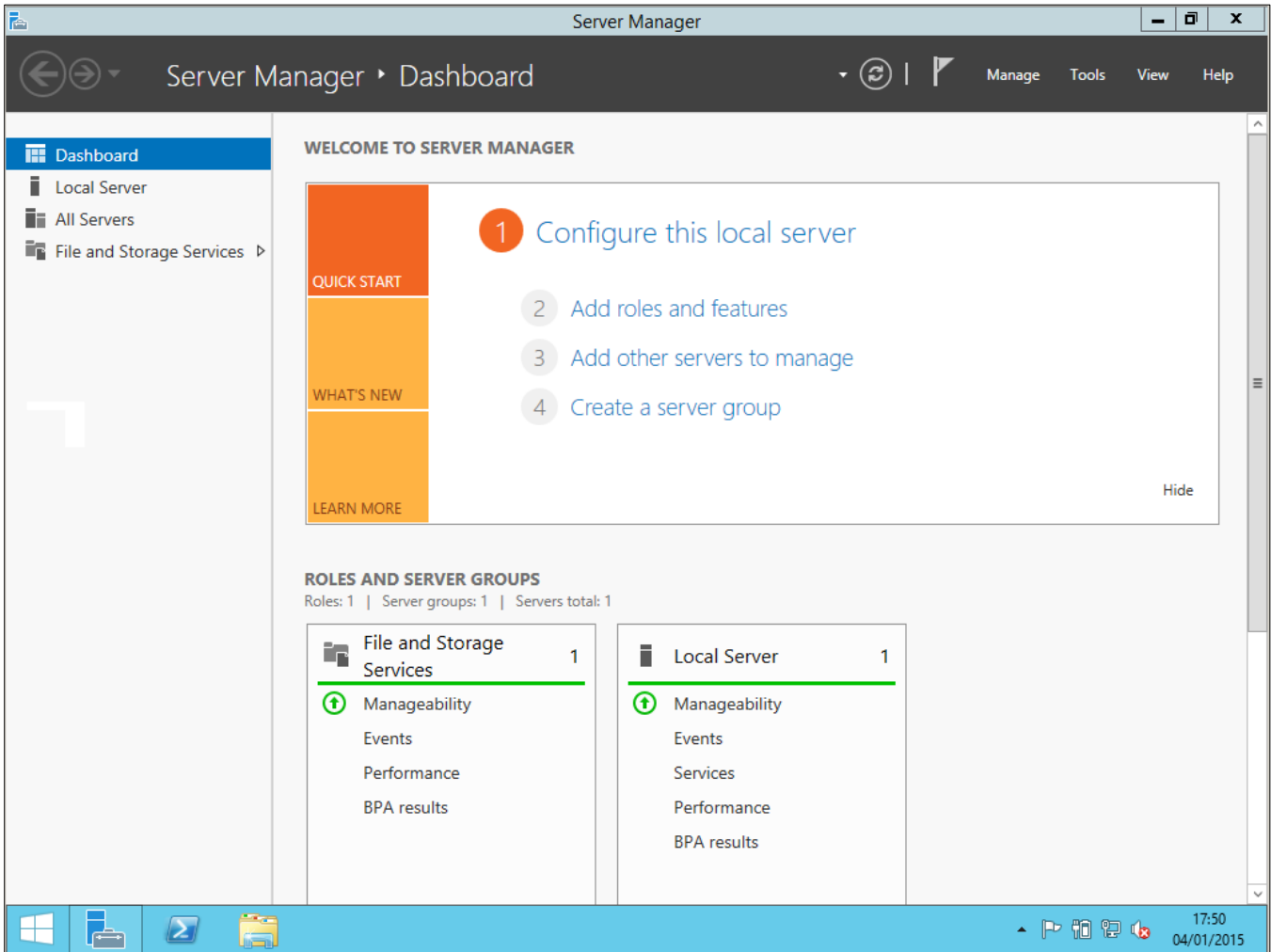
Figure 13: Server Manager Dashboard

The first step is to configure networking. On the left-hand panel, click where it reads **Local Server** and the screen will change thus:
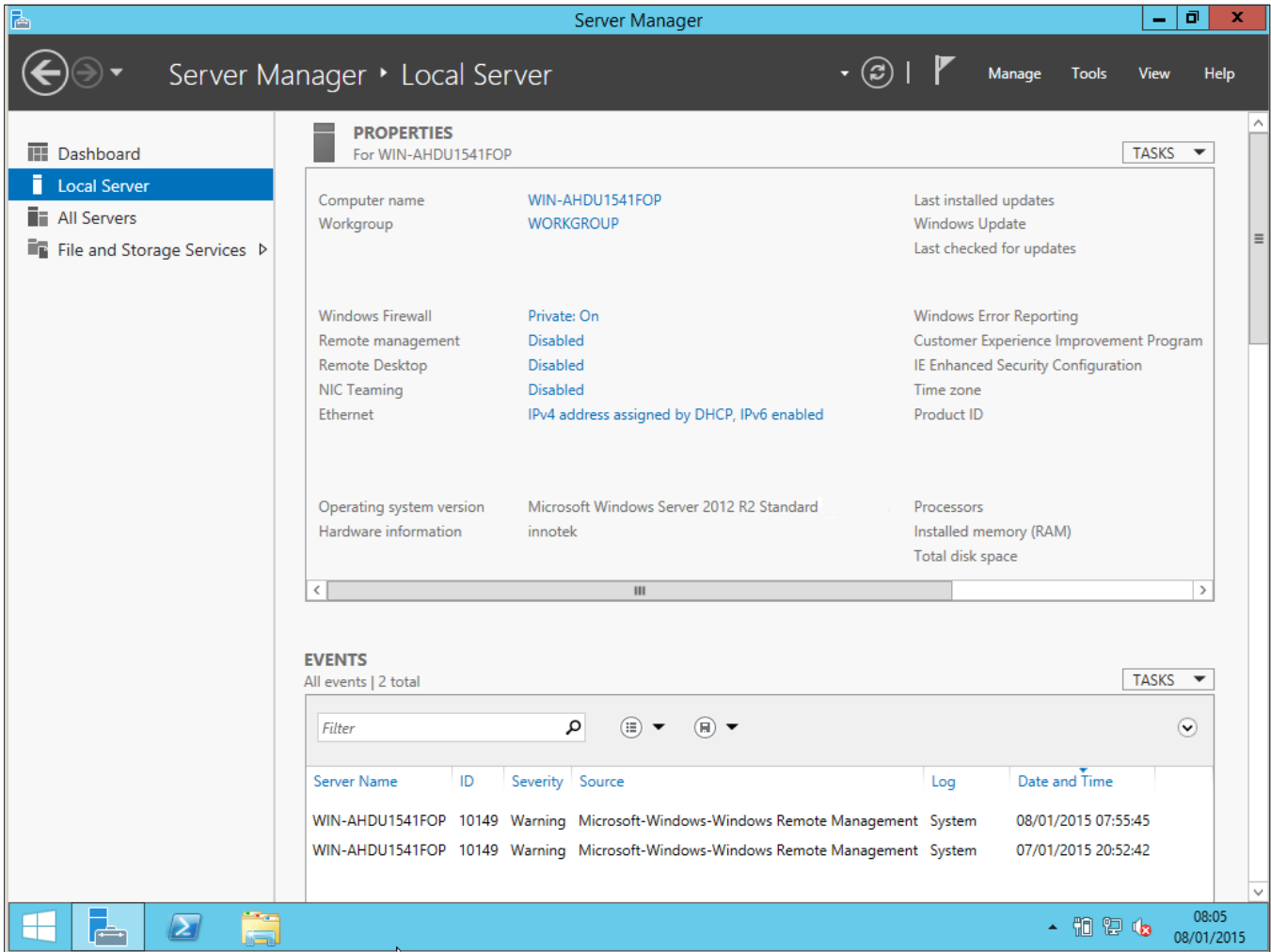
Figure 14: Local Server panel within Server Manager

On the main panel, look for where it says 'Ethernet'. Click where it reads **IPv4 address assigned by DHCP, IPv6 enabled** and the network adapter(s) will be shown (there may only be one on a small server; if there are more than one choose the one that is connected. Further information about using multiple adapters can be found in 13.2 Multiple Network Adapters (NIC Teaming)). Right-click the adapter and choose **Properties**. On the resultant panel highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. At present, the adapter will be set to *Obtain an IP address automatically* – change it to **Use the following IP address**. The actual address to use depends upon the IP scheme in use; in our example we are using a 192.168.nnn.nnn addressing scheme with the router on 192.168.1.1. The server should be given an adjacent address, such as 192.168.1.2. The **Default gateway** is the address of the router; the **Subnet mask** should be 255.255.255.0 and the **Preferred DNS server** is also the address of the router. Make the changes and click **OK**, followed by **Close** on the subsequent screen:

Figure 15: Specifying the IP address for the server

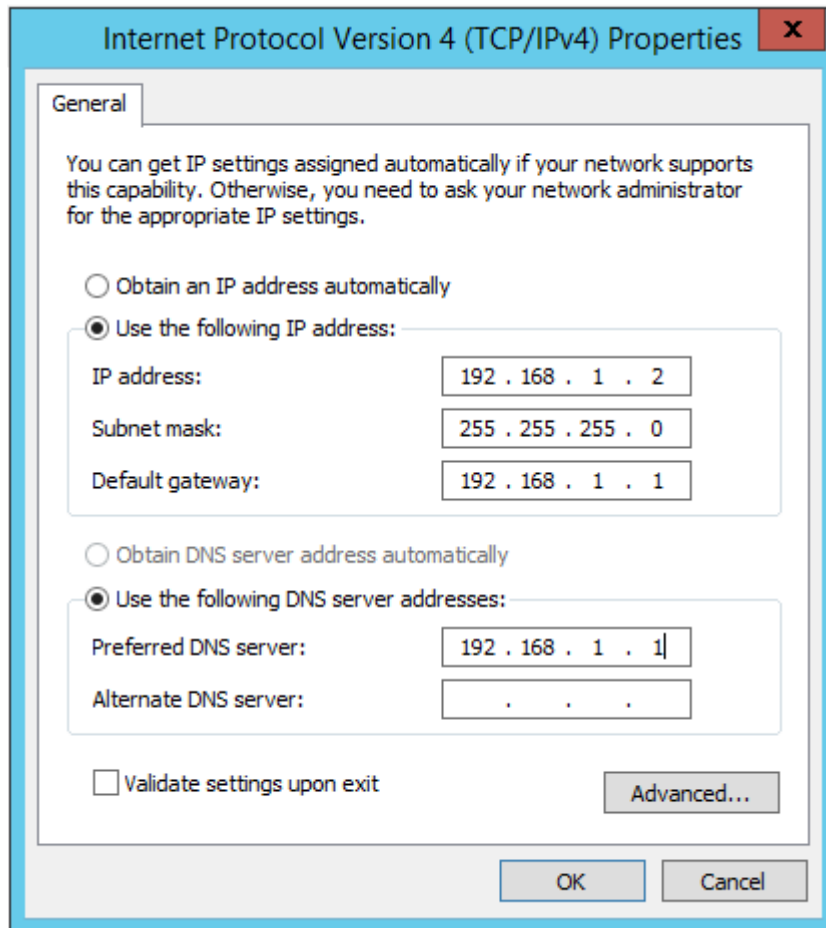Close the Network Connections window to return to the main Server Manager (Local server) screen. On the right-hand panel, look for where it says 'Computer name'. Click the value, which will currently be something random (e.g. WIN-AHDU1541FOP) and the System Properties panel will be displayed. Click the **Change** button on the **Computer Name** tab and change the name to something more meaningful. In a small network with a single server you can simply call it *server*, but in a larger network there will need to be a convention for naming the servers. This could be along the lines of *server01*, *server02*, *server03* and so on, or could be based on location (*newyork, london, berlin* etc.) or function (*accounts*, *sales*, *marketing* etc). Click **OK** and there will be a message advising that the server needs to be restarted. Click **OK** followed by **Close**, then click the **Restart Now** button.

After the server has restarted, logon and you will be returned to the Server Manager screen. Before continuing, one optional thing to consider is labelling the disk volumes to reflect their roles. For instance, the C: drive could be labelled *System* and the D: drive labelled *Data*. To do this, launch *File Explorer*, which has an icon on the Taskbar. Right-click on each drive in turn and choose **Rename** from the pop-up menu.

Returning to the Server Manager screen, click **Dashboard** followed by **2 – Add roles and features**. The initial screen lists some pre-requisites but is not important, so tick the **Skip this page by default box** and click **Next**. On the subsequent screen choose **Role-based or feature-based installation** (which is the default) and click **Next**:
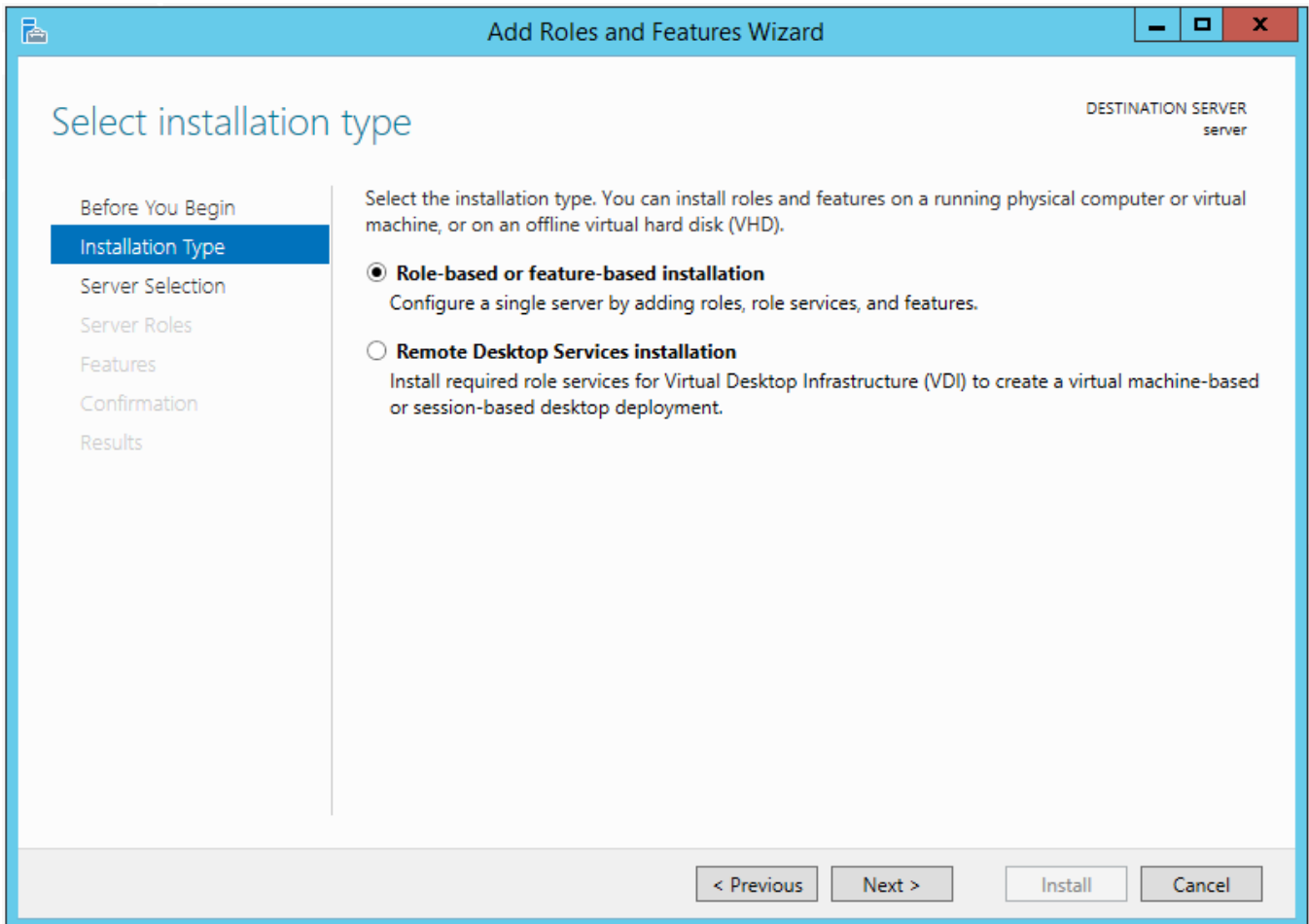
Figure 16: Add Roles and Features Wizard

On the following screen only one server should be listed - the one you are working on – although in a large organization other existing servers may also be listed. Click **Next** to continue:
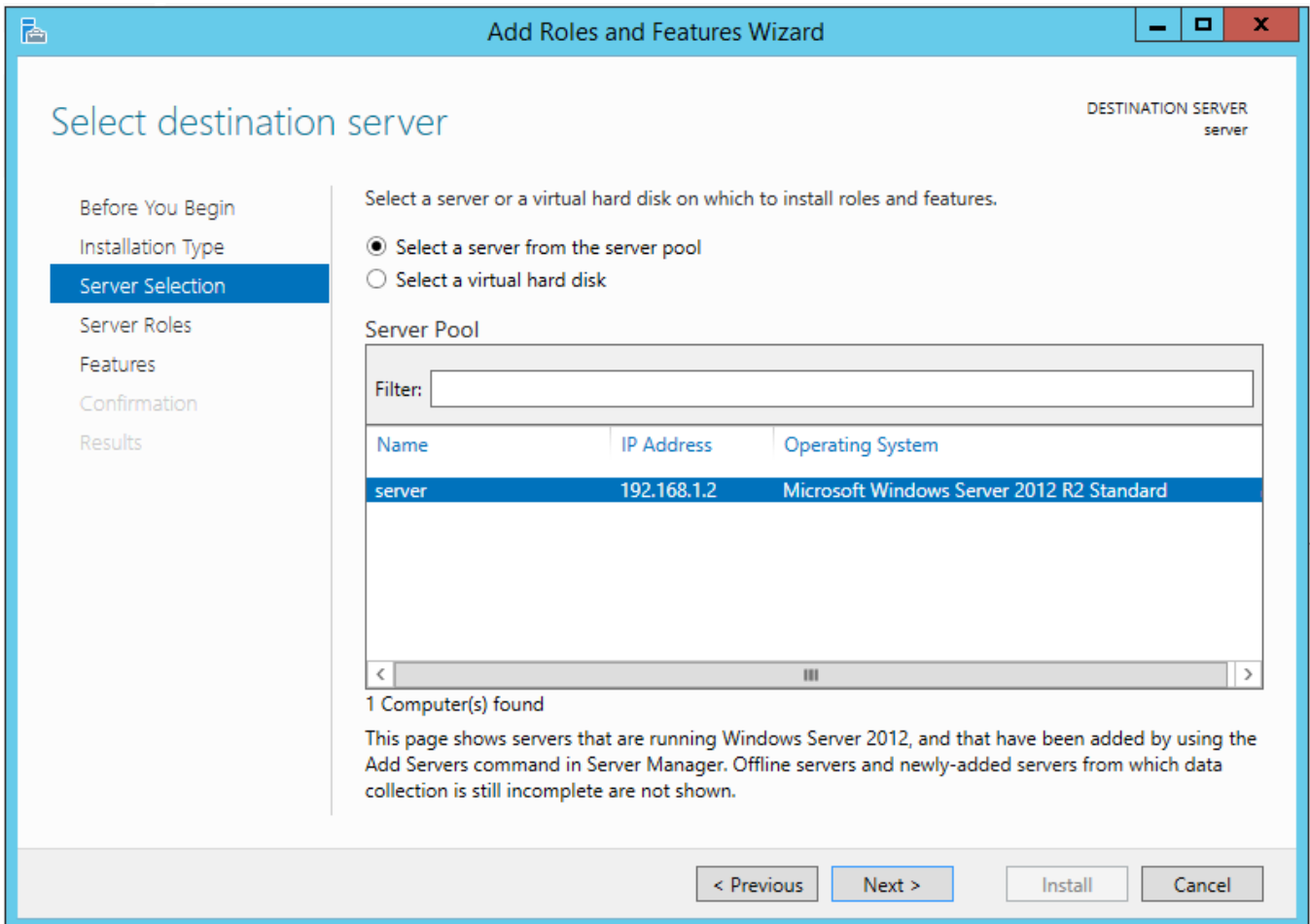
Figure 17: Select the destination server

There are some 20 roles listed on the following screen. The ones that should be installed depend upon the purpose of the server, for instance in a network with multiple servers the roles can be shared out for reasons of performance and resilience. In our example, there is a single server that will run everything required in a typical installation for a small organization. Accordingly, only the following roles need to be setup: *Active Directory Domain Services*; *DHCP Server*; *DNS Server*; *File and Storage Services* (which will in fact already be installed at this stage). These services do the following things:

Active Directory maintains details of all the objects (computers, printers, users and so on) in the network and handles security and logons. For a more detailed explanation look at this article: http://en.wikipedia.org/wiki/Active_Directory.

DHCP Server provides and manages IP addresses for devices on the network. For a more detailed explanation look at this article: https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

DNS Server translates between names (which human beings prefer) and IP numbers (which computers prefer). For a more detailed explanation look at this article: https://en.wikipedia.org/wiki/Domain_Name_System

Start by clicking on **Active Directory Domain Services**. The defaults are generally fine so just click the **Add Features** button:
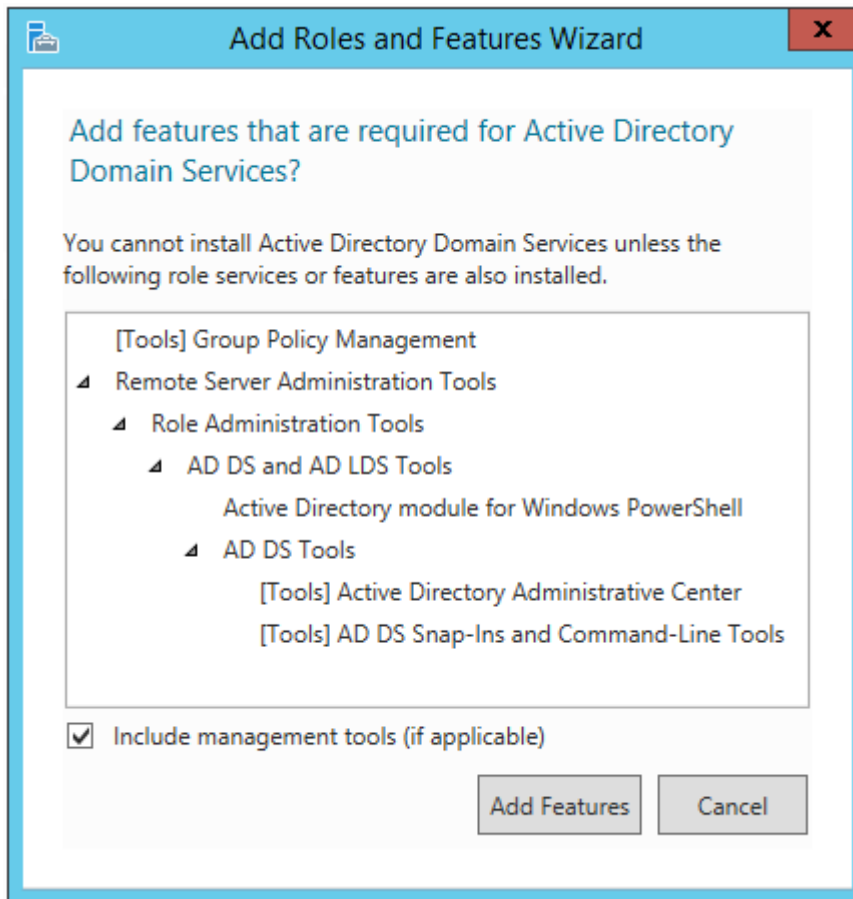
Figure 18: Prompt about adding features

You will be returned to the previous screen – click **Next**, **Next**, **Next.** Tick the **Restart the destination server automatically if required box** and click **Install**. It will take several minutes to install Active Directory, during which time an Installation progress screen will be shown. When installation is complete, click **Close**.

Having installed Active Directory Domain Services, the next stage is to 'promote' the server to be the Domain Controller. If you have used earlier versions of Windows Server you may be familiar with the DCPROMO command, which was previously used to do this. This does not exist in Windows Server 2012 R2; instead, promotion is done from the Server Manager screen. Looking at Server Manager, there will now be a new entry on the left-hand panel, marked *AD DS*:
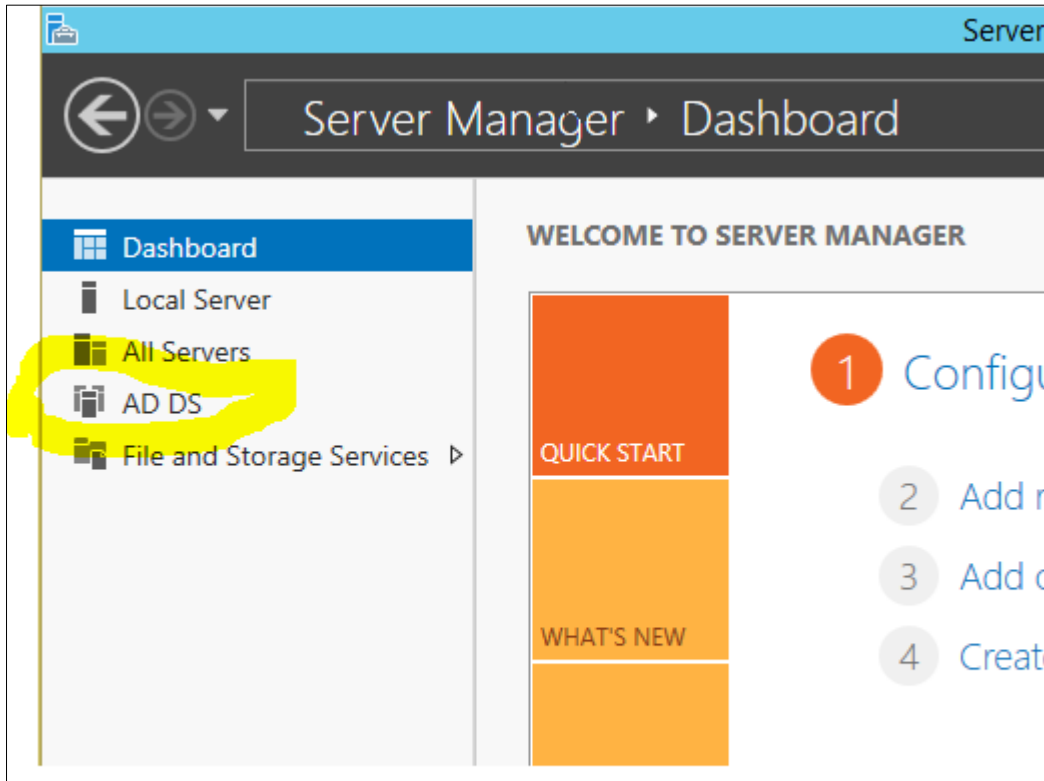
Figure 19: Entry for Active Directory in Server Manager Dashboard

Click on **AD DS**. On the resulting screen is a warning message that further configuration is required:
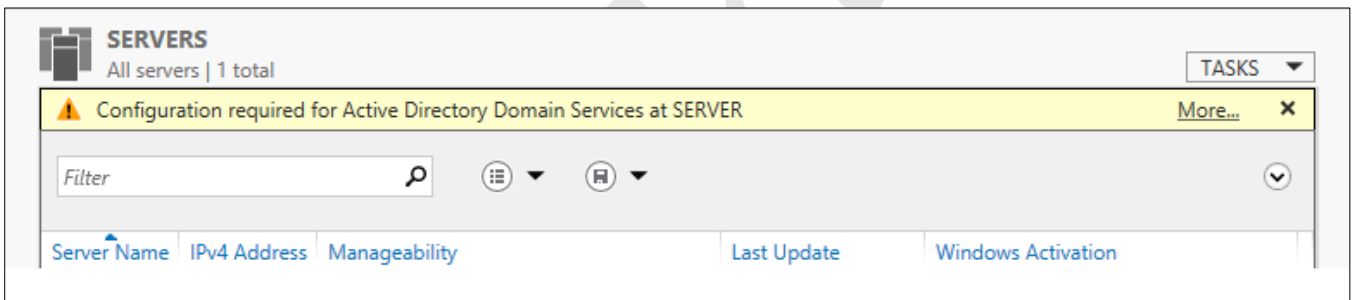
Figure 20: Message about need for additional configuration

Click where it reads **More…** and an additional panel will appear:
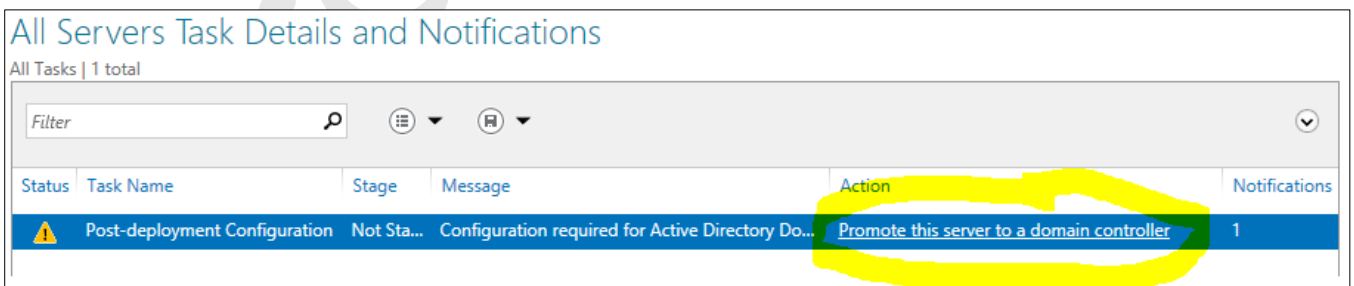
Figure 20: Option to promote server to be a domain controller

Click where it reads **Promote this server to a domain controller** and the *Deployment Configuration* panel is displayed. Choose the **Add a new forest option** and specify a **Root domain name**. In large organizations with multiple servers and/or locations, it is common to use the internet domain name prefixed by some other information to identify the separate locations or functions e.g. *london.ctacs.co.uk*, *liverpool.ctacs.co.uk*, *edinburgh.ctacs.co.uk*. In a small organization with a single server the domain name would commonly be the name of the organization with a suffix of

.local added e.g. *ctacs.local* (people with experience of installing servers may be aware of some debate over the use of *.local* but we will stick with it here). Click **Next**:
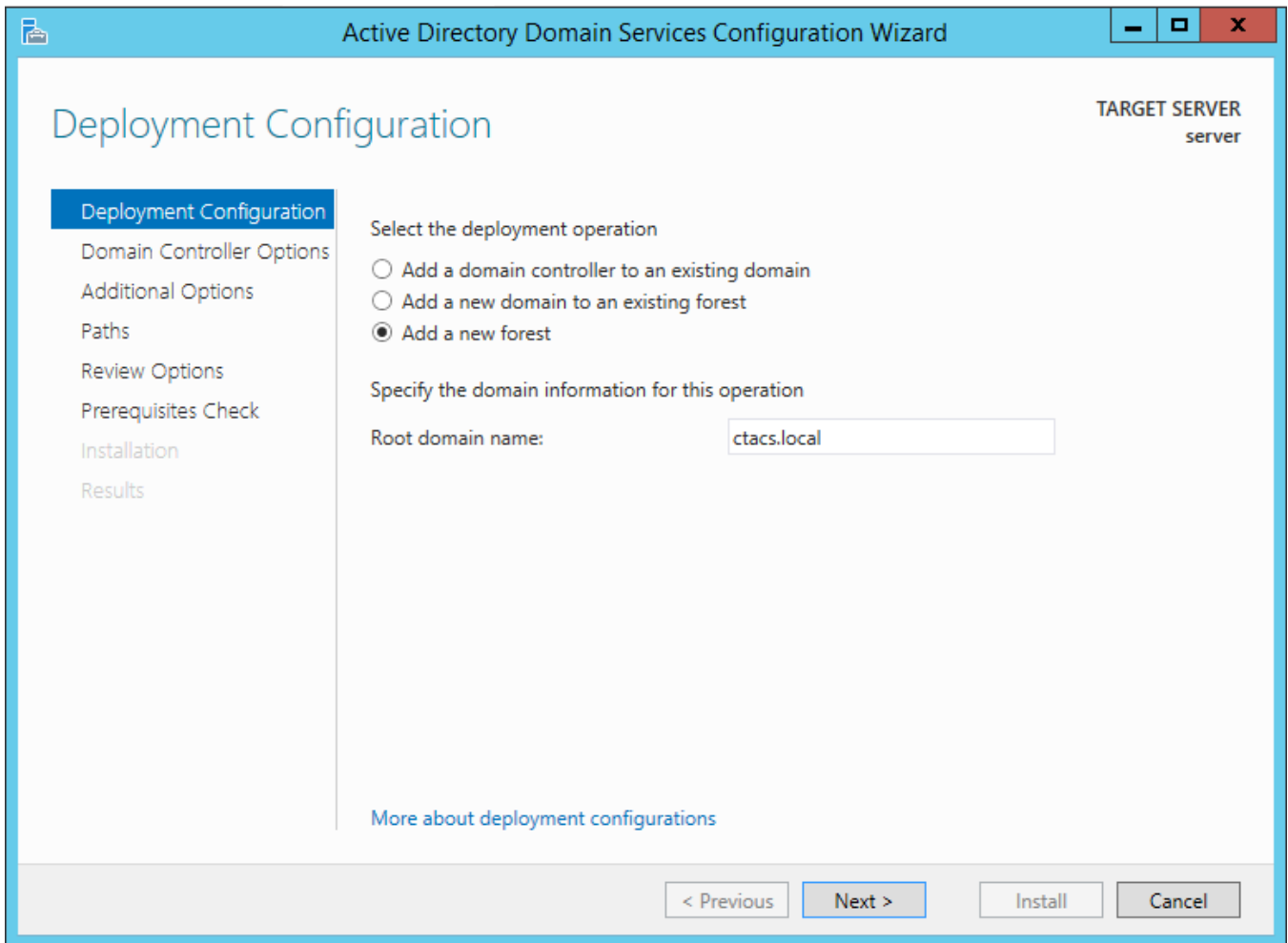
Figure 21: Specify options for the domain

After a short while the following screen is displayed. The **Forest functional level** and **Domain functional level** should both be set to *Windows Server 2012 R2* (alternative settings are available but would normally only be used if other, older versions of Windows Server were already in place). Leave the **Domain Name System (DNS) server** and **Global Catalog** boxes ticked. A password has to be specified – for convenience, you could use the same one as the Administrator account. Then click **Next**:
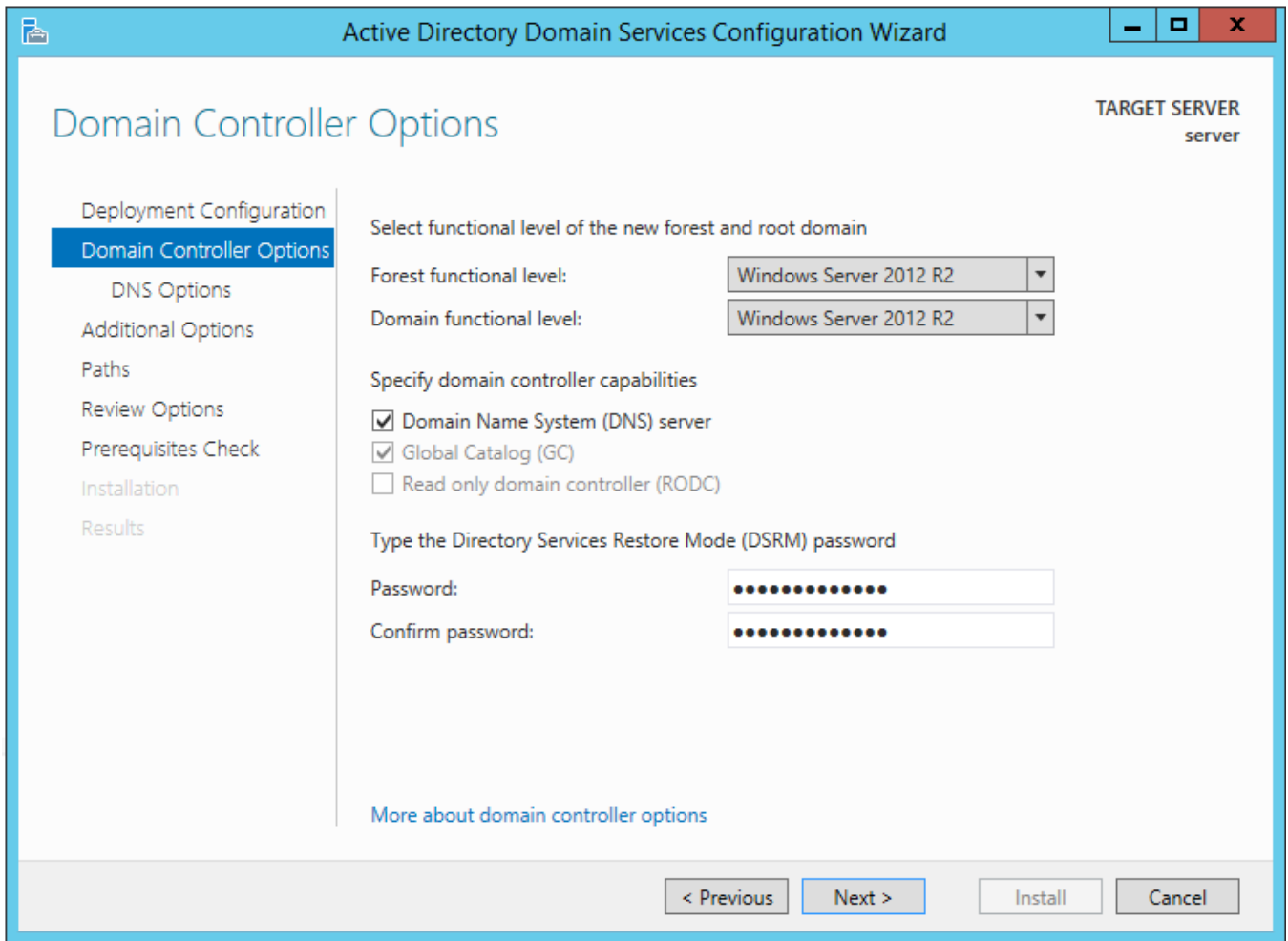
Figure 22: Options for the domain controller

On the next screen a warning may be displayed relating to DNS; the usual cause of this is that you are using an all-in-one internet router that is providing DNS and the message can be ignored for now. Click **Next**:
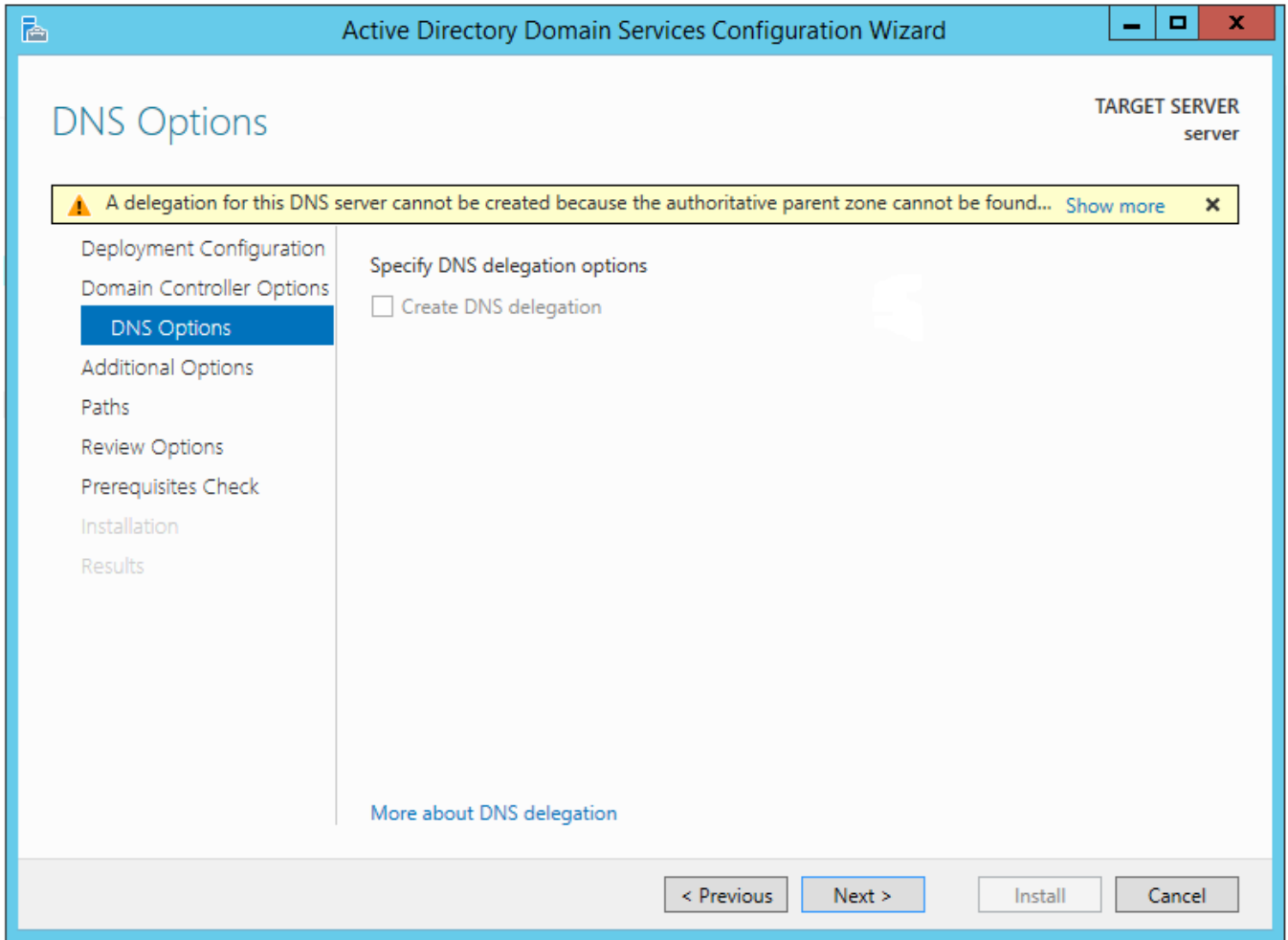
Figure 23: Message about DNS

The following screen asks you to verify the NetBIOS name. This will be the same as the domain name you chose and usually you just click **Next. T**he exception to this would be if it is more than 15 characters in length, in which case you need to shorten it.
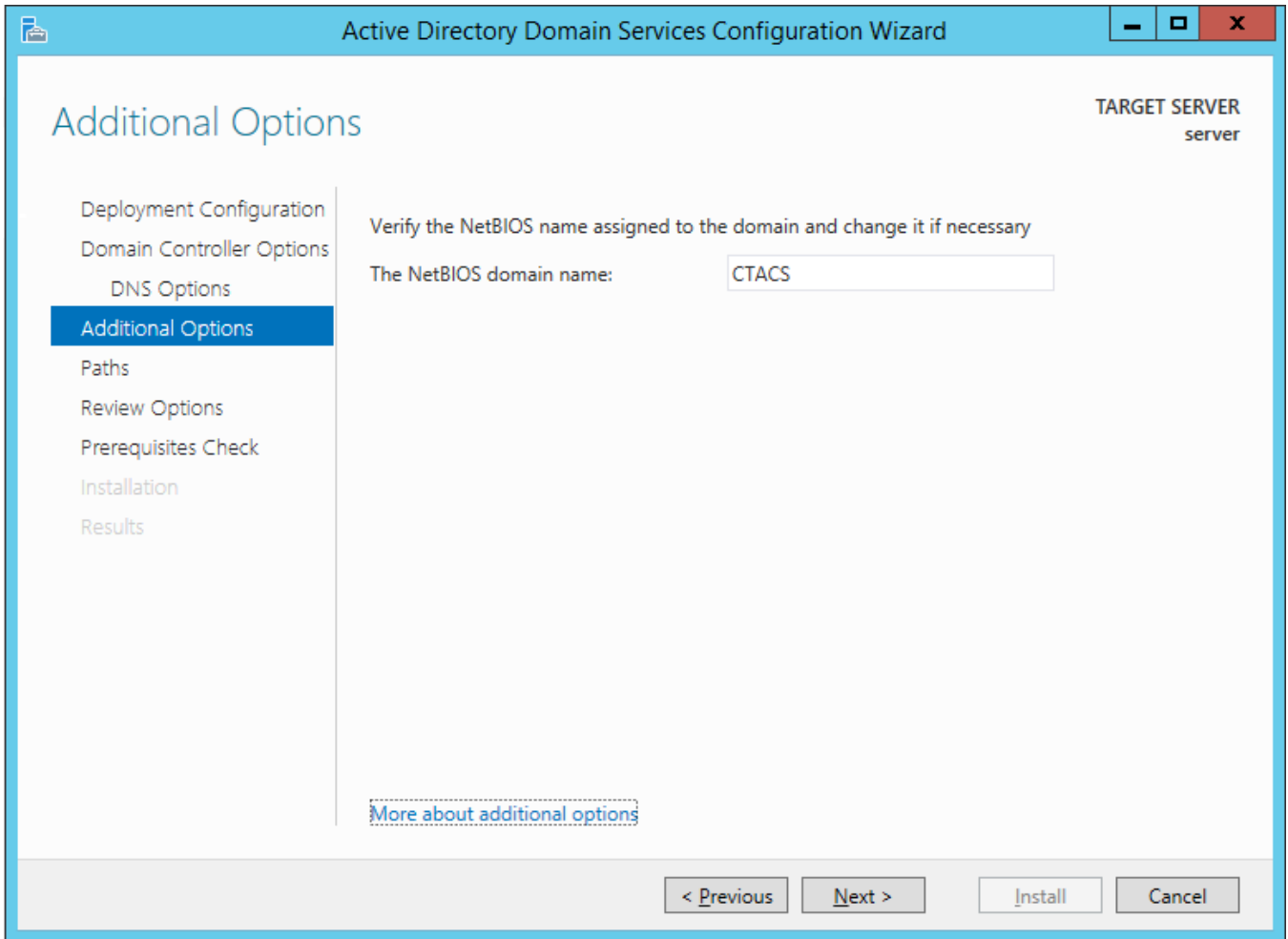
Figure 24: NetBIOS domain name

The next screen allows control over the location of the various files and logs associated with Active Directory. On a small system there is no need to change any of this so just click **Next**:
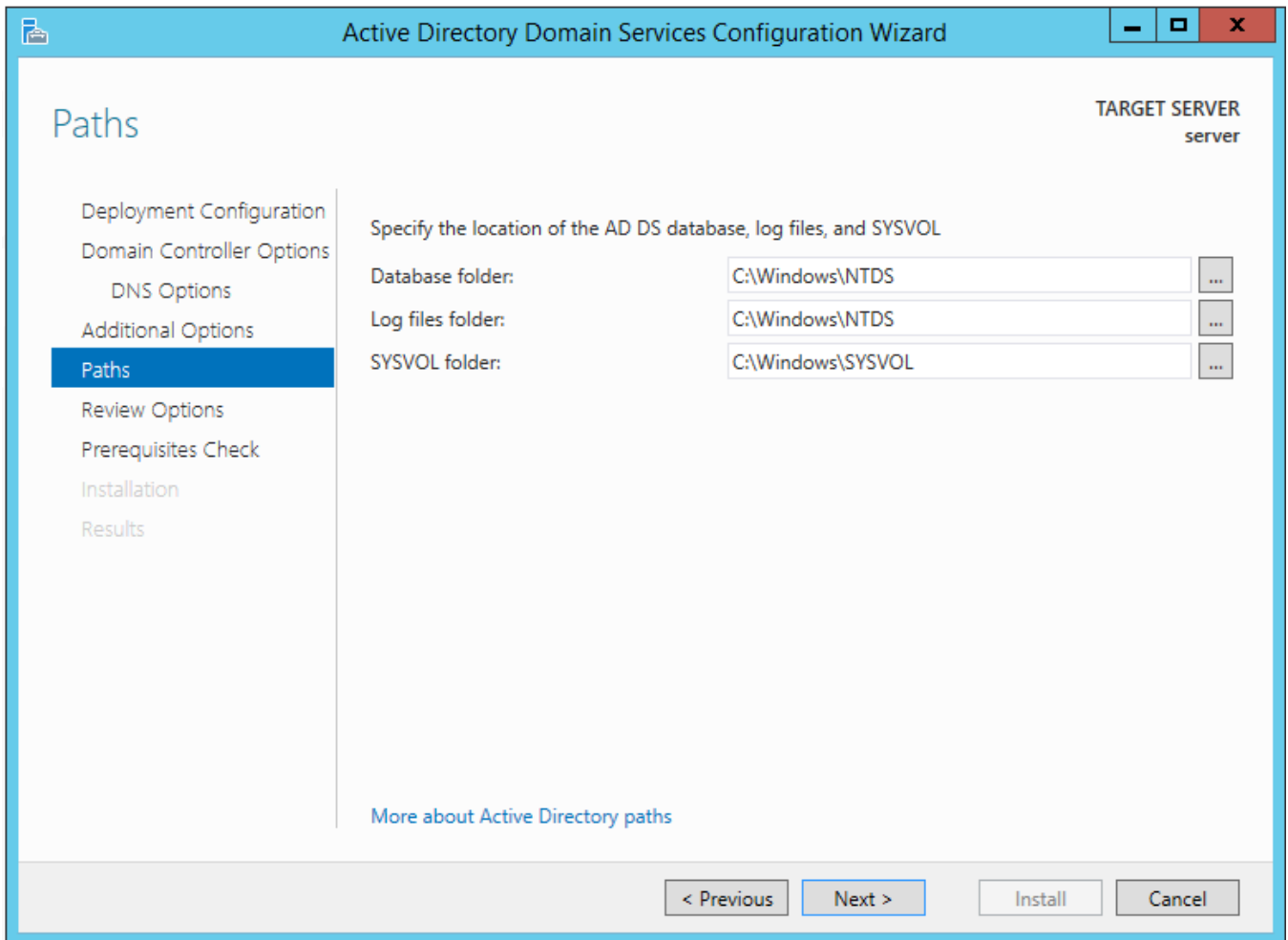
Figure 25: Active Directory paths

The subsequent screen is a summary of the various selections and settings - just click **Next**. Windows Server runs a 'Prerequisites check'; this will probably generate some warning messages, which can be unsettling, but usually they are just theoretical or obscure issues and can safely be ignored. Click **Install** to begin the installation proper, which will run for several minutes and after which the server will restart. Log back on as Administrator.

What needs to be done next depends upon the local infrastructure. If the server is connected to an all-on-one router that provides DHCP services (typically the case in a very small network) or is part of an existing network that already includes servers then continue with the next section, 3. STORAGE AND SHARED FOLDERS. However, if this is the *only* server and it is *not* connected through a router that provides DHCP, then it will be necessary to install the DHCP service on the server itself *before* continuing. How to do so is described in 13.1 Installing DHCP.

3. STORAGE AND SHARED FOLDERS

Important: If you are **not** using Storage Spaces, go to section 3.2 Folder Structure and Shares at this point. If you **are** using Storage Spaces continue first with the section below.

3.1 Setting up Storage Spaces

As described earlier, *Storage Spaces* is a feature of Windows Server that allows systems with multiple hard drives to be better utilized and managed. There is a common perception that it is just a low cost alternative to RAID; in fact, it is an extremely sophisticated feature, but in this example we will stick to the basics as applicable to a small network. If you are going to use Storage Spaces, it should be setup **now** before creating any users and folders on the system.

In this example, the server has a smallish hard drive, upon which Windows Server has been installed. Two further drives, each of 2TB, have now been added and Storage Spaces will be used to join them together to create a larger, protected volume. These drives can be internal hard drives or external USB or eSATA drives.

First make sure that the new drives are being recognized. Go into **Server Manager**, click **Tools** and choose **Computer Management**. From there, click **Disk Management**. There may be a message about having to initialize the new drives, so do so. However, it is not necessary to format them. Exit from Computer Management. Next, click **File and Storage Services** from Server Manager. On the left-hand side panel, click **Storage Pools** and the screen should appear as follows:
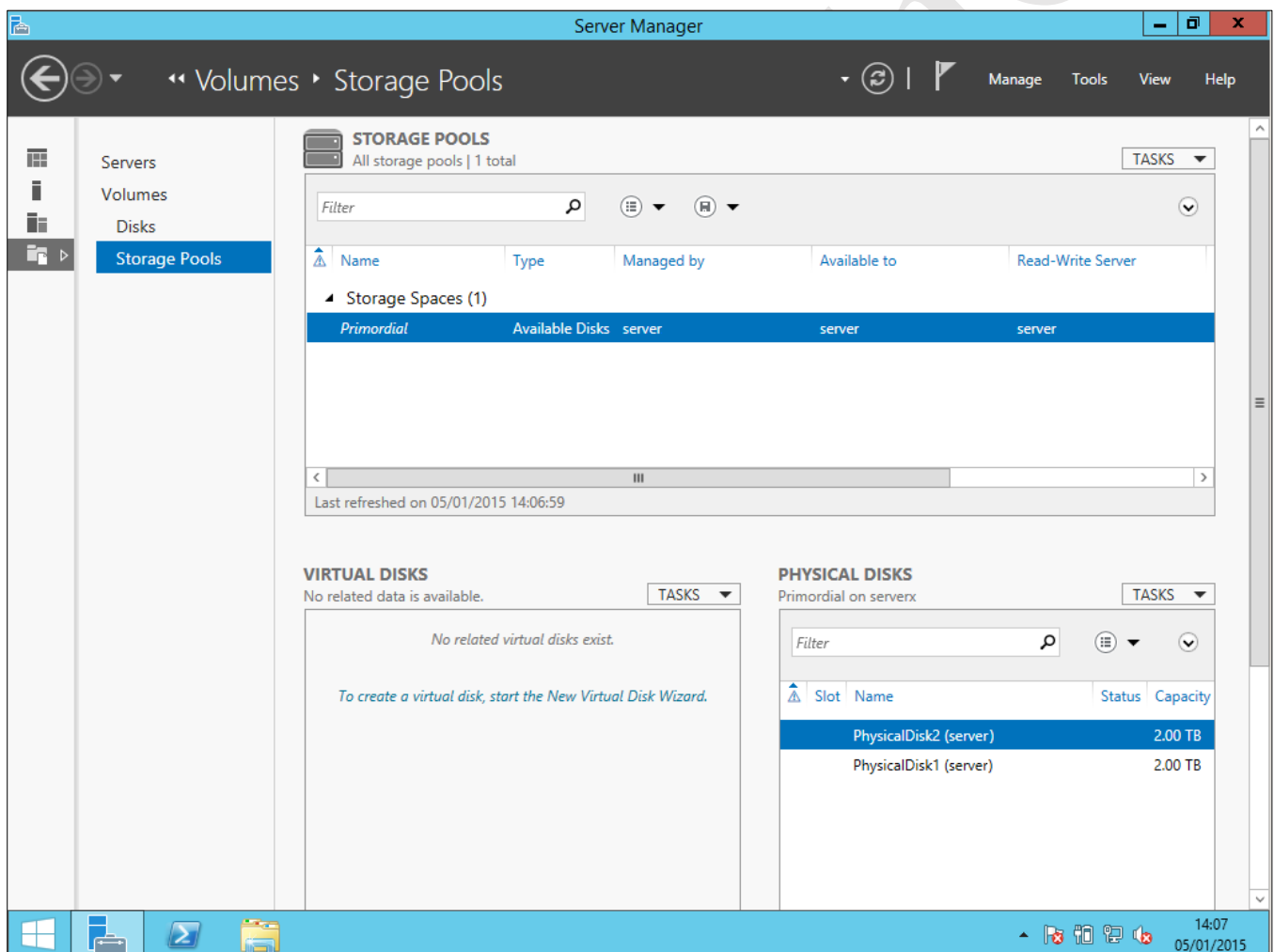
Figure 26: Server Manager Storage Pools

The screen is divided into three main panels: *Storage Pools*, *Virtual Disks* and *Physical Disks*. In the top-right hand corner of each panel is a dropdown called *TASKS*; click on the TASKS dropdown for Storage Pools and select **New Storage Pool** to invoke the *New Storage Pool Wizard*. Click **Next** to display the following panel. Enter a Name (e.g. *Datapool*), optionally enter a Description and click **Next**:
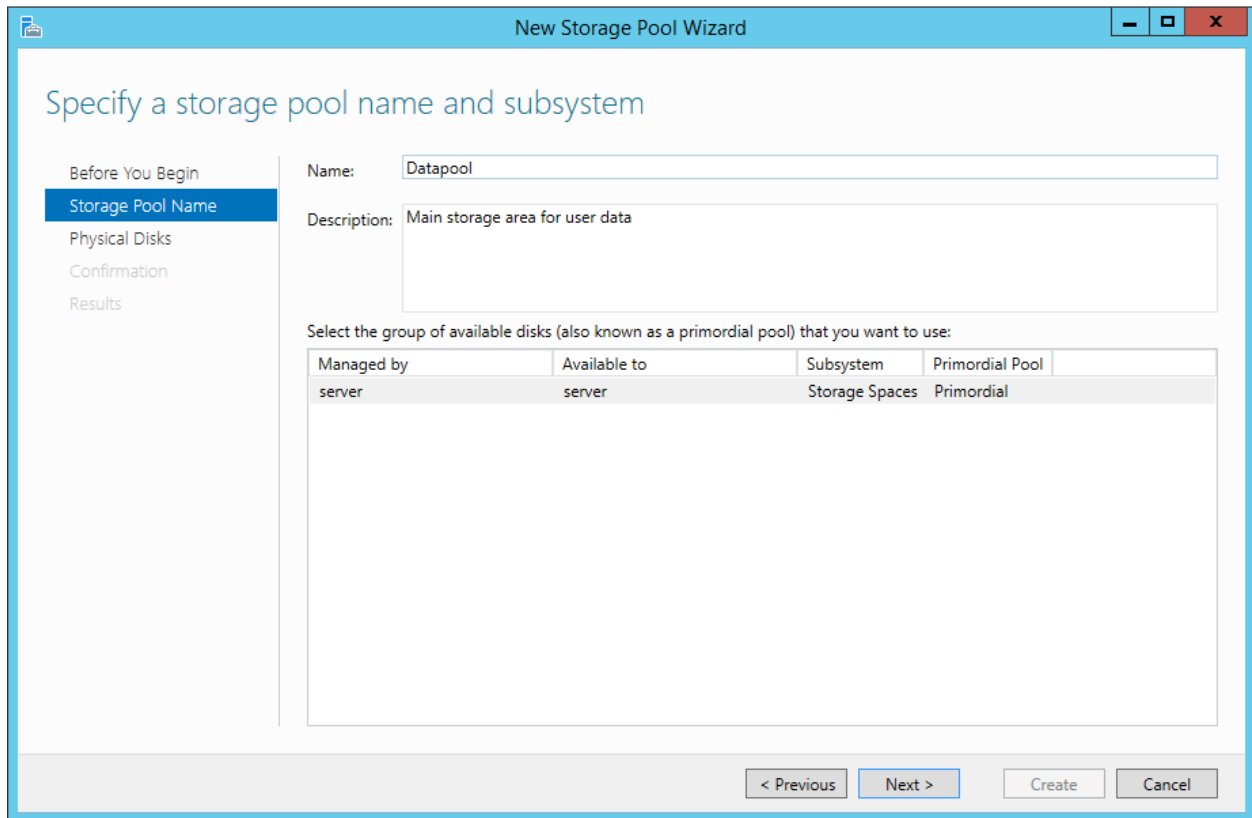
Figure 27: New Storage Pool Wizard

On the subsequent screen, tick the boxes for each disk. Then click **Next**:
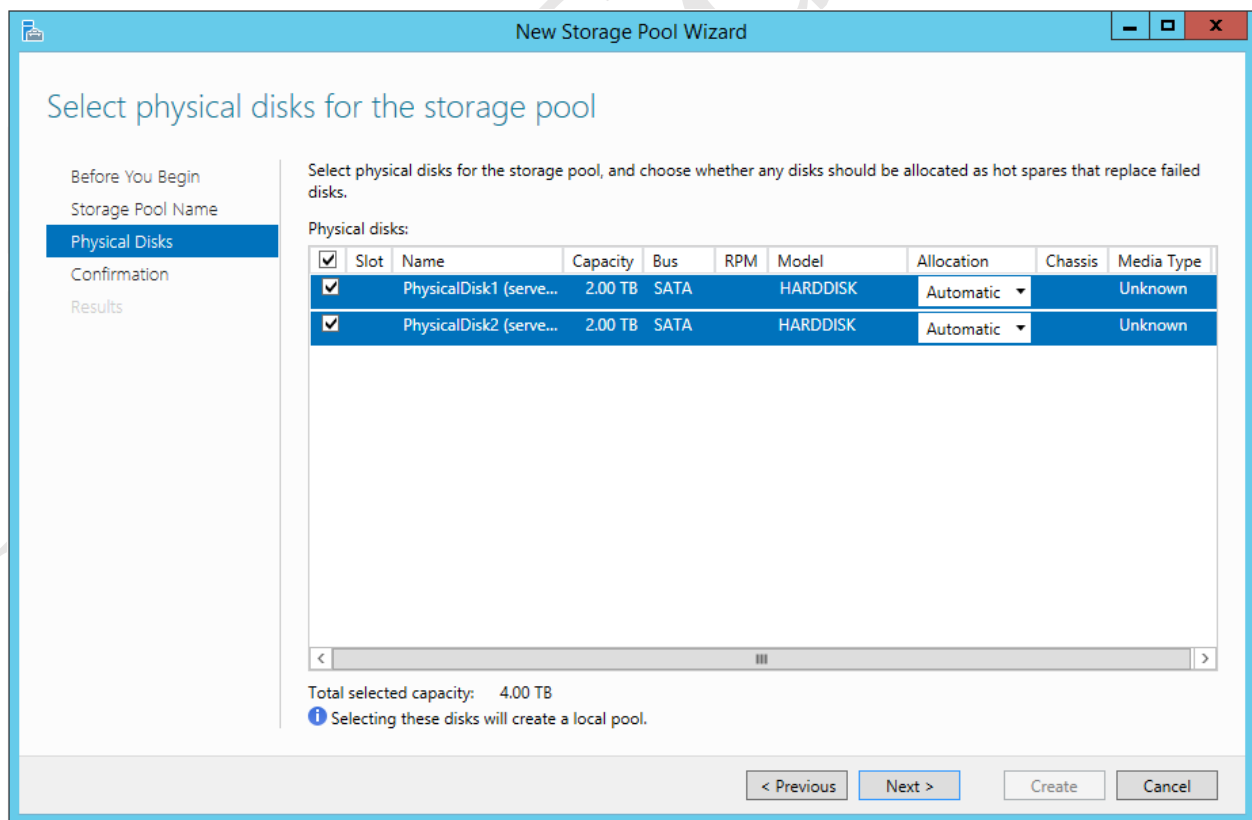
Figure 28: Select disks for the storage pool

A summary screen will be shown – click the **Create** button. After a short while the *Storage Pool Wizard* will complete – click **Close** to finish.

The next step is to create a *Virtual disk*. From the main Storage Pools screen, make sure the newly created Storage Space is highlighted. Then, in the Virtual Disks section click TASKS and choose **New Virtual Disk** to invoke the *New Virtual Disk Wizard*. Click **Next** on the first and second screens and on the third screen specify the virtual disk name (e.g. 'data') and an optional description, then click **Next**. The following screen appears:

Figure 29: New Virtual Disk Wizard

There are three types of storage to choose from:

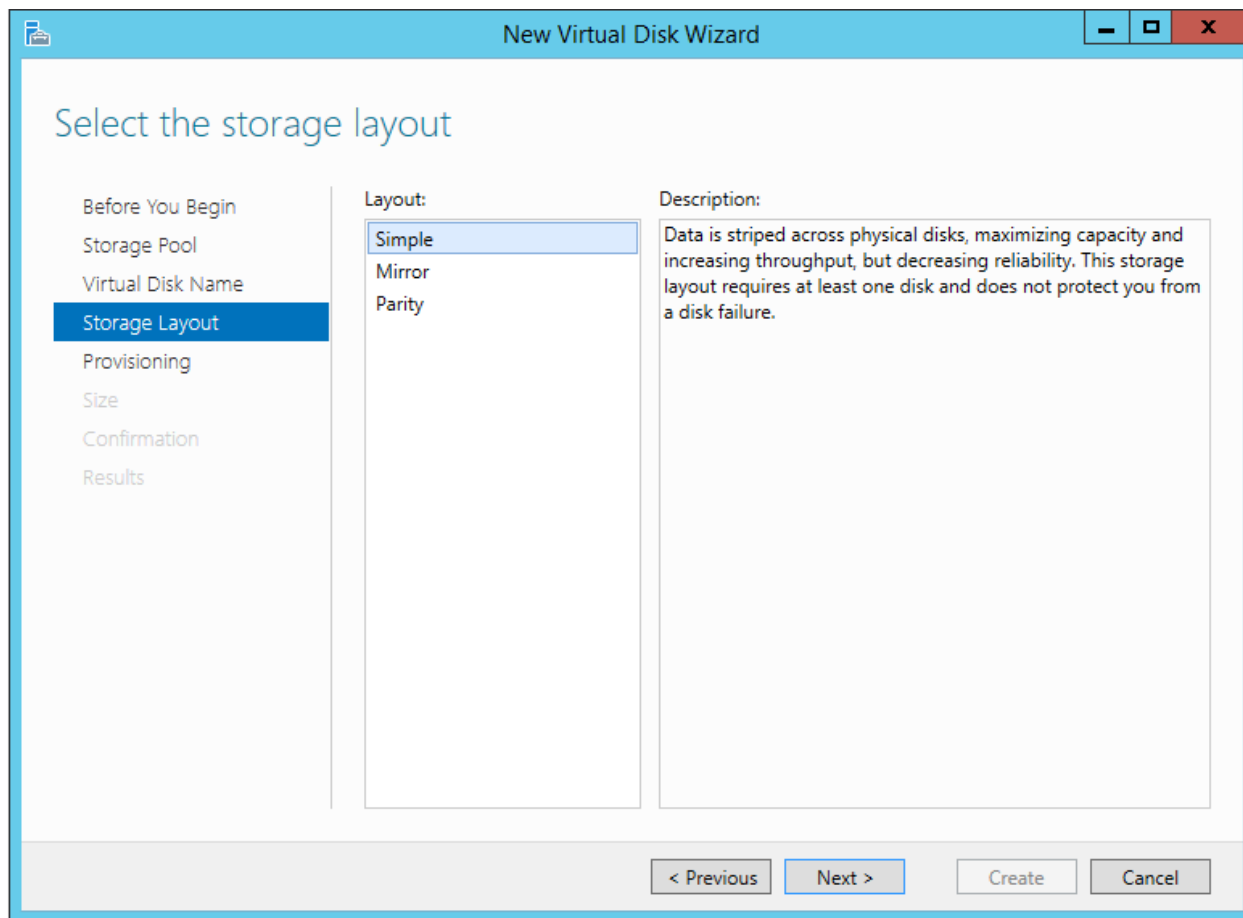- *Simple* - in which the drives are aggregated to create a single large volume, analogous to RAID 0 or JBOD (*Just a Bunch of Disks*) in other computing environments
- *Mirror* – in which data is duplicated on each drive in order to provide redundancy, analogous to RAID 1 in other computing environments. Requires at least two physical drives in the underlying Storage Space.
- *Parity* – here data is stored across all the drives. Additional information (known as *parity*) is used by the system, such that data is preserved in the event of drive failures, analogous to RAID 5 or RAID 6 in other computing environments. Requires at least three physical drives in the underlying Storage Space.

The amount of storage space available depends upon the option selected. In our example, we are using a pair of 2TB drives. If these are configured in *Simple* mode then the total amount of storage is 4TB; if configured in *Mirror* mode then the amount of available storage is 2TB. Make a choice depending on your requirements and the number of disks available, then click **Next**.

On the follow-on screen, there is a choice between *Thin* or *Fixed Provisioning*. This describes whether the disk space is allocated at the beginning ("Fixed") or starts small and grows as required ("Thin"). In a small setup you would generally choose **Fixed**; Thin is of more interest in a larger network with many servers, typically sharing common disk space. On the next screen you can further specify the size of the virtual disk – choose **Maximum size** and click **Next**. A confirmation screen is displayed – click **Create**. After a short while, depending on the options chosen, a completion screen is shown. Notice that the **Create a volume when this wizard closes** box is ticked:
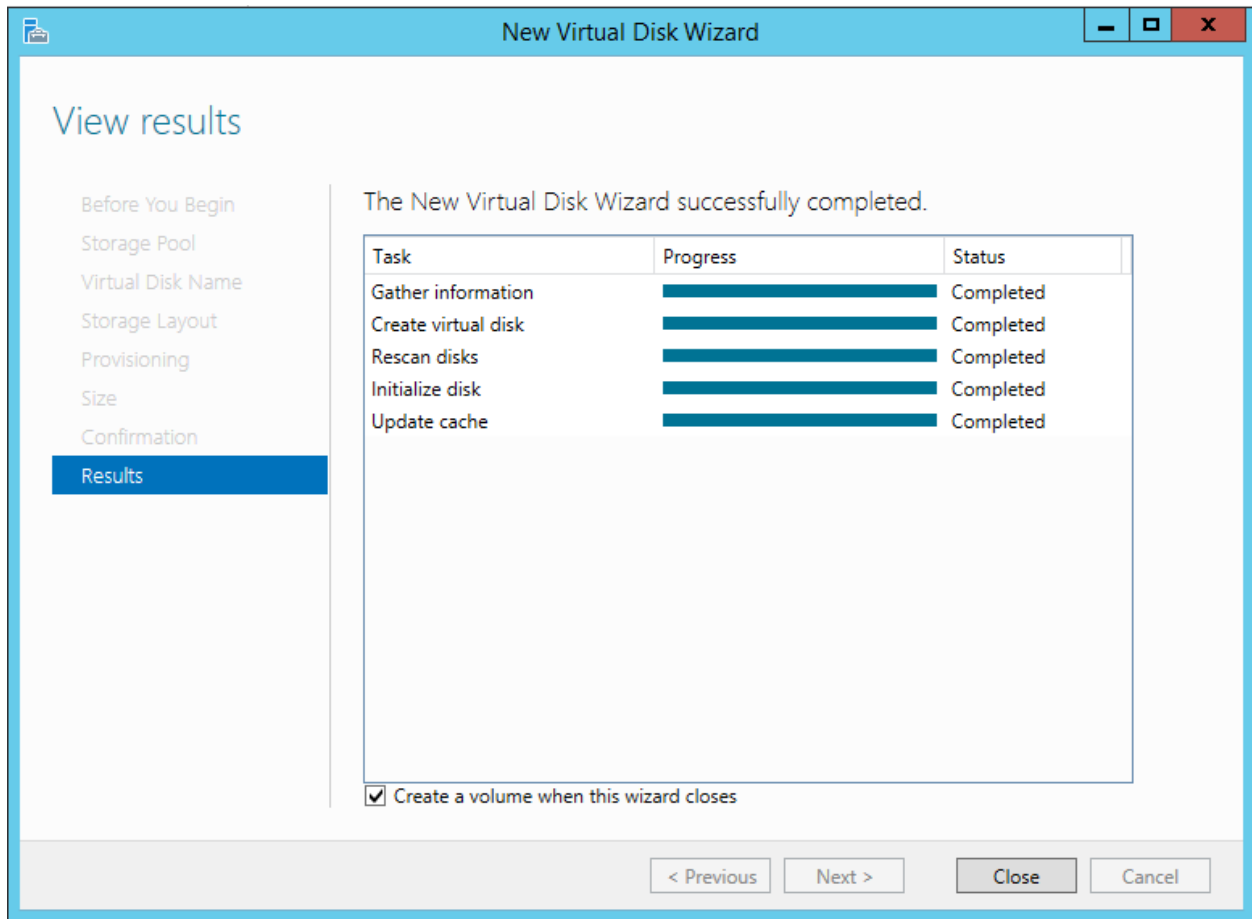
Figure 30: Virtual Disk Wizard completion screen

Click **Close** to start the *New Volume Wizard*. Click **Next** on the first screen. On the subsequent screen click **Next**:
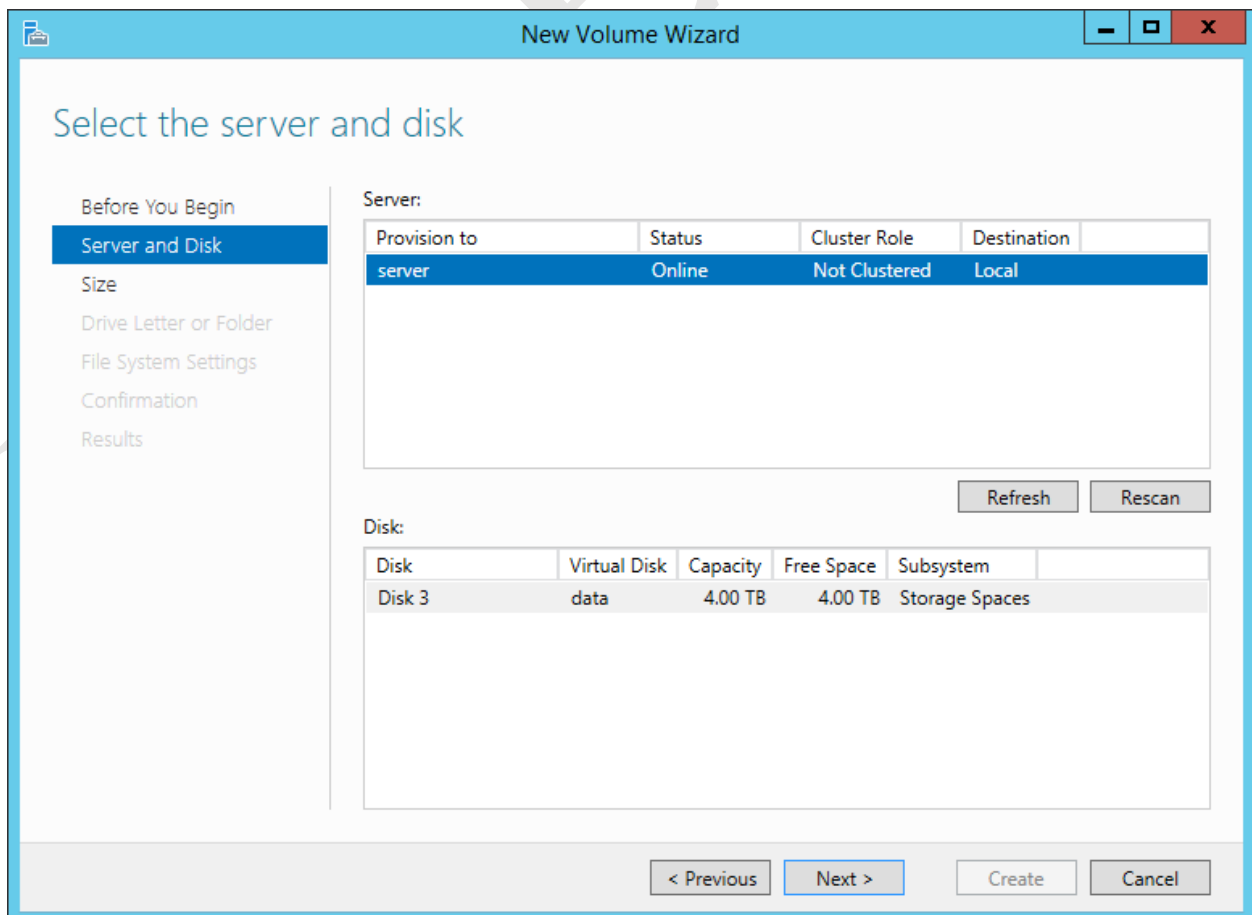
The size of the volume can now be specified. Unless you have very specific reasons to do otherwise, make it as large as permitted:
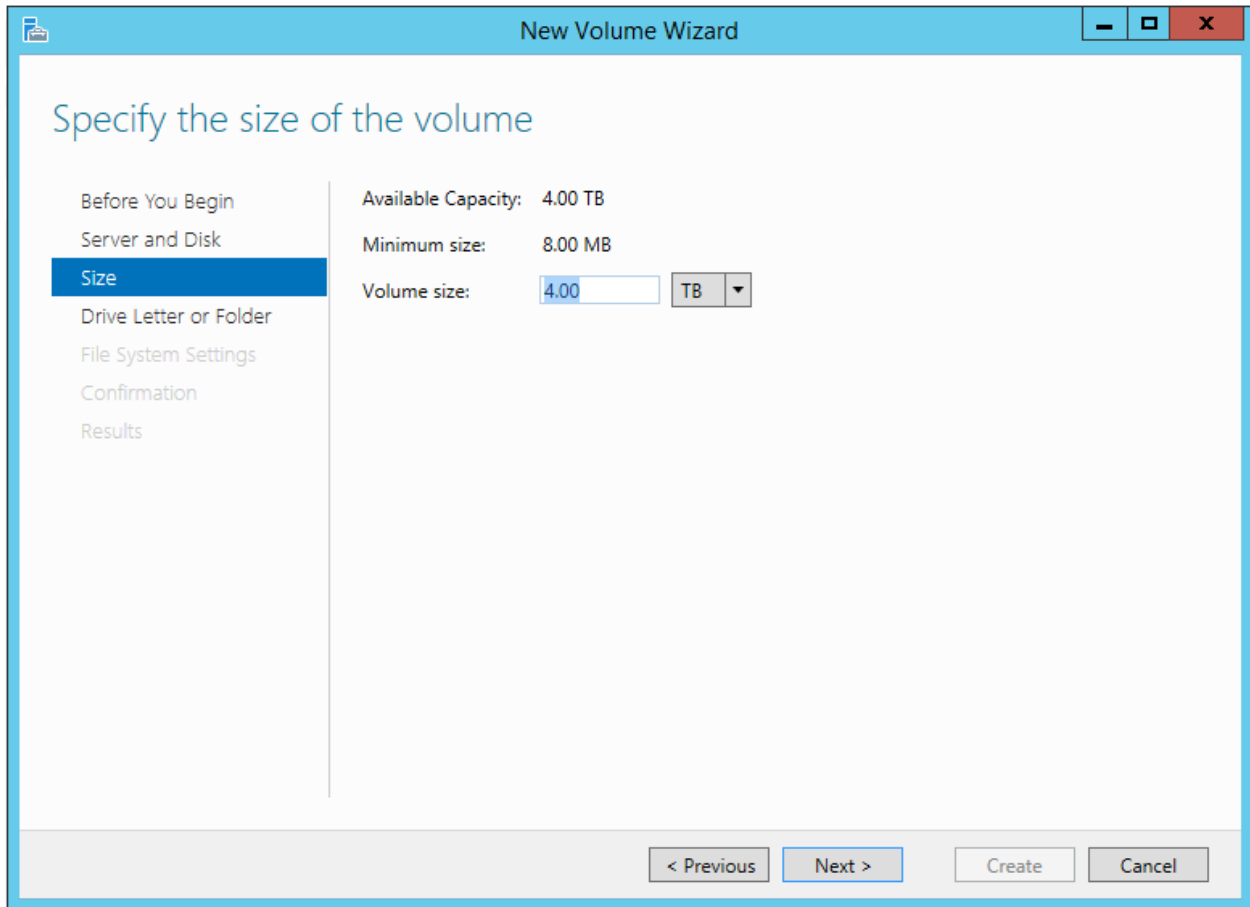
Figure 32: Specify the size of the new volume

On the subsequent screen, assign a free drive letter to the new volume. In this example we will make it the D: drive:
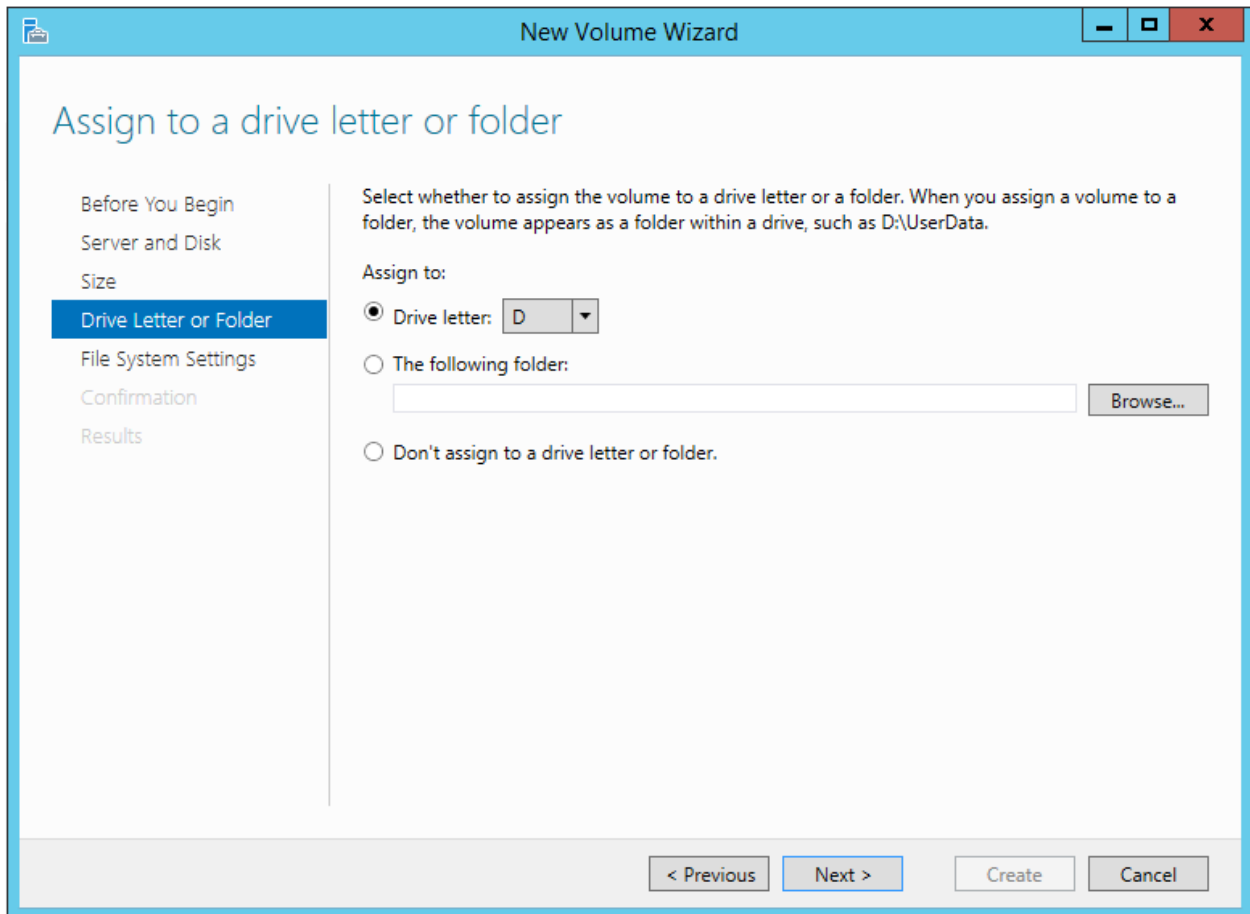
Figure 33: Assign a drive letter to the new volume

Next, check the *File System* type (usually NTFS) and assign a Volume label (e.g. "Data"). Click **Next**:
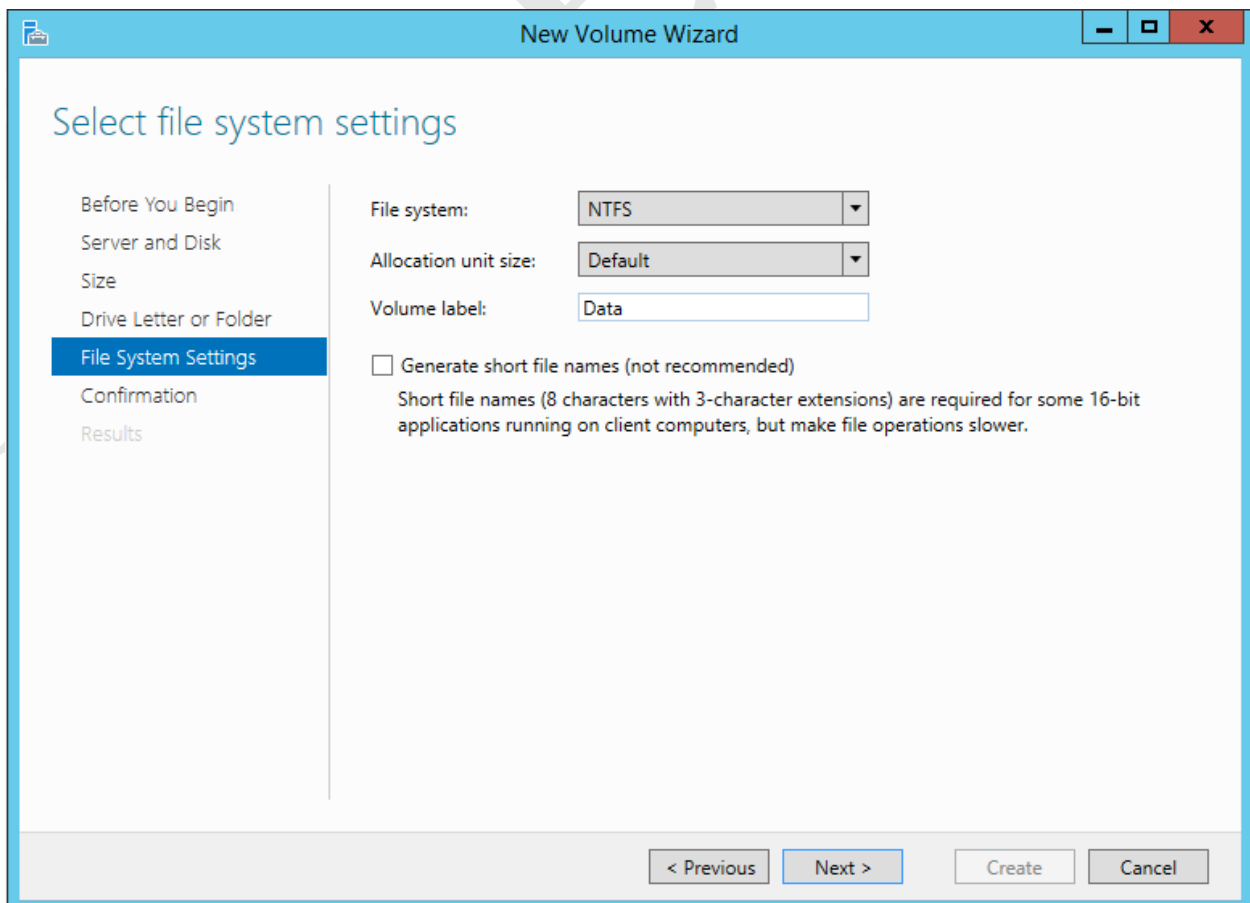
A confirmation screen is displayed; assuming everything is okay click **Create**. After a while a completion screen is shown – click **Close**. The new drive should now be visible in File Explorer.

3.2 Folder Structure and Shares

The main purpose of a network is to provide an environment in which users can store and share information. This is done by creating folders on the server, some shared and some private, then defining access rights to control who sees what. The structure of these folders will depend upon the requirements of the organization, but a typical arrangement might be:

- One or more shared company folders that everyone has access to
- Folders for the different departments and functions within the business
- Individual private home folders for each user

In our example, we have two volumes, one for the operating system (the C: drive) and one for the data (the D: drive). On the data volume the following structure will be created:
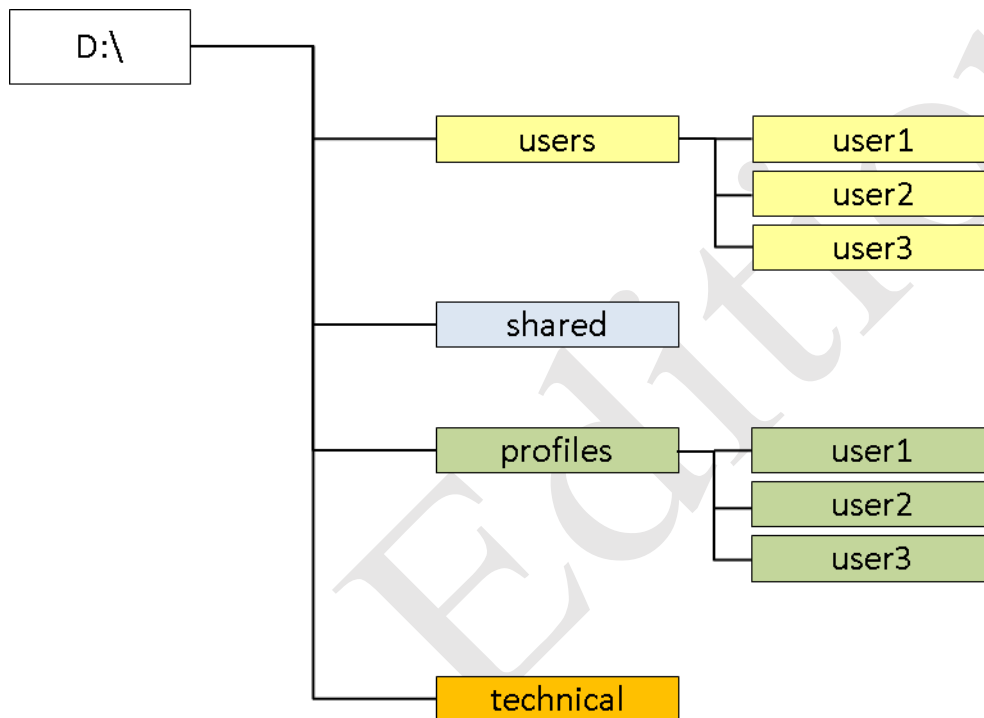
Figure 35: Example folder structure

The folders are used as follows:

Users - Holds the individual home folders for users

Profiles - Top-level folder for user profiles (the purpose and use of profiles is discussed later)

Shared - Holds data that can be used by everyone

Technical - For use by the person(s) supporting the system and contains master copies of software, utilities, technical documentation and so on.

Begin by creating four top folders in the D: drive called *users*, *shared*, *profiles* and *technical*. The easiest way to do this is by using File Explorer. Whilst viewing the D: drive, right-click and choose **New** > **Folder** to create a folder.

Having created the folder structure, a number of shares need to be created. To create a standard share, right-click the folder to be shared in File Explorer and choose **Share with > Specific people**. On the resultant panel use the drop-down to select the user and click **Add**. Then, click on the user, set the **Permission Level** accordingly and click **Share** followed by **Done**.
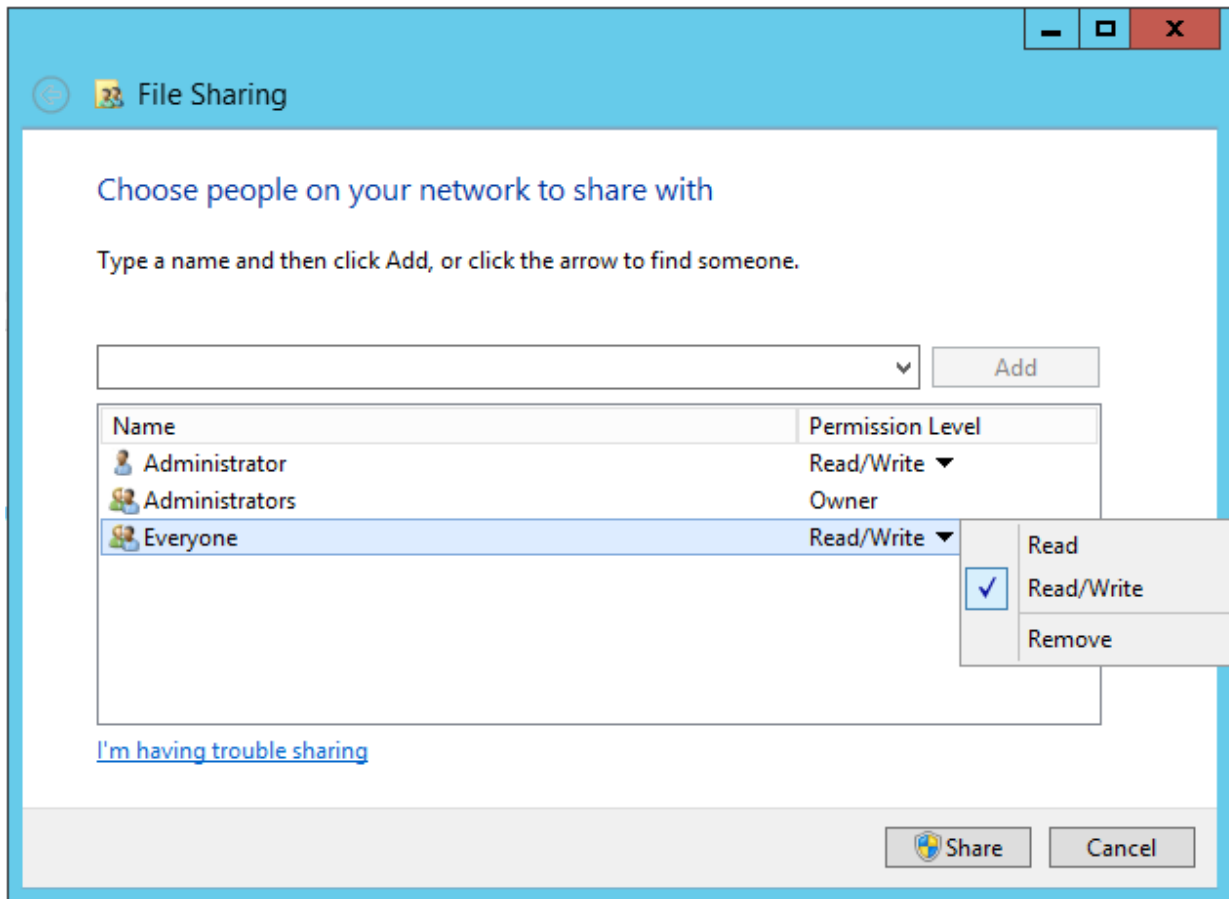
Figure 36: File Sharing panel

Create two shares as follows:

Folder name	Share name	Notes
D:\users	users	Give Read/Write access to Everyone
D:\shared	shared	Give Read/Write access to Everyone

Shared folders are normally visible to all users, but can be made hidden. The purpose of doing so is partly related to security, but also to keep the overall system tidy and avoiding confusing users with a superfluous number of folders, as there may be dozens or even hundreds on a network. Shares are made hidden by placing a dollar sign ($) at the end of the share name and the overall process is as follows:

Right-click on the *technical* folder, choose **Properties** and click the **Sharing** tab. Click the **Advanced Sharing** button. On the next panel tick the **Share this folder** box. Specify the share name; this will default to the name of the folder but by adding a $ sign at the end (e.g. *technical$*) it will become a hidden share:
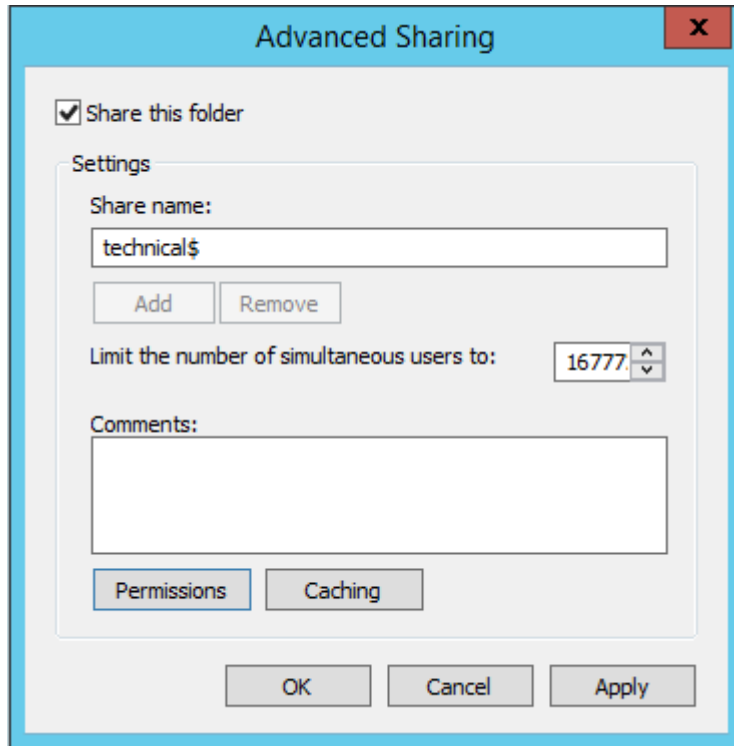
Figure 37: Advanced Sharing panel

Click the **Permissions** button then click **Add**. In the field that reads **Enter the object names to select** type in the name of the user(s), in this case *Administrators*. Click **Check Names**; if it is a valid user name it will become underlined. Click **OK**.
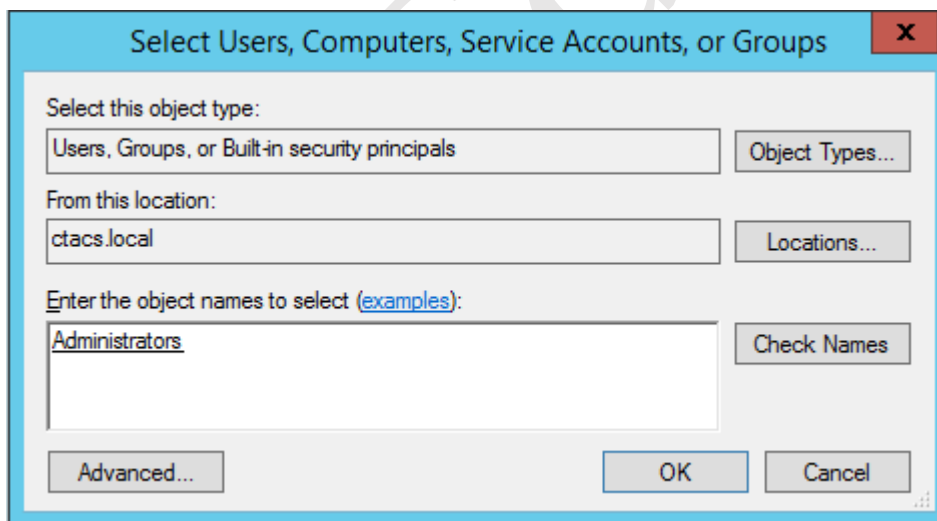
Figure 38: Searching for and selecting a user

On returning to the previous screen, give *Administrators* the rights to do everything and give *Everyone* no rights at all. Then close down the dialogue box (ignore any warning messages in this example).
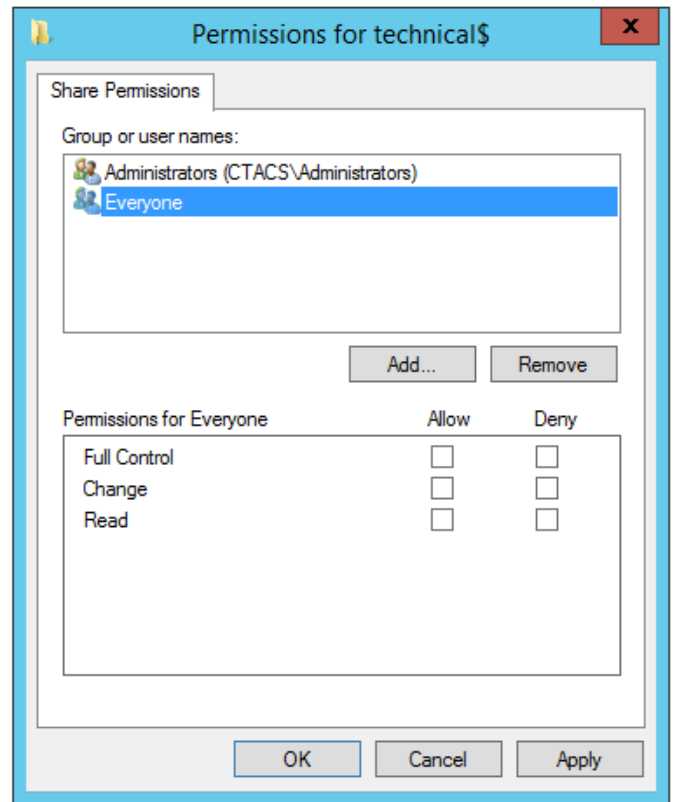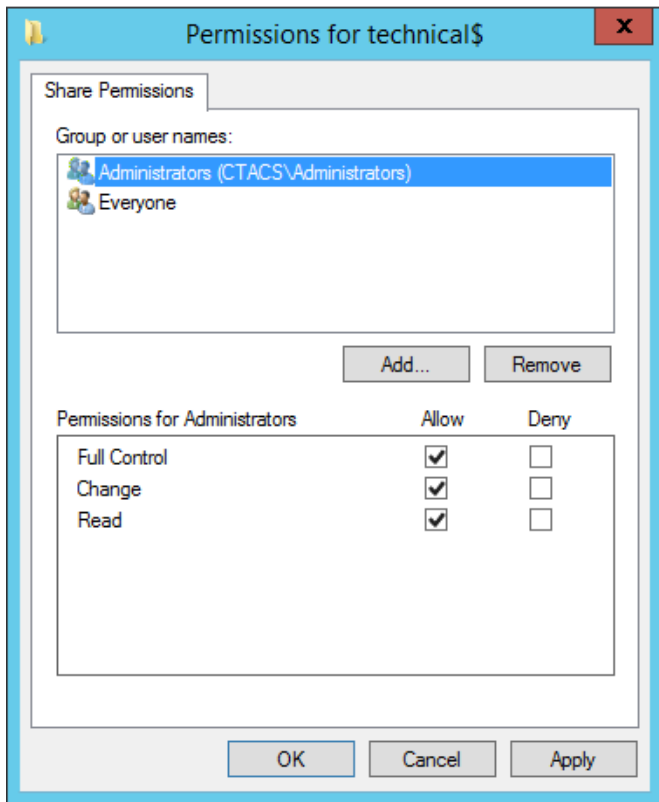
Figure 39: Setting Permissions

Now create a hidden share called *profiles$* using the same method. In this instance, give **Full Control** to *Everyone*.

4. USERS

Before creating the users, some thought should be given to a naming convention. As a general principle, aim for consistency. For user names, two common conventions are to use the first name plus the initial of the surname, alternatively the initial of the first name plus the surname, although in some parts of the world other conventions might be more appropriate. In the case of particularly long names and double-barrelled names it might be a good idea to abbreviate them. For example:

Name of person	User name
Nick Rushton	nickr
Mary O'Hara	maryoh
Ian Smith	ians
Amber Williams	amberw

Alternatively:

Name of person	User name
Nick Rushton	nrushton
Mary O'Hara	mohara
Ian Smith	ismith
Amber Williams	awilliams

4.1 Creating Users

Users can be created using *Active Directory Users and Computers* or the *Active Directory Administrative Centre*. We will use the former, which is arguably simpler (and also happens to be the same as in earlier versions of Windows Server, which may be helpful for some people). It can be accessed in two different ways:

- Within **Server Manager**, click **Tools** in the top-right hand corner and choose **Active Directory Users and Computers** from the drop-down list.
- Click **Start** or press the Start key to show the **Start Screen**. Click the **Administrative Tools** icon and from that choose **Active Directory Users and Computers**.
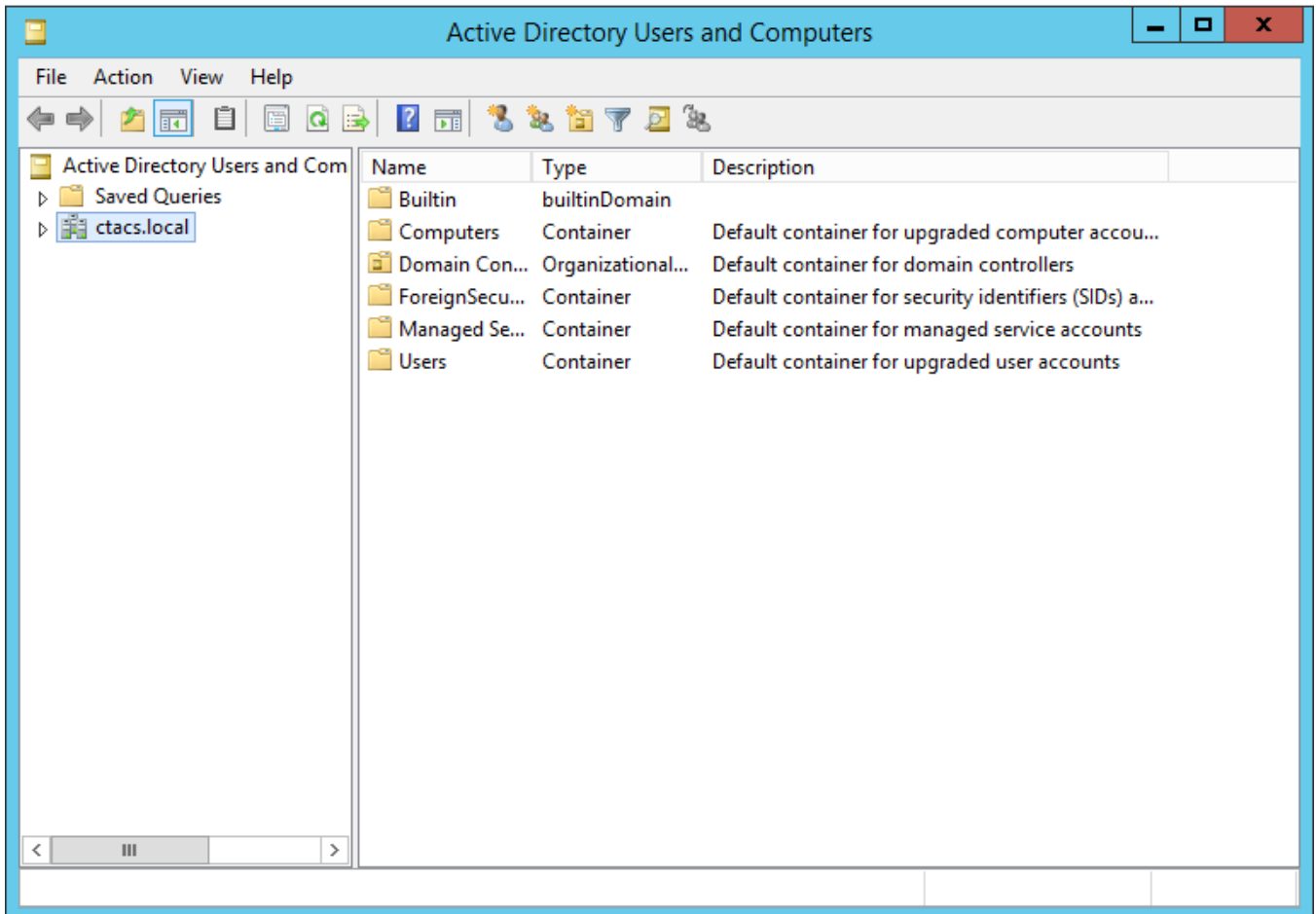
Figure 40: Active Directory Users and Computers screen

Assuming the domain is highlighted on the left-hand side of the screen – *ctacs.local* in our example – the right-hand side will list the *Containers* inside it. Containers are the different type of objects that exist in the system and built-in ones include *Computers* and *Users*. By keeping objects in containers it makes them easier to manage and, in addition to the built-in ones, you can create your own. For instance, double-clicking the *Users* container reveals that the system already contains a number of pre-defined special users (albeit many of which are never used, except in the largest of networks) such as *Administrator*. When you create users on a small system, you can place them in this container. But in a large organization, with hundreds or maybe thousands of users, you may wish to create additional containers first and place them in those, organized according to department or location, for instance.

In our example, we will assume that we have a relatively small number of users. Click the *Users* container to highlight it, then choose **Action** > **New** > **User** from the menu (there is also an icon to create a new user). The following panel is displayed:

Figure 41: Creating a new user

Complete the panel and specify the **User logon name** in accordance with the convention you are following, then click **Next** for the password panel**:**

Figure 42: Specifying password options

Enter and confirm the password. The best passwords are: non-obvious; not the user's name; not too short; a mixture of upper and lower case letters plus numbers and special characters (such as exclamation marks). There are four tick-boxes to be considered:

- User must change password at next logon – this is the default and is generally a good idea

- User cannot change password – useful when several people share an account or in some educational settings
- Password never expires – again, of use with shared accounts
- Account is disabled – prevents the user logging in. Useful when people leave the organization

After clicking **Next**, a summary screen in shown. Click **Finish** to continue and the user is created. If the password does not meet the criteria described above the following message is displayed:
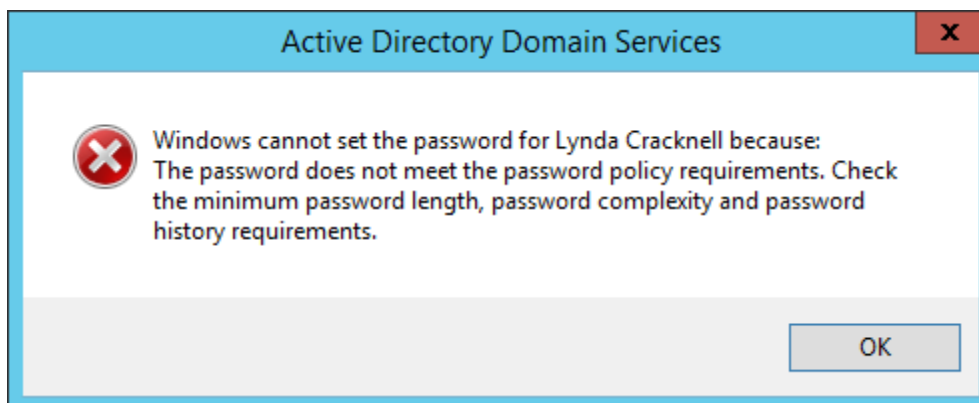

Figure 43: Warning message about password complexity

If it does not, then the password will need to be changed. Whilst not generally recommended, it is possible to remove the requirement for complex passwords altogether and how to do so is described in section 8.6 Changing the Password Policy.

Creating users can be time consuming. In a small network this may not be an issue, but in an organization with hundreds of users it may well be. Fortunately, tools are available to bulk-create users. A free one comes with Windows Server; it is called *csvde.exe* and is located in the *C:\Windows\System32* folder. The basic principle is that a CSV file containing the names of the users and other information is created in Excel. In some instances, it might be possible to generate a suitable file from another application, such as a payroll or human resources system. Or, if this is a replacement network, a list of user names can be exported from Active Directory on the old system and then imported into Active Directory on the new one using *csvde.exe*. However, the tool is fairly basic and some effort is still required. Easier and more sophisticated commercial alternatives are also available.

4.2 Creating Users from the Command Prompt

Some people are wary of working using the command prompt, but it is a very efficient way of doing some things and, particularly if you have multiple users to create, somewhat quicker than other techniques. The caveat is that the users will be 'plain vanilla' and it will probably be necessary to later edit them or provide additional details using *Active Directory Users and Computers*, but even so it can be a time saver.

You can use the traditional Command Prompt (if you are old enough you may still think of this as the 'DOS prompt') or the more sophisticated *Windows PowerShell*. Once you have a Command Prompt, type *net user username password /add /domain*

For example: *net user laurar !zel892!ee# /add /domain*

When you have finished creating the users, type exit and press Enter to return to the system.

If you are an experienced user, you will probably realise that you could create a script ('batch file') that could be used to create multiple users at once.

As mentioned, the user details will need to be filled out using *Active Directory Users and Computers* and you may find the technique described in 4.8 Editing Multiple Users Simultaneously of some help.

4.3 Resetting a Password

There is often a need to reset or change a user's password; for instance, they may have forgotten it or it has become compromised. To do so, right-click the user's name within **Active Directory Users and Computers** and choose **Reset Password**. In the resultant dialog box specify and confirm the new password, then click **OK**.

4.4 Disabling an Account

When a user leaves the organization, their account should in the first instance be disabled to prevent it being used. It is preferable to do this rather than immediately deleting the account, as there may subsequently be a need to access it or the user may later return. To disable an account, right-click the user's name with **Active Directory Users and Computers** and choose **Disable Account**. To re-enable at any point, right-click and choose **Enable Account**.

4.5 Deleting an Account

To delete an account, right-click the user's name and choose **Delete**. Note that once an account has been deleted it cannot be restated; for this reason, it is suggested that accounts are normally disabled rather than deleted as per the previous point.

4.6 User Groups

In an organization with a small number of users, specifying who has rights to folders is fairly easy to manage. But if there are more users it becomes far more time consuming; for instance, you might have to specify the level of access for hundreds or even thousands of individual people. Such organizations are usually large enough that they contain departments or teams to carry out the different functions; for instance, there might be several people working in accounts, several in sales, several in marketing and so on.

To support these typical business structures, Windows Server features the concept of *groups*. A group consists of a number of users who have something in common within the organization, for instance they are all members of the same team. Access rights can be specified for a group, which means they then apply to all members of that group. If a new person joins the team they just have to be defined as a member of the relevant group, at which point they inherit all the relevant access rights.

To create a new group, go into **Administrative Tools** and launch **Active Directory Users and Computers**. On the left-hand panel, right-click the entry for *Users* and choose **New** > **Group**. In the dialog box, specify the **Group name** (note that the name will automatically duplicate below in the obsolete 'Group name pre-Windows 2000' field). The 'Group scope' and 'Group type' radio buttons can be left as 'Global' and 'Security' respectively. Click **OK**.
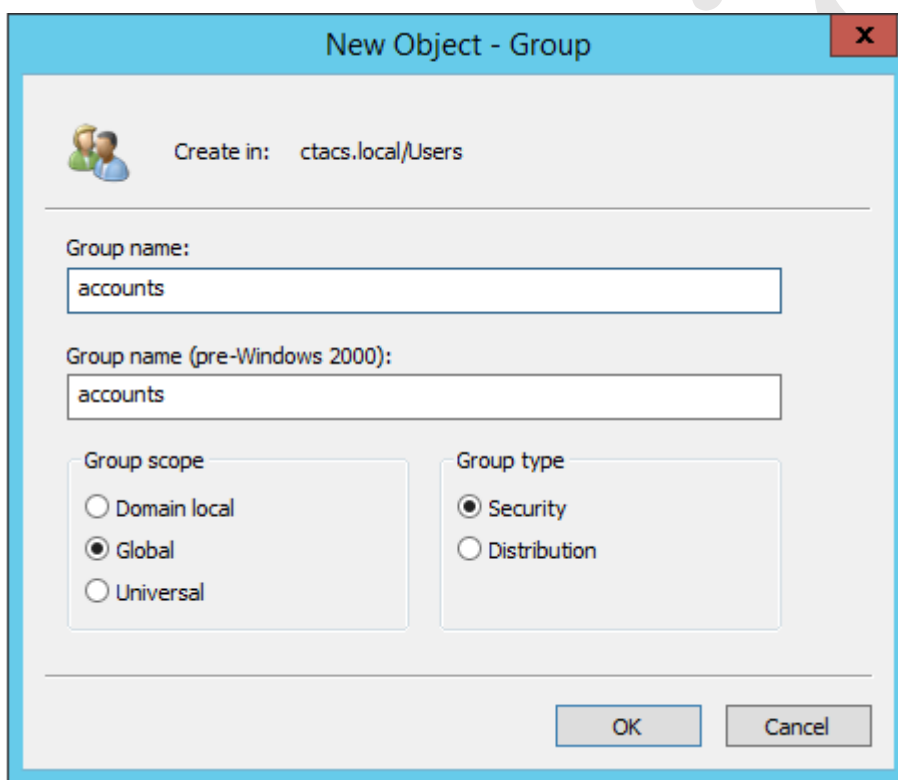
Figure 44: Creating a new Group

There are two ways to make particular users members of a group:

In **Active Directory Users and Computers**, right-click the user name and from the pop-up member choose **Add to a group**. A small dialog box is displayed. Type in the name of the object (i.e. the name of the group) and click the **Check Names** button. It will be validated and if correct will then appear underlined. Click **OK**.
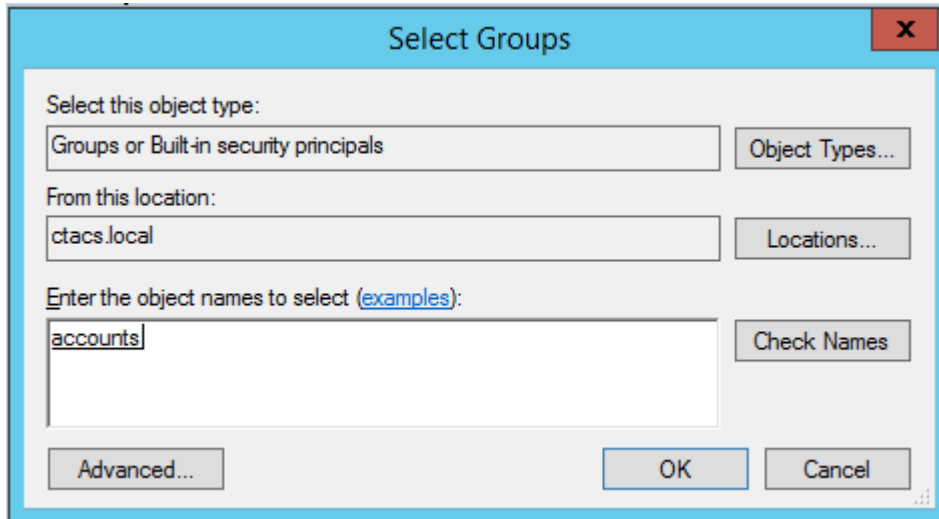
Figure 45: Selecting a Group object

Alternatively, in **Active Directory Users and Computers**, double-click the group name. In the display that appears click the **Members** tab. Click the **Add** button. The 'Select Groups' box is displayed. Type in the name of the object (i.e. the name of the user) and click the **Check Names** button. It will be validated and if correct will then appear underlined. Click **OK**.
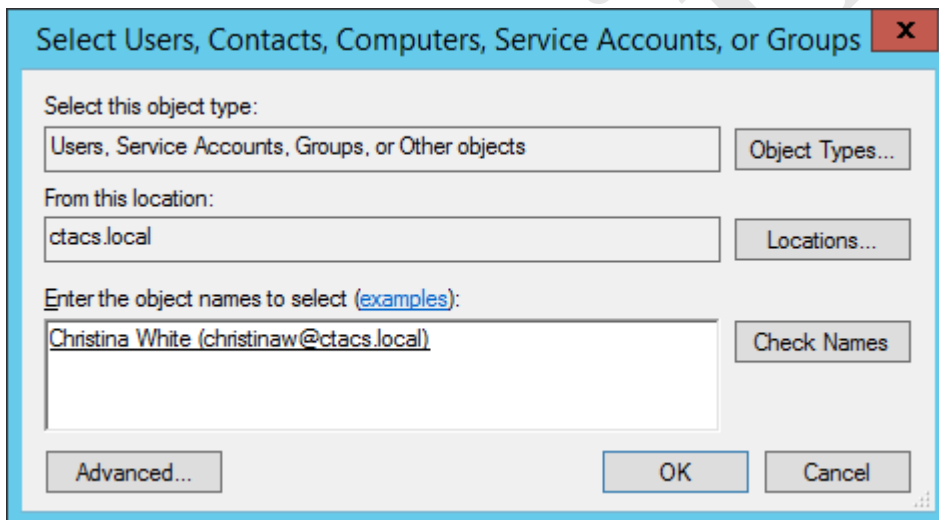
Figure 46: Selecting a user

4.7 Home Folders, Logon Scripts and Profiles

Chapter 3 described a structure of shared folders for the system, including home or personal folders for each user. These home folders have to be created. Also, most users are accustomed to working with drive letters e.g. C: drive, D: drive and so on and hence it is useful to be able to relate the shared folders to drive letters – a process known as *drive mapping*. Furthermore, Windows Server supports a feature called *user profiles*. A profile is a collection of settings that personalize a computer for a user, including the desktop background (wallpaper), screen saver, sounds, toolbars and so on. Using a technique called *roaming profiles*, a user's profile is automatically picked up no matter which computer they login to, giving them a consistent, personalized environment. One thing to note is that profiles behave differently between different versions of Windows; to help cope with this, Windows Server supports both the original profiles of Windows XP clients, as well as the *V2* ("version 2") profiles of Windows Vista, Windows 7 and Windows 8. A further complexity is that there are significant differences between V2 profiles in Windows 7 and those in Windows 8, resulting in compatibility and functionality issues. Needless to say, Windows 10 introduced yet another variation, in the form of V5 ("version 5") profiles. Best practice? If at all possible, have all of the client computers running the same version of Windows.

We will begin by creating a *login script*. Login scripts are executed when a user logs on and are commonly used to map drives. This functionality can be achieved via several means but the simplest method is via a batch file. Using Notepad or other simple text editor, create two batch files named *user.cmd* and *admin.cmd* as shown below. These should be placed *in C:\Windows\sysvol\sysvol\domainname.local\scripts* where *domainname.local* is the name of the domain. This folder is automatically mapped by the server as a share called *NETLOGON*.

User.cmd script:

```
@echo off
: User logon script
: Updated 11/11/11 by NR
net use s: \\server\shared /persistent:no
```

Admin.cmd script:

```
@echo off
: Admin logon script
: Updated 11/11/11 by NR
net use s: \\server\shared /persistent:no
net use t: \\server\technical$ /persistent:no
```

Go into **Active Directory Users and Computers**, double-click on a user and then click on the **Profile** tab. In the User Profile section, specify the **Profile path** and **Login script**. The Profile path takes the form *\\server\profiles$\username*, where *username* is the login name of the user e.g. *\\server\profiles$\aarong*. For general purpose users the login script is *user.cmd* whilst for the Administrator it is *admin.cmd*. in the Home Folder section, choose *H:* from the **Connect** drop-down and specify a value of *\\server\users\username* for it e.g. *\\server\users\aarong*. Click **OK**.
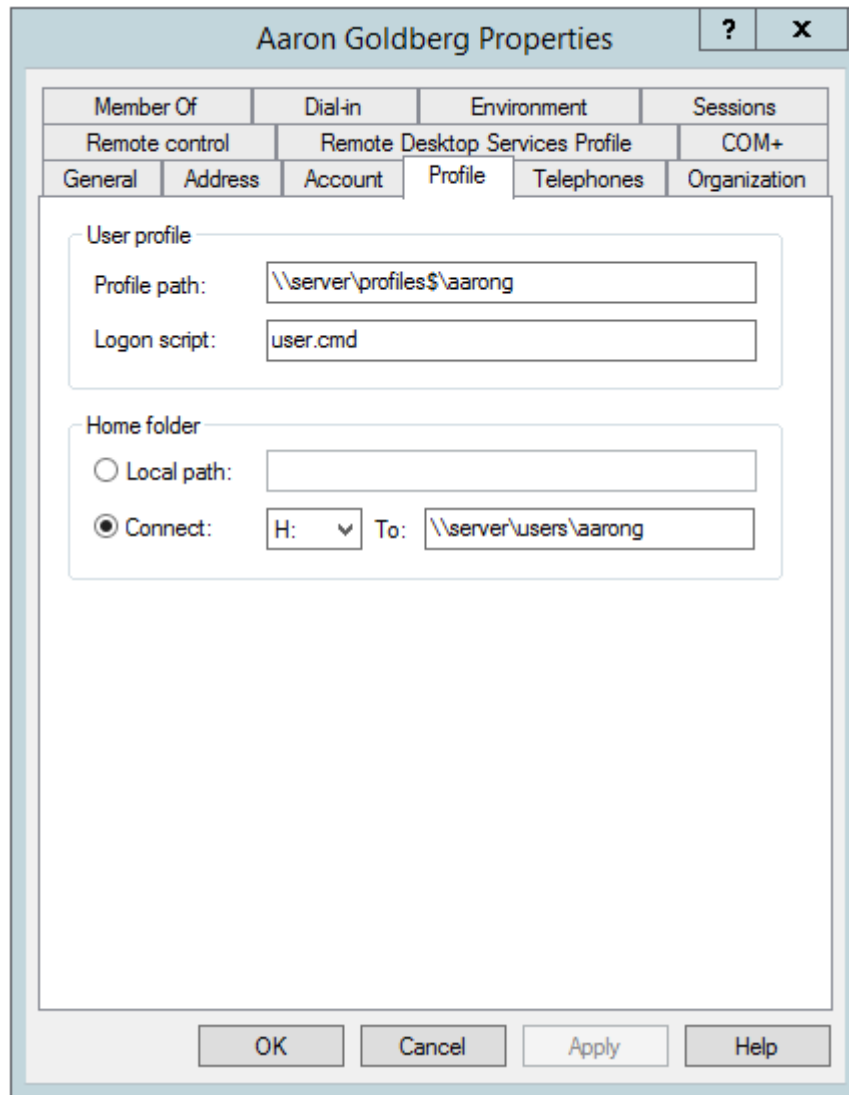
Figure 47: Specify user profile details

The effect of this is that when a user logs on they will have access to two network drives. The shared folder that everyone can see will appear as *S:*, whilst their personal or home folder will appear as *H:*. Note that the profile and user home folder are created automatically the first time that the user logs on.

For the Administrator user(s), specify a logon script of *admin.cmd* rather than *user.cmd*.

4.8 Editing Multiple Users Simultaneously

A useful time saver when assigning profiles to users is the ability to work with multiple users simultaneously. Go into **Active Directory Users and Computers**, locate the users and, holding down the Control key, click them one at a time to highlight them. Then, right-click one and choose **Properties** from the pop-up menu. A screen with five tabs is displayed: *General*; *Account*; *Address*; *Profile* and *Organization*. Click **Profile** – this is the same dialog box as shown above but anything entered here will apply to all the selected users. It is thus a very fast way of assigning, say, the same logon script to many users at once.

5. CONNECTING COMPUTERS TO THE SERVER

To connect to the domain, the client computer must be running a Professional or better version of Windows such as: Windows 10 Professional; Windows 8.1 Professional; Windows 7 Professional; Windows Vista Professional; Windows XP Professional. The following operating systems are not supported: versions prior to Windows XP; Home or Starter editions of Windows; Macintosh OS X; Linux; iOS; Android. Also note that Windows XP is no longer supported by Microsoft and mainstream support for Windows Vista ended several years ago, meaning that these are not good choices, although they are still covered in this chapter for reasons of completeness. Best practice is that all computers should be running the same version of Windows and, when planning a network installation or upgrade, you should aim to achieve this. Regardless of the actual operating system, make sure that all available Windows updates have been applied before connecting a computer to the domain.

Each computer must have a unique name within the network to identify it. It is best to follow a scheme of some sort; this could be as simple as PC01, PC02, PC03 etc., or a scheme that relates to its location or function. To change the name of a Windows computer, go to **Control Panel** > **System** and click **Change settings** in the *Computer name, domain and workgroup* settings section.

Having created the users and connected the computers to the domain, as many individual user logins as possible should be checked to make sure that they are working correctly. Check that users have correct access to their folders, can get on the Internet and are able to print. Any anomalies should be investigated and resolved.

5.1 DNS Settings with All-in-One Routers

In a very small business, internet connectivity is frequently through an all-in-one router that also provides DHCP and DNS services, rather than have Windows Server itself provide DHCP and DNS. This can cause problems with DNS, such that computers on the network cannot "see" each other. As a consequence, attempting to connect a computer to the server may result in failure, with a message to the effect that "a domain controller cannot be found":
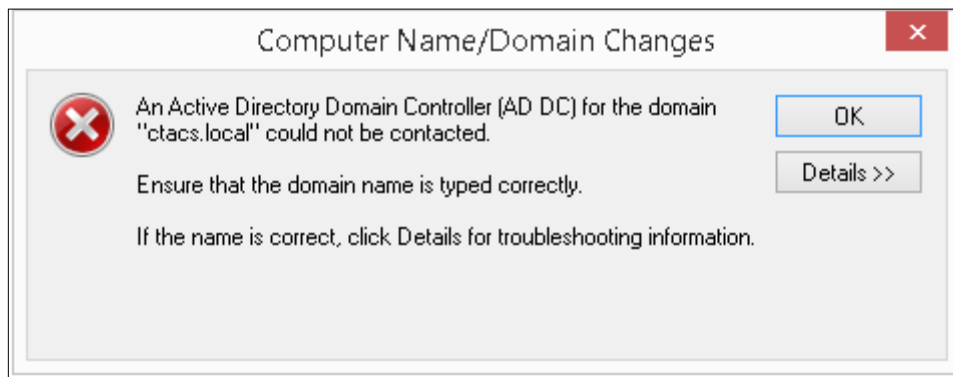
Figure 48: DNS-related error

The easiest fix for this is to explicitly force the client computers to point to the server for DNS. To do so, go into the network adapter settings for each PC (**Control Panel** > **Network and Sharing Center** > **Change Adapter Settings** in most versions of Windows). Click the **Use the following DNS server addresses** option and for the **Preferred DNS server** specify the IP address of the file server. This will cause DNS lookups to initially go through the server rather than the router.

Figure 49: Manually specify the DNS server

If this still does not work, also try disabling IPv6 protocol on the client computer (assuming your organization does not need to use IPv6 for some reason).

5.2 Connecting Windows XP Clients to the domain

- Click the **Start** button, right-click My **Computer** and click **Properties**
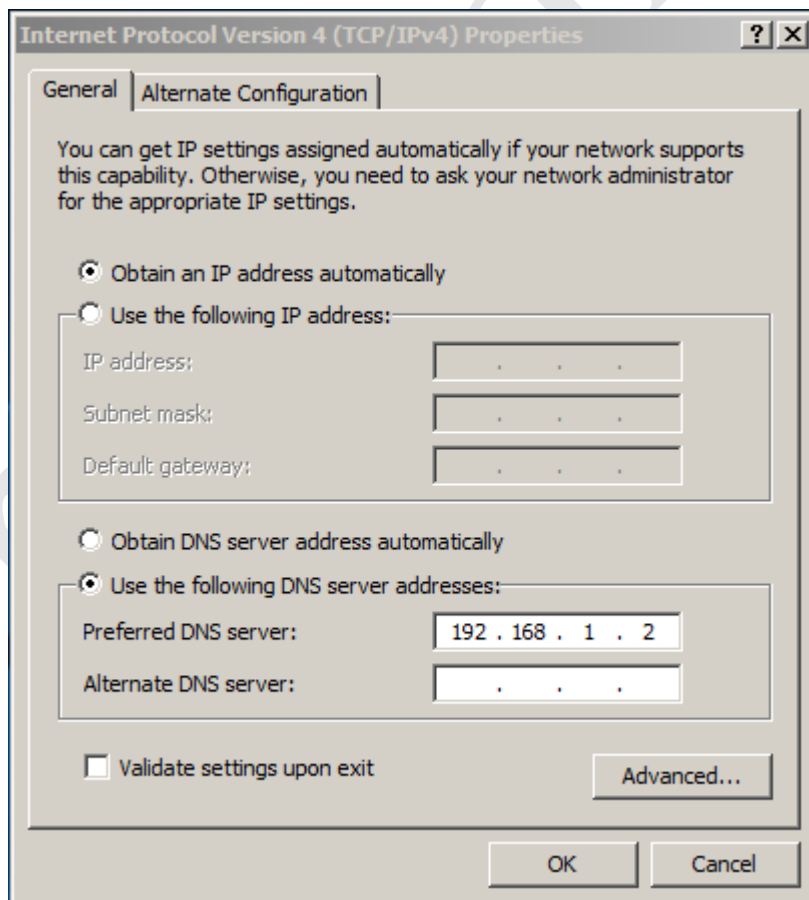- Click the **Computer Name** tab
- Click the **Change** button
- Under the 'Member of' section click **Domain**. Enter the name of the domain followed by a suffix of *.local,* for example, *ctacs.local*.
- You will be prompted to enter the Administrator name and password for the domain
- After a short delay you will receive a 'Welcome to the domain' message
- Follow the instructions to restart the computer
- Check that you can logon as Administrator

5.3 Connecting Windows Vista Clients to the domain

- Click the **Start** button, right-click **Computer** then click **Properties**
- Under 'Computer name, domain, and workgroup settings', click **Change settings**. Respond to any security messages generated by UAC.
- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab
- Click the **Change** button
- Respond to any prompt for an Administrator password or confirmation
- Under 'Member of' click on **Domain**. Enter the name of the domain followed by a suffix of *.local,* for example, *ctacs.local*.
- You will be prompted to enter the Administrator name and password for the domain
- After a short delay you will receive a 'Welcome to the domain' message
- Follow the instructions to restart the computer
- Check that you can logon as Administrator

5.4 Connecting Windows 7 Clients to the domain

- Click the **Start** button, right-click **Computer** then click **Properties**
- Under 'Computer name, domain, and workgroup settings', click **Change settings**
- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab
- Click the **Change** button
- Respond to any prompt for an Administrator password or confirmation
- Under 'Member of' click on **Domain**. Enter the name of the domain followed by a suffix of *.local,* for example, *ctacs.local*.
- You will be prompted to enter the Administrator name and password for the domain
- After a short delay you will receive a 'Welcome to the domain' message
- Follow the instructions to restart the computer
- Check that you can logon as Administrator

5.5 Connecting Windows 8.1 Clients to the domain

A couple of considerations apply when using Windows 8. Firstly, when installing or configuring Windows 8, specify that it is to use a local ID rather than a Microsoft ID. Secondly, make sure that it is running Windows 8.1 (a free upgrade from Windows 8 to Windows 8.1 is available through the Windows Store for computers running Windows 8).

Right-click the **Start** button and choose **System**.

- Under 'Computer name, domain, and workgroup settings', click **Change settings**
- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab
- Click the **Change** button
- Respond to any prompt for an Administrator password or confirmation
- Under 'Member of' click on **Domain**. Enter the name of the domain followed by a suffix of *.local,* for example, *ctacs.local*.
- You will be prompted to enter the Administrator name and password for the domain
- After a short delay you will receive a 'Welcome to the domain' message
- Follow the instructions to restart the computer

- Check that you can logon as Administrator

5.6 Connecting Windows 10 Clients to the domain (Classic Method)

There are two methods for connecting a Windows 10 computer to the domain: a 'classic' way which is the same as with earlier versions of Windows, plus a 'modern' way that was introduced with Windows 10. With both methods the computer should have initially been setup to use a local account rather than a Microsoft account.

Right-click the **Start** button and choose **System**.

- Under 'Computer name, domain, and workgroup settings', click **Change settings**
- 'System Properties' are displayed. Make sure you are on the 'Computer Name' tab
- Click the **Change** button
- Respond to any prompt for an Administrator password or confirmation
- Under 'Member of' click on **Domain**. Enter the name of the domain followed by a suffix of *.local,* for example, *ctacs.local*.
- You will be prompted to enter the Administrator name and password for the domain
- After a short delay you will receive a 'Welcome to the domain' message
- Follow the instructions to restart the computer
- Check that you can logon as Administrator

5.7 Connecting Windows 10 Clients to the domain (Modern Method)

The key difference with the 'modern' method is that you do not have to be an Administrator in order to join the computer to the domain. Rather, as long as the user has been defined on the server (as described in 4.1 Creating Users) then they can add themselves using their own user name and password. If you are accustomed to the traditional method of connecting a computer to a domain this may seem a little strange at first, but this self-help approach actually makes a lot of sense and can reduce support overheads.

- Click **Start** > **Settings** > **Accounts** > **Work Access** > **Join or leave a domain**
- Click the **Join a domain** button
- In the panel that appears enter the name of the domain followed by a suffix of *.local,* for example, *ctacs.local*.
- On the subsequent screen the user should enter the user name and password that were defined on the server
- A third panel appears, wanting to know the default *User account* for the computer. This will default to the user name that was just used, which is usually fine. The *Account type* can be specified – the usual choice here is **Standard User**. Click **Next**. Note that you can actually choose to Skip this screen altogether
- Click the **Restart** now button when prompted
- Check that the user or the Administrator can logon

5.8 Connecting Computers running Home Editions of Windows

In theory, only computers running Windows Professional or better can be connected to Server 2012 R2. However, it is possible to connect computers running Home Editions of Windows from Windows XP upwards, albeit in a simplified fashion. It is possible to access shared data folders, although not to take advantage of the specific features that Windows Server offers in terms of control and management. This is because such computers can be workgroup members only and cannot join the domain.

To connect a computer running a Home Edition of Windows, click **Start** (or right-click **Start** in Windows 8.1) and choose **Run**. Alternatively, hold down the **Windows key** and the **R key** simultaneously. In the dialog box that appears, type *server* or \\ followed by the IP address of the server (e.g. *192.168.1.2*). The user will be prompted to enter their user name and password; if they are the only person that uses that particular computer tick the **Remember my password** or **Remember my credentials** box:
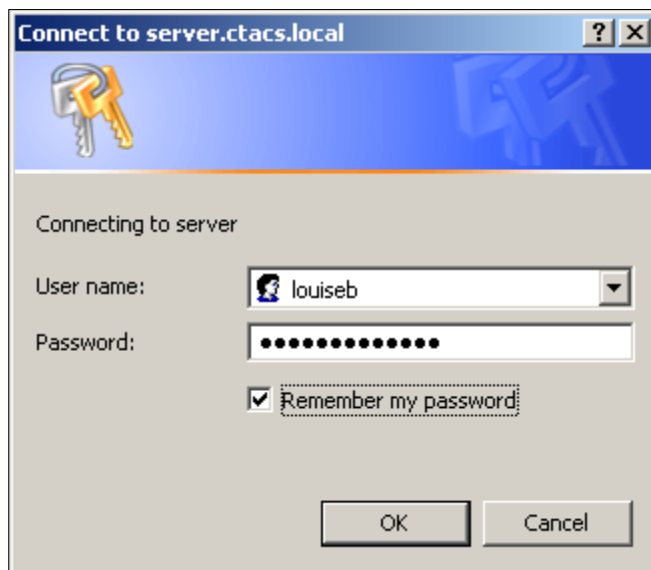

Figure 50: Enter user name and password

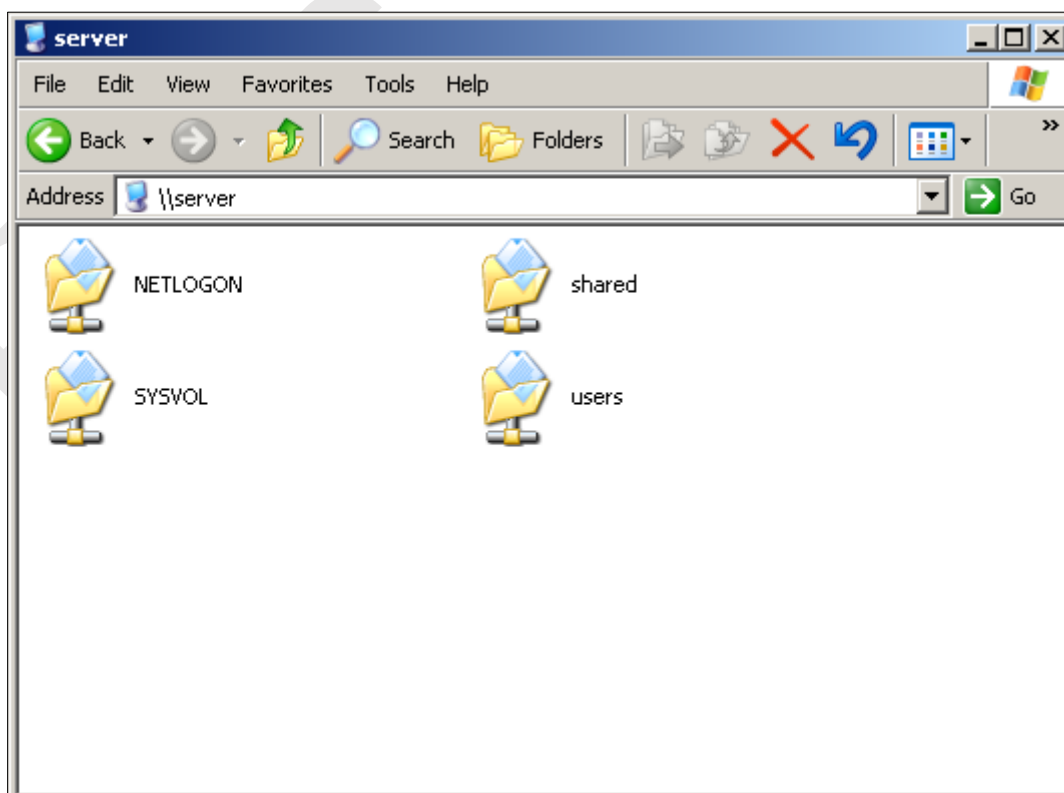A list of shared folders on the server will be displayed:

The user can work with any of the folders to which they have been granted access. To access their home folder, double-click the *Users* folder then double-click the folder that has the same name as their user name. Note that although they can see the names of other people's home folders, they will not be able to access them because of security permissions.

5.9 Connecting Macs

There are several different methods for connecting Macs to Windows Servers, some easier than others. The options available may vary depending on the version of Mac OS X being used, but the main consideration is what type of access is required i.e. occasional or frequent.

Workgroup Access

This is the simplest method for connecting a Mac and may be suitable for smaller organizations requiring occasional access to the server. The Mac does not connect to the domain; rather it connects as a workgroup member, in much the same way as computers running unsupported versions of Windows can as described in section 5.8 Connecting Computers running Home Editions of Windows. It should work with all versions of OS X.

In Finder click **Go** followed by **Connect to Server**. Alternatively, press **Command K**. Enter the IP address of the server prefixed with *smb://* and click **Connect**:
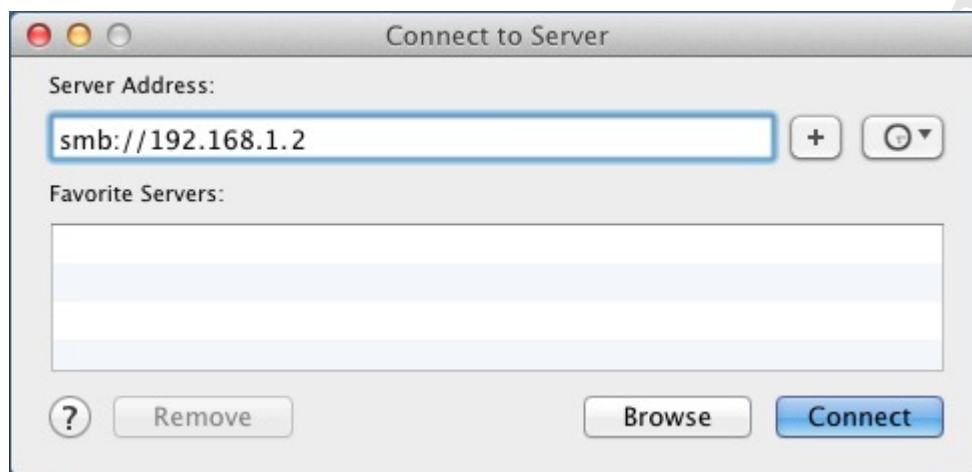

Figure 52: Connect to Server

Click **Registered User** and enter the *Name* and *Password* of the user as defined on the Windows server (not a local Mac user). Click **Connect**:

Figure 53: Enter name and password

A list of shared folders – *volumes* in Mac parlance – are listed. Choose the required folder. To mount multiple volumes simultaneously, hold down the **Command key** and click on the required folders in turn:
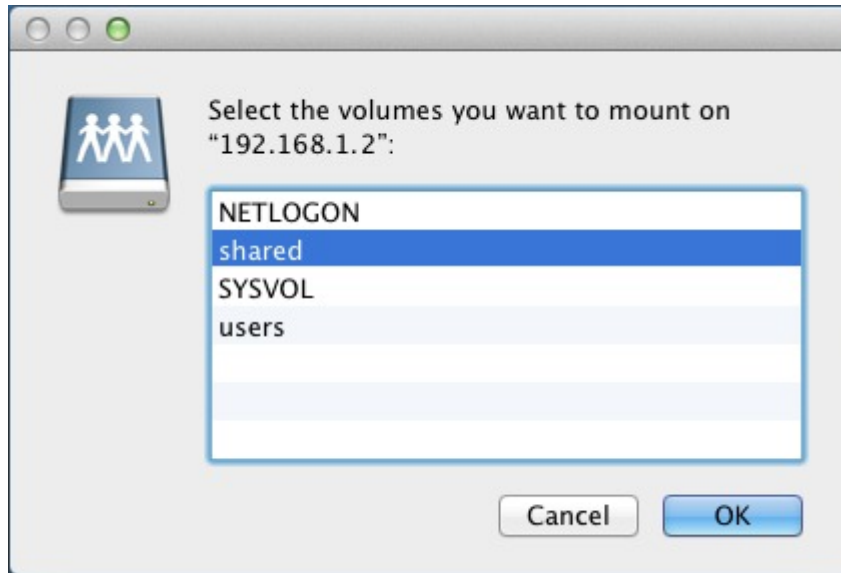
Figure 54: Choose the folders/volume(s) to mount

Icons for the folder(s) will appear on the desktop and can be clicked to open them and work with the contents:
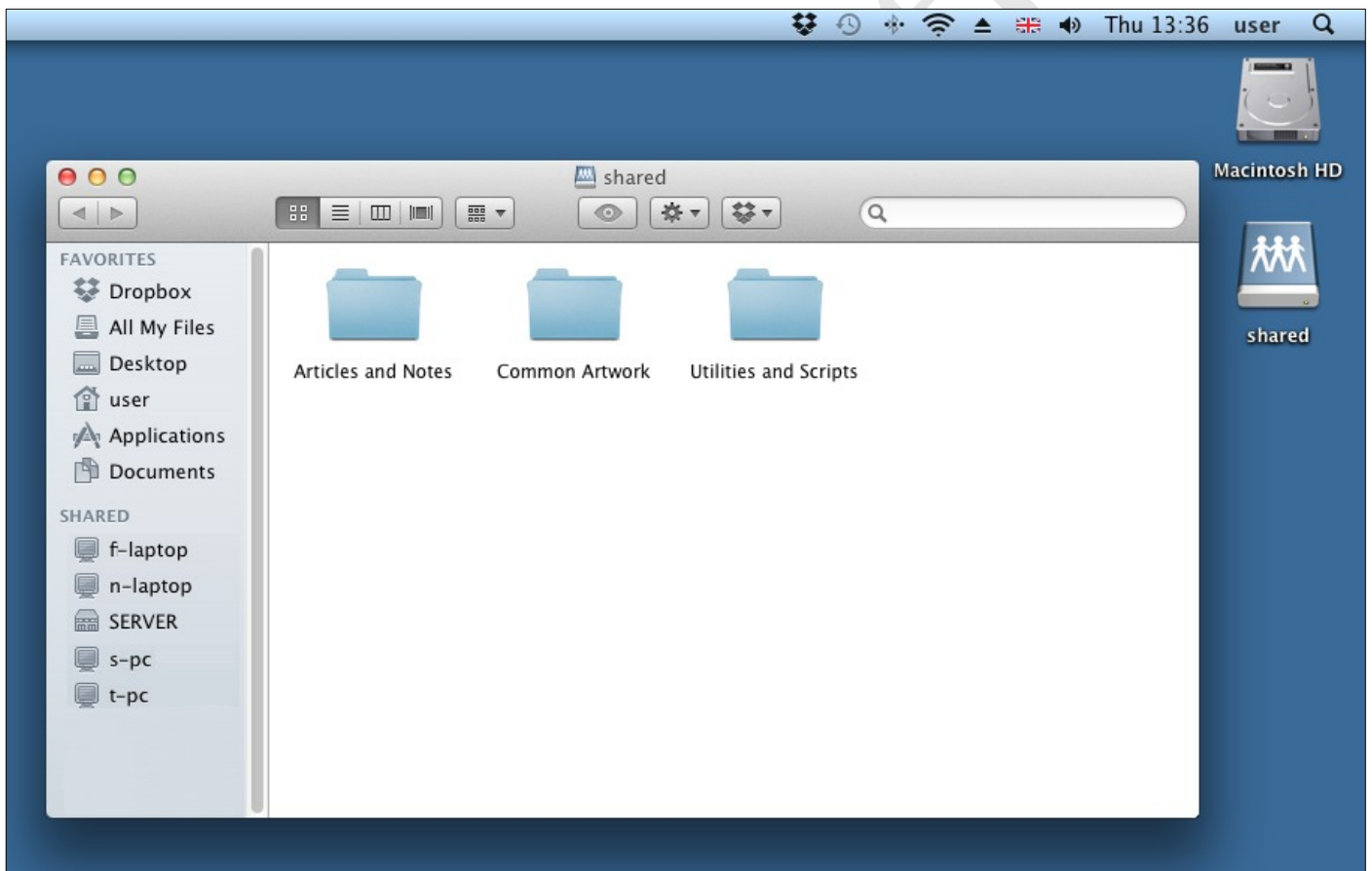

Figure 55: Contents of a mounted folder

Boot Camp

Apple's *Boot Camp* utility allows a copy of Windows to be installed on a Mac in addition to OS X, enabling it to start up using OS X or Windows as required. There are two limitations: firstly, only one operating system at a time can be used. For instance, if the computer is running Windows and you want to use OS X (or vice versa) then it is necessary to restart it. Secondly, only the most recent versions of Windows are supported on modern Macs, although older machines with earlier versions of OS X and Boot Camp may be able to use older versions of Windows. A licenced copy of Windows has to be obtained and used for the installation and it needs to be a Professional edition or better.

This approach may be suitable for individuals who need to work in both Windows and Mac environments and are able to accept the restriction of having to regularly reboot the computer.

Virtualization

Virtualization software enables the Mac to operate as normal under OS X but to run a separate copy of Windows in its own self-contained window at the same time, as though it was just another application. This is particularly useful where a user prefers to work predominantly in a Mac environment, but also needs to connect to the Windows server. The copy of Windows can be any version – none of the restrictions imposed by the Boot Camp method apply. One possible downside is that the computer needs sufficient memory (RAM) to run both operating systems simultaneously, say a minimum of 8GB. Virtualization software is available from several sources: a well-regarded commercial program is *Parallels* from the company of the same name, whereas a free alternative is *VirtualBox* from Oracle.

A licenced copy of Windows has to be obtained and used for the installation and it needs to be a Professional edition or better.

6. BACKUPS

Servers have to be backed up on a regular basis so that data can be recovered in the event of loss or other problems. There are several ways of doing so and the best solution will depend upon the number of servers, their roles and locations. In a single server environment, such as might be the case in a small organization, the easiest way is to use the built-in backup program of Windows Server in conjunction with a plug-in external USB hard drive. The USB drive should be at least equal in capacity to the total amount of storage in the server e.g. if the server has 2TB disc storage then the backup drive should be at least 2TB as well. If the server has USB 3.0 ports then be sure to use a USB 3.0 drive, as the performance will be better. Begin by connecting a suitable drive; it is suggested that you format it as NTFS, plus make sure that Windows assigns a drive letter to it. Be aware that anything already on the drive will be lost during the formatting process.

6.1 Installation of Windows Server Backup

Windows Server Backup is a standard component of Windows Server 2012 R2 but first has to be installed. To do so, go to **Server Manager** and click **Manage** followed by **Add Roles and Features**. Choose **Role-based or feature-based installation**, click **Next**, select the server on the follow-on screen and click **Next**. Click **Features** on the left-hand side and **Windows Server Backup** on the right-hand side, followed by **Next**. On the subsequent screen click **Install**. The installation will only take a minute or two; when complete, click **Close**.

Returning to the **Server Manager**, click **Tools** followed by **Windows Server Backup**. On the left-hand panel, click **Local Backup** and the screen should appear as follows:
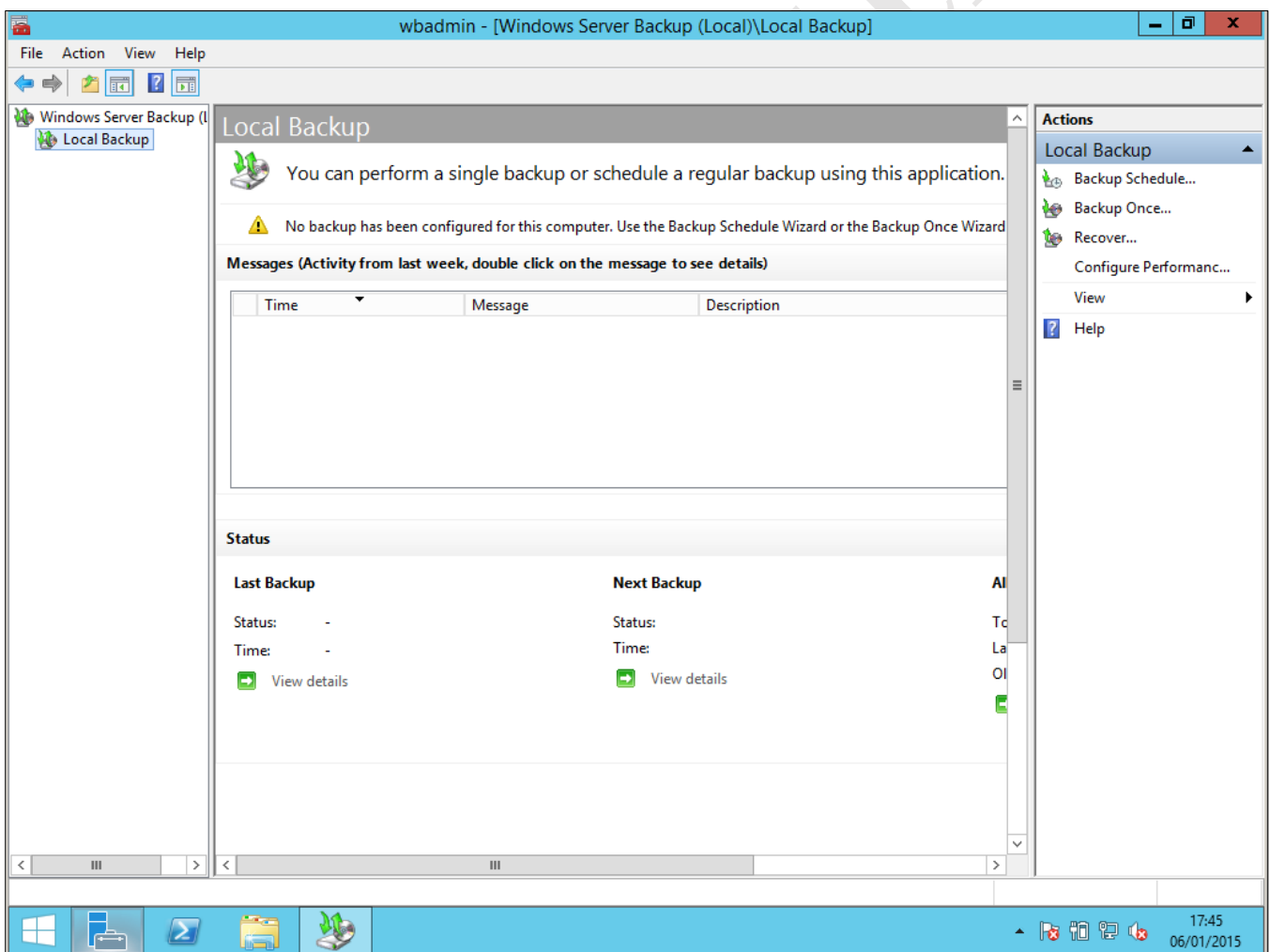

Figure 56: The main Windows Server Backup console

6.2 Setting up a Scheduled Backup

Backups can be run as and when required or, more usefully, scheduled to run on a regular basis. To setup a scheduled backup, click **Backup Schedule** on the right-hand of the screen, listed under **Actions**, which will cause the *Backup Schedule Wizard* to appear:
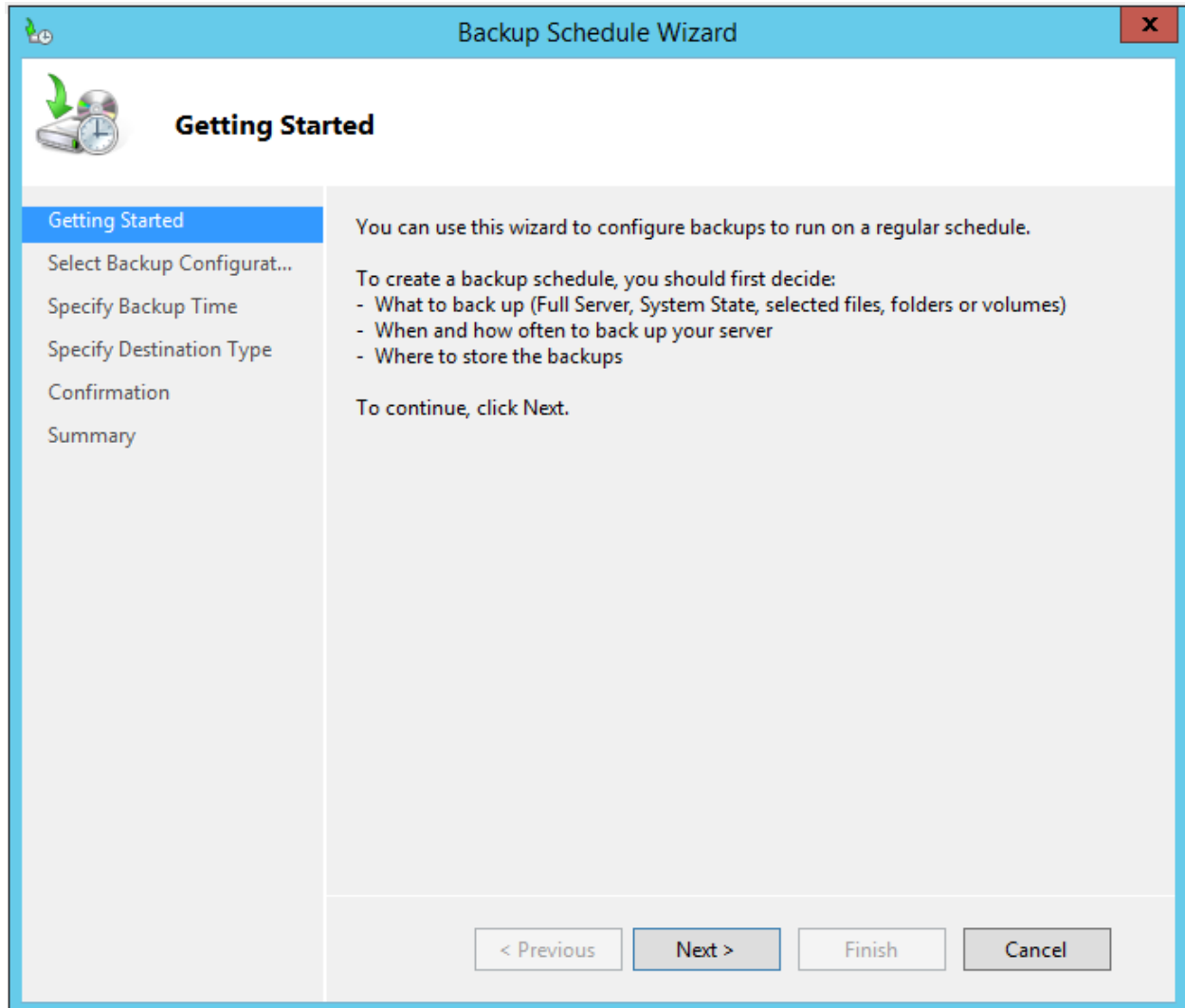

Figure 57: The Backup Schedule Wizard

Click **Next**. On the subsequent screen there is a choice between a 'Full Server backup' or a 'Custom backup'. As the name implies, the former backs up absolutely everything whereas the latter allows greater control over what is backed up. We will choose **Full Server backup**. Click **Next** and a screen to specify the backup time is shown:
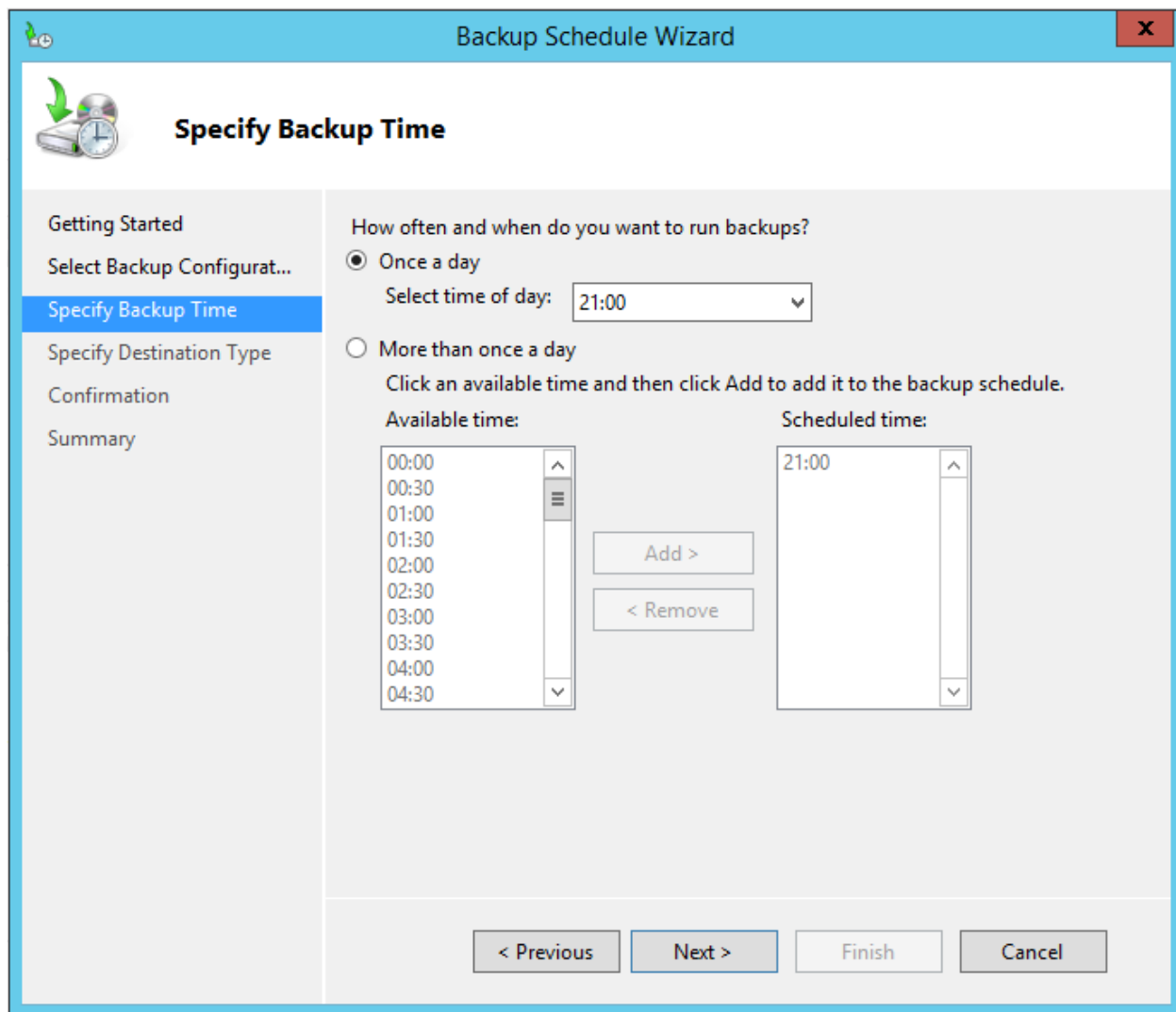
Figure 58: Specifying the Backup time

The default of a daily backup performed at 21:00 (9pm) will be fine in many instances. As a general principle, the backup should be scheduled to run outside of normal working hours or at least during a quiet time, as it can severely impact server performance. Click **Next**.

The destination of the backup is specified on the following screen. Usually the first option – **Back up to a hard disk that is dedicated for backups (recommended)** – is used, although we will also look at another option later on. However, do not click **Next** just yet:
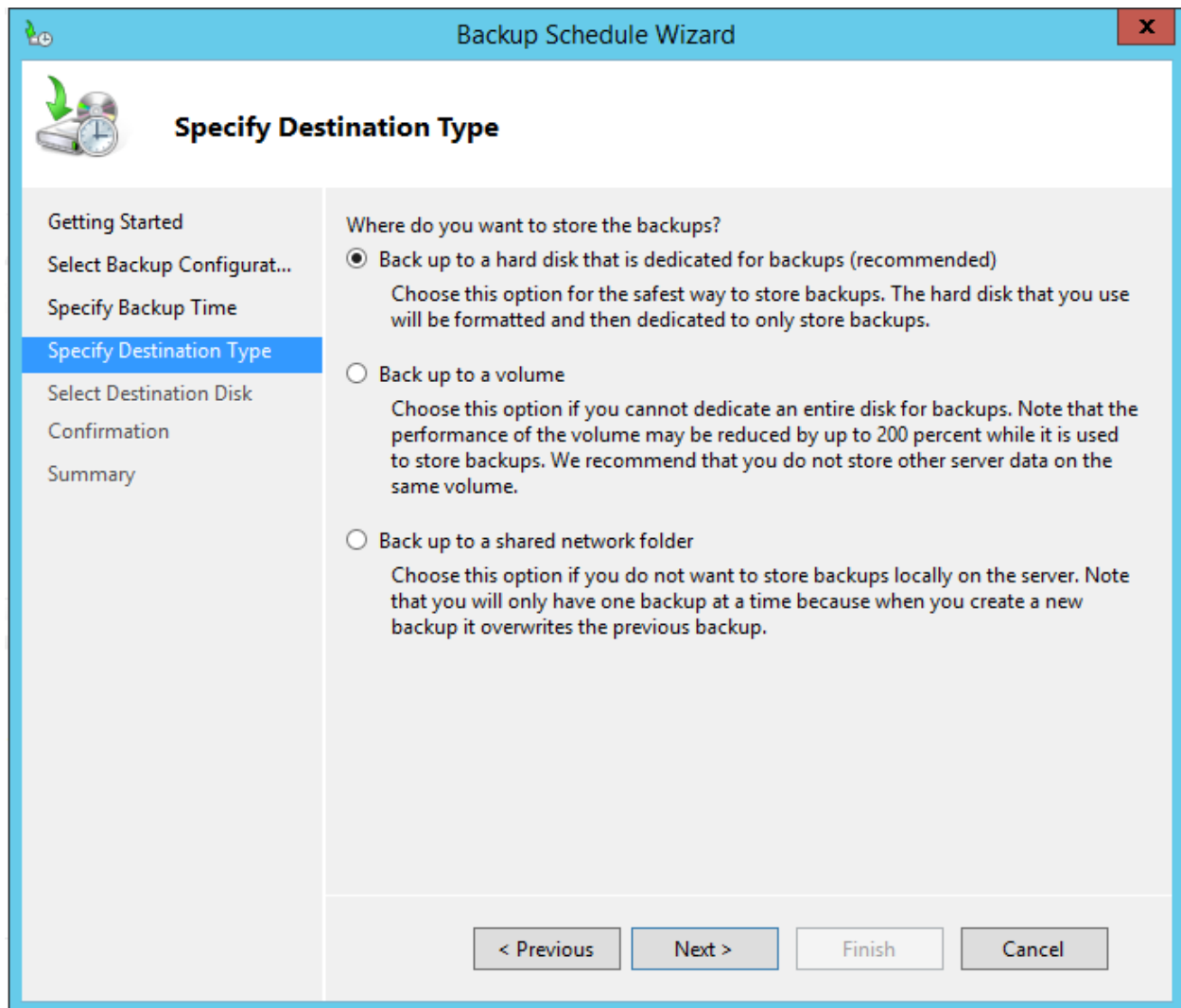
Figure 59: Specify the destination type for the backup

Plug-in the external hard disk, make sure that Windows has recognized it, then click **Next** to show this screen:
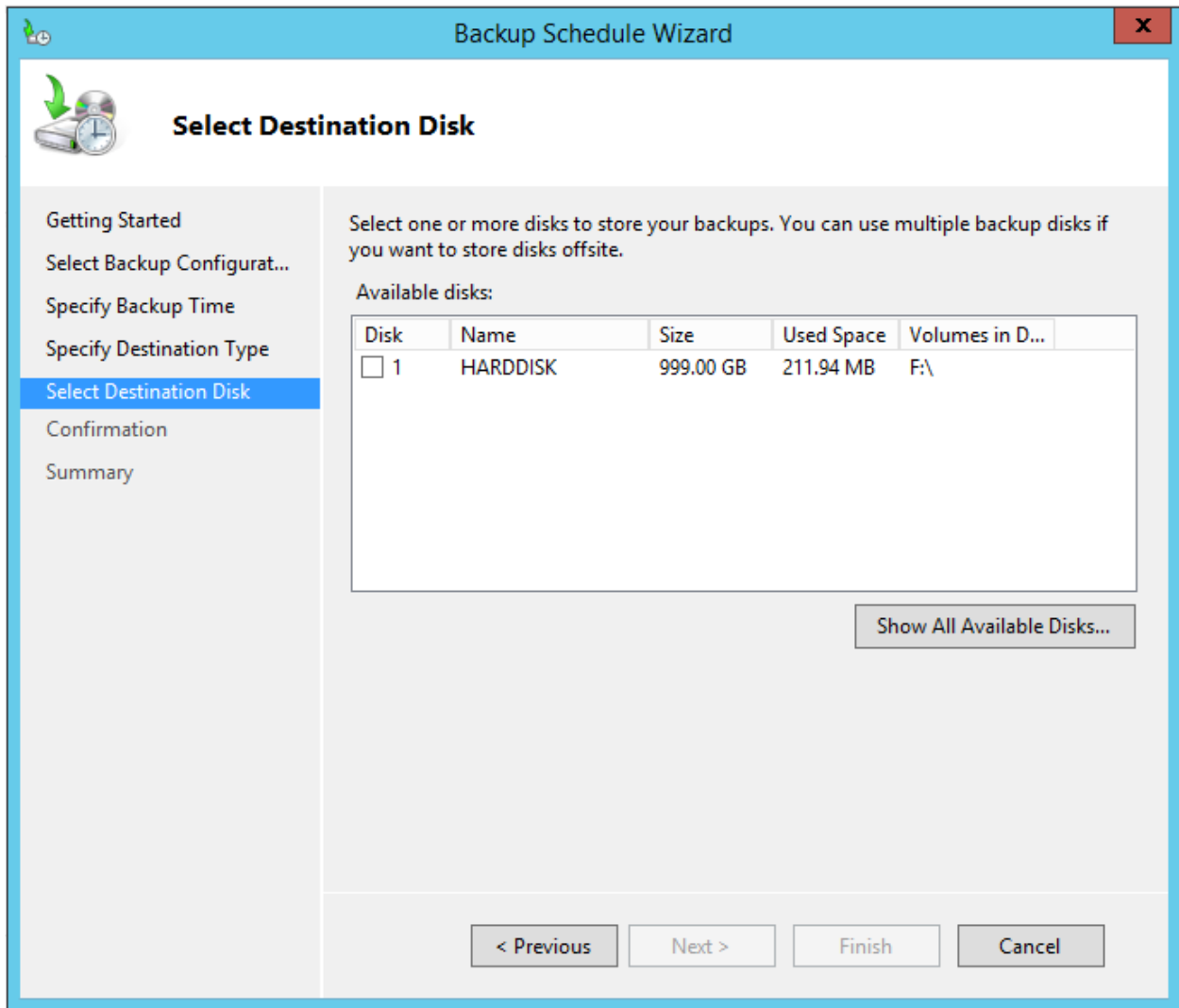
Figure 60: Specify the destination disk for the backup

Tick the external drive to be used. If no drives are listed, wait 10-15 seconds then click the **Show All Available Disks** button. Having selected the drive, click **Next**. The backup program might detect that the external drive will be *included* within the backup rather than used as a separate backup drive, which you do not want as it would be backing up itself! If the following message is received click **OK** to fix this problem:
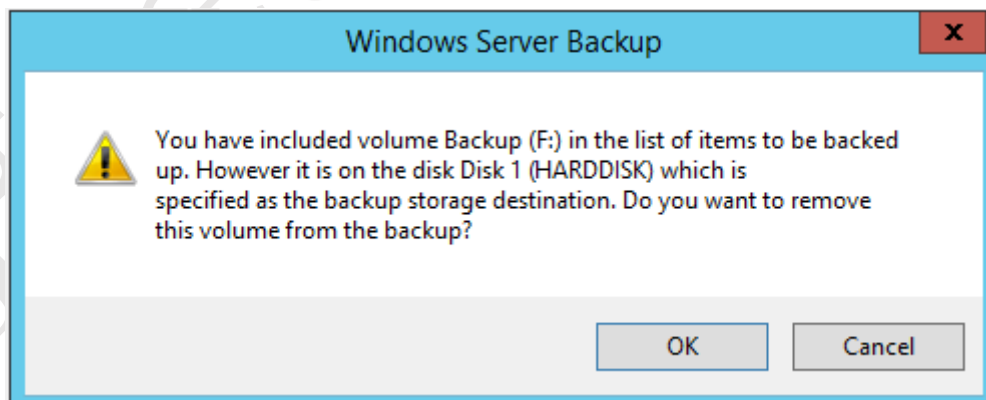

Figure 61: Warning message about backup destination

There will be a warning message about formatting. Note that backup disks use a special file system that is not visible to regular Windows and it is not possible to plug a backup disk into a standard Windows computer and read it like a normal USB drive once it has been formatted for backup purposes. Click **Yes** to the message and **Finish** on the Confirmation screen that follows. The backup drive will be formatted, which may take some time depending on its capacity. When it has done so a Summary screen will be displayed. Click **Close**:
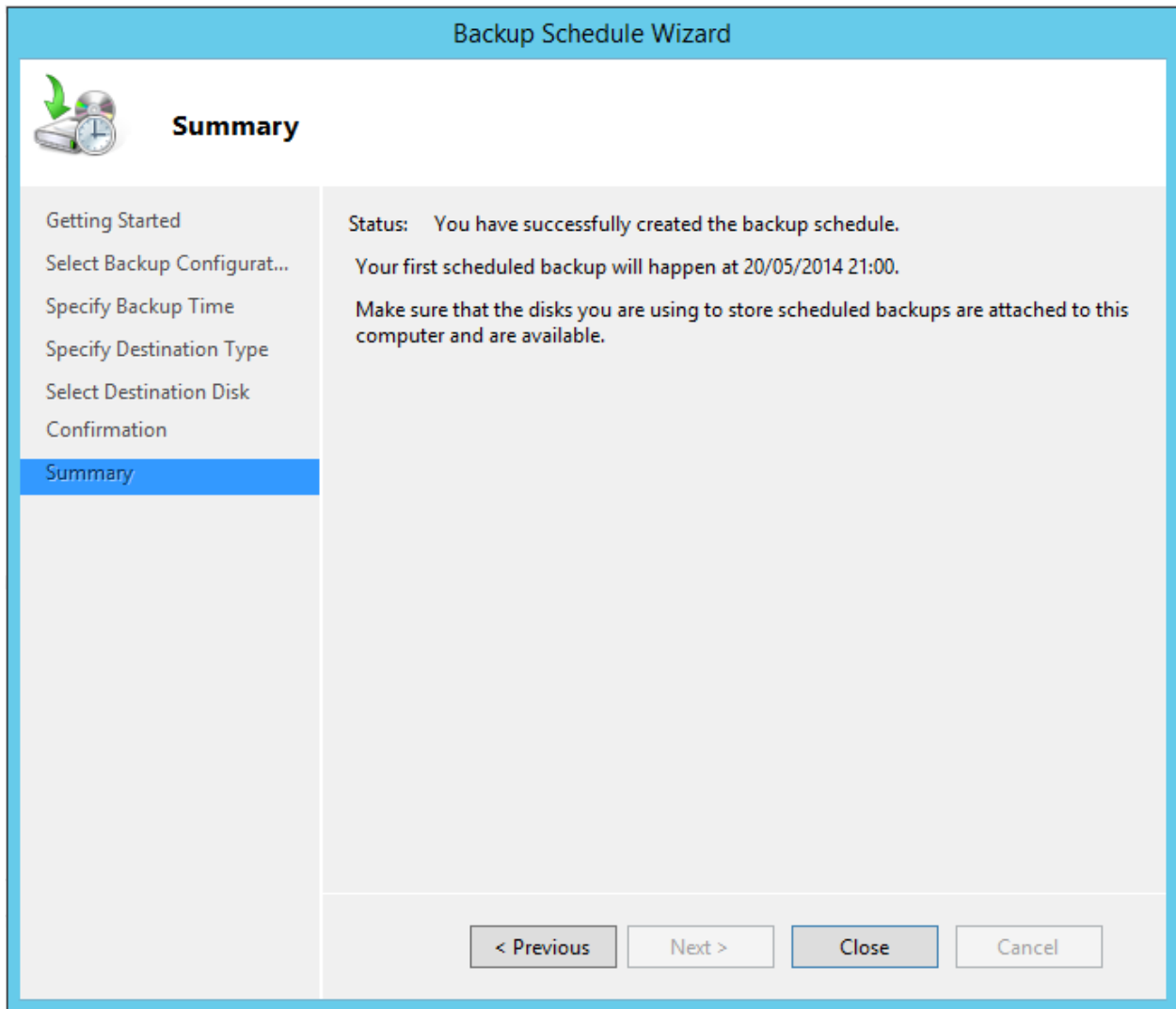
Figure 62: Summary screen from the Backup Schedule Wizard

Using the Windows Server Backup screen, the backup job can be checked each day to make sure that it has completed successfully.

6.3 Recovering Files

In the event of data loss or there being a need to recover (i.e. restore) deleted or older versions of files, the *Recovery Wizard* can be used. Launch Windows Server Backup (**Server Manager** > **Tools** > **Windows Server Backup)**. On the left-hand panel, click **Local Backup** and on the right-hand of the screen, listed under **Actions**, click **Recover,** which will cause the *Recovery Wizard* to appear. Make sure **This server (SERVER)** is selected and click **Next**:
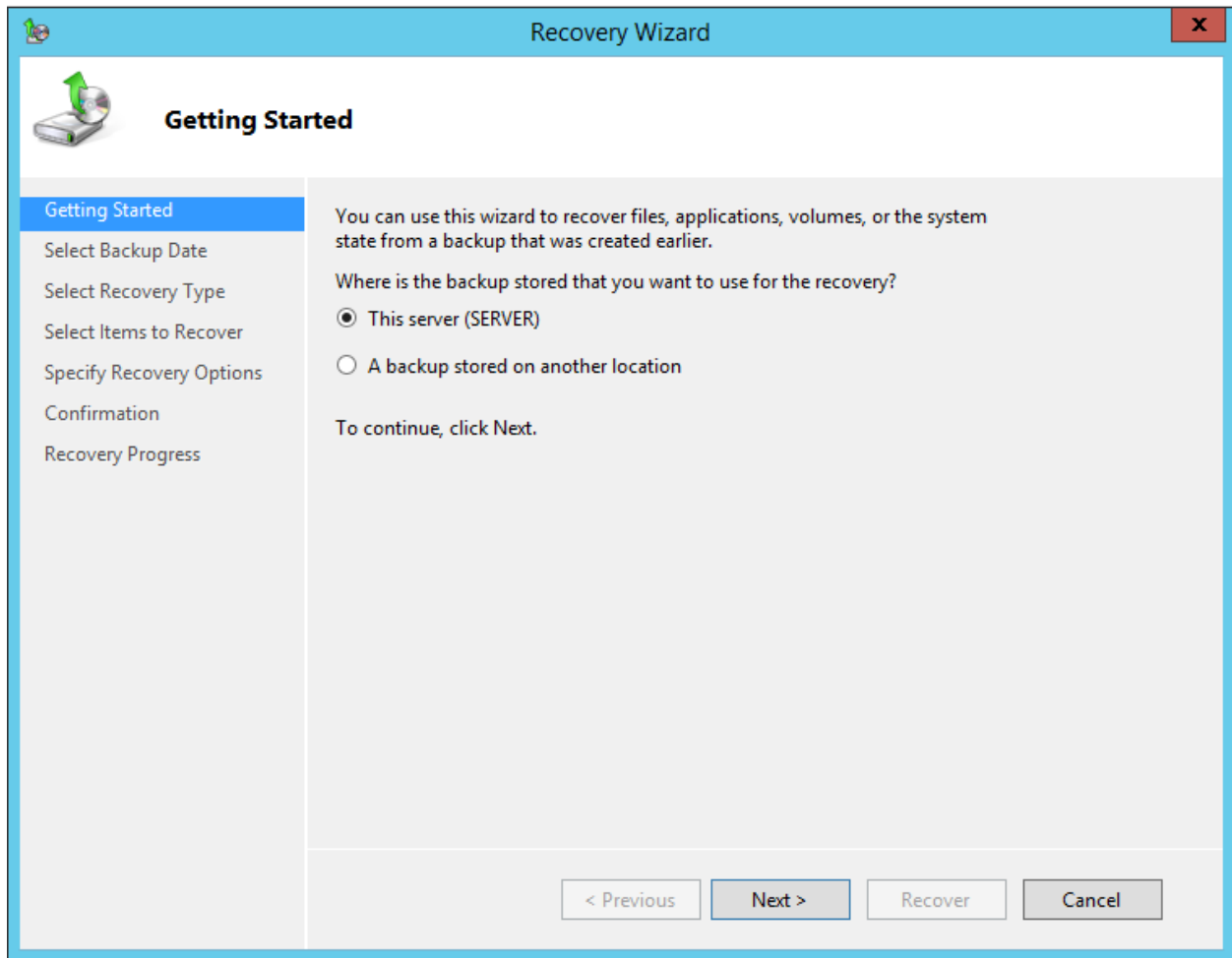

Figure 63: Recovery Wizard Getting Started screen

On the next screen, select a backup to be restored using the calendar and time fields, then click **Next**:
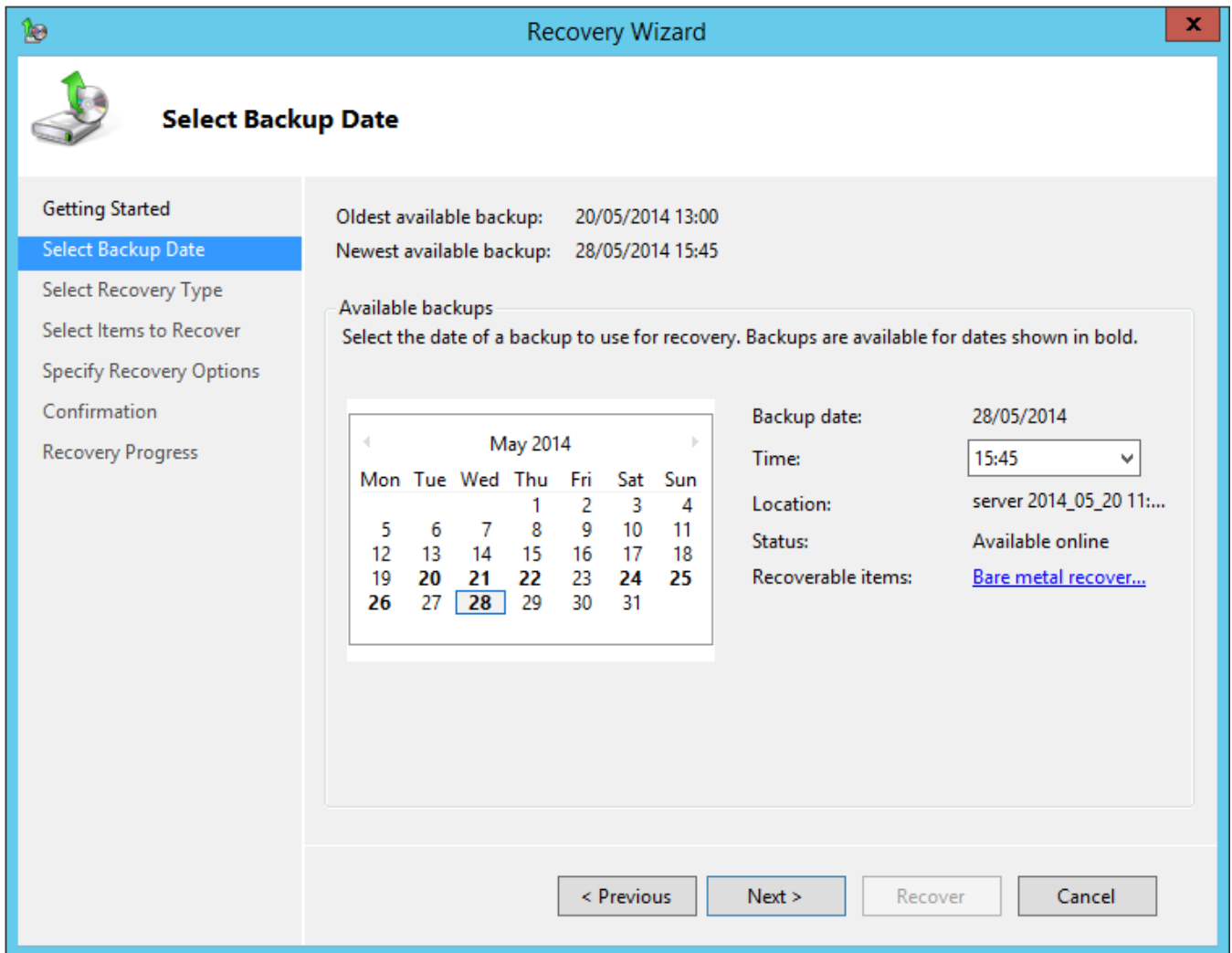
Figure 64: Choose a backup to recover from

The subsequent screen is for specifying what needs to be recovered. Most commonly, you would be recovering files and folders:
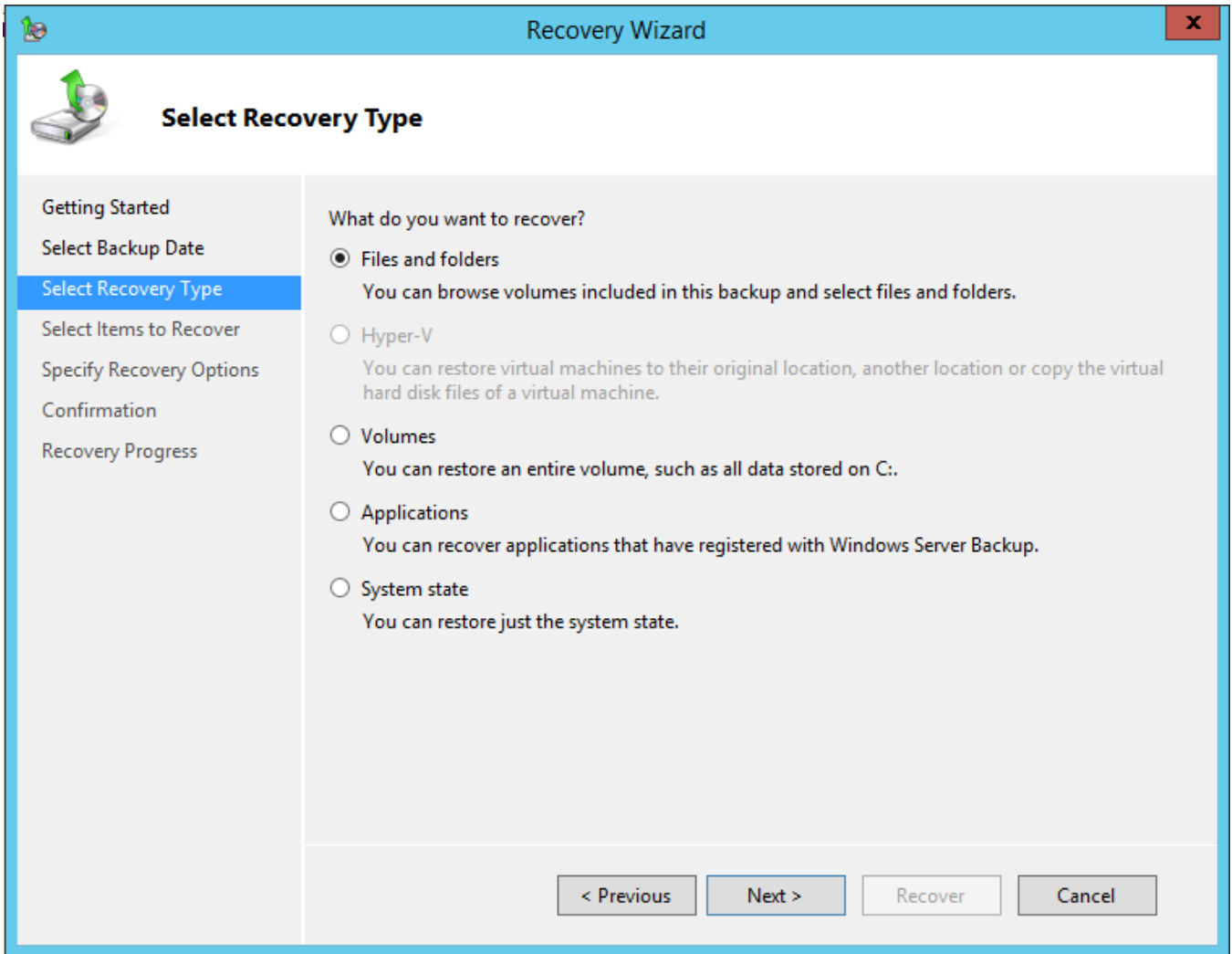
Figure 65: Select the recovery type

This is followed by a screen where the actual folders and files to be recovered are specified:
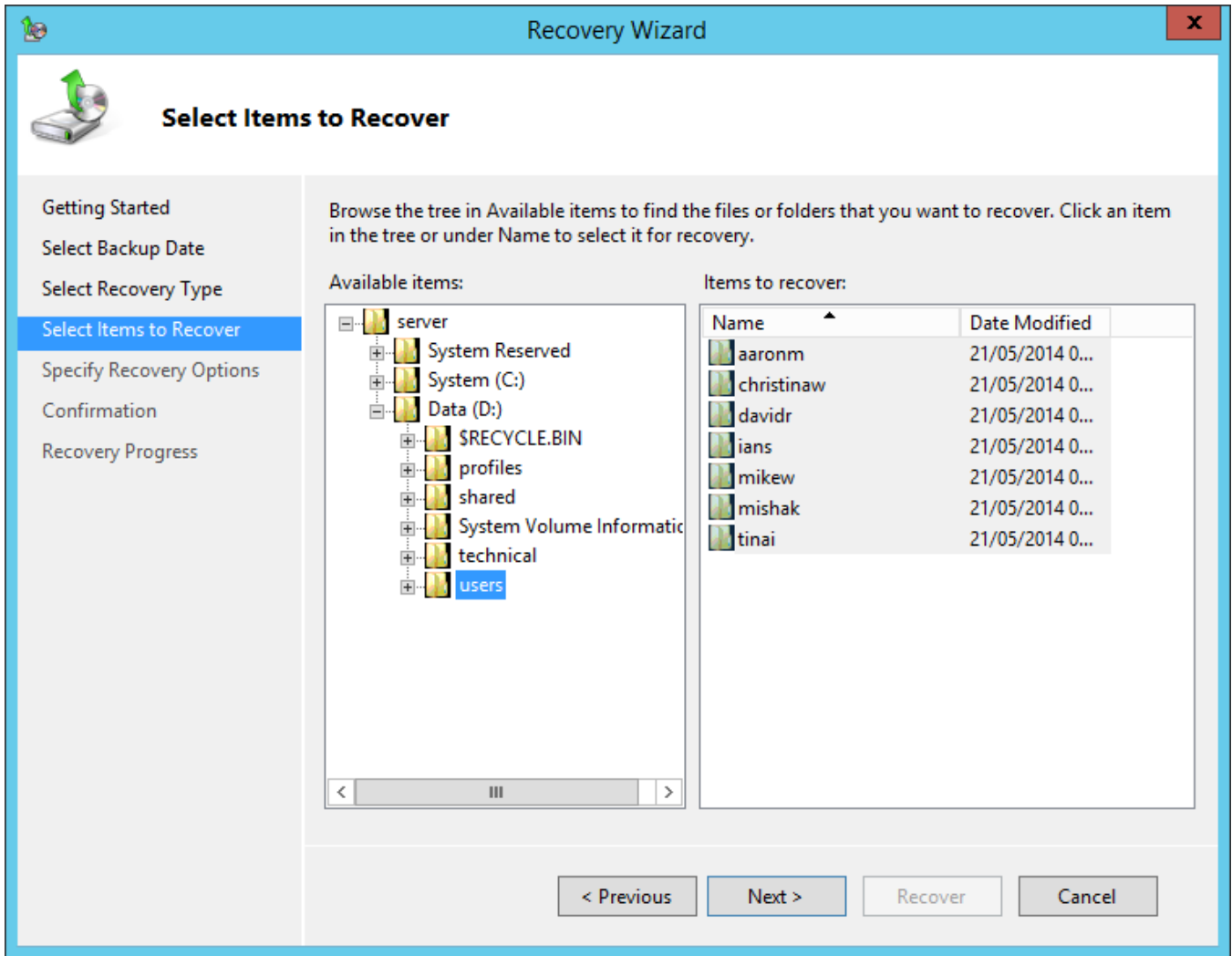
Figure 66: Select the items to recover

The next screen is for specifying options when recovering files. Specifically: (a) should they be recovered to the original location or to another location and (b) what to do when duplicates are found:
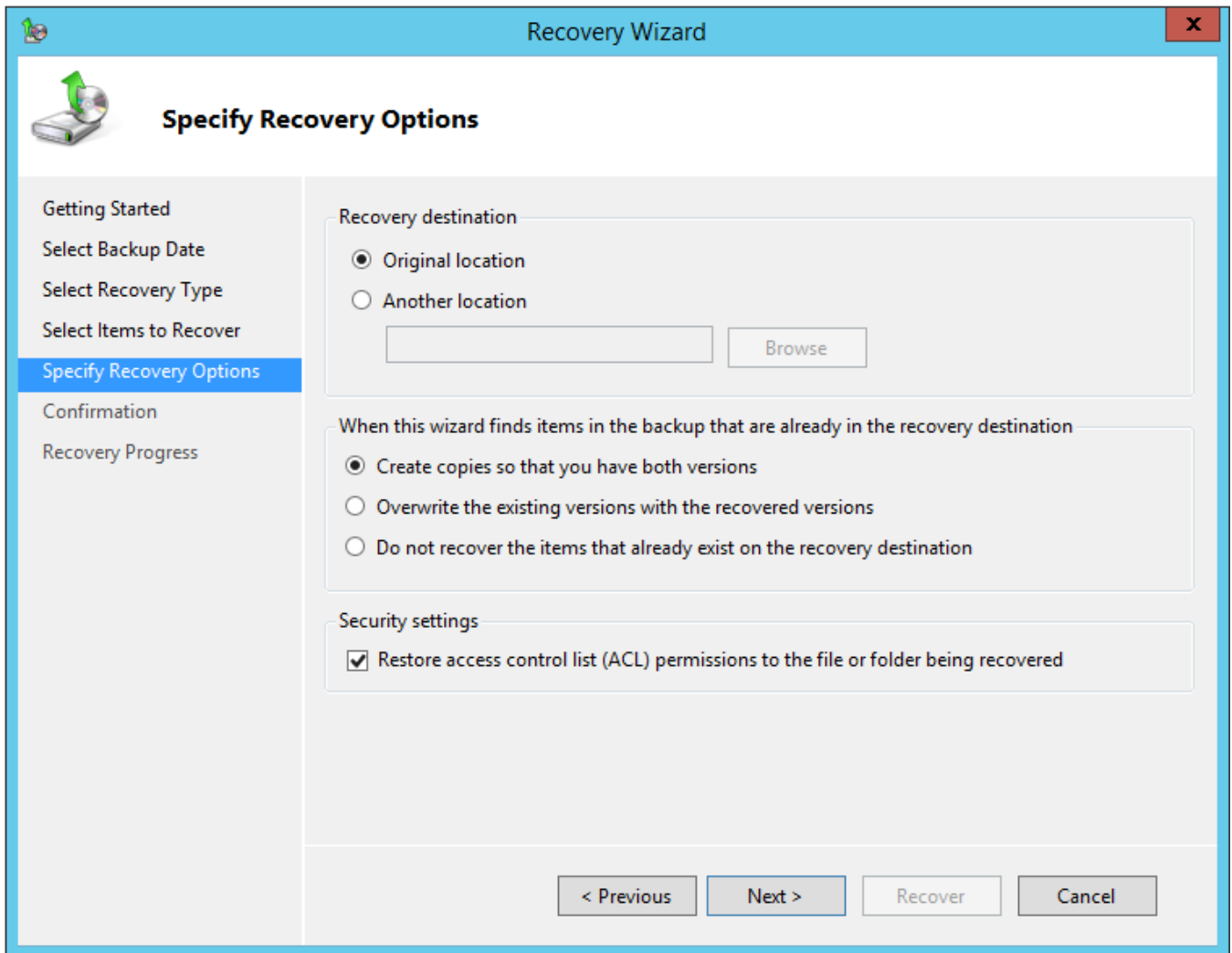
Figure 67: Specify recovery options

After clicking **Next**, a Confirmation screen is displayed. Click the **Recover** button to begin restoring the folders and files, during which time a status screen is shown. When complete, click **Close**.

6.4 Backing up to a Network Drive

One potential downside of using an USB drive for the backups is that it has to be physically located close to the server. In the event of a disaster – for instance, fire, flood or theft – not only might the server be lost but the backup drive might be as well. One way to mitigate against this is to use a network drive for backups, such as a NAS (Network Attached Storage) device. This gives a lot more flexibility as to where it is located, such as in a totally different part of the building. The network drive can be in addition to or in place of the USB drive.
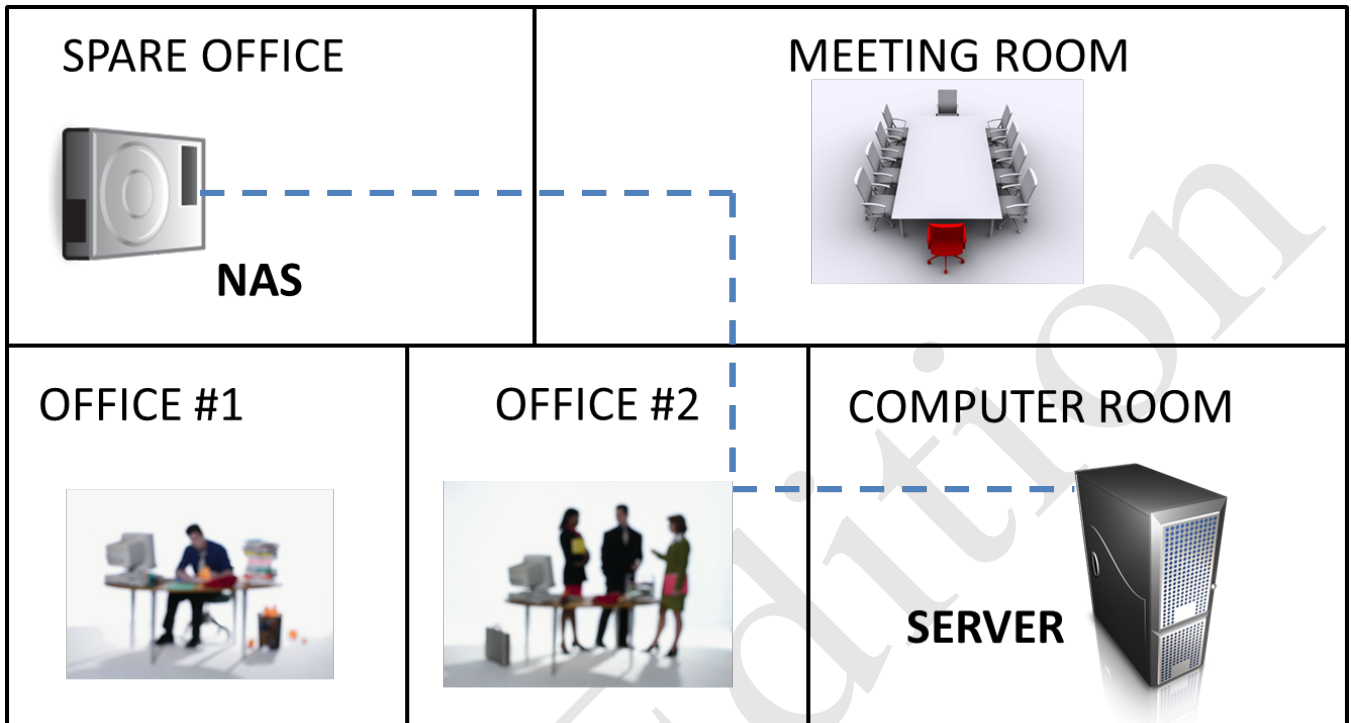

Figure 68: Locate the NAS drive in a separate part of the premises

As there are many different brands of NAS to choose from (e.g. Synology, QNAP, Netgear and so on) the specifics of setting up a particular model will not be covered and the manufacturer's documentation should be referred to. However, the basic principle is that a dedicated shared folder for backups with read/write access should be created on the NAS, along with a dedicated user backup account which will typically have administrative rights.

On the server, run Windows Server Backup and create a new backup job. On the **Specify Destination Type** screen, choose **Remote shared folder** rather than **Local drives**. Enter the full name of the shared folder on the NAS device in the format *nas_name\shared_folder_name* (in our example it is *elan\serverbackup*). For Access control choose **Do not inherit**. After clicking **Next,** you will be prompted to enter the network credentials (logon and password) for the dedicated user account that was defined on the NAS.
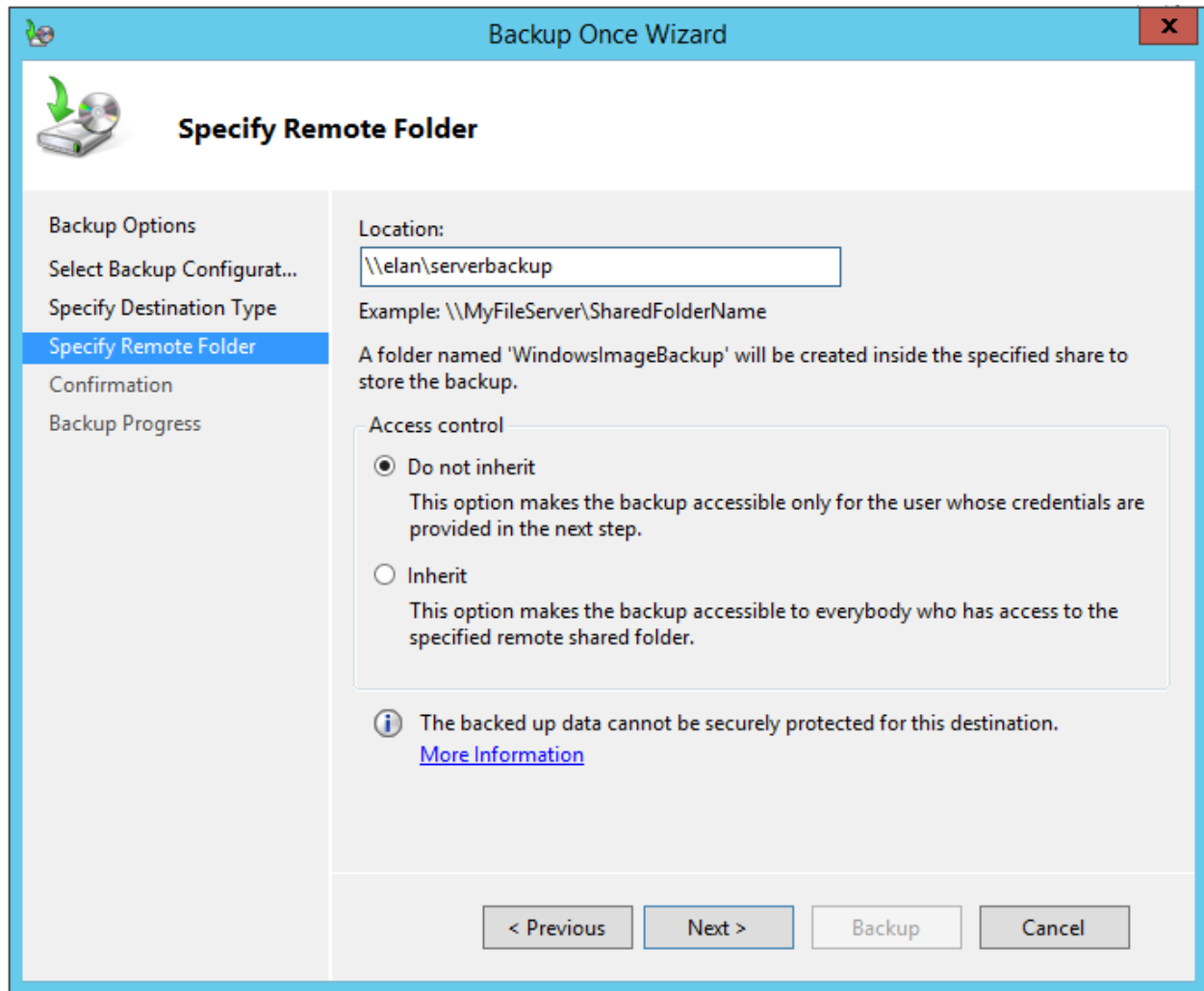
Figure 69: Specify Remote Folder

Thereafter it is a matter of following the normal steps in setting up a backup as described previously.

An additional advantage of using NAS devices is that they can be of higher storage capacity than an USB drive. For instance, suppose the server had, say, 10 TB of data. At the time of writing it is not possible to buy USB drives of this capacity, whereas this amount of storage is readily achievable with a NAS. However, one disadvantage of using a NAS is that whereas an USB drive can hold multiple backups, when used with Windows Server Backup a network drive can only hold a single backup i.e. the most recent one. This implication of this is that in the event of problems it is only possible to roll-back to the last successful backup.

6.5 Backing up Computers to the Server

If users store data on their computers rather than on the network, then there is probably a requirement to be able to backup that data. This can be done using the built-in backup programs in Windows clients, with the actual backups stored on the server. A good destination for the backups would be the individual user's home folder (the H: drive), which will enable them to manage the process themselves. As the server itself is being backed up, this will ensure multiple copies of the data, hopefully enough to cope with any eventuality.

Backing up Windows 7 Computers

Click **Start**, followed by **All Programs**, **Maintenance** then **Backup and Restore**. Click on **Set up Backup**:
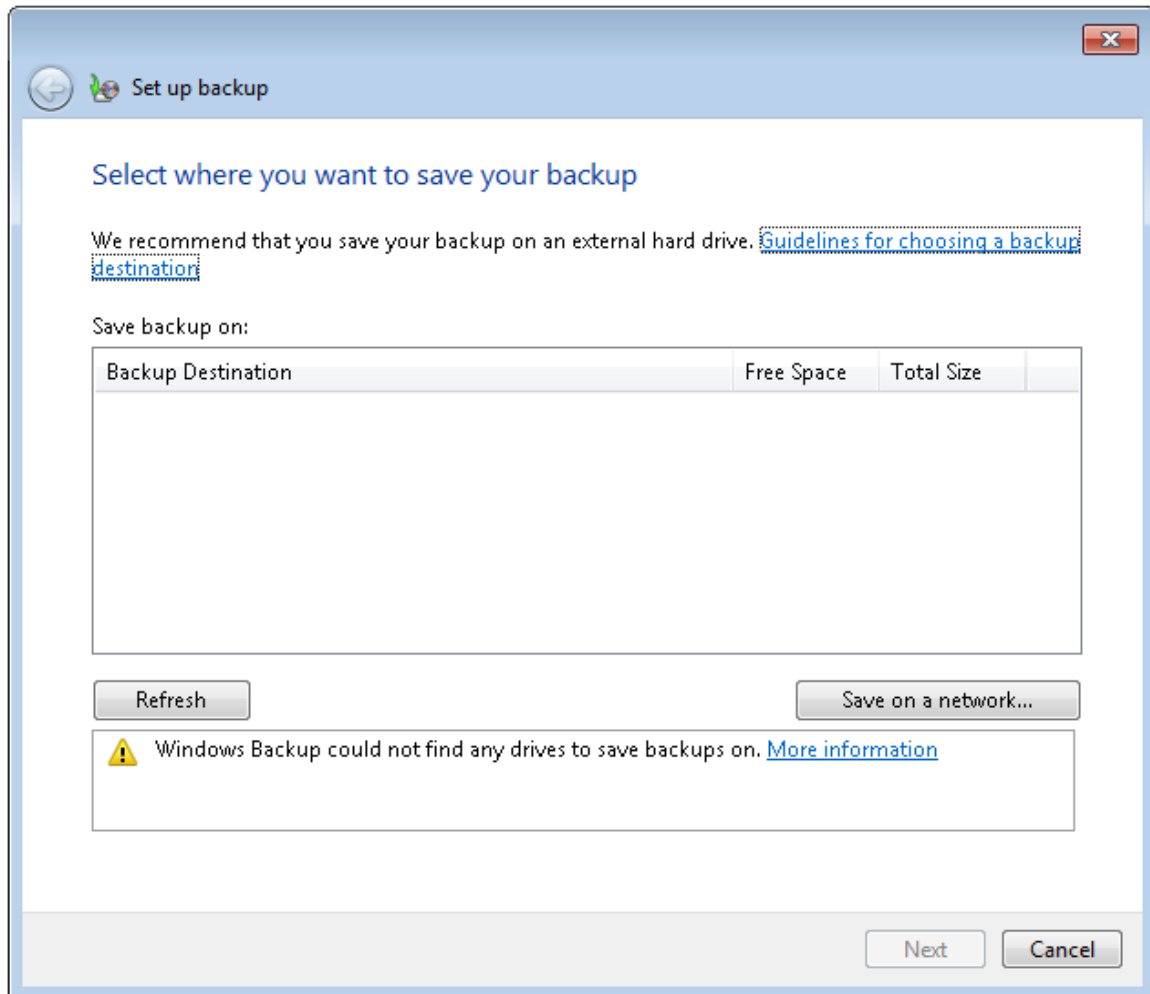

Figure 70: Select destination for backup

Click the **Save on a network** button. On the next panel, enter the **Network Location**. Specify the user's home folder, using the format *\\server\homes\username* (or click the **Browse** button to navigate to it). You may possibly be prompted to logon - enter the user name and password as defined on the server then click **OK**:
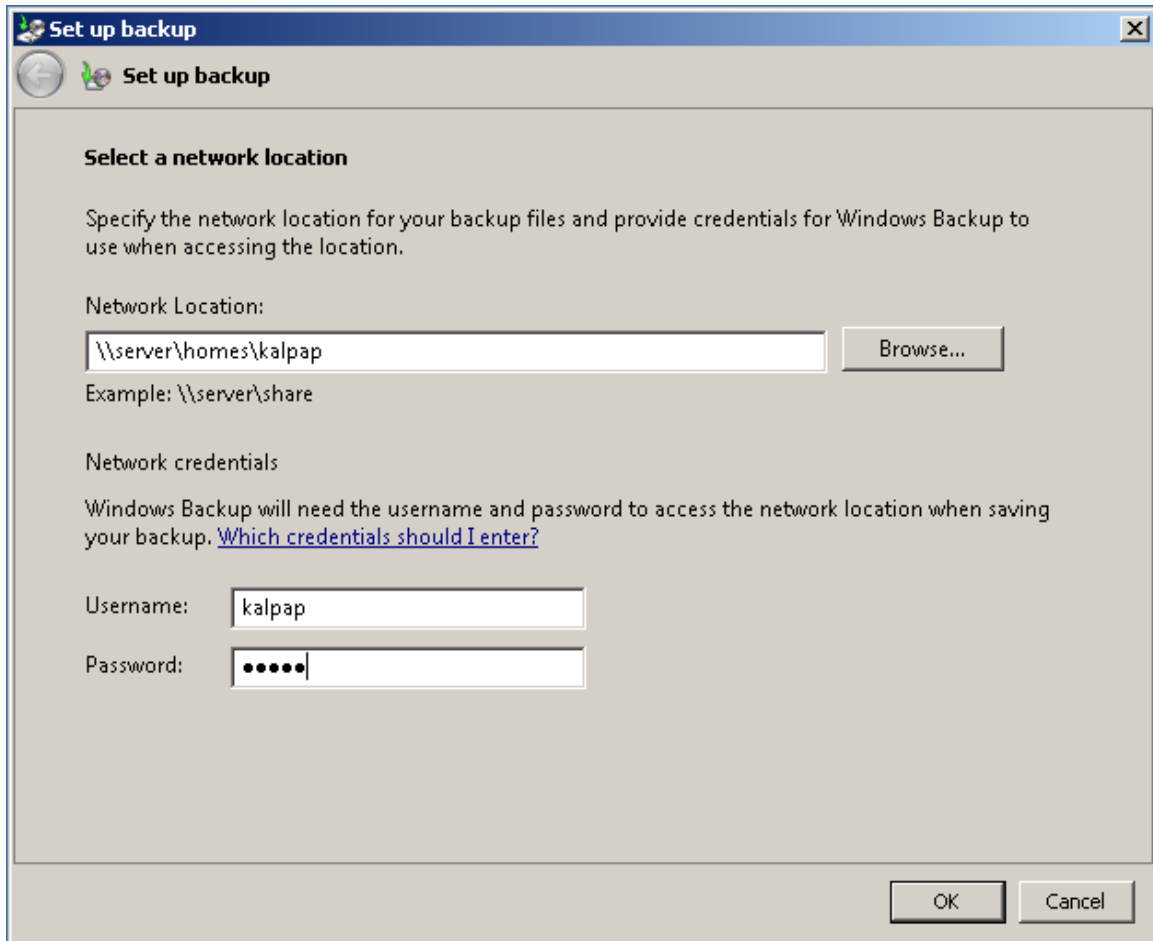
Figure 71: Enter network details

The subsequent screen is for choosing which data files are backed up. The default option of **Let Windows choose (recommended)** is fine in most cases so just click **Next**:
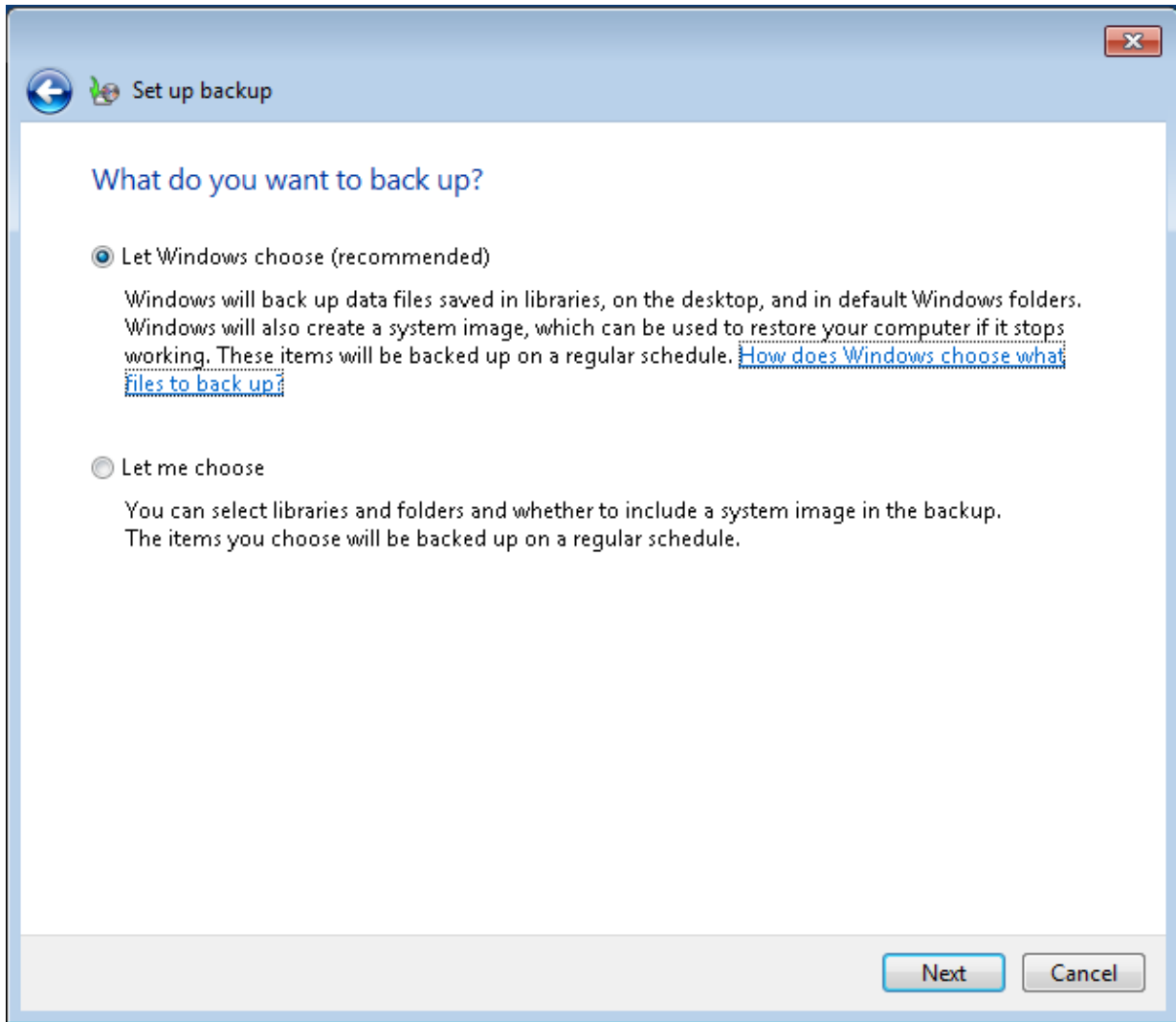
Figure 72: Choose the items to backup

The follow-on screen is a summary of settings; click **Save settings and run backup**:

Figure 73: Review backup settings

The backup will then run for the first time, during which the status is displayed. By default, Windows has defined a schedule to subsequently run backups automatically on a regular basis (in this case, every Sunday at 7:00pm). If this setting is not suitable it can be changed by clicking **Change settings**.
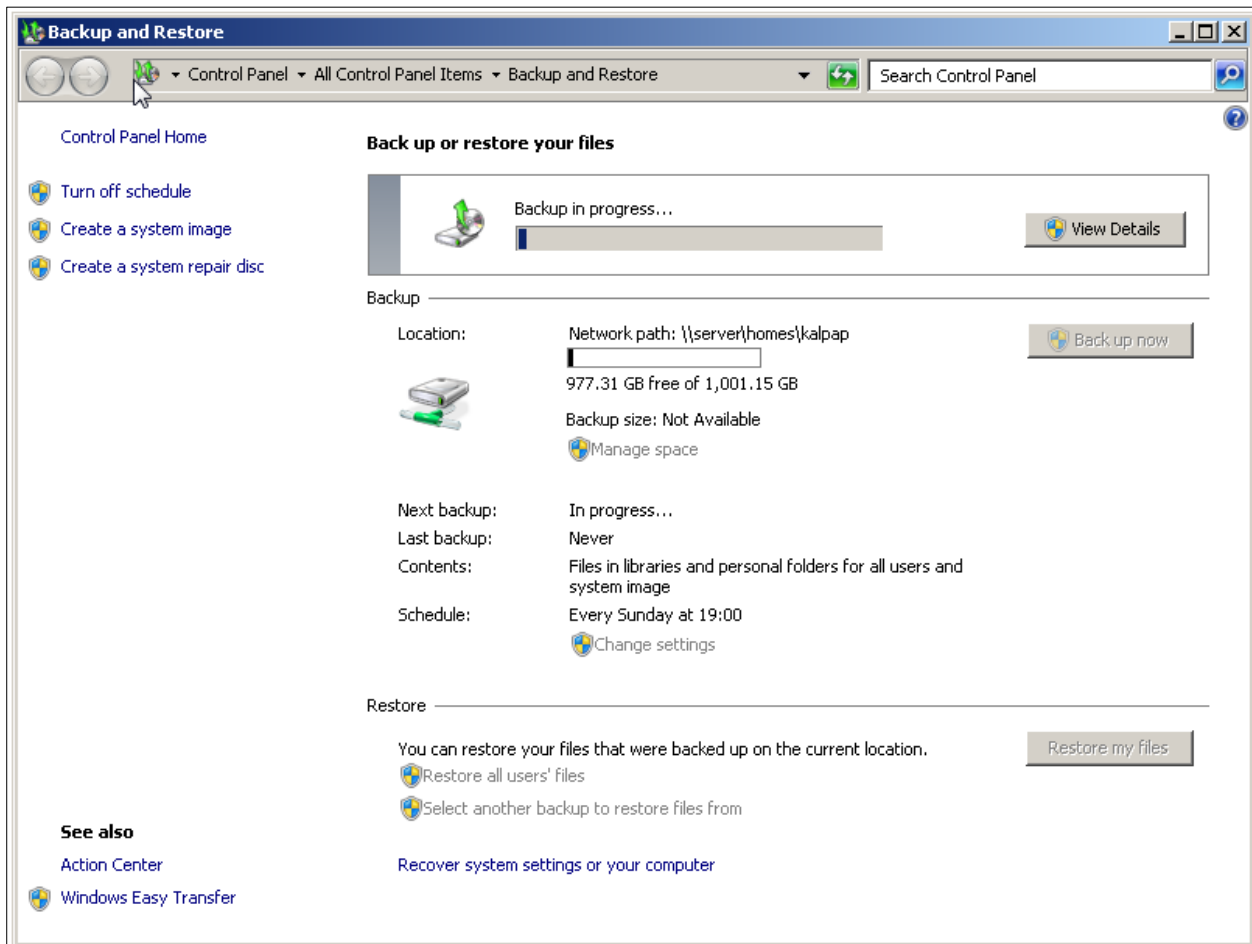
Figure 74: Backup in progress

Backing up Windows 8/8.1 Computers

Go into the **Control Panel** and click **File History** (in Windows 8.1 you can right-click the **Start** button to find the Control Panel):
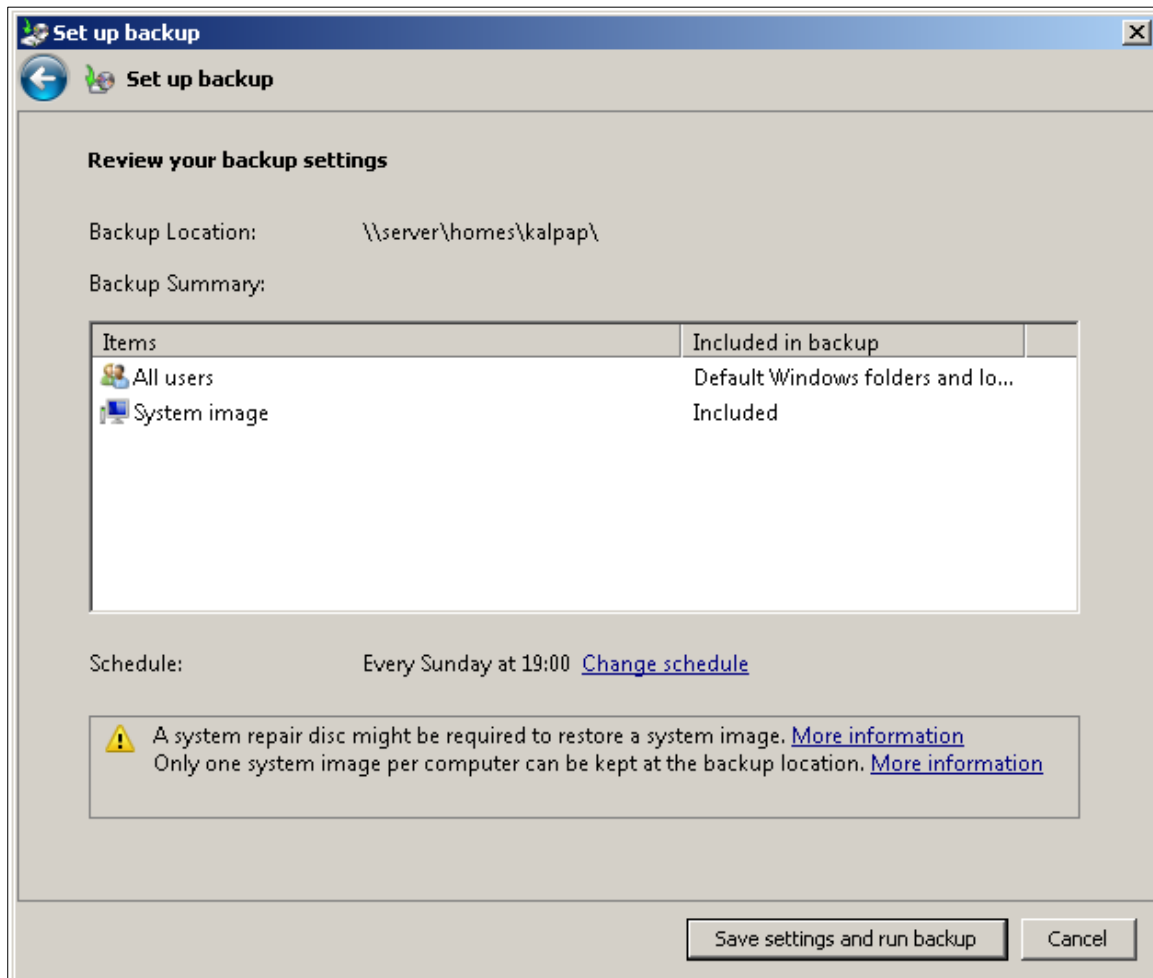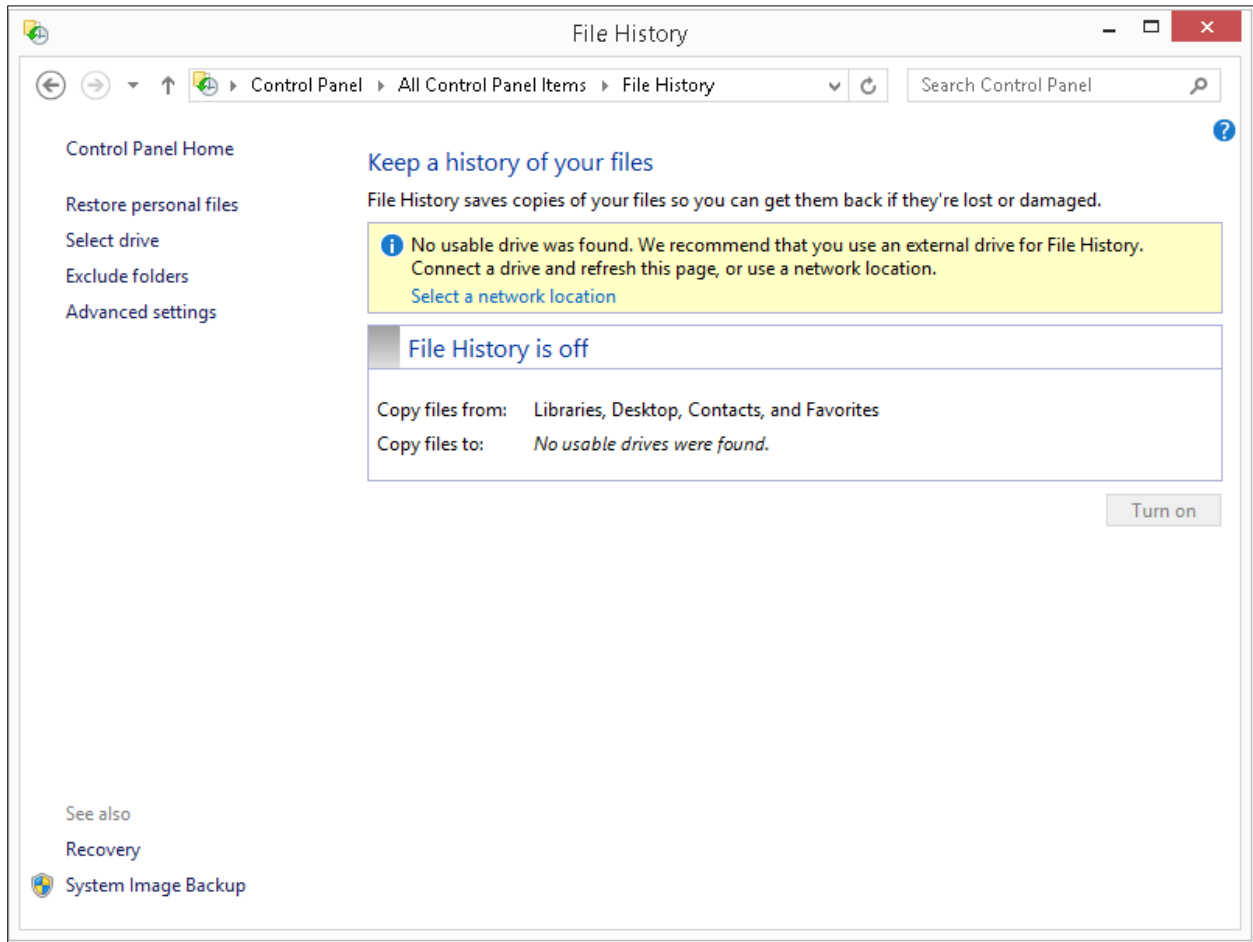

Figure 75: Initial screen in File History

Click **Select a network location**. On the screen that is displayed click **Show all network locations**. From the list, choose the user's home folder and click **Verify your credentials**. Enter the user name and password as defined on the server if prompted; if the computer is only ever used by one person you can tick the **Remember my credentials** box.

Click **OK** to return to the initial File History screen and there click the **Turn on** button. After a few seconds, the backup will run for the first time. Thereafter, it can be run at any point by clicking **Run now**.

Figure 76: Turn on File History

For greater control over the process, such as controlling the frequency at which the backup runs, click **Advanced settings**:
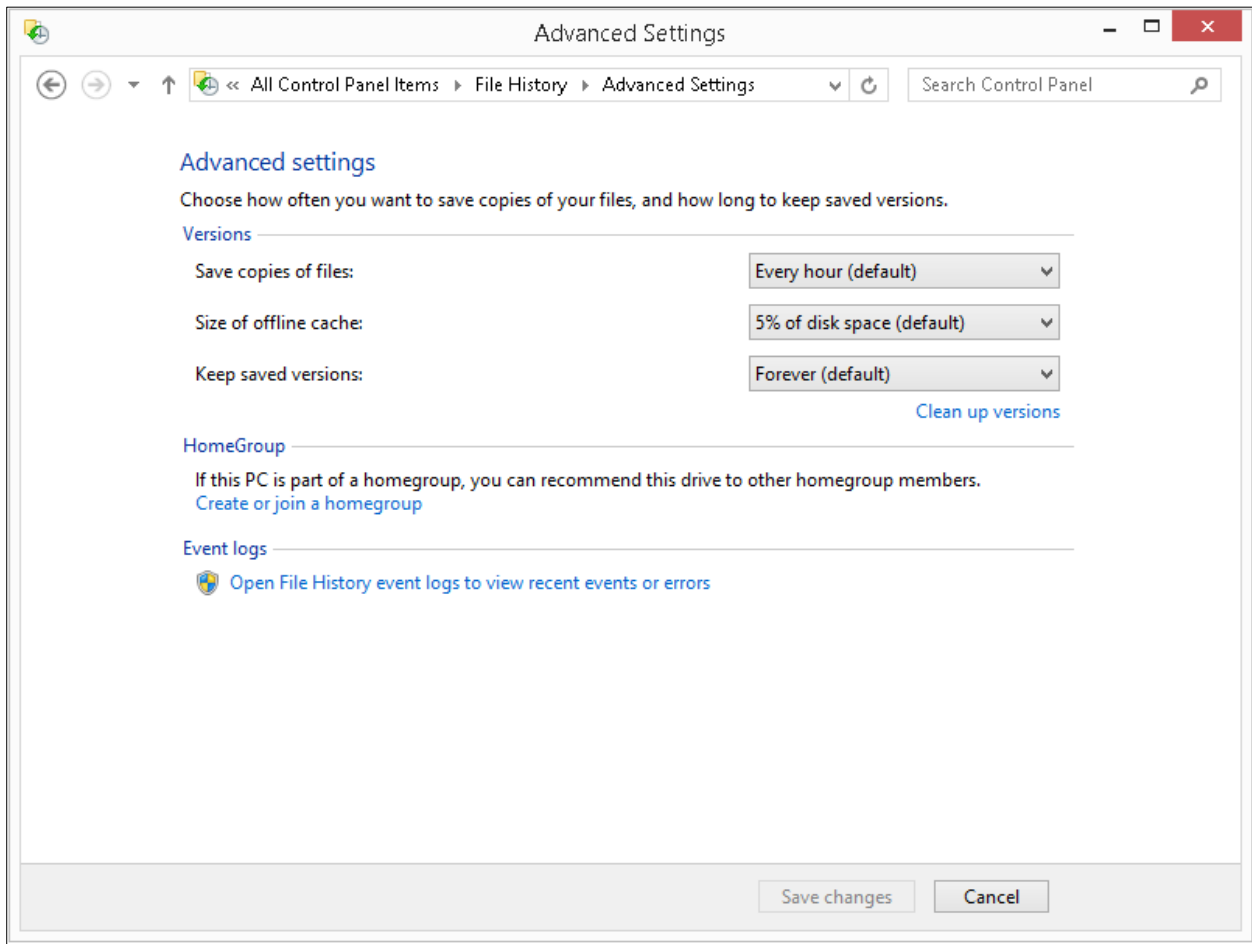
Figure 77: File History Advanced settings

Backing up Windows 10 Computers

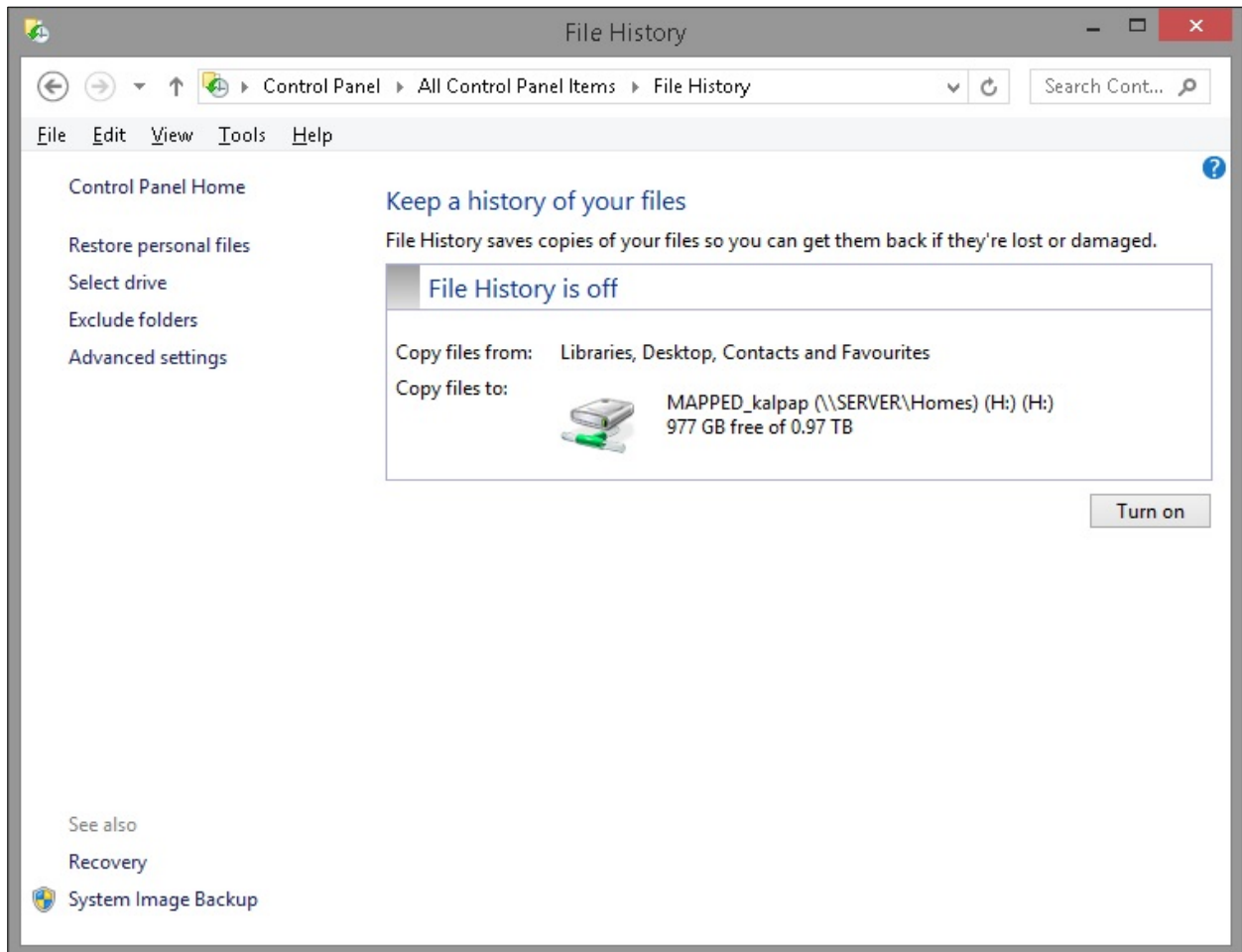Click **Start** > **Settings** > **Update & security** > **Backup**. Click **Add a drive** and after a few seconds the list of mapped drives will be displayed – click on the user's home drive:
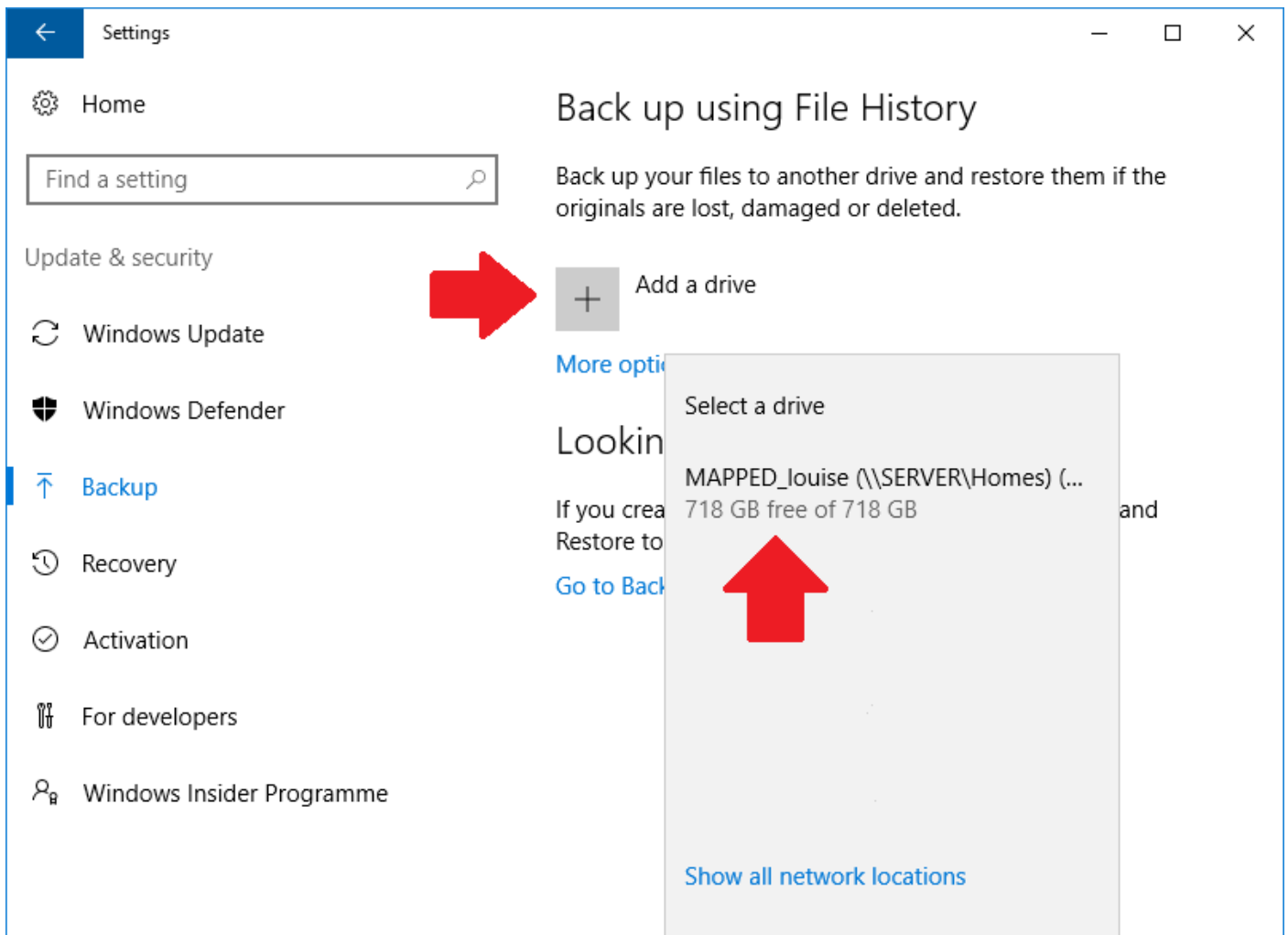
Figure 78: Specify the home folder as the backup drive

Having done so you will be returned to the main Backup panel, where an option to *Automatically back up my files will have appeared* and been set to **On**. That's it – a backup will now run on an hourly basis, copying the user's files from the computer to their home drive on the server.

For greater control over the process, such as controlling the frequency at which the backup runs, click **M**ore options. From here you can: review the backup status; make the backup run immediately; change the backup frequency (anything from every 10 minutes through to 1 day); change the retention period for the backed-up data.

7. PRINTING

An advantage of networking is that it allows printers to be shared, thus potentially saving money as well as physical space. There are several different techniques for setting up printers in a networked environment and two of them are discussed in this chapter. Each of them has benefits and disadvantages and there is probably no such thing as 'the best' solution; however, some explanation is given as to when you might take a particular approach.

Before beginning, identify the client operating systems that are in use and download all the appropriate printer drivers from the printer manufacturer's website. In general, there will be a driver that works with 32-bit versions of Windows (usually referred to as x86 or x32) and a driver that works with 64-bit versions of Windows (usually referred to as x64); however, some printers have a single driver for all variants. Some manufacturers offer an additional choice of drivers, for instance a basic one as well as a full-featured one. Use the basic one – the 'full feature' ones sometimes have superfluous features designed to capture marketing information and try to sell you more consumables. Also, be aware that with some multifunction devices (combined printers/copiers/scanners) not all functions may be available in a networked environment, or may require additional software from the manufacturer to fully utilise them.

Next, physically setup the printer and configure it with a fixed IP address consistent with the IP addressing scheme used in the network. Check that the printer is working correctly before beginning the installations on the clients.

Suggestion: a good location to store the printer drivers is the *technical* share, accessible as *\\server\technical$* by administrative users.

7.1 Independent Networked Printer

Most printers, other than very low cost and elderly models, have built-in network adaptors, either wired and/or wireless. This means that they can operate independently of the file server, with the computers talking to them directly. This is the simplest and most effective method for setting up a printer in a relatively small network. This approach also works very well in a scenario where multiple operating systems are in use.

The printer(s) should be installed **before** the computers are added to the domain.

- Visit each individual computer and login as a local user with administrative rights. Or, if developing a master disk image that will subsequently be cloned - also referred to as *Ghosting* - work on that image.
- Install the printer through the standard Windows method (**Control Panel** > **Devices and Printers** > **Add Printer**) or using the manufacturer's provided installation program
- Specify the printer as being on a TCP/IP port. Provide the fixed IP address of the printer
- Set the printer as the default printer
- Change any defaults if necessary (e.g. paper size, print quality etc.)
- Remove any superfluous virtual printers (e.g. OneNote, fax, XPS and so on)
- Print a test page to verify correct operation

The computers can then be added to the domain. The printer will appear in the list of printers for each user, although they may have to explicitly choose to make it their default printer.

7.2 Shared Printer on Server

With this method, the printer(s) are installed initially on the server and defined as shared resources; users can then choose to connect to them from their computers if they so wish. This technique has merit where there are multiple printers in use and where the users are technically savvy. Also, it allows new printers to be installed retrospectively after the network has already been setup, in contrast with the previous method where the printer(s) are installed before the computers are connected to the domain. However, with this approach the users need to have administrative rights on the domain or at least be given the administrator password - one technique is to set up an additional or dummy administrative account as described in 11.8 Create Alternative Administrator Account(s).

- Install the printer on the server through the standard Windows method (**Control Panel** > **Devices and Printers** > **Add Printer**) or using the manufacturer's provided installation program
- Specify the printer as being on a TCP/IP port. Provide the fixed IP address of the printer
- On the Printer Sharing screen click **Share this printer so that others on your network can find and use it**. Give it a meaningful **Share name** and use the **Location** and **Comment** fields to provide other helpful details. Then click **Next**:
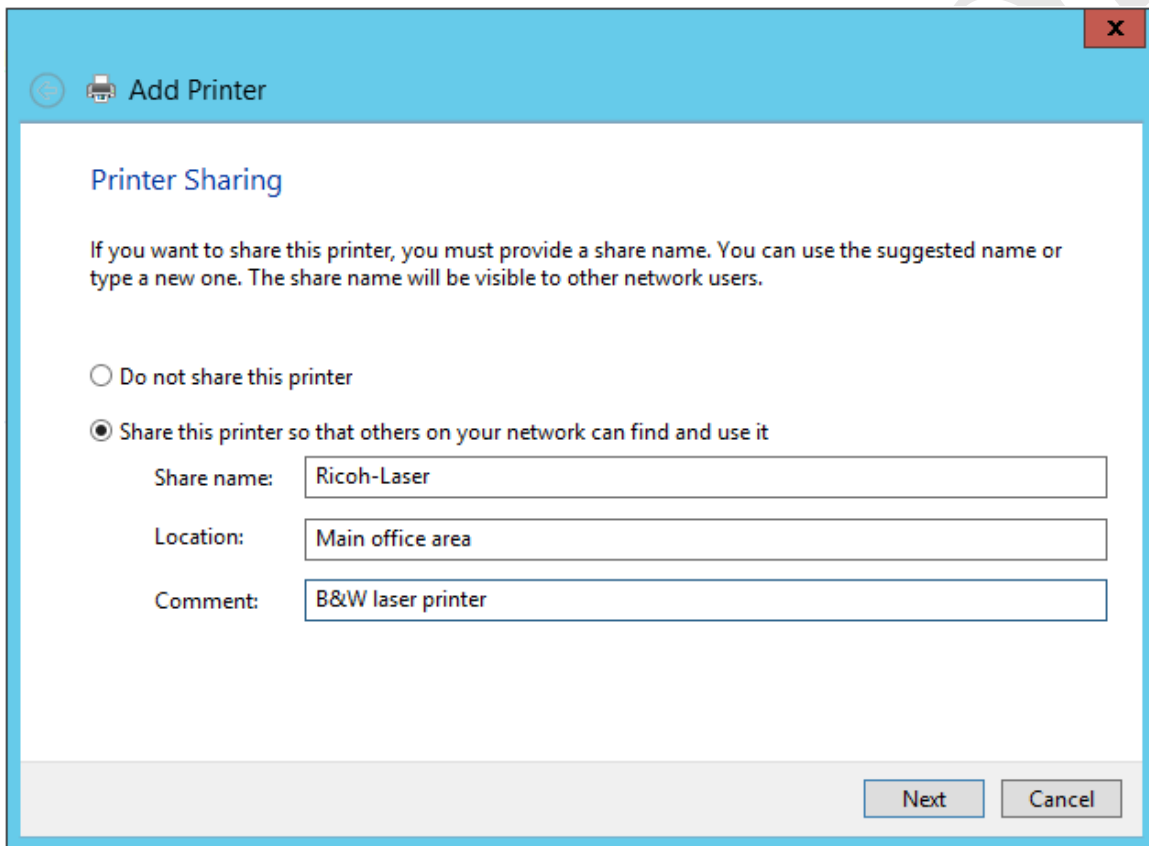

Figure 79: Printer Sharing

Complete the installation and check that it is working by printing a test page. Then, within **Devices and Printers** right-click the printer and choose **Printer Properties**. Click the **Sharing** tab. Make sure that the **List in the directory** box is ticked:
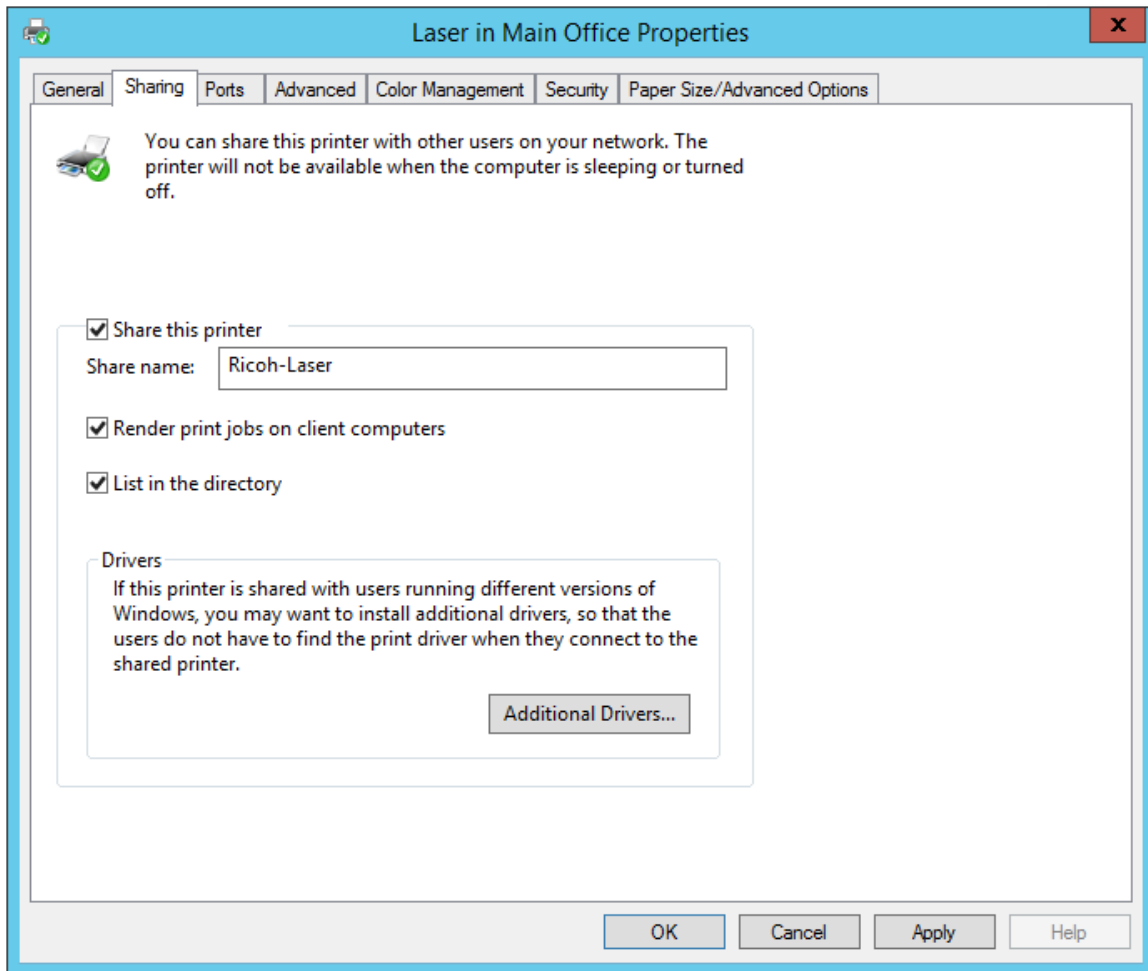
Figure 80: Properties for shared printer

If all the client computers are using 64-bit versions of Windows, then we are complete on the server side. However, if any client computers are using 32-bit versions of Windows then click the **Additional Drivers** button. On the next panel, tick the **x86** box followed by **OK**. Note: this reflects the most common scenario with printers, referred to by Microsoft as *Type 3* printers. With some printers – usually more recent models known as *Type 4* printers – this step is not needed as the drivers will work with all modern versions of Windows regardless of whether they are 32-bit or 64-bit:
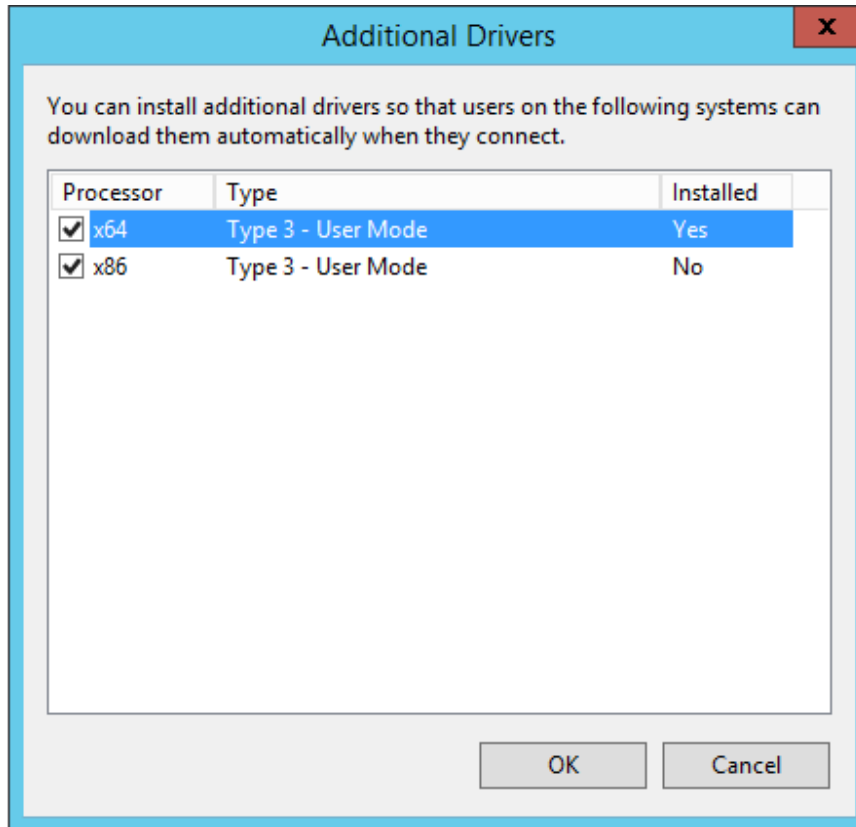
Figure 81: Additional printer drivers

Having clicked **OK**, you will then be prompted to enter the location of the x86 ("32-bit") driver. Follow the screens through then click **Apply** followed by **OK**.

The printer can now be installed on the client computers. To do this, a user must have administrative rights or, when prompted, enter the account details for an administrative user. From **Devices and Printers**, choose **Add Printer**. Choose **Add a network, wireless or Bluetooth printer** and click **Next**:
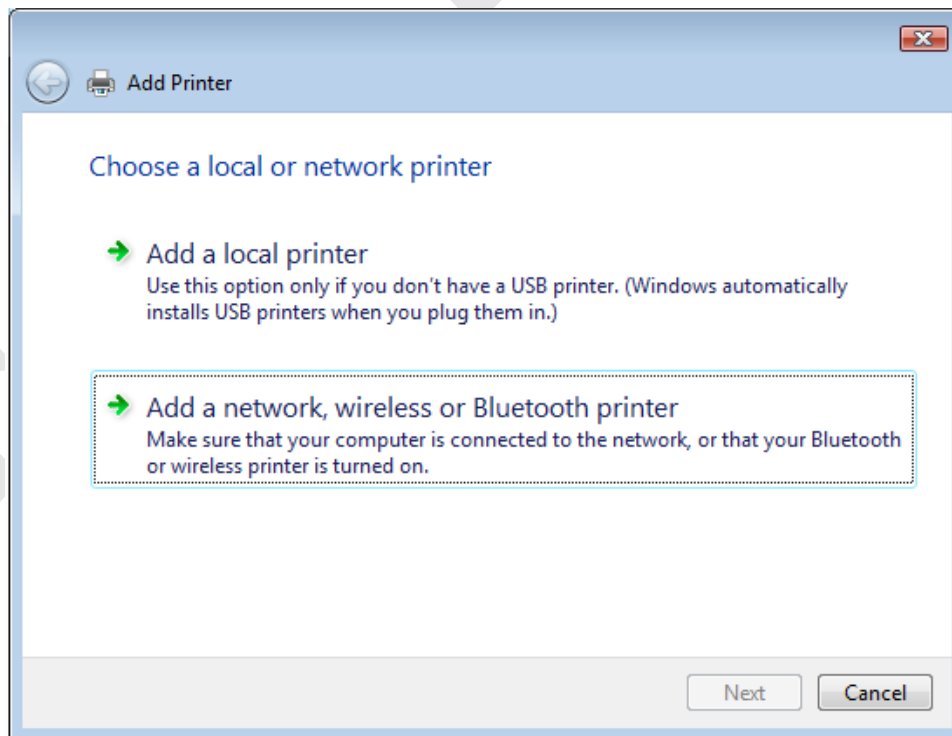
Figure 82: Adding a printer

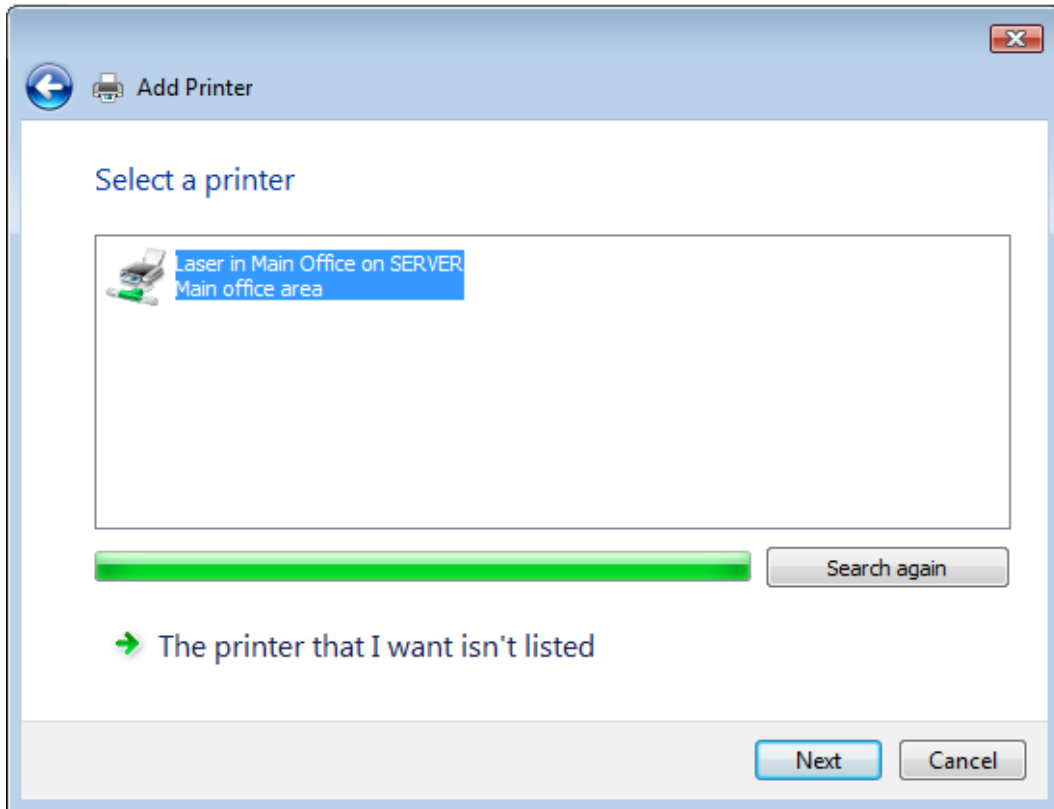The shared printer(s) will be listed. Highlight it and click **Next**:

Figure 83: Select a printer

A message about the need to install a printer driver is likely to be displayed. Click **Install driver**:
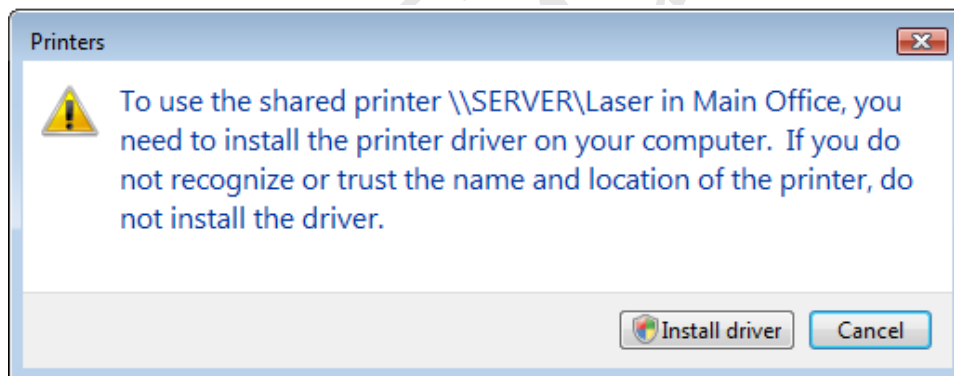

Figure 84: Message about printer driver

If necessary, enter the account details for an Administrator to complete the installation. Once the printer is installed, print a test page to confirm that it is working.

8. GROUP POLICY

This chapter is concerned with making the network more professional, easier to use and more manageable by using a facility called *Group Policy*. Computers and user accounts have many hundreds of settings that control their behaviour, such as how often passwords need to be changed, what items appear on the Desktop, the default home page within Internet Explorer and much more. Building upon Active Directory, Group Policy enables such things to be defined and then enforced across groups of computers and users, thereby creating a more consistent and controlled environment. This chapter is not intended as an in-depth tutorial about Group Policy, rather it is concerned with some simple practical examples of using it.

8.1 Installation of Group Policy Management

In order to use Group Policy, it is first necessary to install the *Group Policy Management* facility. To do so, launch Server Manager. Click **Manage** followed by **Add Roles and Features**. Click **Next** on each screen until you reach the one called *Select server roles*; on it click **Features**, tick **Group Policy Management** and click **Next** and then **Install** on the screen after that. When installation is complete – which will only take a minute or two – click **Close**.
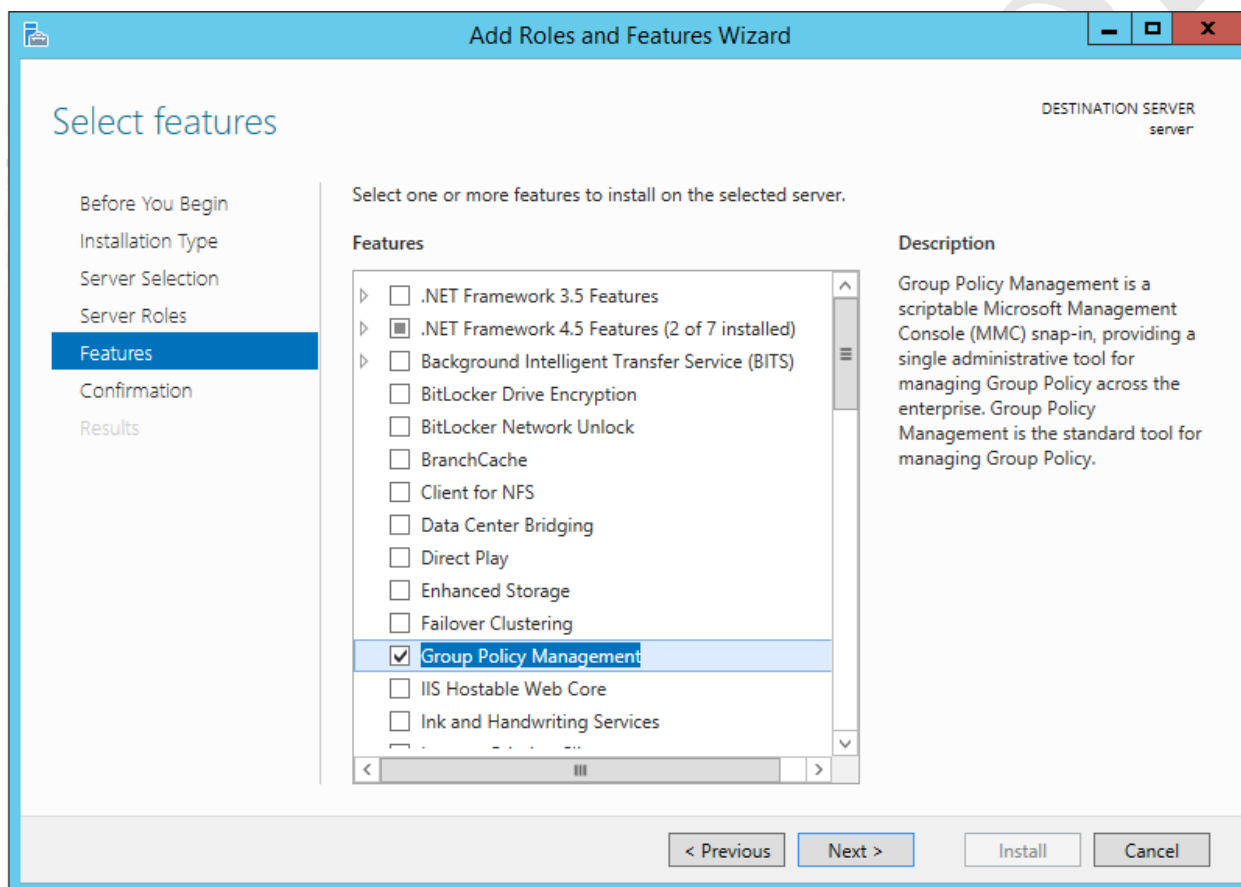

Figure 85: Installing Group Policy Management

8.2 Group Policy Management Console

Group policies are created and controlled using the *Group Policy Management* console. It is one of the Administrative Tools and can be accessed in several ways:

- Click the **Administrative Tools** icon on the Start Screen. Double-click the **Group Policy Management** icon
- Right-click the **Start** button, choose **Control Panel** and from there double-click the **Administrative Tools** icon followed by **Group Policy Management**
- In the Server Manager Dashboard, click **Tools** followed by **Group Policy Management**
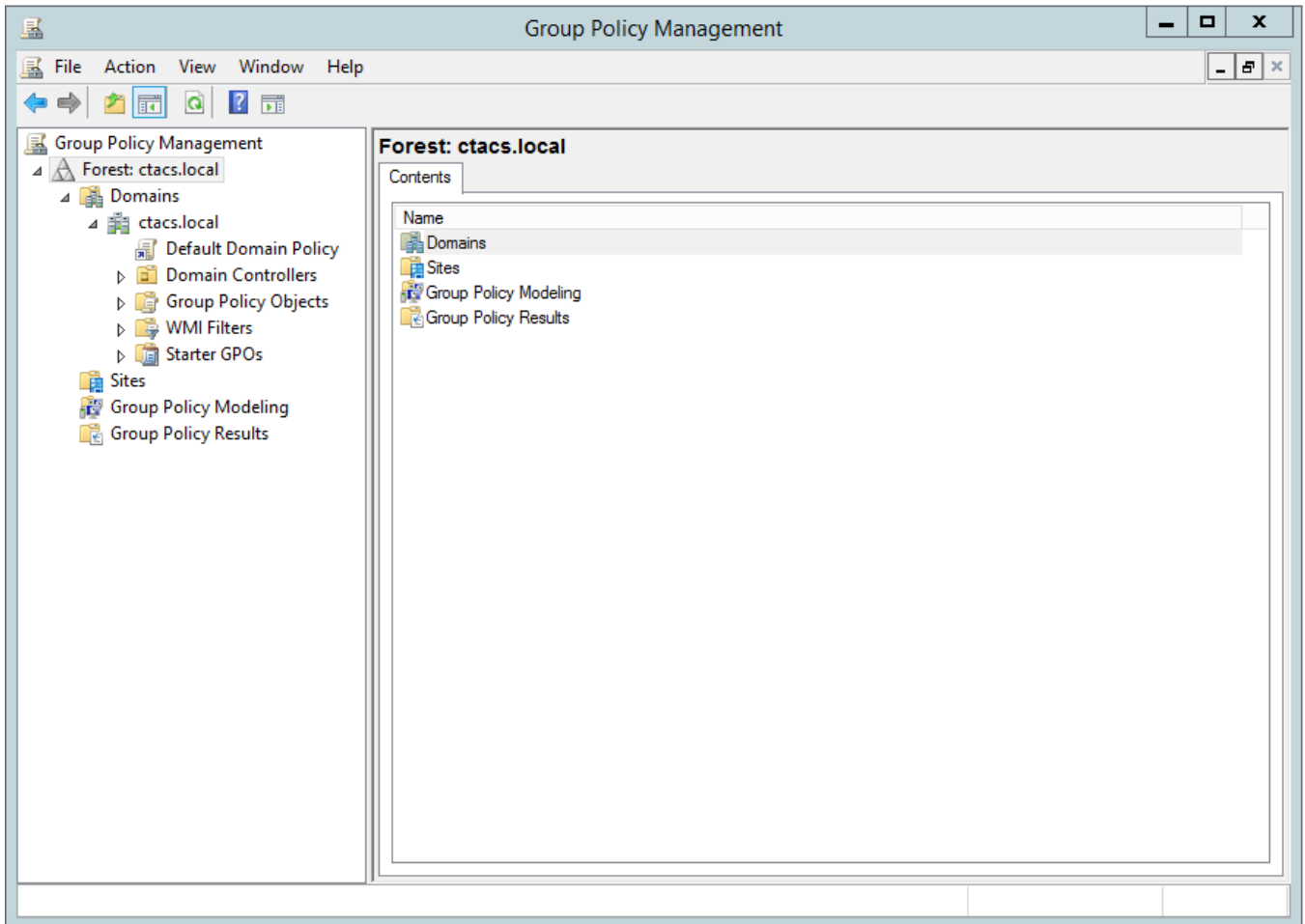
The console looks like this:

Figure 86: Group Policy Management console

Expand the tree in the left-hand panel to display the overall structure of the domain. In the above example, the default structure for a newly-created domain using a single server is shown. The structure can be added to but to keep things simple we will leave things as they are. Notice an entry called *Default Domain Policy*; as the name implies, this covers default settings for the entire network. Any changes to this will therefore apply to all computers or users in the system and our efforts will focus on this.

Making a change involves right-clicking an item – such as *Default Domain Policy* – and choosing **Edit**. Policies are created or modified for the *Computer Configuration* or *User Configuration*, the former affecting all computers and the latter affecting all users. There is no mechanism to explicitly save changes, as it is implicit when making modifications. The policies and preferences do not immediately propagate, rather they are applied the next time a client logs in to the network or when a computer starts up. However, it is sometimes possible to expedite matters by bringing up a command prompt ("DOS prompt") on a workstation and typing the command *gpupdate /force*.

One thing to note is that some Group Policy settings are operating system dependent. For instance, some may only be applicable to (say) Windows 7 and not work on (say) Windows XP at all. However, the majority are applicable to all versions of Windows.

8.3 Specifying Home Page Using Group Policy

Some organizations require that all users have a standard home page within Internet Explorer, for example the company's website or an email system such as *GMail* or *Office 365*. Group Policy can be used to enforce this.

Launch the **Group Policy Management Console**. Expand the tree in the left-hand panel, right-click the entry for *Default Domain Policy* and choose **Edit**. In the new window, expand the tree and drill down to **User Configuration** > **Preferences** > **Control Panel Settings**. Right-click the entry for **Internet Settings** and choose **New**. A pop-up listing the various versions of Internet Explorer is shown; note that most of these are now obsolete and should no longer be in use, also that the current version, Internet Explorer 11 (nor the Edge browser for that matter) is not listed at the time of writing, although it will in fact use the Internet Explorer 10 settings:

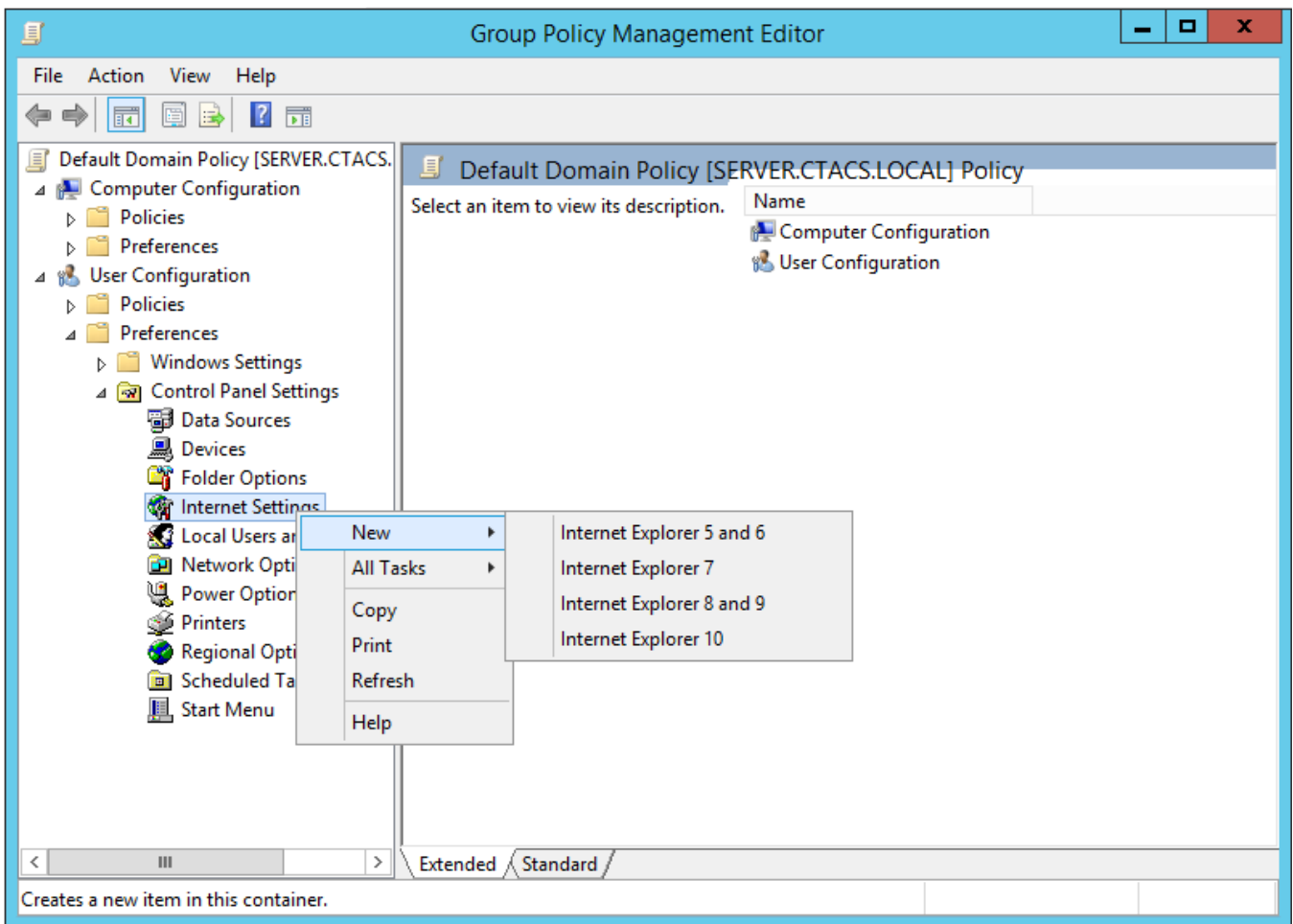

Figure 87: Choose the version of Internet Explorer

On the assumption that the organization is indeed using IE10 or IE11, click **Internet Explorer 10** and the properties box is displayed. Enter the details for the desired standard home page:
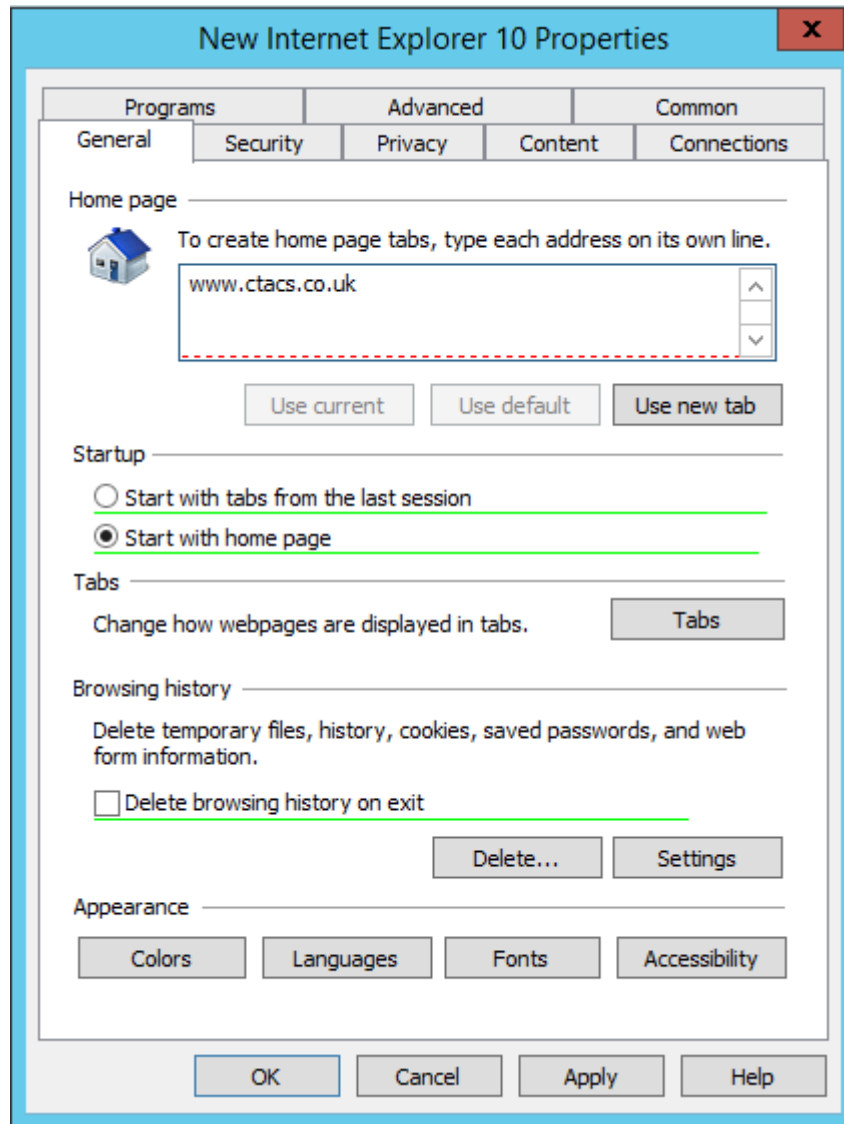
Figure 88: Specify the home page settings

In the 'Home page' section there is a red dotted line – press the **F6** key and it will change to a solid green line. **Note:** this is very important – unless this is done the setting will not apply. Click **OK**.

The effect of this is that all users will now have the specified page as their home page within Internet Explorer.

Internet Explorer is the only browser supported by Microsoft through Group Policy. If Firefox, Chrome or Edge are used then various solutions and workarounds can be found by Googling the topic.

8.4 Windows Logon Behaviour

By default, Windows 7 and later clients display the name of the last person to use the computer. This can be confusing in an environment in which people share computers, as it necessary for the next person using it to specify "Logon as other user", which is a difficult concept for some people. However, this behaviour can be changed, such that a blank user name and password are always presented to users and this is done through Group Policy.

On the server, launch the **Group Policy Management** Console. Right-click the *Default Domain Policy* and choose **Edit**. Drill down to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options.** Find **Interactive login** and Enable '**Do not display last user name**'. Click on **OK**.

8.5 Logon Warning/Security Message

Group Policy can be used to specify a message that appears at the logon screen. For instance, the message could state the name of the organization ("ACME Inc.") along with an advisory or warning message ("Do not attempt to use this computer system unless you have been authorized to do so"). There are two entries that need to be set: one for the title and one for the message itself.

On the server, open the **Group Policy Management** Console. Right-click the *Default Domain Policy* and choose **Edit**. Drill down to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**. Find **Interactive login: Message title for users attempting to logon**. Tick the **Define this policy** setting box, enter the name of the organization and click **OK**. Then repeat for **Interactive login: Message text for users attempting to log on** and specify the detailed warning or greeting message. Click **OK**.

8.6 Changing the Password Policy

By default, Windows Server 2012 R2 has a password policy of *complex passwords*, which means that passwords have to comprise a mixture of letters, numbers and special characters. By using complex passwords, security is enhanced. For instance, it is very unlikely that an unauthorised user or hacker would be able to guess a password like *!!40#mgzjeu23!398ab*. However, in some scenarios such passwords are too difficult to manage - for example, in a school or in a work environment with many casual users - in which case the policy can be adjusted.

To do so, go into the **Group Policy Management Editor;** expand the tree to display the *Default Domain Policy*, right-click it and choose **Edit**. Drill down to: **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Account Policies** > **Password Policy**:
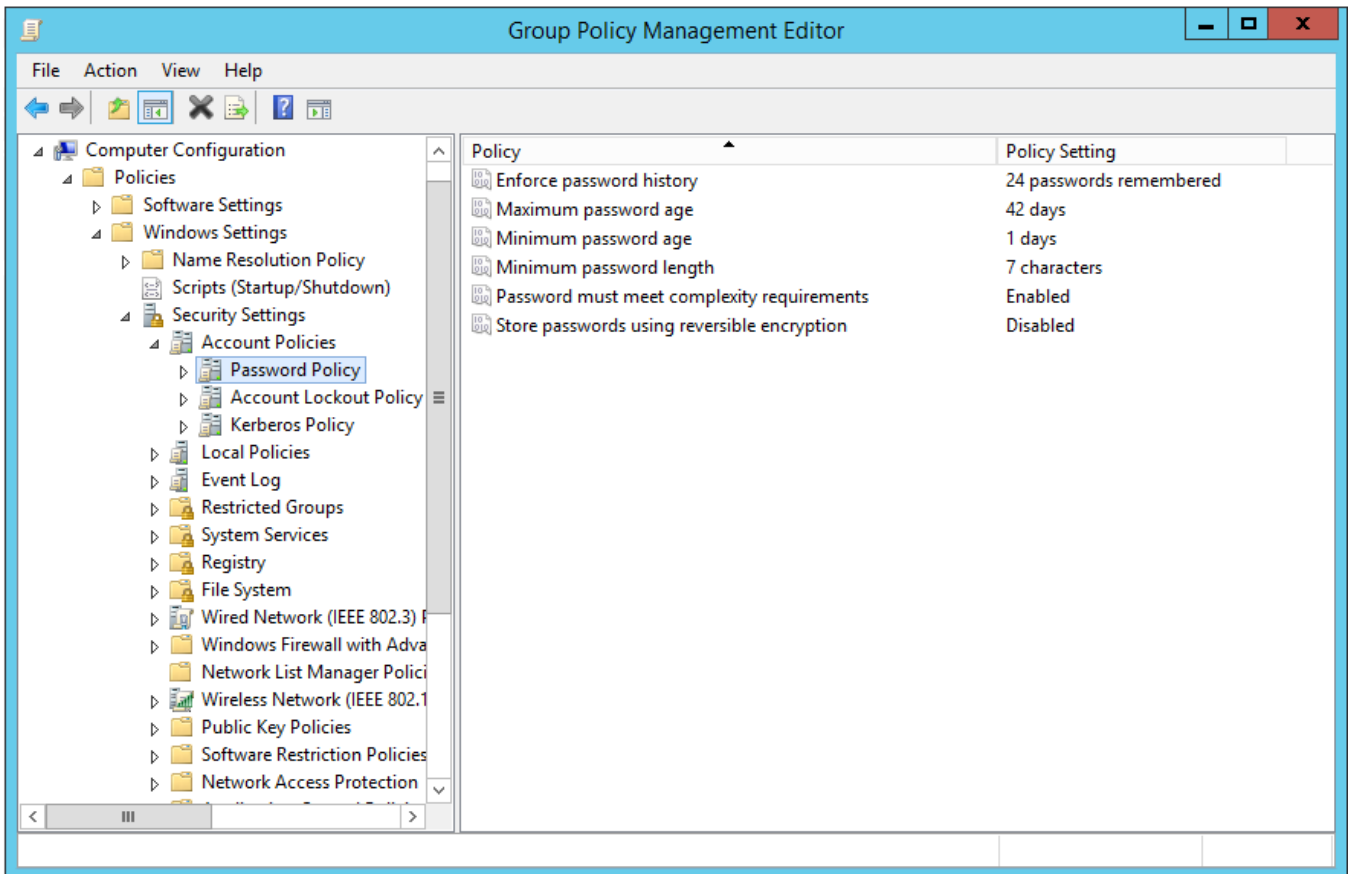

Figure 89: Specifying the Password Policy

To remove the requirement for complex passwords, change **Password must meet complexity requirements** to **Disabled**.

To prevent users being forced to change their passwords on a regular basis, change **Maximum password age** to 0 and **Minimum password age** to 0.

To remove the requirement for passwords to be of a minimum length, change **Minimum password length** to 0.

8.7 Redirect the User's Documents Folder

The purpose of this is to redirect the user's *Documents* folder (also sometimes known as *My Documents*) from their computer to their home drive on the network. By doing so, any files the user creates will automatically be stored on the network and hence be available from any computer on the network, without the user having specifically to remember to store them on the H: drive. Another consequence of redirecting the home folder is that a feature called *offline folders* is also enabled; users who have laptops will still have their home folder documents available when working offsite and any changes made will be automatically synced when they come back into the office.

- Launch the **Group Policy Management** console
- Expand the console tree. Right-click the *Default Domain Policy* and choose **Edit**
- Expand the tree to **User Configuration** > **Policies** > **Windows Settings** > **Folder Redirections** > **Documents**
- Right-click **Documents** and choose **Properties**
- On the **Target** tab, change the **Setting** to *Basic - redirect everyone's folder to the same location* and the **Target folder location** to *Redirect to the user's home directory*.
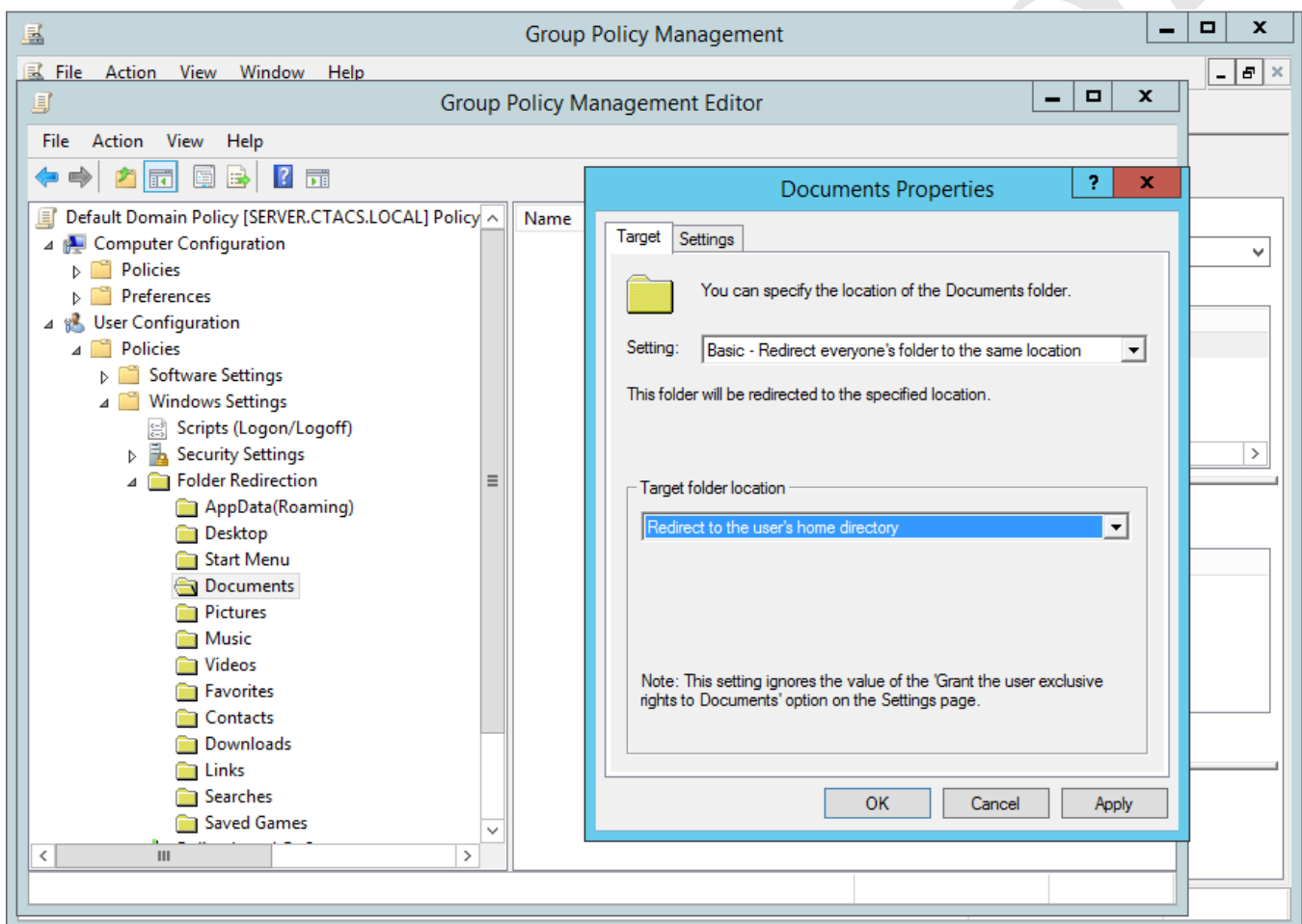- Click **Apply**, then click the **Settings** tab.

Figure 90: Specify location of the Documents folder

- Make sure it looks as shown below. If older versions of Windows are in use at the site, ensure the box for Windows XP and other earlier operating systems is ticked. Then click on **Apply** and **OK**.
- A warning message may be displayed. This can safely be ignored – just click on **Yes**.
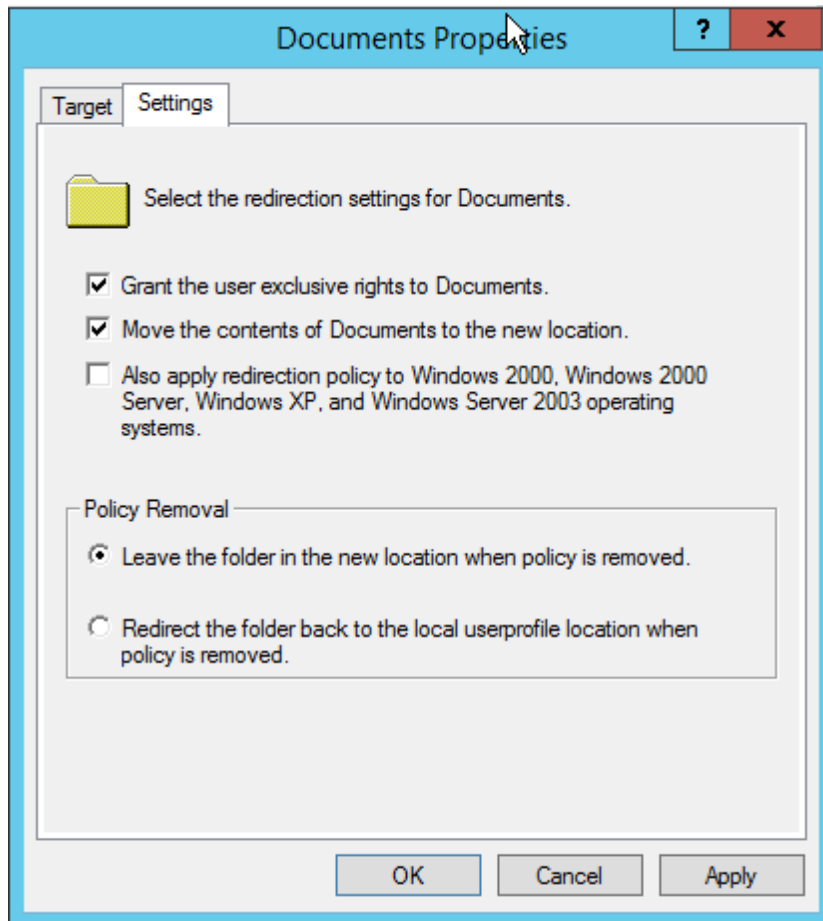
Figure 91: Redirection settings

An additional step is needed:

- Launch **Group Policy Management**
- View Settings for the *Default Domain Policy*
- Expand to **Computer Configuration** > **Policies** > **Administrative Templates** > **Network** > **Offline Files**
- The setting for **Allow or Disallow use of the Offline Files Feature** should be set to **Enabled**.
- The setting for **Subfolders always available offline** should be set to **Enabled** if Windows XP machines are in use

Troubleshooting. Unfortunately, it is not uncommon to experience problems with the Offline files facility, particularly with older versions of Windows. If it is not working, try this additional change to Group Policy. For the *Default Domain Policy*, go to **Computer Configuration** > **Policies** > **Administrative Templates** > **System** > **Logon**. Enable the **Always wait for the network at computer startup and logon** option.

9. USING DROPBOX WITH WINDOWS SERVER

Windows Server has a number of features to enable remote working, although they can be difficult to configure and operate. However, a simple and popular method that can complement these and provide additional capabilities is to use a Cloud-based file sync service such as *Dropbox*, which can provide remote access to data in a simpler method with less effort and on a wider range of devices, plus provide controlled access to selected files for third parties via emailed links. It can also or alternatively be used as a way of backing up data from the server, providing offsite storage to complement the internal backup. Microsoft have a similar offering in the form of *OneDrive* and Google has *Google Drive*, but in practice Dropbox seems to work a lot better.

There are a number of considerations when using Dropbox with Windows Server.

1. A single Dropbox account has to be used for everyone (create one first if necessary).
2. The account should have sufficient space. A standard free account only has 2GB of space, plus any additional space gained through referrals. This is unlikely to be enough in a business environment so consider a paid account; for instance, a Dropbox Pro account provides 1000GB space for $9.99 US equivalent per month, plus larger storage plans are available.
3. Whether it will be used for additional backups or as a means of providing remote access to data when out of the office.
4. Who has access to it. If used for backups only, then only the server administrator needs access. If a wider range of users, be aware that any of the users can make changes (such as delete data) that affect other people.
5. Who will be responsible for managing it, which is usually the person who administers the server.

Install the Dropbox client on the server, which is best done by downloading it directly from the Dropbox home page. Note: this will be easier if you first disable the Internet Explorer Enhanced Security feature as described in 11.1 Disabling Internet Explorer Enhanced Security. Immediately after the initial installation, click the **Advanced Settings** option as this allows you to specify the location of the Dropbox folder. Choose the shared folders location, which is *D:\shared* in our example system and which will result in the creation of a folder called *D:\shared\dropbox*. Dropbox automatically installs itself as a service, meaning it will start-up automatically each time the server starts.
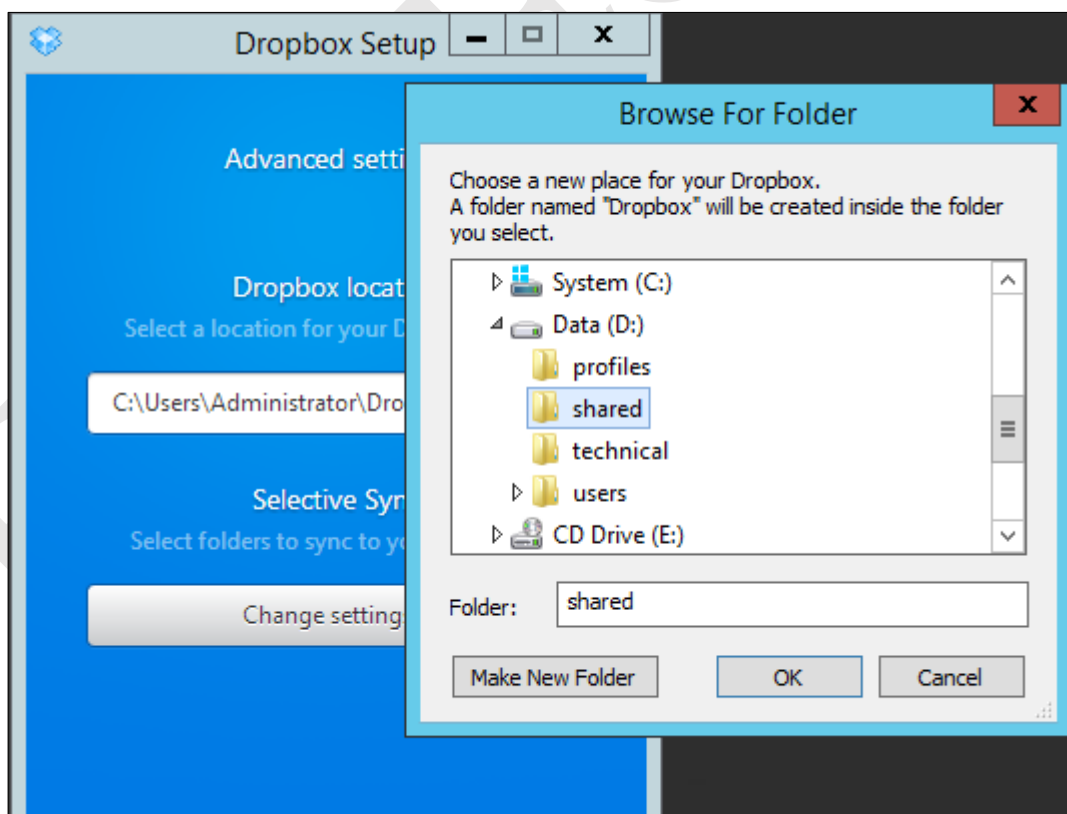
Figure 92: Dropbox folder location on server

To gain access, the permitted users should have the Dropbox client installed on the devices they use outside of the office, downloadable from *www.dropbox.com*. It is suggested that the users are not given the password and allowed to install

it themselves, so as to reduce the risk of errors or abuse. At the time of writing, Dropbox is available for: Windows, Mac OS X, iPad & iPhone, Android, Windows Phone, Blackberry plus selected Linux distributions.

To make files available outside of the office, they simply have to be placed in the *Shared\Dropbox* folder.

One thing to consider is what happens when people leave the organization, as if they have Dropbox installed on a home computer they will continue to have access to whatever is stored on the server's Dropbox folder. In such circumstances it will be necessary for the administrator to change the password of the Dropbox account and advise remaining staff of the new password or reset it for them. Dropbox Pro and Dropbox for Business both have the capability to 'remote wipe' data on devices and this can be used to remove the organization's data from the former user's computer.

10. WORKING WITH IPADS AND OTHER PORTABLE DEVICES

Most portable devices such as iPads, iPhones and Android tablets and cell phones are not able to directly connect to domain-based Windows networks in the sense that a PC can. However, this does not mean that they cannot access data and be used in a productive manner. A variety of apps and techniques are available to both access data and administer Windows Server and some of the main ones are discussed below.

10.1 Accessing the File System with File Browser

For iOS users, *File Browser* from Stratospherix is a good way of accessing folders and files on the server. It is a commercial product obtainable from the App Store, but is inexpensive and well worth buying. It is not specifically designed for Windows Server, rather it is a generic tool for accessing any networked computer. To use, enter the IP address of the server along with a valid user name and password; the user can then see any of the folders to which they have been granted access (for example, the *shared* folder). To access their home folder, double-click the *Users* folder then double-click the folder that has the same name as their own user name. Note that they can see the names of other people's home folders, but will not be able to access them because of security restrictions. Files can be viewed, but not edited.
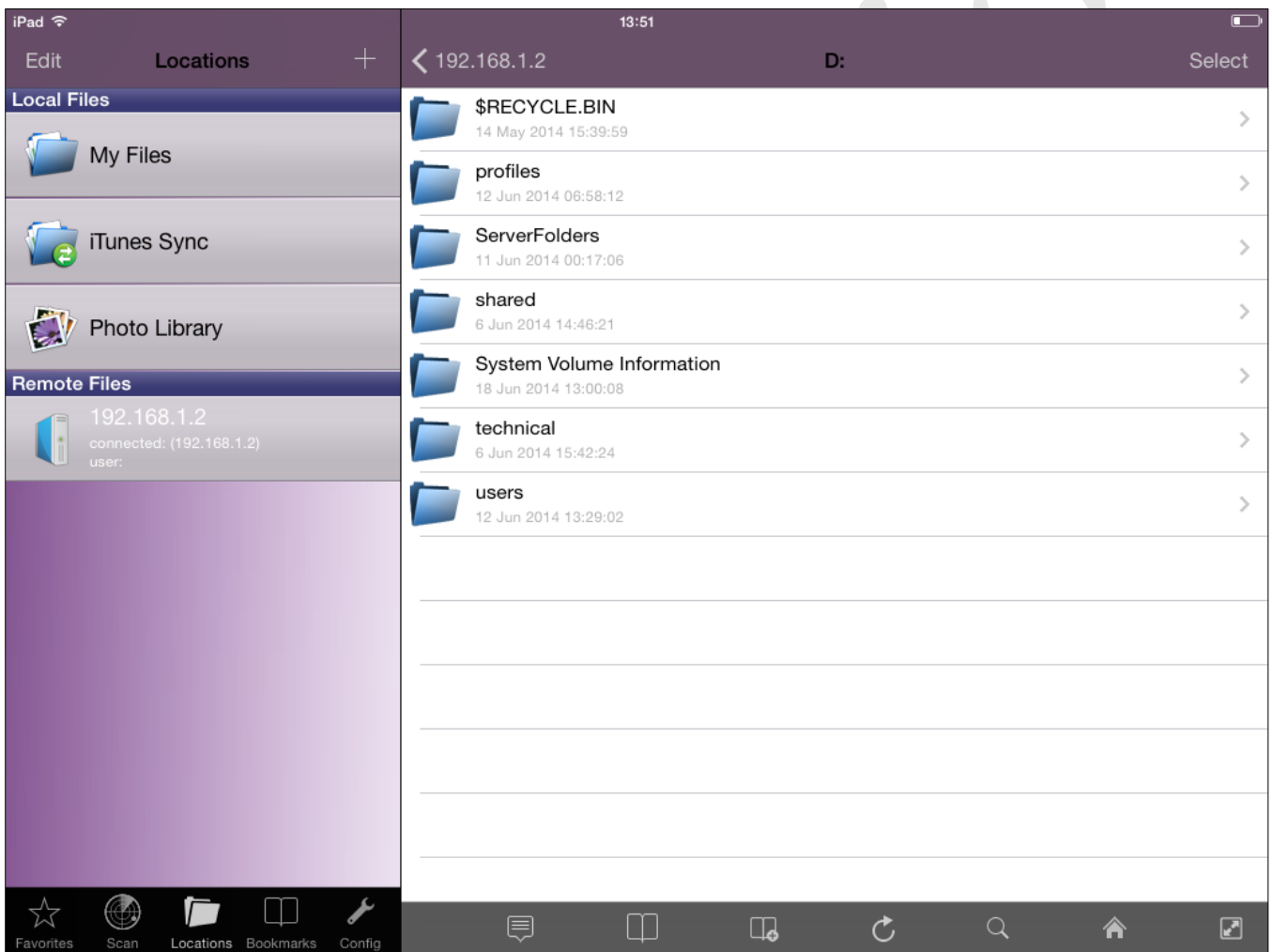

Figure 93: File Browser from Stratospherix on iPad

10.2 Using Cloud-based File Sync Services

Cloud-based file sync services such as Dropbox, Google Drive and Box provide an indirect route to accessing data on the server. They have a number of advantages: firstly, they are available on a wide range of portable devices including those running iOS, Android, Windows Phone and Blackberry. Secondly, they require minimal knowledge to get them up and running on the client devices. Thirdly, they are free or can be, depending on the amount of storage the organization requires. Installation of Dropbox on Windows Server is covered more comprehensively in section 9. USING DROPBOX WITH WINDOWS SERVER.

10.3 My Server App for Windows Phone

My Server is an official app from Microsoft for use with Windows Phone devices. It is really designed for managing Windows Essentials servers, but if the Windows Server Essentials Experience is installed on top of regular Windows Server it may be useful (see 12. WINDOWS SERVER ESSENTIALS EXPERIENCE). It is used for managing users, devices and alerts, analogous to a mobile version of the Essentials Dashboard. It also provides access to the shared folders, although some people find it fairly rudimentary.

10.4 Microsoft Remote Desktop app for iOS

Microsoft have an official app for iOS that enables a Windows server to be accessed remotely for administrative purposes. It is basically an RDP client and can be downloaded free of charge from the App Store.

Whilst working on a small screen with no physical keyboard imposes some restrictions, Microsoft have done a good job with this tool. To improve usability, the Remote Desktop app has a virtual keyboard and a screen zoom facility. Pressing down with a finger for a couple of seconds is equivalent to a right-hand button mouse click, which is very useful.
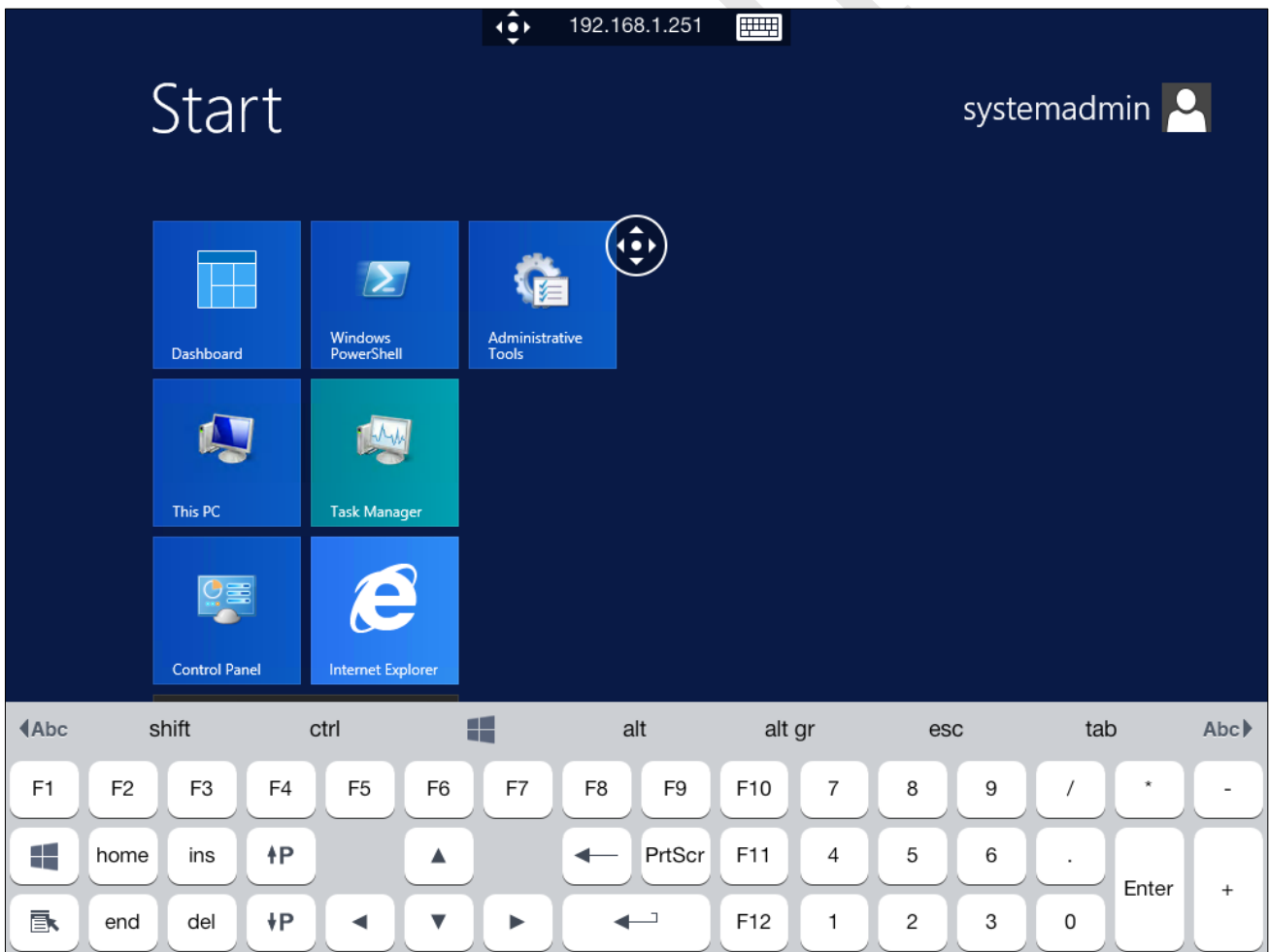

Figure 94: Microsoft Remote Desktop app running on iPad

10.5 Chromebooks

Chromebooks are an increasingly popular computing choice for many people. In essence a Chromebook is a laptop that only runs a browser; the key idea is that data is stored online on the cloud rather than as folders and files on the local computer or a network. The operating system – Chrome OS – is relatively minimalist compared to Windows or Mac OS X and this limits its capabilities.

Nevertheless, a Chromebook can be used in several different ways:

- A Chromebook can be used to remotely administer the server (see section 11.9 Remote Desktop for general information on this topic). To do so requires RDP client software; there are several examples available, but one that works quite well is *Chrome RDP* from Fusionlabs.net. This is available from the Chrome Store; it is a commercial application but the license is only US $9.99 (a 7-day trial version is available for those who want to try-before-they-buy).
- If a Cloud-based file sync service such as Dropbox, Google Drive or Box is being used with the server, then it will be possible to access the data from the Chromebook by logging in to the appropriate website. Of these services, Google Drive is possibly the most useful because of the tight integration with Chrome and the ability to edit files using Google Docs.
- To directly access the files and folders of the server in a more conventional manner, *File System for Windows* may be useful. This is a free download from the Chrome store and extends Chrome OS to understand the SMB protocols used in Windows networks.

11. HOUSEKEEPING AND MONITORING THE HEALTH OF THE SERVER

Servers need to be checked on a regular basis to ensure there are no problems and that they are in good health. Clearly some type of problems will be immediately apparent, for example if the server is powered down for whatever reason then nobody will be able to use it. But there are plenty of other things that need to be monitored; for instance: Has the backup completed successfully? Is the server running out of storage space? Additionally, there are some housekeeping tasks that need to be carried out on an occasional basis. This section also includes some ideas for making the server more convenient to work with for the administrator.

11.1 Disabling Internet Explorer Enhanced Security

By default, Windows Server has limited internet connectivity due to a feature called *Internet Explorer Enhanced Security* being enabled. There are good reasons why general internet browsing is not a good idea on a server, but not being able to access the internet freely makes things difficult, particularly in a small network. It is therefore useful to disable Enhanced Security.

Go into **Server Manager** and click **Local Server** to display the Properties for the server. On the right-hand side of the first panel is an entry for IE Enhanced Security Configuration; click where it reads **On** and the following dialog box will be displayed:
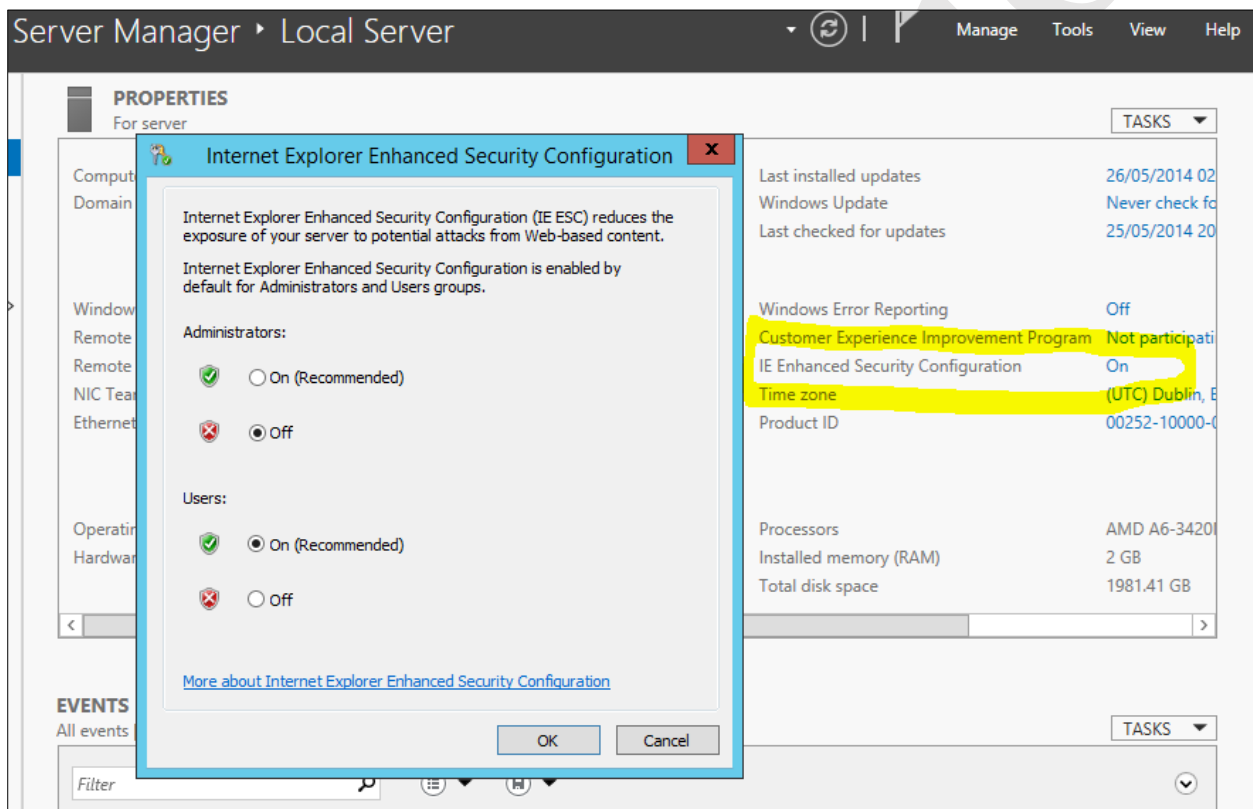

Figure 95: Internet Explorer Enhanced Security Configuration

Change the entry for Administrators to **Off** and click **OK**. It is not necessary to change the entry for Users as nobody other than an Administrator should ever have direct access to the server.

11.2 Checking the Event Logs

Windows Server maintains comprehensive records of the myriad events that take place during the operation of the server. Some of these are simply records of normal usage (user logs on, user logs off and so on), whereas others are generated in response to error conditions and can be used to help diagnose problems. The events are categorized into several main types and recorded in log files, which should be specifically checked in the event of problems and otherwise on an occasional basis.

To access the Event Logs, right-click the **Start** button and choose **Event Viewer**. A screen along the following lines is displayed (it may take some seconds to fully populate):
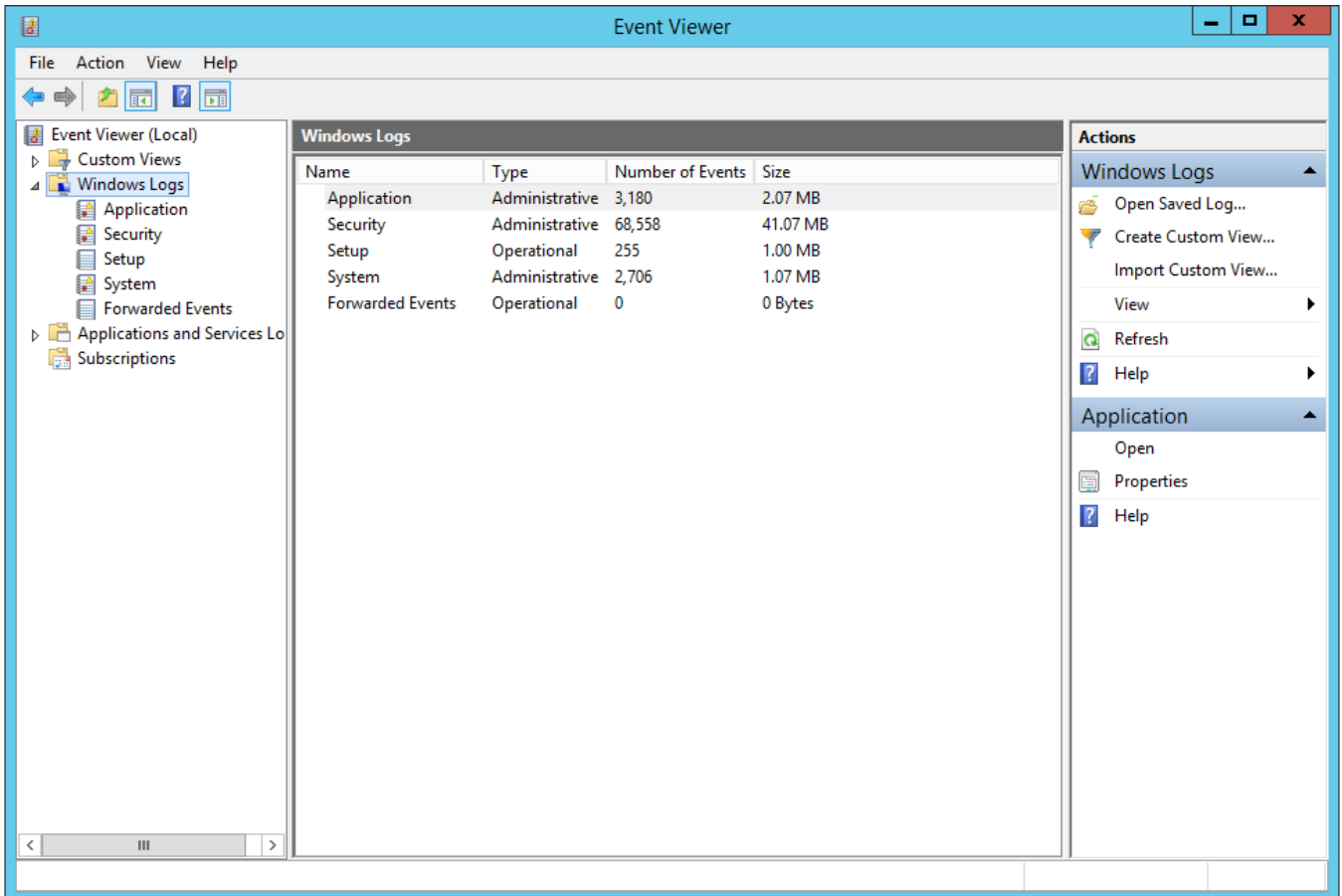
Figure 96: The Event Viewer

Some of the event logs are more useful than others. In the left-hand panel, expand the tree to display the **Windows Logs** section. There are five main logs: *Application*, *Security*, *Setup*, *System* and *Forwarded Events*. To view a particular log, click on it. Each event is categorized as an error, a warning or information, along with a timestamp plus a short description. The listing can be sorted by clicking on the heading for a column:
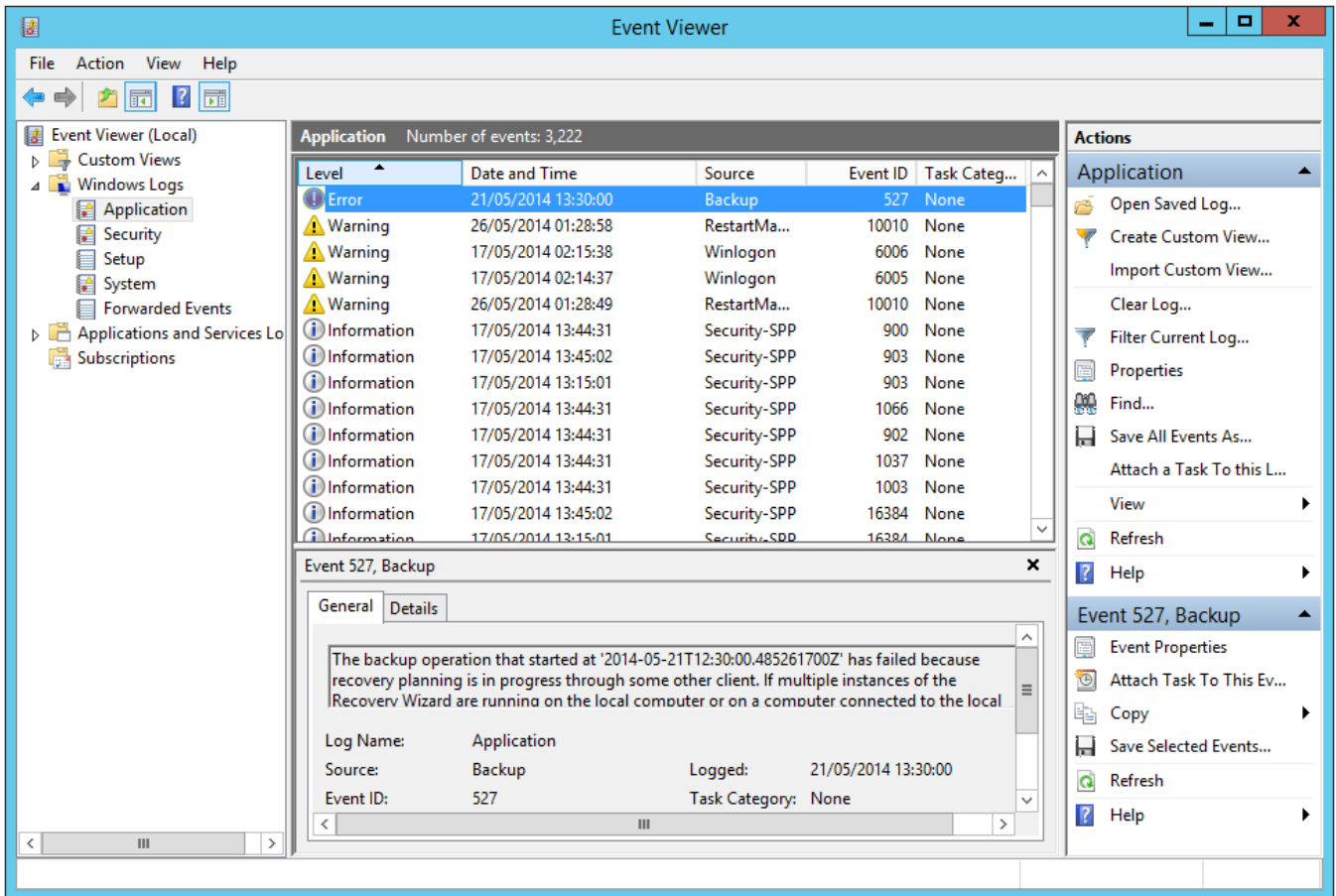
Figure 97: Example of an Event log

For most purposes the System and Application logs contain the most relevant information. If a server crashes or freezes – which is a very rare occurrence – there may well be clues in the System log. If there are suspected security violations, then the Security log may contain details. However, note that the Security log is very "noisy" and may generate thousands of events every hour.

The Event logs will eventually start to overwrite when they are full. If required, they can be archived as permanent records or to preserve evidence. To do so, right-click on an Event Log and from the pop-up menu choose **Clear Log**. A message is displayed offering three choices – click the **Save and Clear** button. In the resultant dialog box specify a name for the file: a good choice is its name plus the date e.g. *setup-12092017*.

11.3 Optimizing the Hard Drives

The hard drives on the server should be optimized (defragmented) on a regular basis to reduce file fragmentation and maximise performance. As with all modern versions of Windows, this can be scheduled to take place automatically.

Display the Start Screen and click the icon for **Administrative Tools**. On the resultant list of tools double-click the icon for **Defragment and Optimize Drives** to show the following panel:
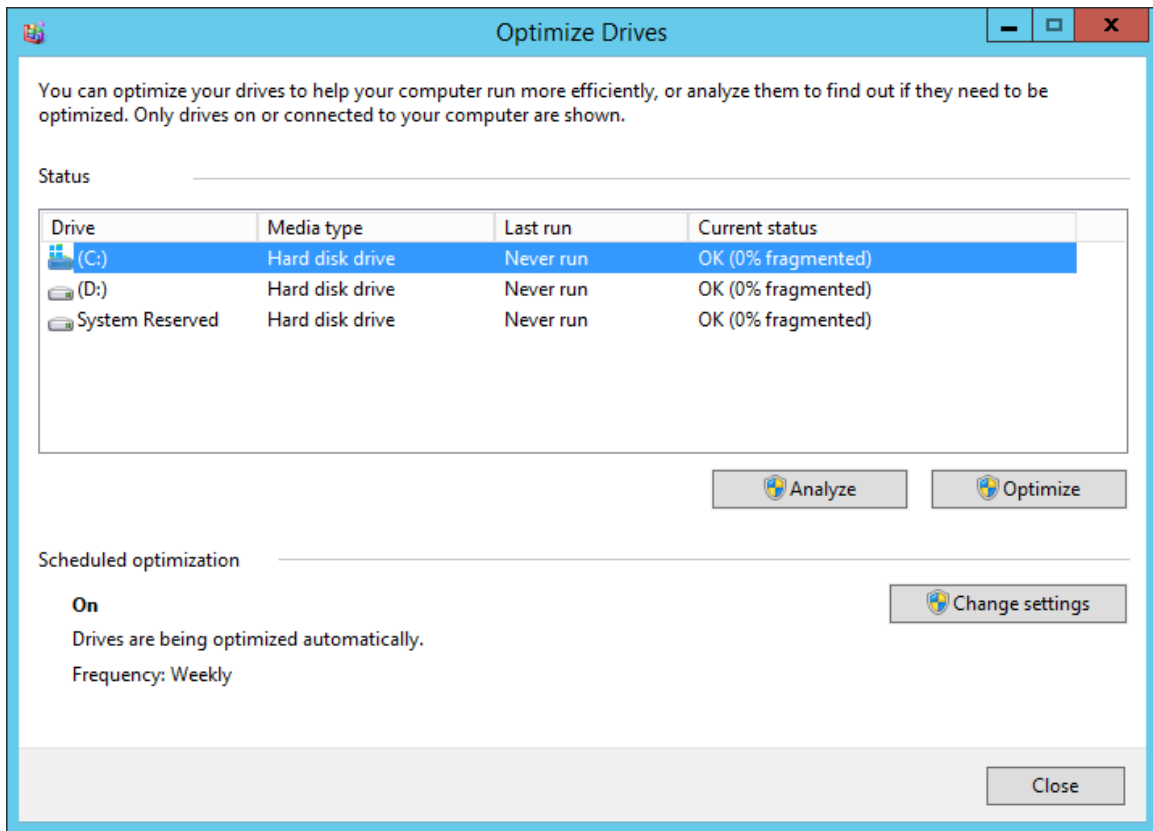

Figure 98: Optimize the hard drives

Towards the bottom left-hand corner it should read that Scheduled optimization is 'On' and that the drives are being optimized automatically on a weekly frequency. If this is not the case, click the **Change settings** button and adjust the settings accordingly.

Important: if the server includes any Solid State Drives (SSD's) then they should not be optimized – it is not necessary and will shorten their lifespan. Turn off scheduled optimization and optimize any remaining conventional hard drives on a manual basis every week or so. This can be done using the panel displayed above: highlight the drive, click **Analyze** to determine its status then click **Optimize** if necessary. Windows Server is usually smart enough to identify the SSD's itself, but it is worth checking in case it has not done so.

11.4 Applying Windows Updates to the Server

It is important to check for and apply the updates to Windows Server that Microsoft makes available on a regular basis. Such updates may provide improved or additional functionality, but more typically address security issues that could compromise the system. On regular desktop and laptop computers, Windows updates are often applied automatically; however, it is suggested that automatic Windows updates are not enabled on servers. The reason for this is to ensure total control over the process and stop the risk of the server rebooting of its own accord following an update. Also, it is suggested that updating is done out of hours so as to avoid any disruption to service, perhaps on a monthly basis.

Go into **Control Panel**. If it is currently set to view by Category, change it to view by **Large Icons**. Click the **Windows Update** icon followed by the **Turn on Automatic updates** button, which will force the system to check for updates. After a couple of minutes, the screen will refresh and display a message that *"nnn important updates are available"* (where *nnn* is the number of such updates). Click the message and on the next screen click the **Install** button at the bottom of the screen. The updates will download and install; this may take some time and may necessitate the server having to restart to complete the process.

Once the server is up-to-date, go back into Windows Update and click **Change Settings**. Set it to a value other than 'Install updates automatically' and click **OK**.
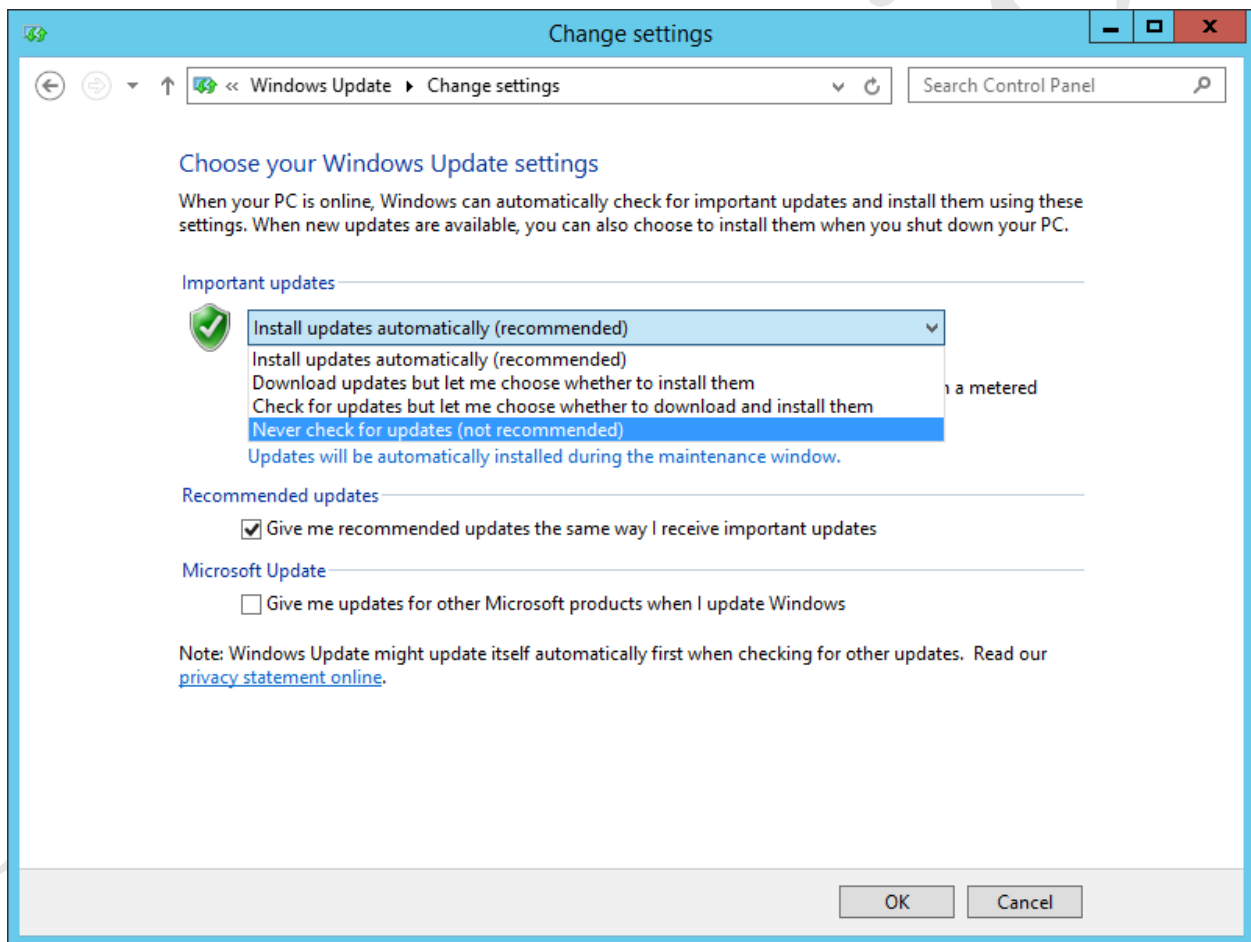

Figure 99: Windows Update settings

11.5 Shutting Down and Restarting the Server

The server is usually left running continuously but there will be occasions when it needs to be restarted (e.g. following updates) or shutdown (e.g. to add hardware). To do so:

Right-click the **Start** button and choose **Shutdown** or **sign out**. Choose the desired option form the list. You will be prompted to enter a reason for shutting down the server – choose one from the drop-down menu and click **Continue**.

11.6 Install Server Management Software

Many first-tier server suppliers provide some form of management software to help monitor and manage the health of the server hardware e.g. the RAID sub-system, operating temperatures etc. For instance, Dell have a program called *OpenManage*. This should be installed on the server once the main build is complete. It should be checked on a regular basis, as it may provide valuable information about the status of the hardware and the RAID array. Some of the management packages can be configured to generate email alerts in the event of problems, which is useful.
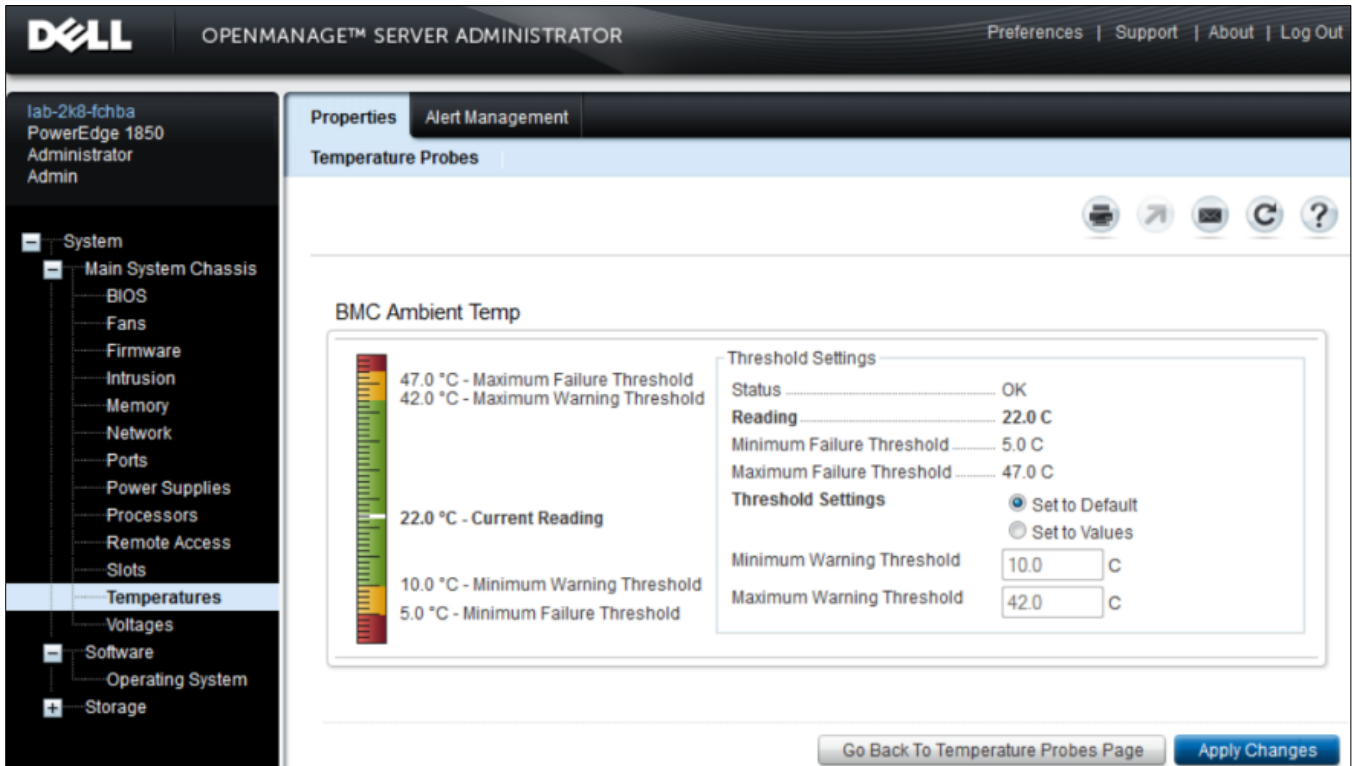
Figure 100: Example of server management software

11.7 Install Anti-Virus/Anti-Malware Software

Servers are susceptible to viruses and malware in the same way that regular Windows computers are and for this reason an anti-virus program should be installed on the server at the earliest opportunity. By and large the standard anti-virus clients intended for desktops and laptops do not work or are otherwise unsuitable; rather, special server or 'business' variants are required. Most of the major vendors offer suitable software and some examples in no particular order are: *AVG File Server Edition*; *Microsoft System Center 2012 R2 Endpoint Protection*; *Avira Server Security*; *Symantec Endpoint Protection*. Most of the products in this category feature management consoles that allow client computers to be managed from the server, reviewing their status, initiating downloads, scans and so on.

Malwarebytes is a highly regarded piece of software for protecting against and cleaning up malware on computers. It will often sort out the 'nasties' that even the best anti-virus software misses, providing a valuable second line of defence. It works well on Windows Server and is available in both free and paid versions. The paid version is very low cost and has the advantage that scans can be scheduled to take place automatically, as opposed to run manually. It is best obtained by downloading it directly from the *www.malwarebytes.org* website.
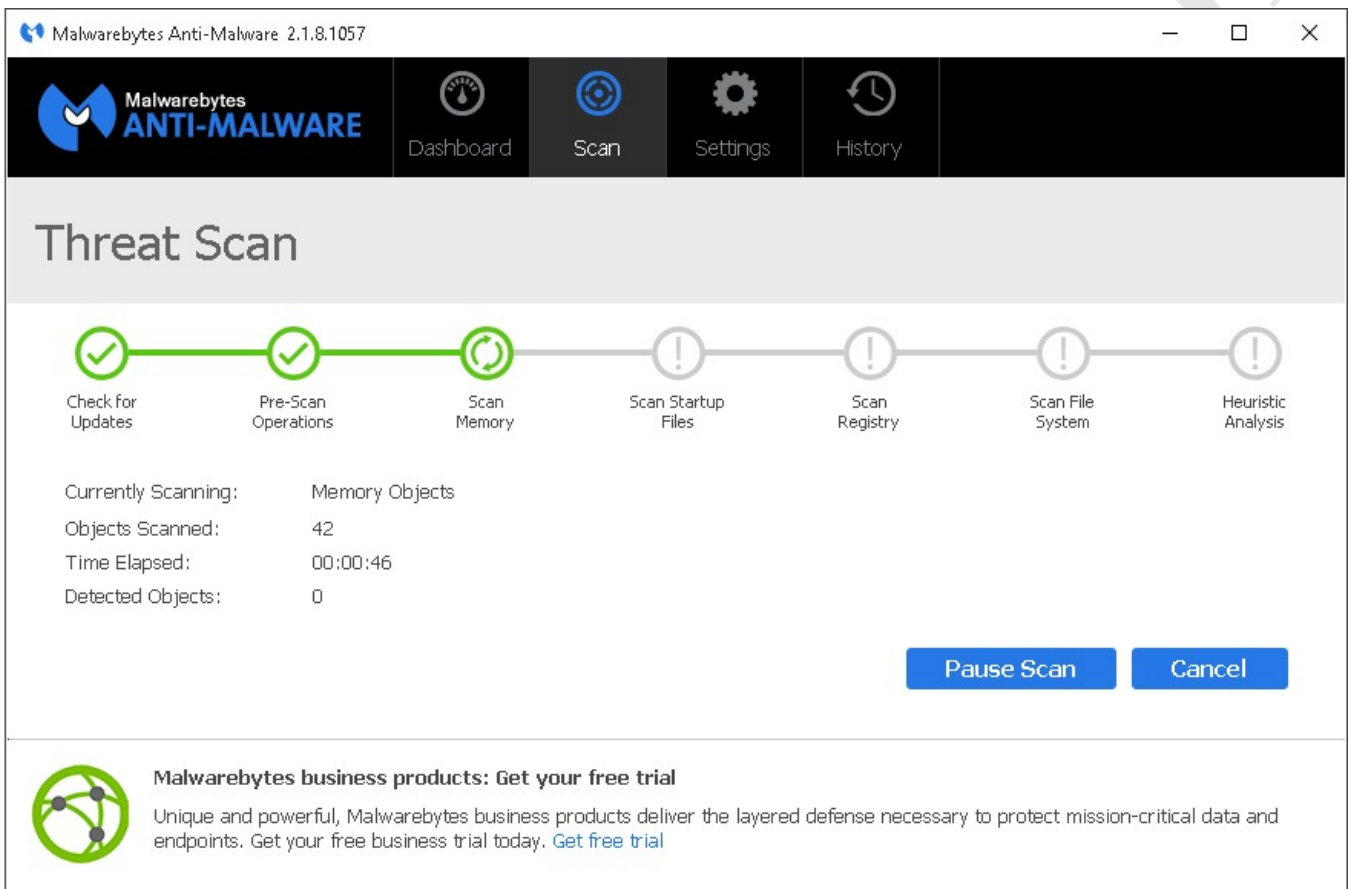
Figure 101: Main Malwarebytes scan screen

11.8 Create Alternative Administrator Account(s)

For a variety of reasons, it is not good practice to use the main Administrator account any more than is strictly necessary. Firstly, in case the account accidentally gets locked or disabled. Secondly, it can be confusing when using Windows 7 clients, which have a built-in local account of the same name. Instead, an alternative administrative account should be setup and, once the server has gone live, this is the one that should be normally used. This could be called *systemadmin*, for instance. To create it:

- Go into **Administrative Tools** and choose **Active Directory Users and Computers**
- Find *Administrator* in the *Users* section
- Right-click on *Administrator* and choose **Copy**
- Complete the dialogue box and create a new user called *systemadmin*. Set the password to the same as that of the *Administrator*
- Having created the user, go into **Properties** and specify any drives, scripts, settings as used by the regular Administrator account

Suggestion: in order to install some software and printers on client PCs, administrative rights may be required. If you wish users to be able to do these things themselves, setup another administrative account, perhaps called *userinstaller*. Do not use the same password as the main Administrator/Systemadmin accounts and do not bother with any profile information. The details of this account can then be passed to selected users.

11.9 Remote Desktop

When installing Windows Server it is necessary to use a standard monitor, keyboard and mouse (usually. Some manufacturers have workarounds). However, once the server is up and running these can be dispensed with and it can be run in so-called *headless* mode. To access it for support purposes, the *Remote Desktop* capability is used. This has several advantages: firstly, the server can be accessed using any computer on the network and it is not necessary to have physical access to the server, which may be a consideration if it is situated in a secure, locked or otherwise inaccessible location. Secondly, dispensing with a physical screen, keyboard and mouse saves space and possibly a small amount of electrical power. Thirdly, in some small organizations the server may have to be physically located in a general purpose office and not having a keyboard and screen will reduce the temptation for staff to treat it as just another computer.

During installation, Windows Server should have automatically enabled Remote Desktop. This can be verified (or if necessary, corrected) by going into **Control Panel** and double-clicking the **System** icon. Click **Remote Settings** and the Remote tab of System Properties will be displayed. Make sure that the **Allow remote connections to this computer** option is selected. All members of the Administrators group have access to the Remote Desktop and it is not necessary to use the **Select Users** button. Click **OK**.
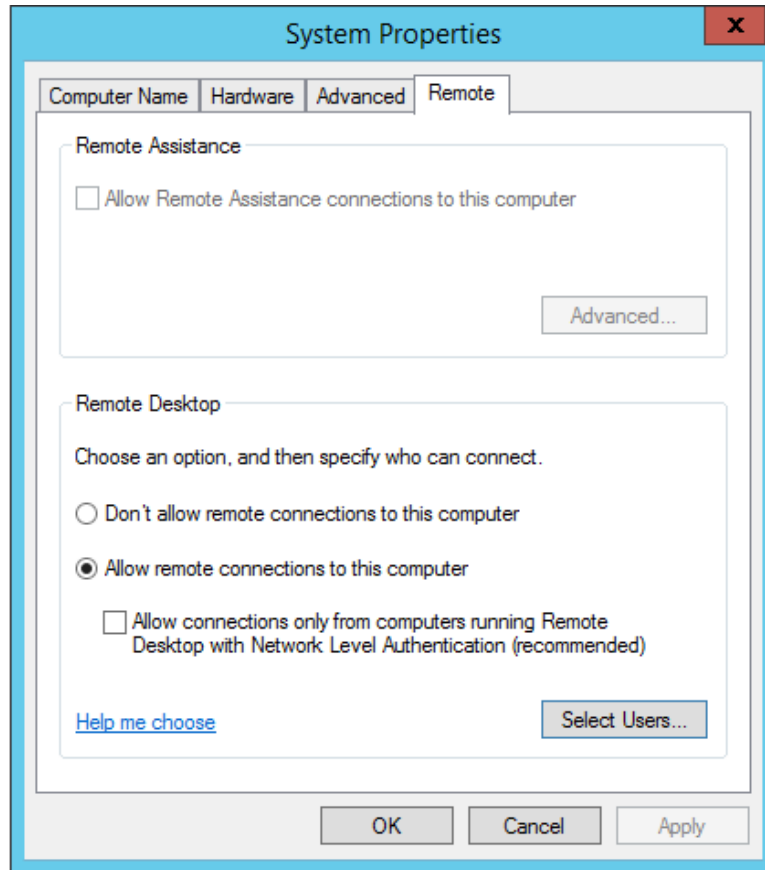
Figure 102: Enabling remote connections on the server

Test the facility by going to a computer on the network and launching the *Remote Desktop Connection* program, which is a standard part of Windows. Enter the name of the server or its IP address. Provide logon credentials i.e. the name of an Administrative account and its password. Once everything has been tested, the physical screen, keyboard and mouse of the server can be dispensed with.

11.10 Task Manager and Resource Monitor

Task Manager and *Resource Monitor* are built-in tools that can be used to help identify bottlenecks on servers that have performance problems, such as running slowly. Whilst the diagnosis and resolution of problems is a specialist topic that goes outside of the remit of this guide, they do provide useful information that most system administrators will find helpful. For instance, if a bottleneck with the network adapter was identified then it might be an option to add a second and 'team' it as described in 13.2 Multiple Network Adapters (NIC Teaming).

Many users will be familiar with the Task Manager as it is common to all versions of Windows. To start it, right-click on the **Taskbar** and choose **Task Manager** from the pop-up menu; it may appear as a blank panel, in which case click the More details button in the bottom left-hand corner to display the following screen:
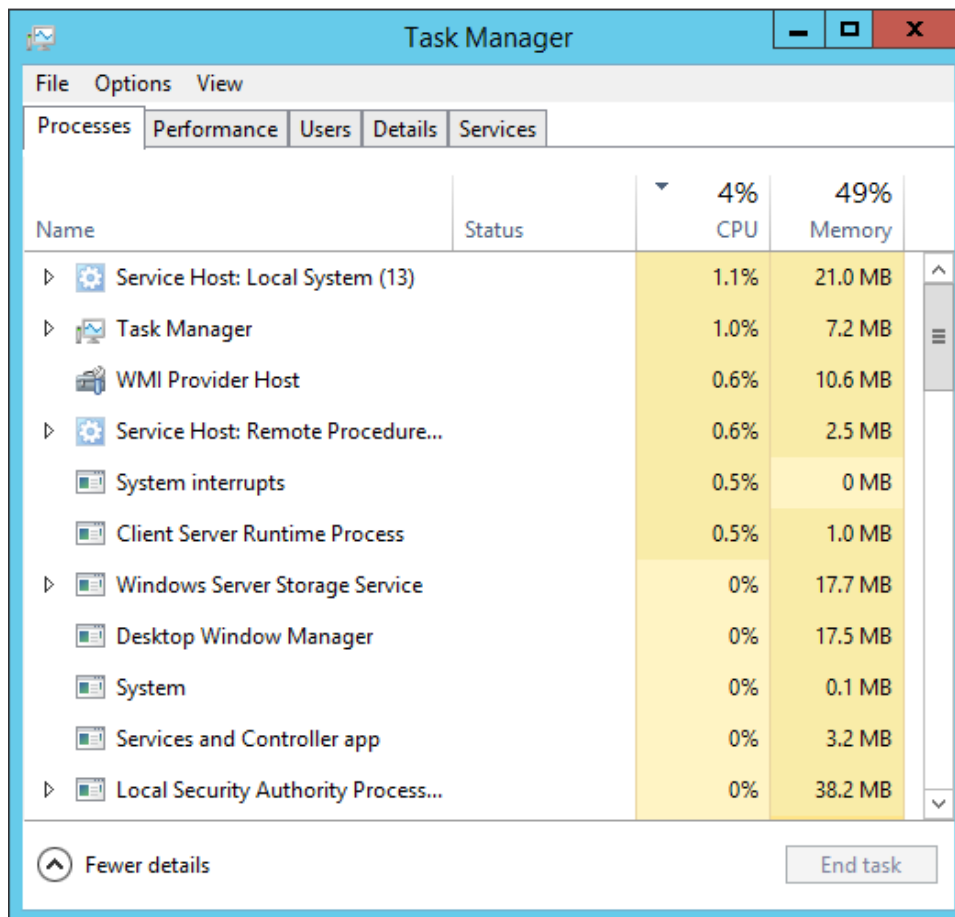
Figure 103: Task Manager Processes tab

On this *Processes* tab, Task Manager provides useful information about how busy the server is and how much memory is being used. For instance, if a process is hogging the CPU or memory it can be identified and, if appropriate, terminated.

Clicking on the **Performance** tab provides information in a graphical format for CPU, Memory and Ethernet (i.e. the network connection), and is useful for monitoring what is happening with the server:
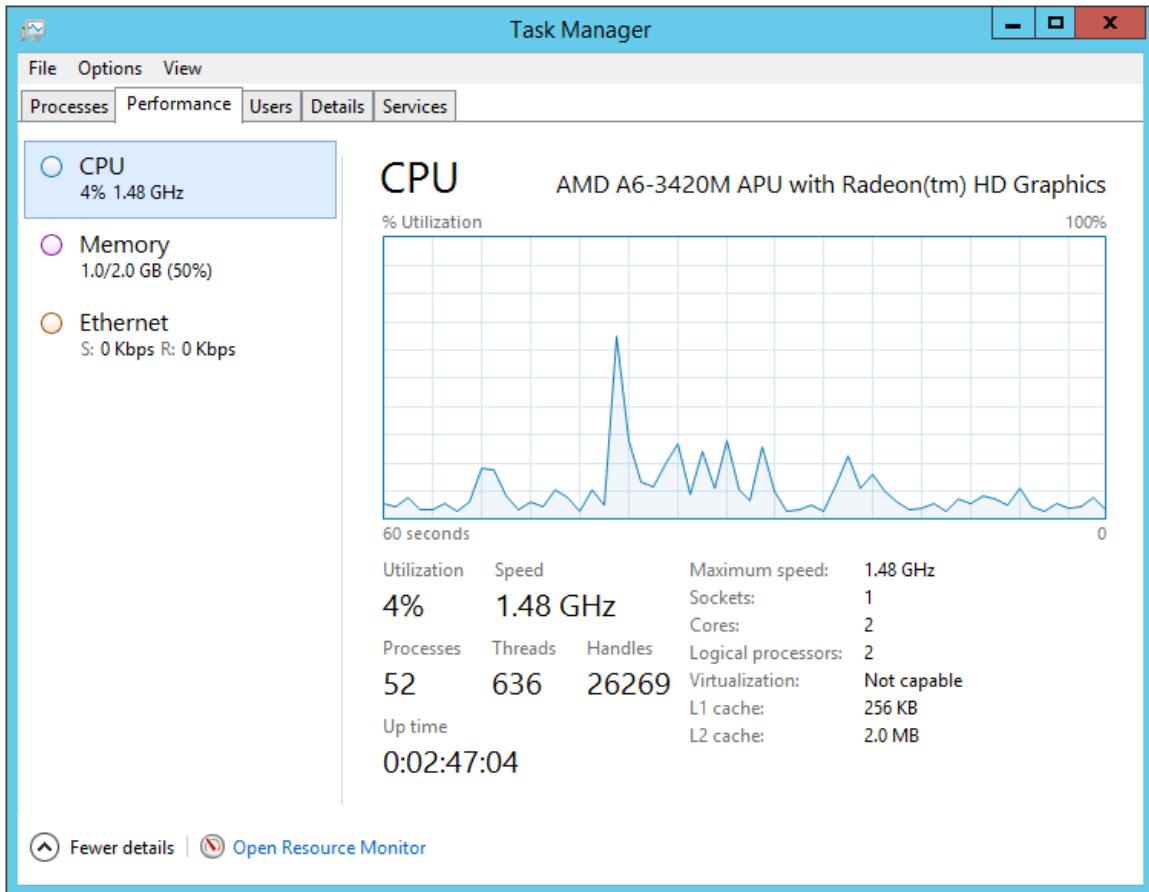
Figure 104: Task Manager Performance tab

More detailed information can be obtained by clicking the **Open Resource Monitor** link in the bottom left-hand corner of the Performance tab screen. This displays the following screen, which can be thought of as the 'Task Manager on steroids'. Resource Monitor can be invoked from Administrative Tools or directly from the Start Screen (when expanded to display all icons):
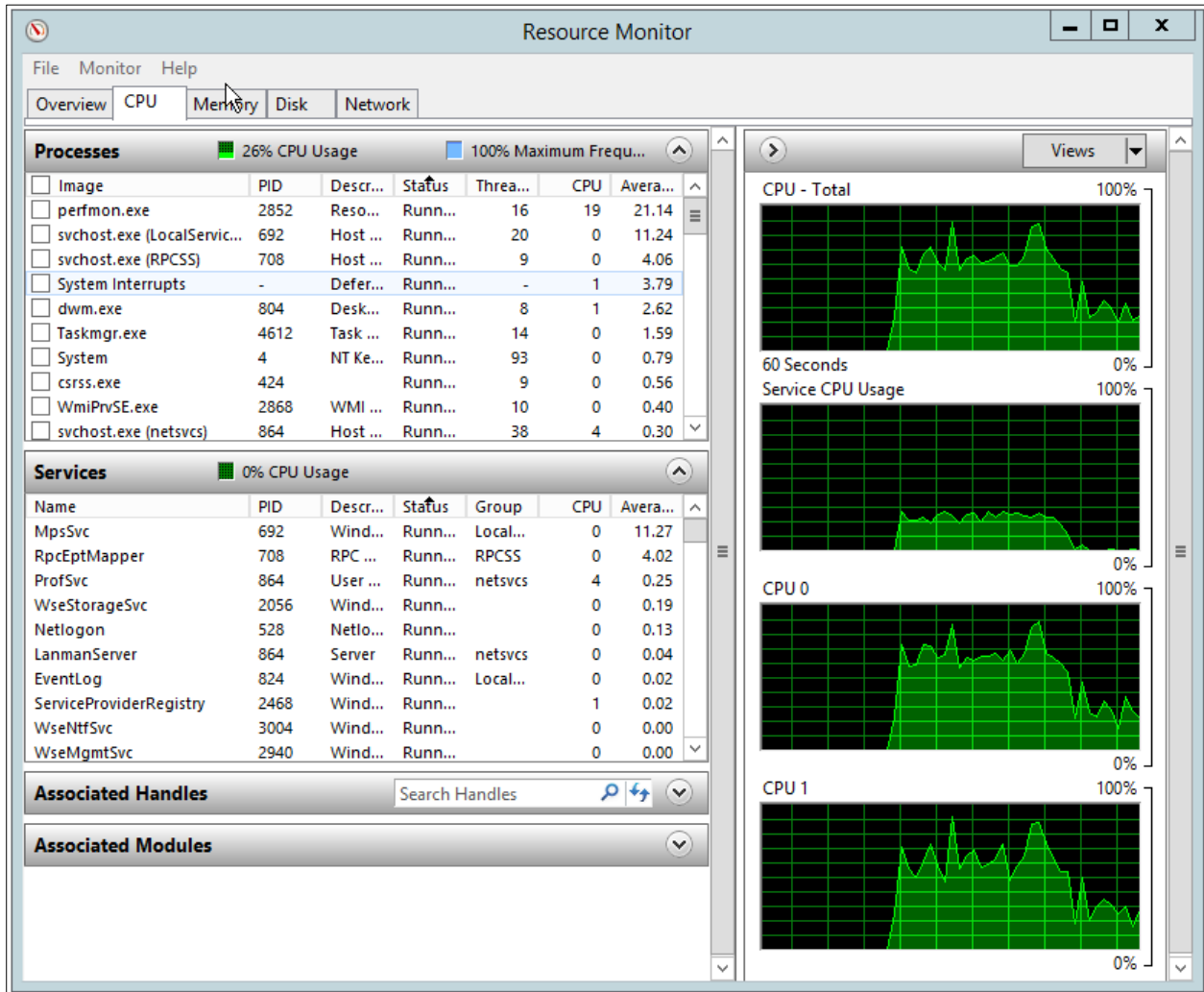
Figure 105: Resource Monitor screen

12. WINDOWS SERVER ESSENTIALS EXPERIENCE

Windows Server Essentials 2012 R2 is an edition of Windows Server specifically aimed at small businesses that do not have in-house IT support. It includes a simplified user interface, designed to make it easier to configure and manage the server. However, beneath the hood it is a regular version of Windows Server and the simplified interface – known as the *Windows Server Essentials Dashboard* – can also be added to the standard versions of Windows Server, where it is known as the *Windows Server Essentials Experience*. Why would you wish to do this? There are three possible reasons. One reason is that Window Server Essentials is restricted to a maximum of 25 users. If an organization outgrew it they would have to move to a regular version of Windows Server, but they may wish to retain the methods of working and systems management that they are accustomed to. The second reason is that the Windows Server Essentials Dashboard is easier to work with than the regular Windows Server tools for everyday tasks. It is thus useful for organizations with limited IT resources. The final reason is that you might just prefer to use it.

12.1 Installing Windows Server Essentials Experience

Launch **Server Manager** and click **Manage** followed by **Add Roles and Features**. Choose **Role-based or feature-based installation** and click **Next**. Select the destination server - there may only be one of course - click **Next**. Tick **Windows Server Essentials Experience** on the subsequent screen, followed by **Next**. A message about the requirement for additional features is displayed – click the **Add Features** button to proceed:
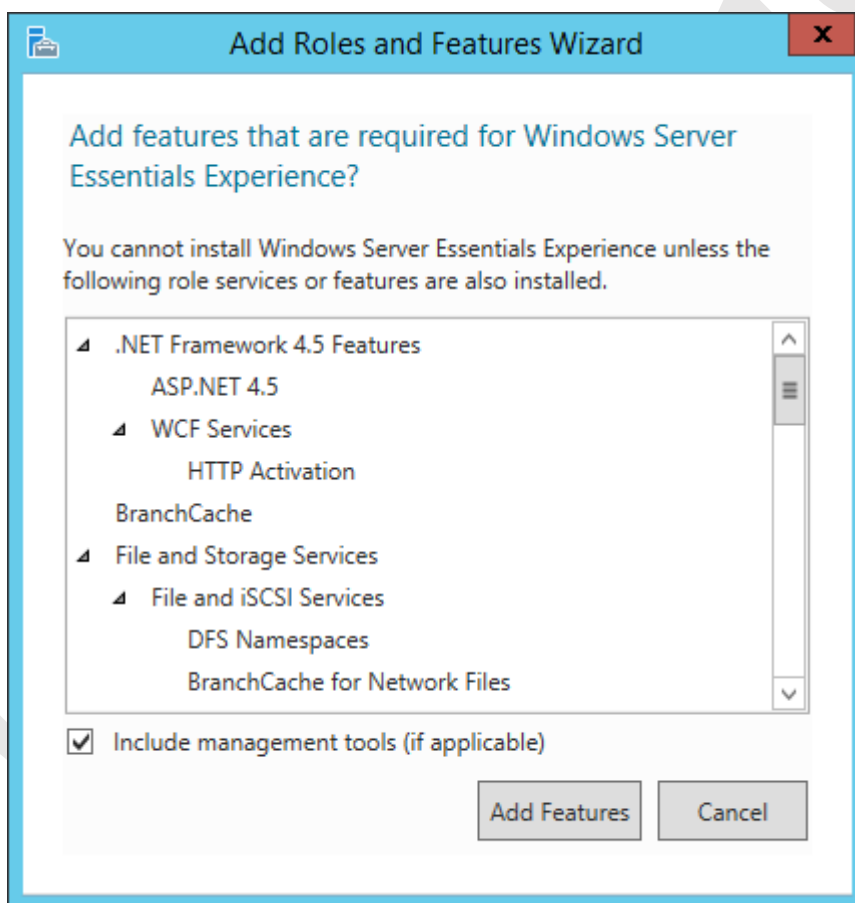
Figure 106: Add Roles and Features Wizard

Click **Next** on the subsequent screens. After a while a screen about the Web Server (IIS) is shown – click **Next** on this, too. A screen to confirm the various options is displayed – tick the **Restart the destination server automatically if required box** then click **Install**.

The installation will run for a number of minutes and the server may restart during this time. When it is completed, login and go to **Server Manager**. On the Dashboard there will be a notification flag to the effect that additional configuration work is required – click the message to start the process. After a short while a screen entitled *Configure Windows Server Essentials* is displayed; click the **Configure** button. The configuration process will then take a further several minutes to complete.

A new icon – simply called *Dashboard* – will have been placed on the Desktop of the server. Note that this is the Dashboard from Windows Server Essentials and quite separate from the regular Windows Server Manager Dashboard. Double-clicking it will display the standard console for managing an Essentials server.

12.2 Windows Server Essentials Dashboard: Quick Overview

Double-click the *Windows Server Essentials Dashboard* icon to display the standard console for managing Essentials (it may take a short while to load):
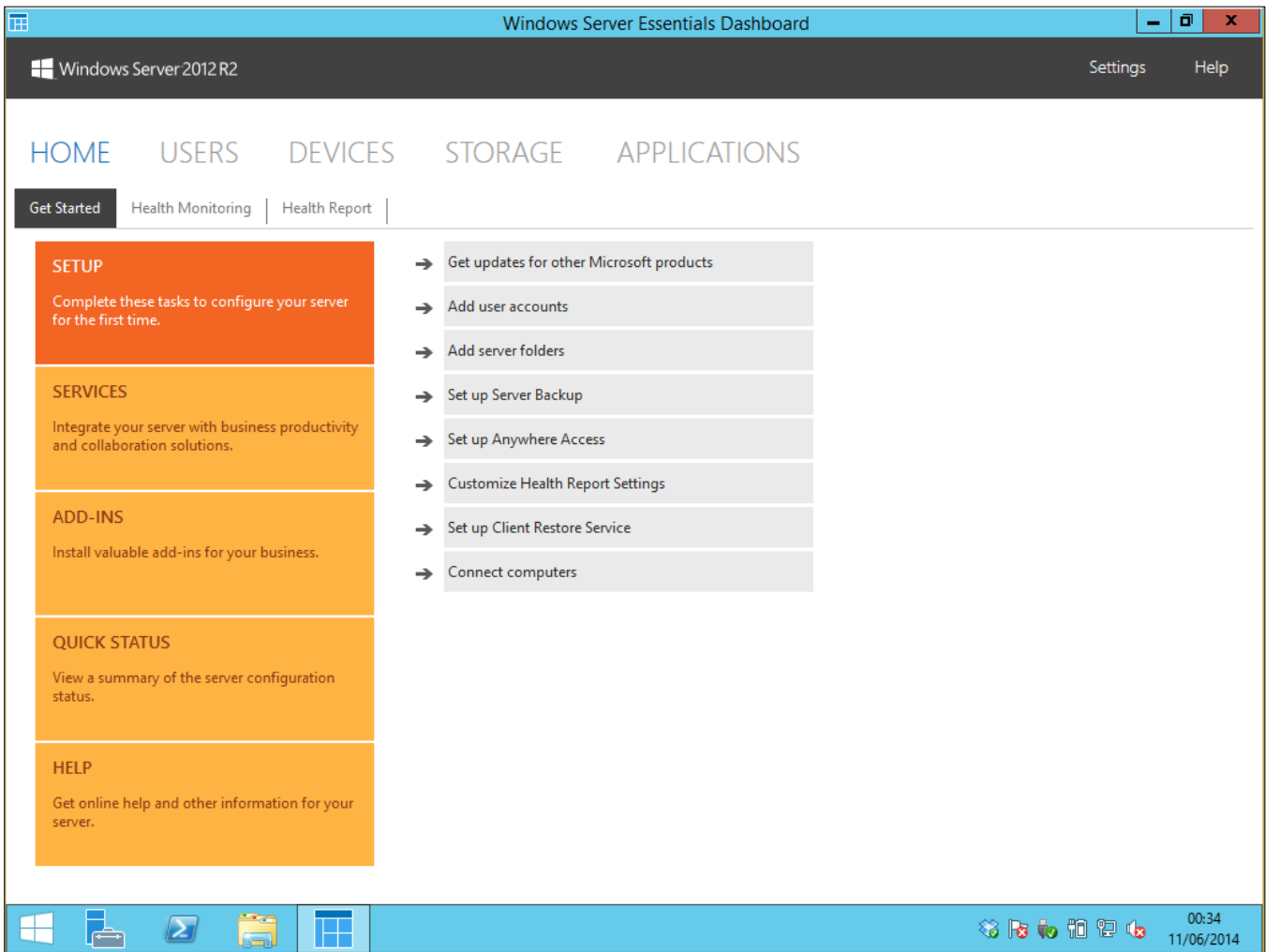
Figure 107: Windows Server Essentials Dashboard

The Dashboard is organized into a number of sections: USERS, DEVICES, STORAGE and APPLICATIONS. Each of these displays the status and characteristics of that topic and lists a number of clickable tasks pertaining to it. The HOME page – displayed above – is structured in a way to help setup the server using a checklist of tasks to be completed: *Add user accounts*, *Add server folders*, *Setup Server Backup* and so on. If you have already performed some of these activities using the standard Windows Server tools, then Essentials should correctly pick up the existing information.

At the top of the screen is a status section and there may sometimes be warning or error messages indicated (see example below). If there are messages, click in the area to expand and then click on them for a more detailed screen. It is necessary to make a judgement about the seriousness of any messages. Generally speaking, they will be fairly trivial and can safely be ignored, often relating to matters such as automatic updates not being switched on. If the server only has a single disk drive there will be a message saying that the data folders are on the same drive as the operating system, which can also be ignored (unless of course your system is supposed to have more than one drive in it, in which case there is a problem).
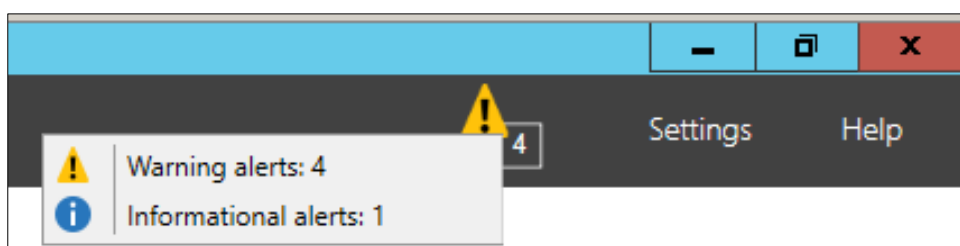
Figure 108: Messages on the Dashboard

12.3 Managing Users from the Windows Server Essentials Dashboard

One of the most common tasks on an operational server is managing users so by way of example we will look at how this is done using Windows Server Experience Essentials. Launch the *Windows Server Essentials Dashboard* and click on the *USERS* tab to display the following screen:
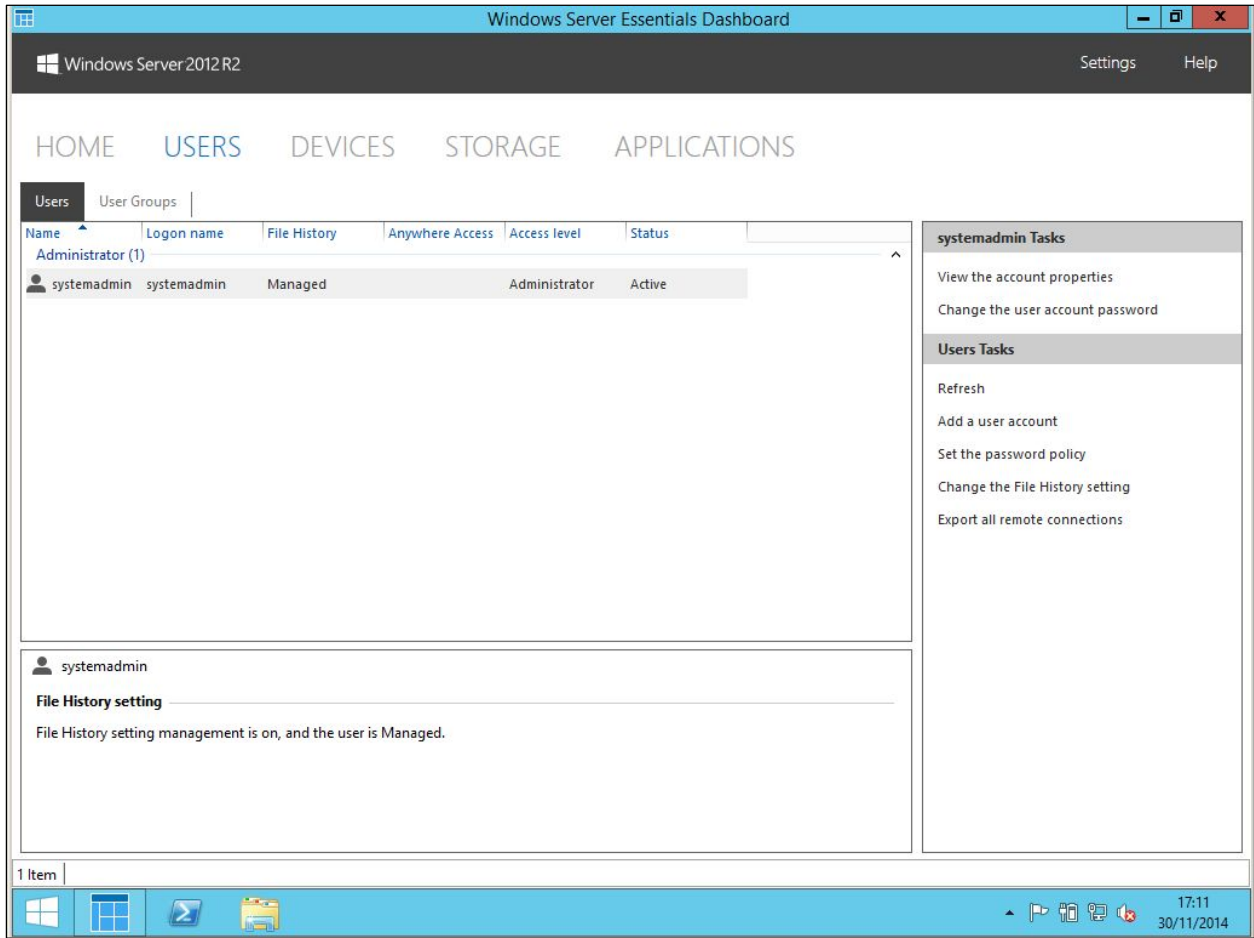
Figure 109: Users tab on the Windows Server Essentials Dashboard

On the right-hand side of the screen is a panel called *User Tasks* - click **Add a user account** to display the following form:

Figure 110: Adding a new user account

Enter the user's first and last names and Essentials will propose a *User account name* (i.e. logon name) of the two concatenated together. However, you might want to simplify things and here we have changed the suggested name of *LouiseBookman* to *louiseb*. If you take this approach, be sure to be consistent for all users. Enter a password according to the policy defined above and confirm it. There are two possible levels of access for users: *Standard* or *Administrator*. As we already have an Administrator account, all users should be Standard users. Try to avoid the mistake of making people administrators simply because they are important within the organization – this is about their role on the network, note their role within the organization. Click **Next**.

The subsequent screen specifies what shared folders the user should have access to. There will always be at least one folder available – a built-in folder called *Company* is created during the installation of Windows Server Essentials Experience and the system is proposing *Read only* access to it; change it to the more useful **Read/Write** and click **Next**. Incidentally, the *Company* folder has most likely been created on the C: drive as a subfolder within one called *ServerFolders*. Unless you have a single drive system this is not an ideal location and can be moved to another drive using the Windows Server Essentials Dashboard by clicking on the *STORAGE* tab followed by **Move the folder**.
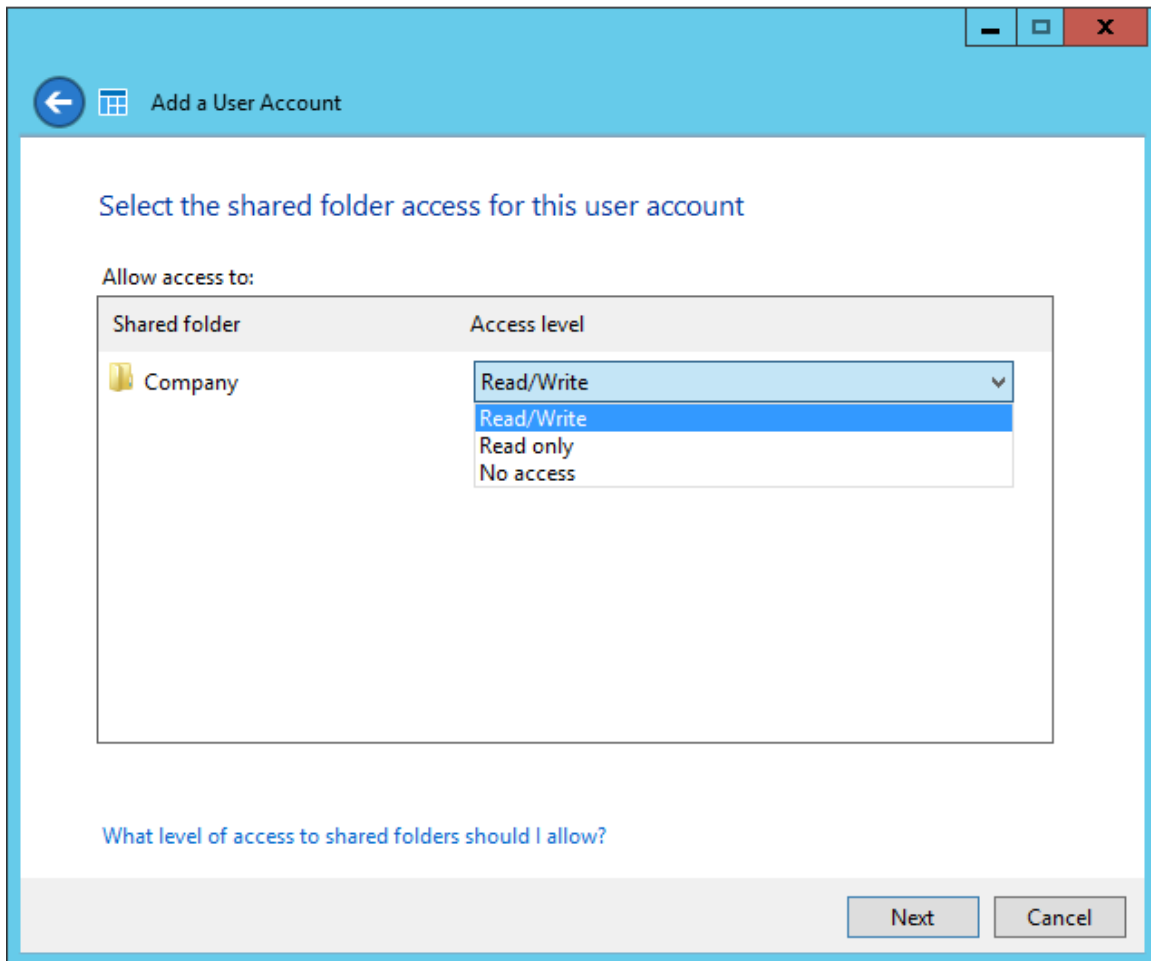
Figure 111: Specify access to folder

The subsequent panel is concerned with remote access i.e. being able to access the server from outside the office over the internet, referred to as *Anywhere Access*. One thing worth knowing is that whereas configuring remote access for Windows Server can be quite complicated, it is a lot easier to do so using the Essentials Experience. The defaults are fine so just click **Create Account**.
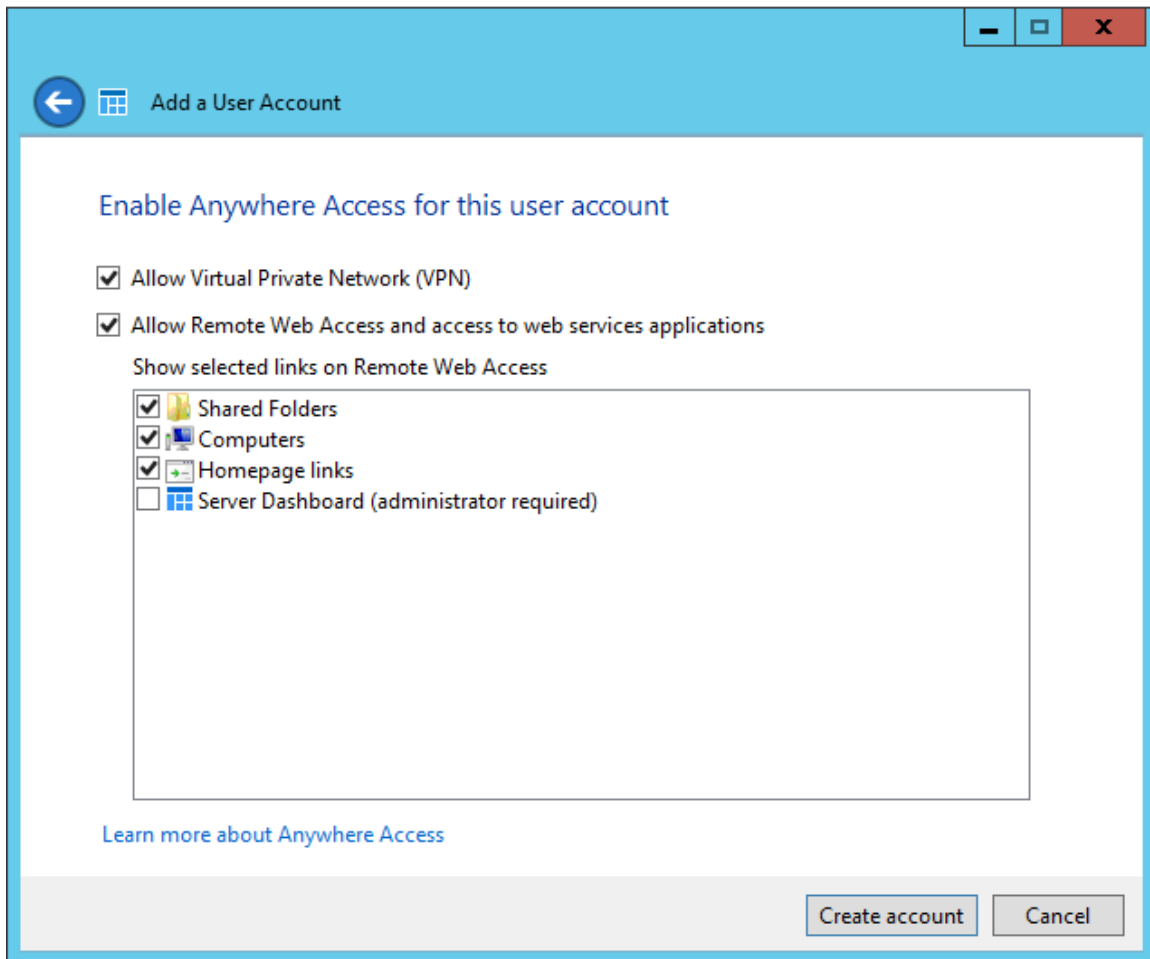
Figure 112: Specify Anywhere Access for user

Essentials will process for a few seconds and then display a confirmation that the user has successfully been created. Check the details then click **Close**.

12.4 Making Changes to Users

To change a user's password, go into the Dashboard and click the **USERS** tab. Click on the user's name to highlight it. On the right-hand panel click **Change the user account password**. Enter the old and new passwords and click **Change Password**.

To delete a user account, go into the Dashboard and click the **USERS** tab. Click on the user's name to highlight it. On the right-hand panel click **Remove the user account password**. Acknowledge the message about the implications of doing so.

To temporarily disable a user – for instance, because they are going on extended leave or because of a disciplinary or security issue - go into the Dashboard and click the **USERS** tab. Click on the user's name to highlight it. On the right-hand panel click **Deactivate the user account**.

13. MISCELLANEOUS TOPICS

13.1 Installing DHCP

If the server is being installed in a small business environment, then it is possibly the case that there is an all-in-one router providing the DHCP service. However, if this is not the case then it will be necessary to install DHCP on the server itself, described below.

Go into the Server Manager and click **Manage**. Choose **Add roles and features**. Click **Next** on the *Add Roles and Features Wizard* and on the resultant screen choose **Role-based or feature-based installation** followed by **Next**. On the next screen make sure the server is highlighted (we are assuming there is only one) and click **Next**. On the list of possible features click **DHCP Server**. A message will appear asking if additional (required) features should be added. Make sure that the **Include management tools (if applicable)** box is ticked and click the **Add Features** button.
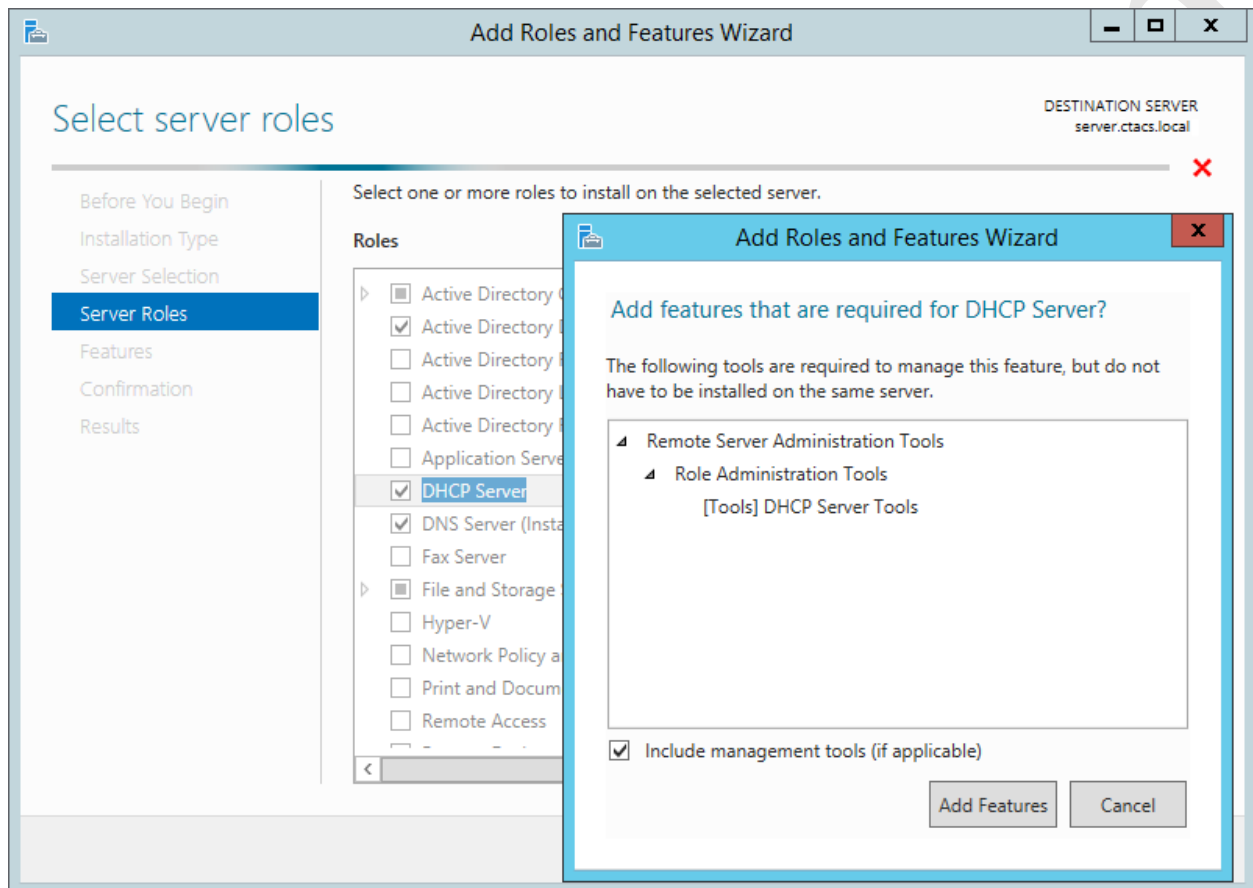
Figure 113: Choose DHCP Server

Carry on clicking **Next** on each subsequent screen. Eventually a confirmation screen is displayed; tick the **Restart the destination server automatically if required** box followed by **Yes** to the message:
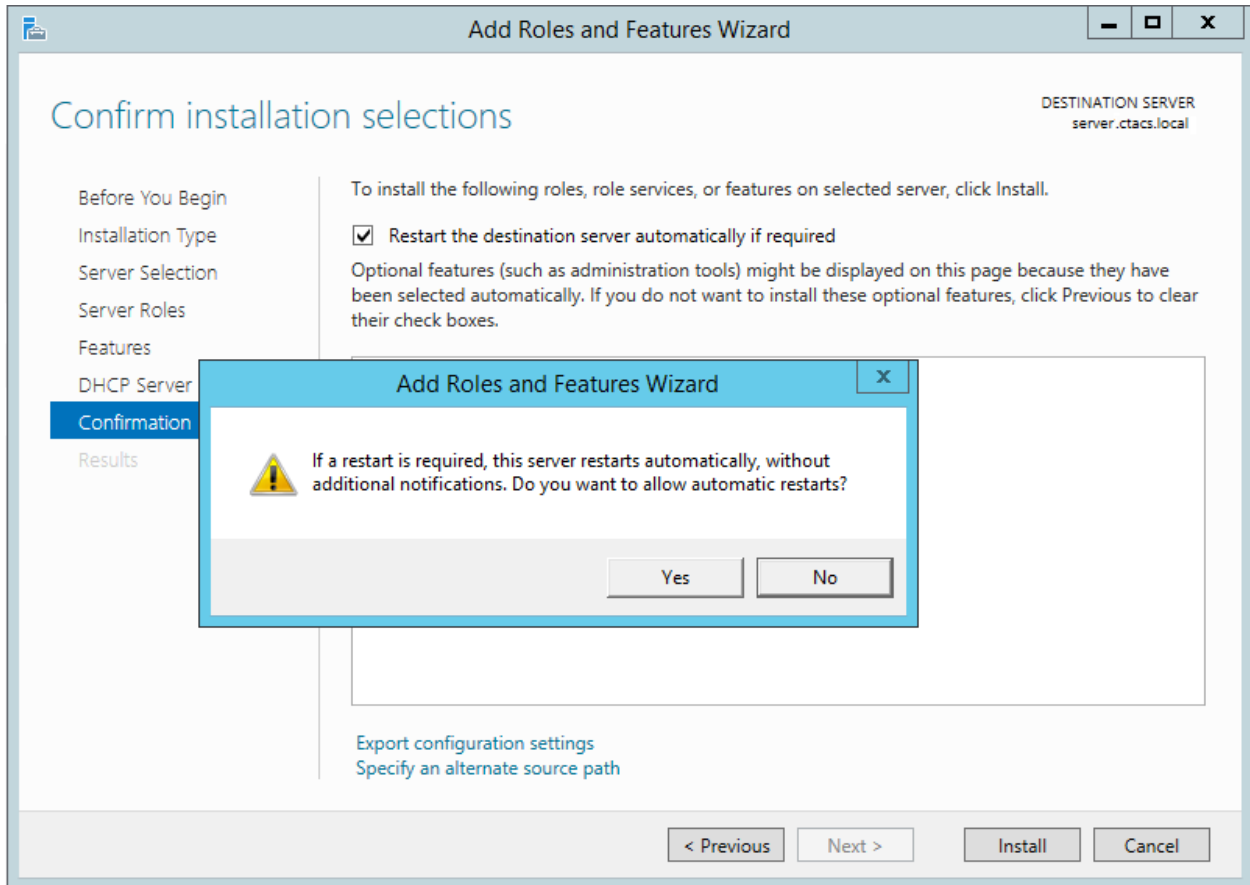
Figure 114: Reminder about automatic restarts

Finally click the **Install** button. Whilst the process is running, which may take several minutes, a progress screen is shown; when complete, click **Close**:
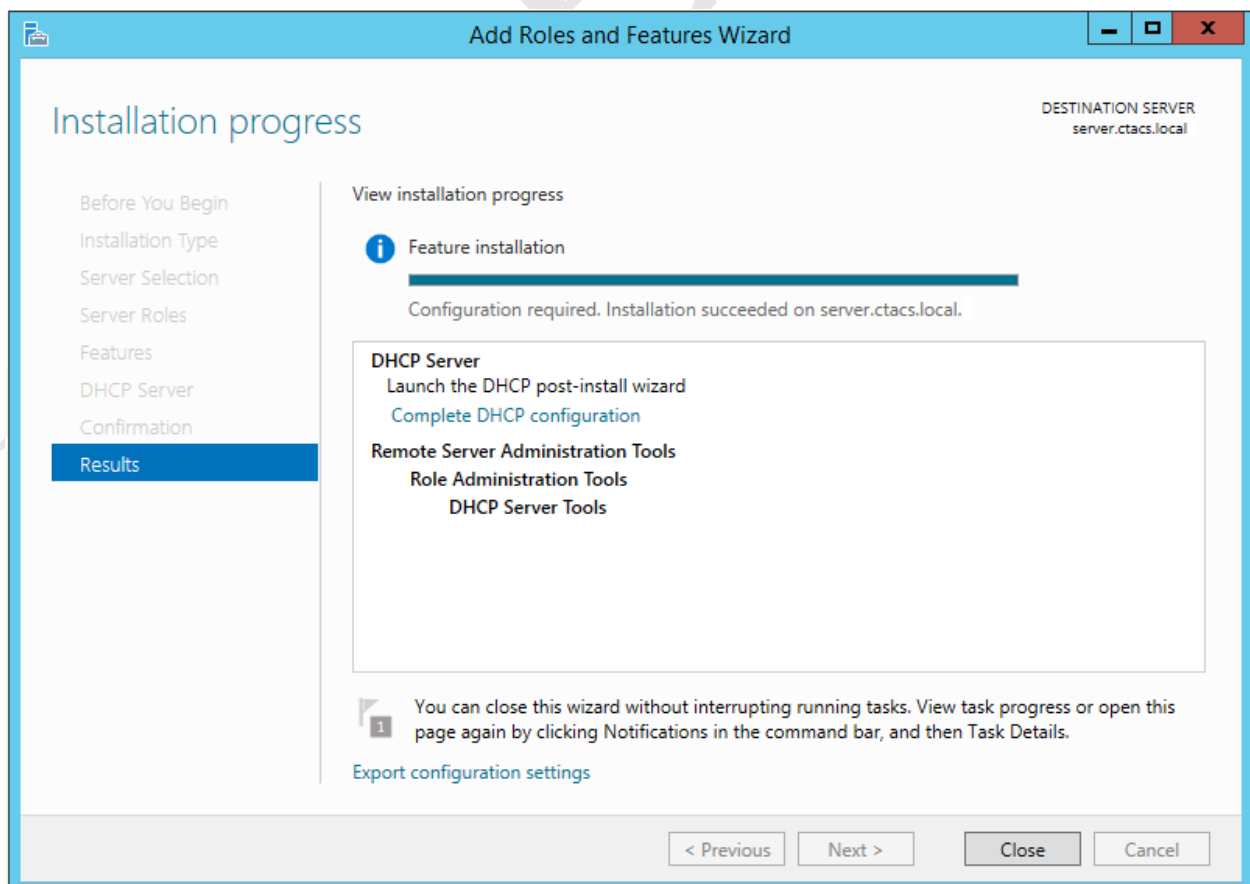
Figure 115: Installation progress screen

Restart the server at this point. When the server comes back up, run System Manager again. There will an entry for DHCP in the left-hand panel – click on it. There is a warning message that configuration work is required; work through the message until a hyperlink entitled **Complete DHCP configuration** is displayed then click on it:
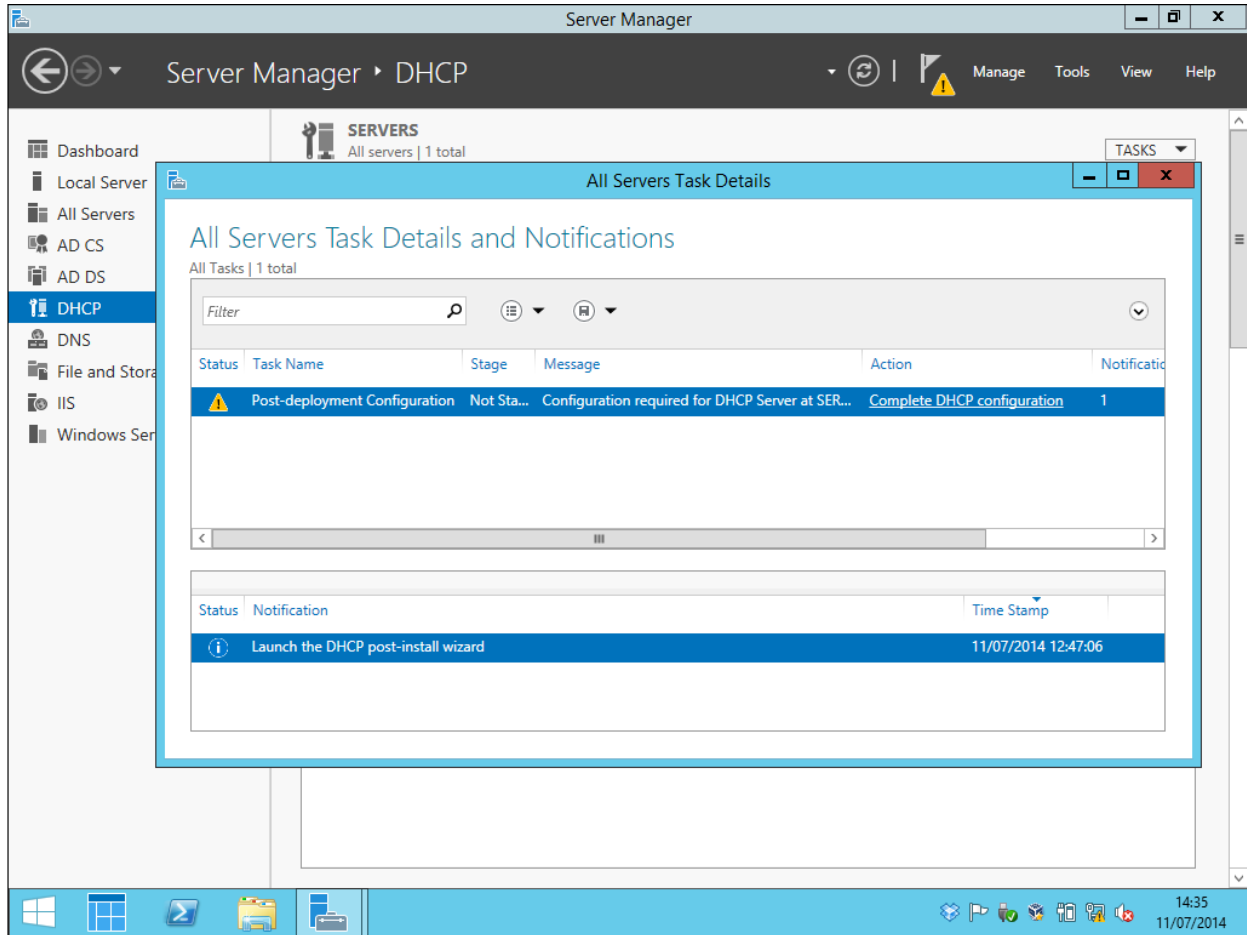
Figure 116: Message about further configuration

The *DHCP Post-Install configuration* wizard appears. Click **Next** to show the following:
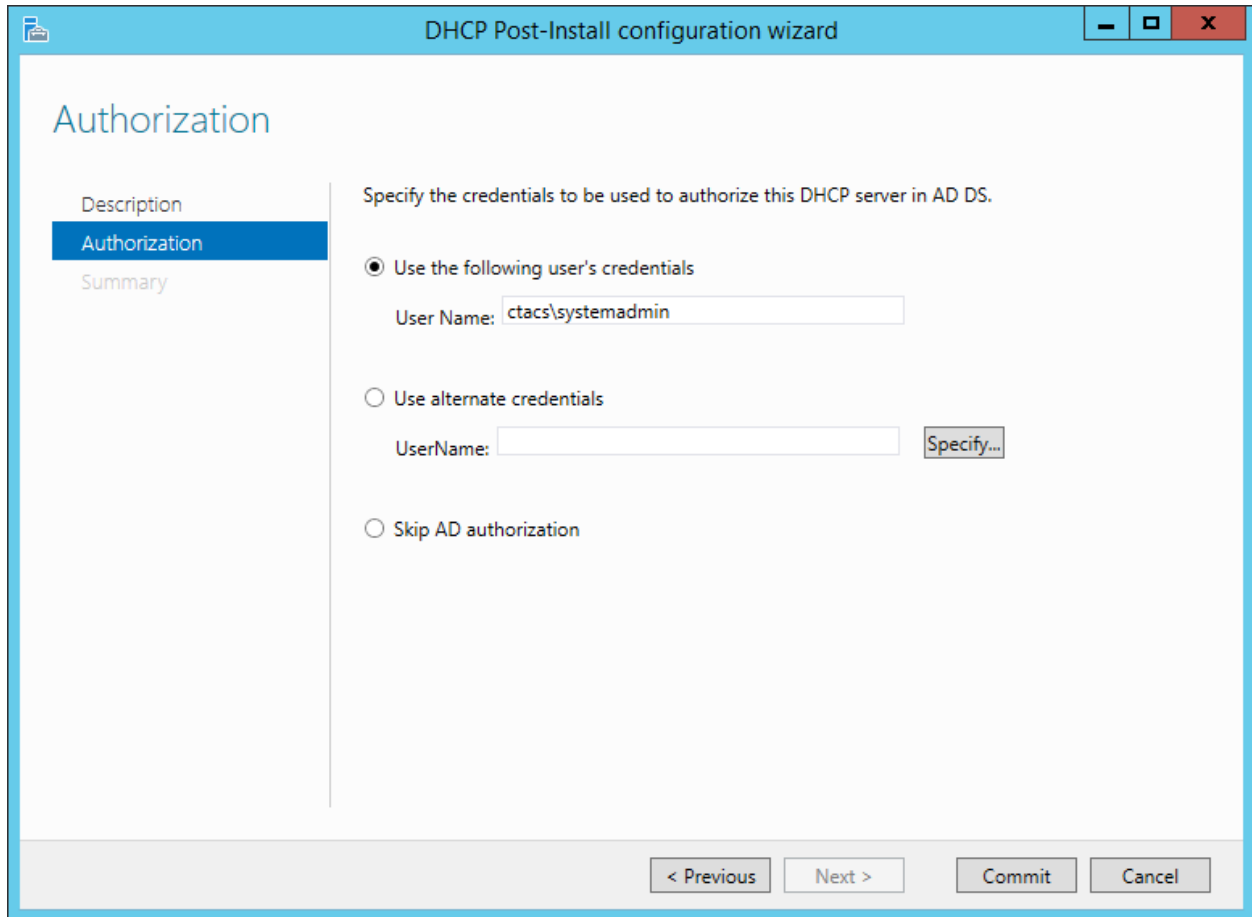
Figure 117: Post-Install configuration wizard

The existing user credentials e.g. *"Administrator"* or *"Systemadmin"* are fine so just click the **Commit** button. After a few seconds a Summary panel will be shown. Click **Close**.

It is now necessary to configure the IP scope. Click on **Administrative Tools** and choose **DHCP**. Expand the tree down the left-hand side so it appears as follows:
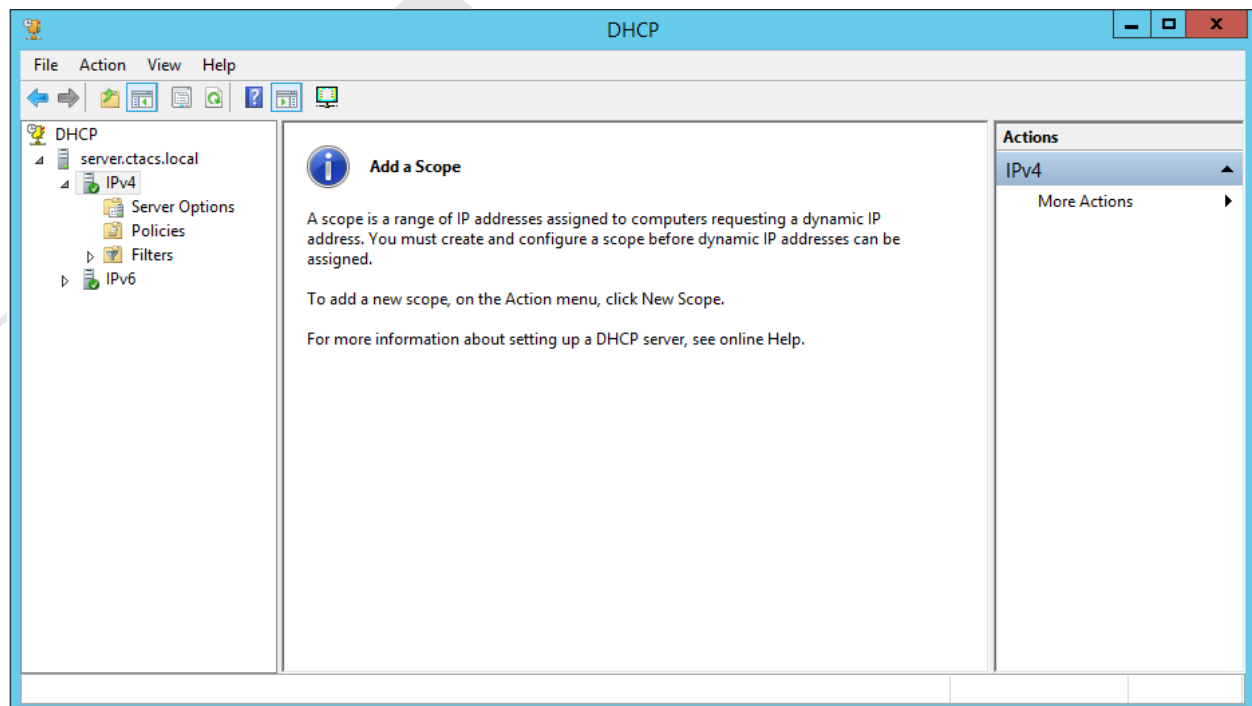
Figure 118: Configure DHCP Server

Right-click on the entry for **IPv4** and choose **New Scope** to bring up the New Scope Wizard. Click **Next** and the following panel is displayed. Give it a suitable name e.g. *workstations* and a description, then click the **Next** button:

Figure 119: New Scope Wizard

On the subsequent screen enter the addresses as outlined in the earlier section *IP Considerations*. In this example, our server is on 192.168.1.254 so the scope for the workstations will be 192.168.1.50 to 192.168.1.250. Set the Length to 24 and the Subnet mask will automatically adjust to 255.255.255.0. Then click **Next**:

Figure 120: IP address range for DHCP server

The next panel allows you to specify any exclusions (gaps) in the IP scope. Unless you have very specific requirements just click **Next**.

Figure 121: Add Exclusions and Delay

The subsequent screen is for specifying how long a lease will last. The default value of 8 days is inappropriate, so reduce it to one day then click **Next**.
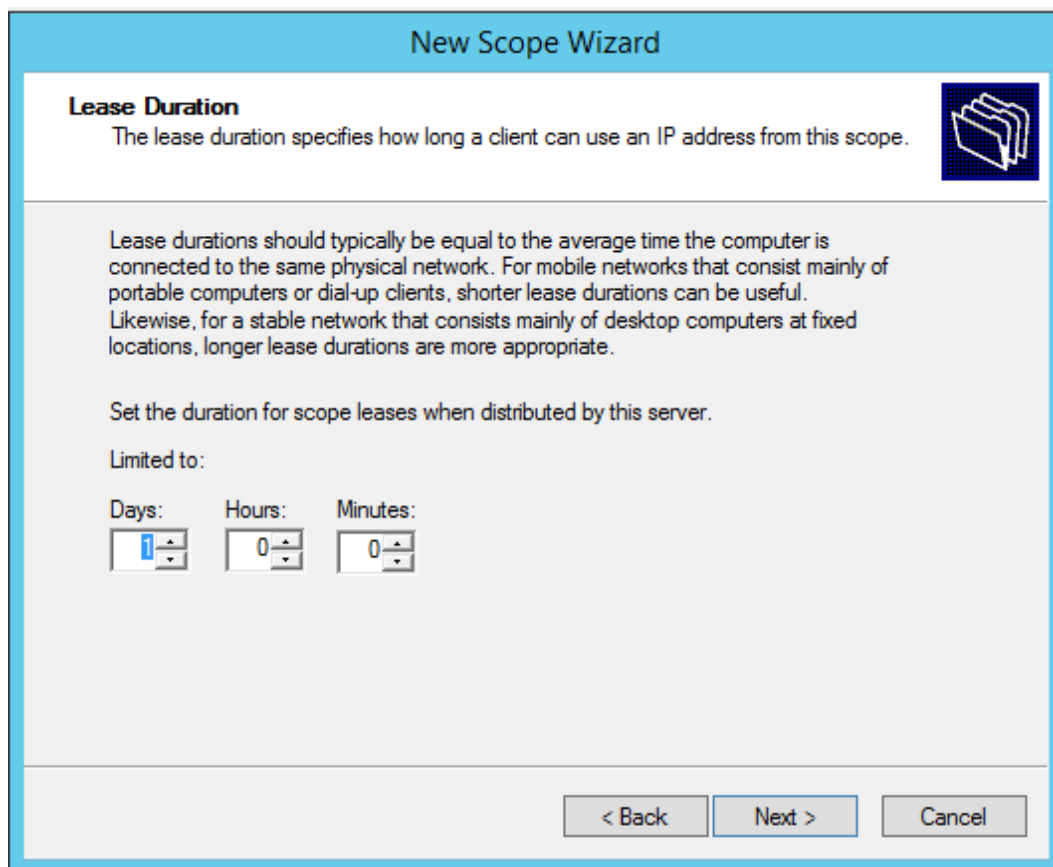

Figure 122: Specify Lease Duration

The following screen is concerned with more sophisticated options. They are of no great importance so choose **No, I will configure these options later** and click **Next**.
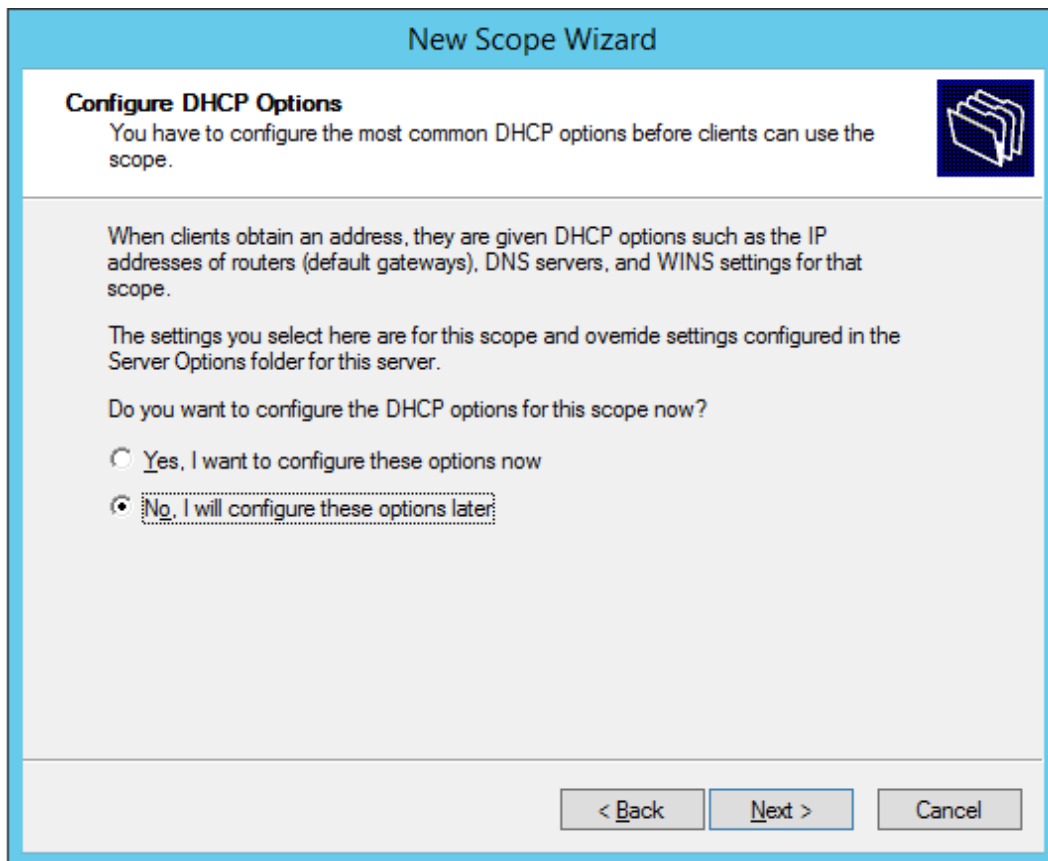
Figure 123: Configure more advanced DHCP options

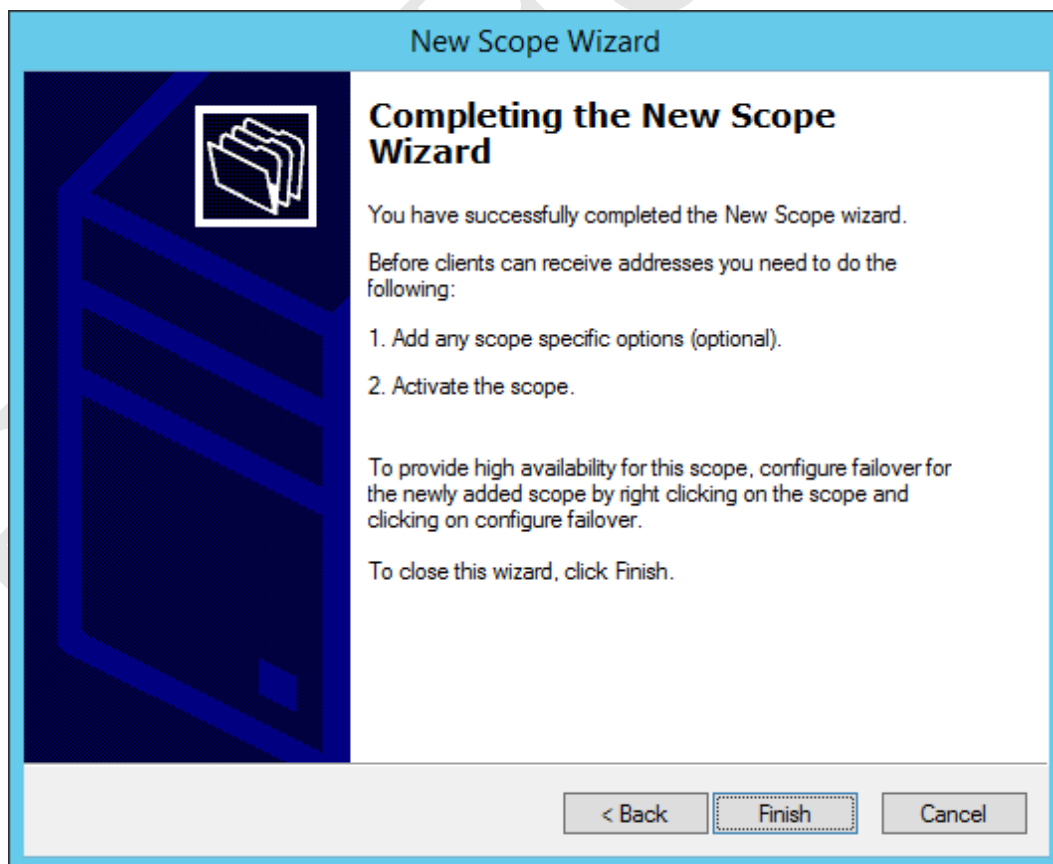Upon completion (which is a matter of seconds) a confirmation screen is shown. Click **Finish**.

Figure 124: Completion notice for New Scope Wizard

The scope now has to be activated. Expand the tree on the left-hand side of the DHCP panel. Currently, the entry for IPv4 will have a blue circle with a white exclamation mark on it. Right-click the new scope that we just created and choose **Activate**. The exclamation mark will be replaced by a green circle containing a white tick mark in it; everything should now be working correctly.
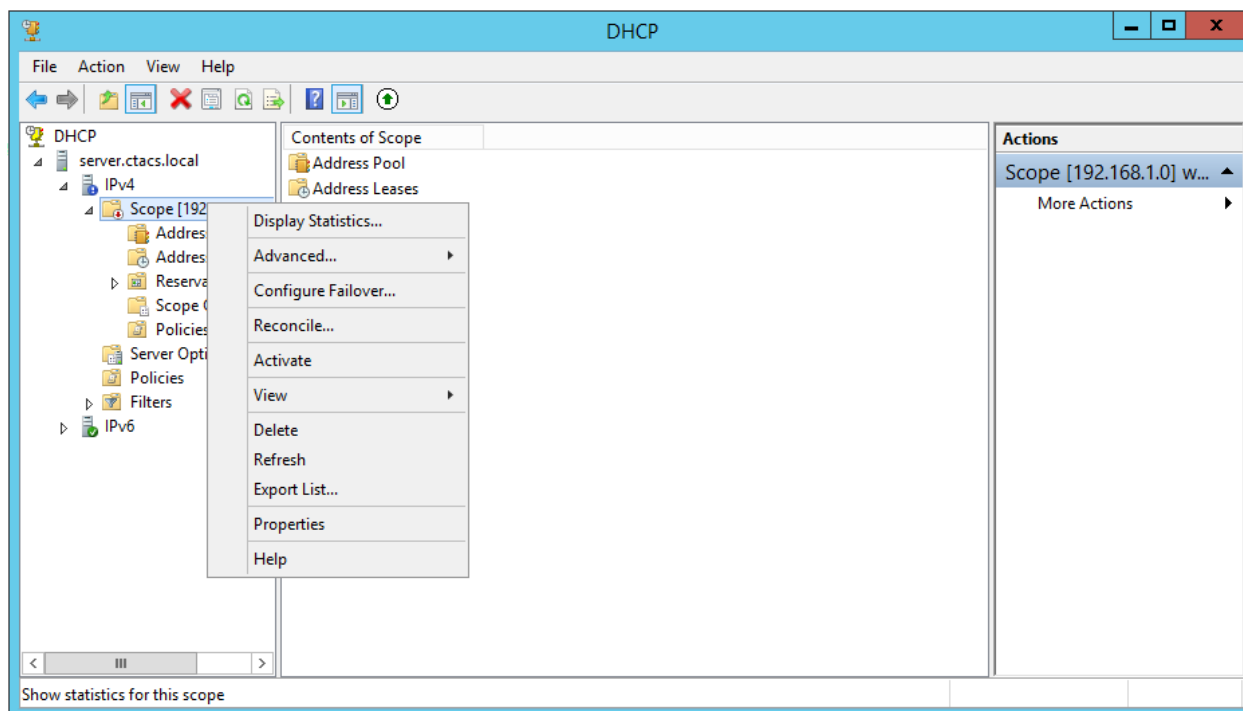

Figure 125: DHCP after configuration

13.2 Multiple Network Adapters (NIC Teaming)

A file server may have more than one network (Ethernet) adapter. Multiple adapters can be used together in different ways to improve resilience and/or performance using a technique known as *Teaming* or *NIC Teaming* (NIC is short for *Network Interface Card*).

In this example, a second Ethernet adapter has been installed in the server to improve network performance. Important: before progressing, make a note of the settings of the first adapter, which was given a fixed IP address in section 2. INITIAL INSTALLATION OF WINDOWS SERVER 2012 R2, as it may be necessary to re-enter them later on.

On the server, launch Server Manager (bring up a command prompt and enter *servermanager* or go the **Start Screen** and click on **Administrative Tools** and run it from there). Click **Configure this local server**. In the Properties panel look for the NIC Teaming entry. Click where it reads **Disabled** and the following panel is shown:
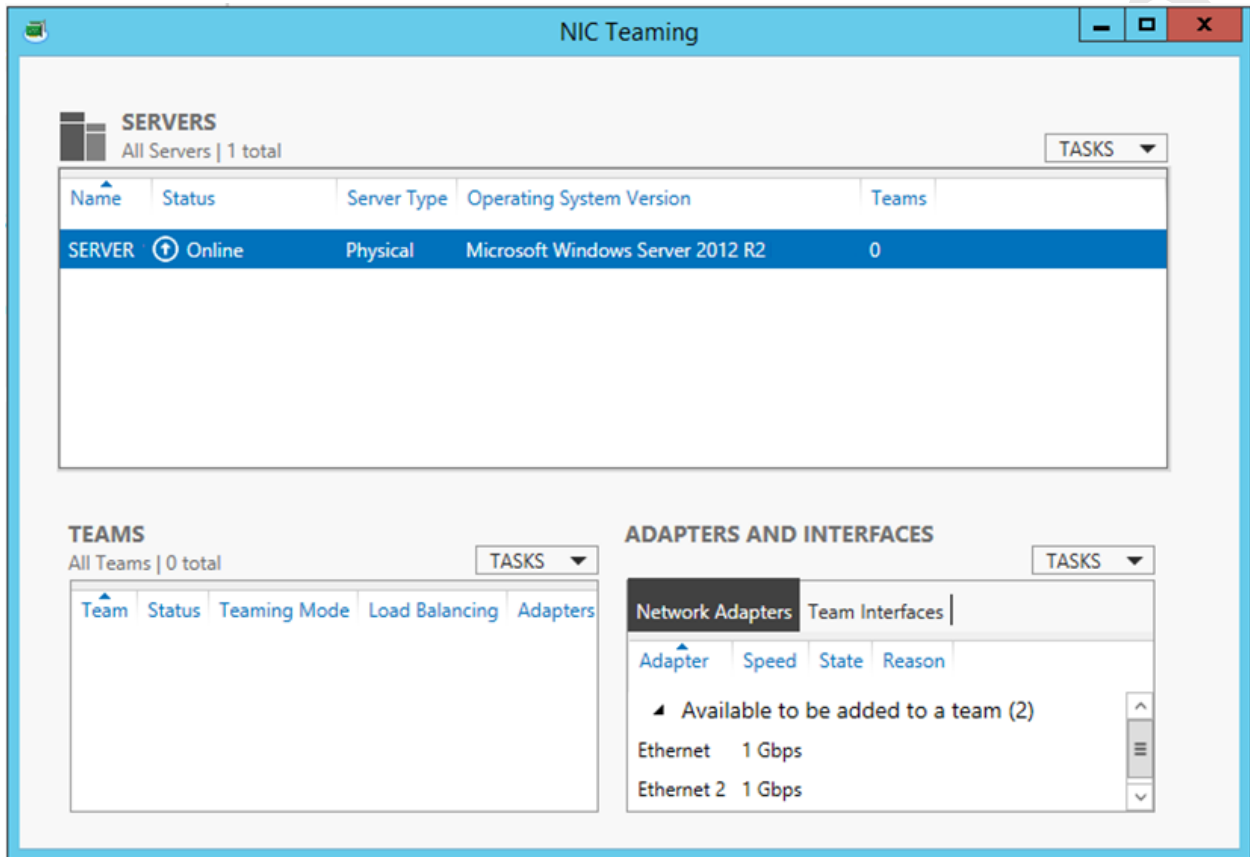

Figure 126: NIC Teaming screen

In the Teams section, click the **TASKS** drop-down and choose **New Team**. On the resultant panel, give the Team a name, tick the boxes for the network adapters and click **OK**. In this example we have called our Team *LAN* and are using two network adapters. The 'Additional properties' entry is for setting more advanced options; for instance if you wish to configure one of the network adapters as a Standby adaptor which will take over if the main one fails:
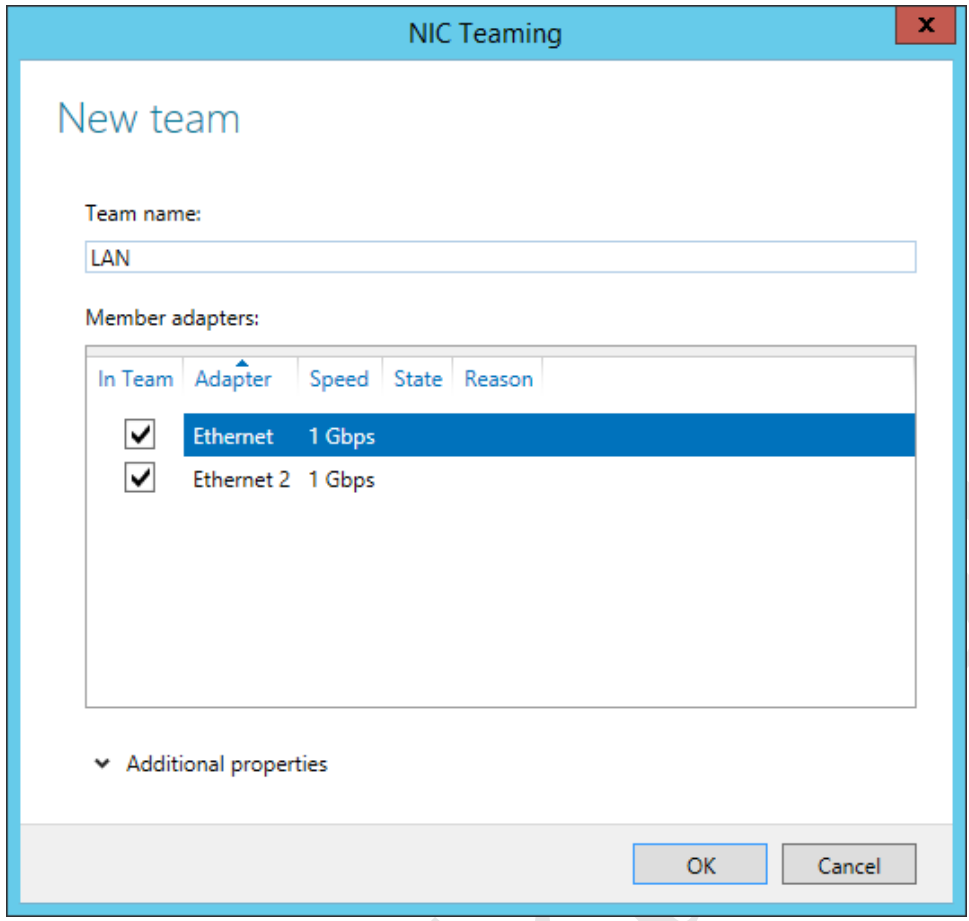
Figure 127: Creating a new team

The server may take a minute or so to adjust, during which time connectivity may be lost and an error status may be displayed on the NIC Teaming screen. When it is settled down it should appear so:
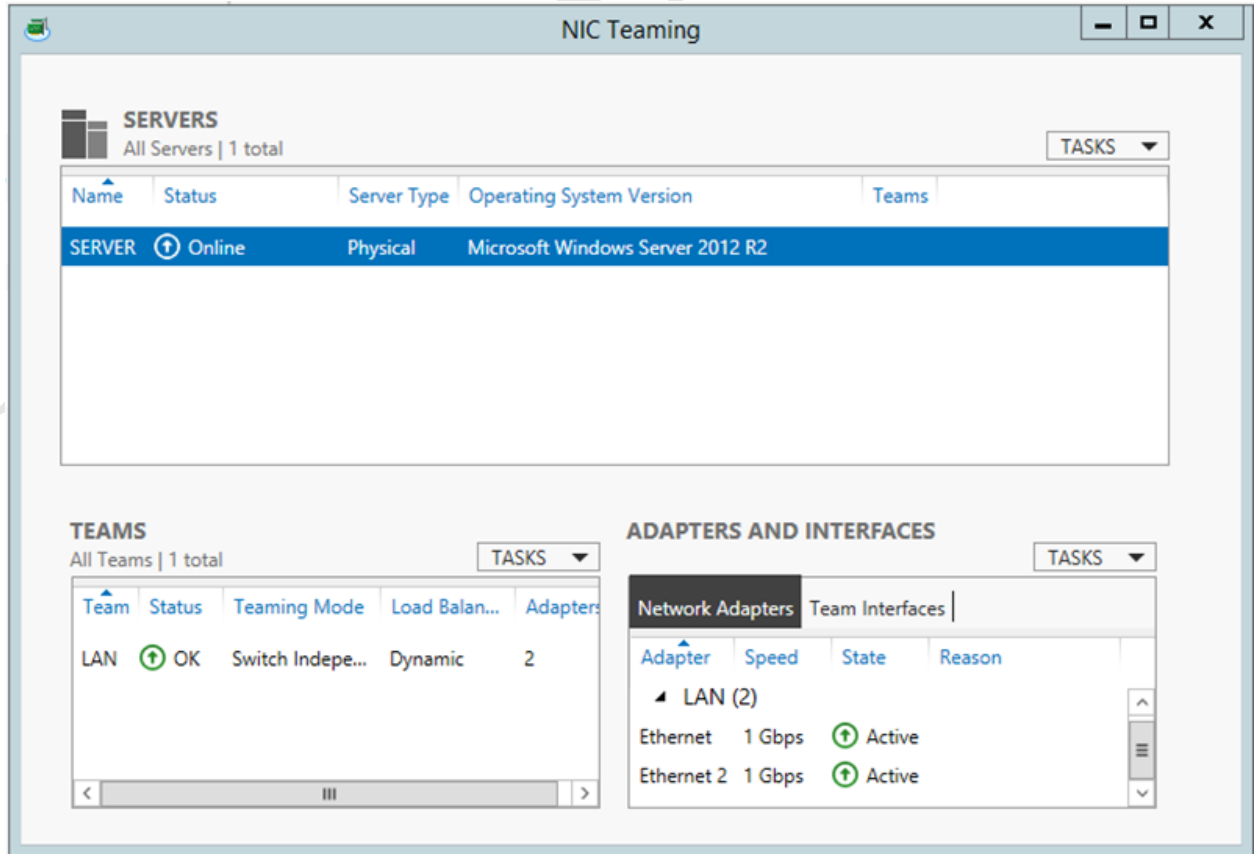
Figure 128: NIC Teaming status

Note that the server's IP address may have changed as a consequence of doing this and it is therefore strongly advised that you immediately check matters. Returning to the server Properties screen within Server Manager – you may need to refresh it - there should now be an entry underneath NIC Teaming for *LAN* (or whatever you called the Team):
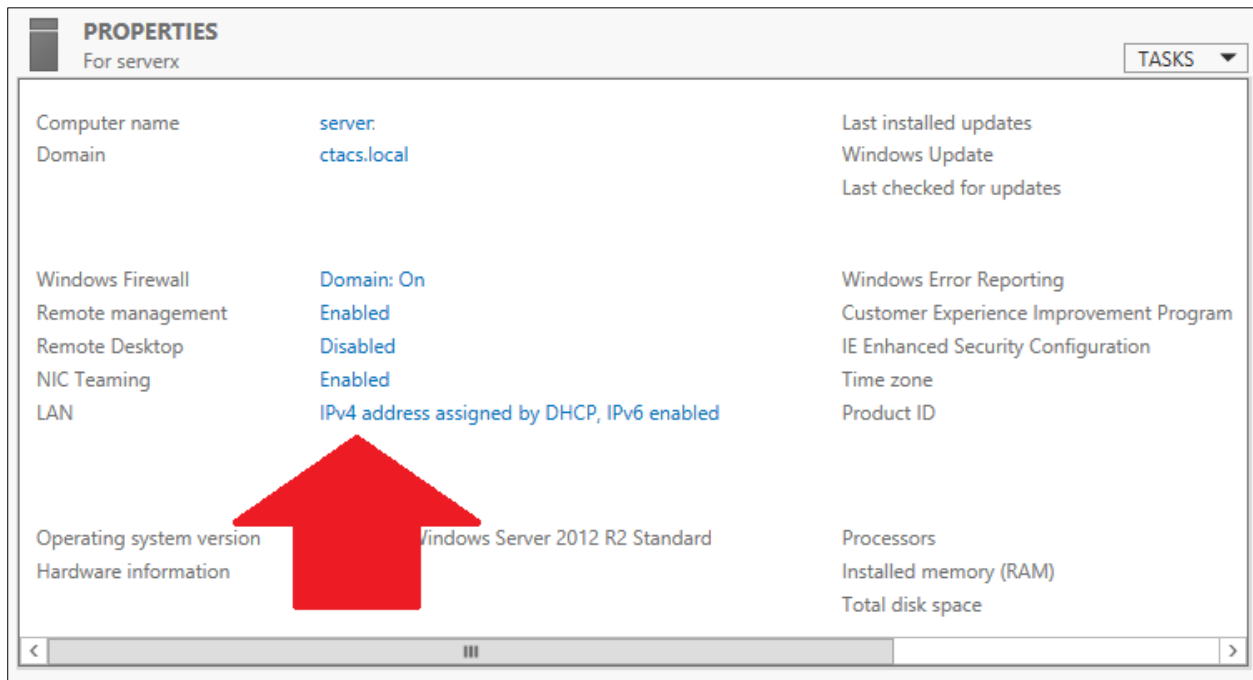

Figure 129: LAN entry in server Properties

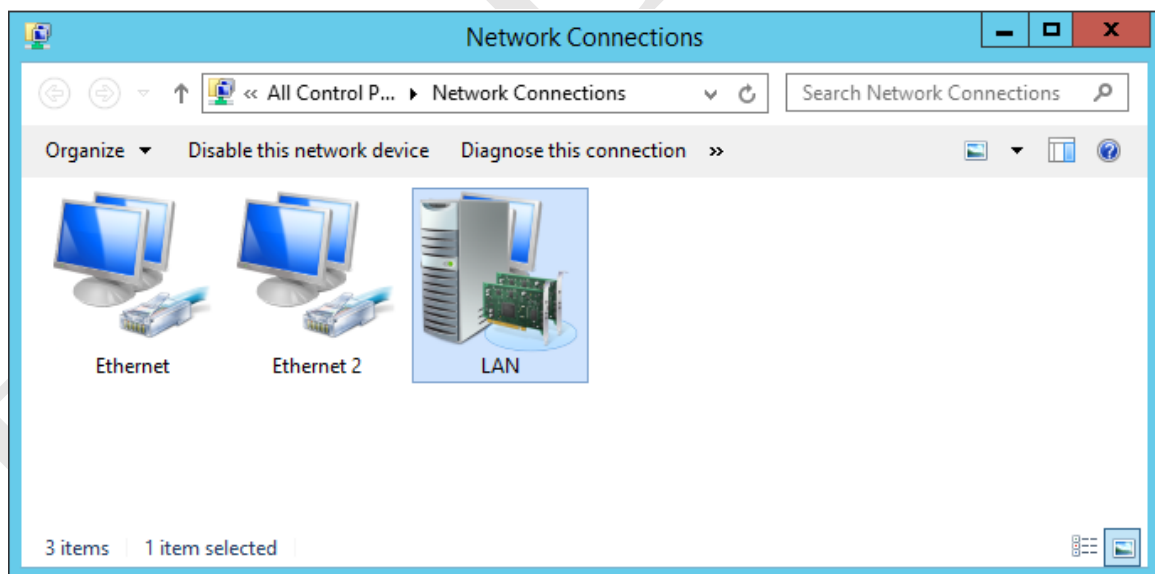Click on the blue writing to the right of *LAN* and it will display the Network Connections:

Figure 130: Network Connections

Right-click the entry for *LAN* and choose **Properties**. Highlight **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**. Change the entries to be the same as the original single adapter was before beginning this exercise. Again, note that there may be an interruption to the connectivity whilst this takes effect.

Thank you!

We hope that you have found this guide helpful and interesting.

We pride ourselves on the accuracy of our guides and they are reviewed and updated several times a year. However, as the software and utilities are regularly updated it is possible that very recent changes may not be reflected. If you have any suggestions or have found errors or areas for improvement, please let us know at enquiry@ctacs.co.uk. Please quote the date that is stated at the beginning of page 2 so we know what edition you have. Thank you.