

**INDUSTRIAL TRAINING REPORT**

**ACTIVE DIRECTORY DOMAIN CONTROLLER AND**

**MANAGING ITS POLICIES**

**at**

**INSTITUTE OF INFORMATION SECURITY , DELHI**

**SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF DEGREE**

**OF BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE**



**SUBMITTED BY:**

**ANKIT VASHISTH**

**Department of Computer Science & Engineering**

**Gurgaon Institute of Technology & Management, Gurgaon**

**(Affiliated to Maharishi Dayanand University, Rohtak)**

**2014-2018**

## **CANDIDATE'S DECLARATION CERTIFICATE**

I hereby certify that the work which is being presented in the report entitled “ACTIVE DIRECTORY DOMAIN CONTROLLER AND ITS POLICY MANAGEMENT” by “**ANKIT VASHISTH**” in partial fulfillment of requirements for the award of degree of B.Tech. (CSE) submitted to Department of Computer Science & Engineering, Gurgaon Institute Of Technology & Management, Gurgaon under MDU, Rohtak is an authentic record of my own work carried out during a period from **2014** to **2018** under the supervision of **MR.NARESH RATHORE**.

Signature of the Student

ANKIT VASHISTH

14-CSE-204

## **ACKNOWLEDGMENT**

I am highly grateful to **Prof. Mukesh Yadav**, Head, Department of Computer Science, Gurgaon Institute of Technology & Management, Gurgaon, for providing this opportunity to carry out the six month industrial training at **INSTITUTE OF INFORMATION SECURITY, DELHI**.

I would like to express my gratitude to other faculty members of Computer Science Department at **GITM**, Gurgaon for providing academic inputs, guidance & encouragement throughout the training period.

The author would like to express a deep sense of gratitude and thank to **PROF. MUKESH YADAV**, Director, GITM, without whose permission, wise counsel and able guidance, it would have not been possible to pursue my training in this manner.

The help rendered by **Mr. NARESH RATHORE** Supervisor **INSTITUTE OF INFORMATION SECURITY, DELHI** for experimentation is greatly acknowledged.

Finally, I express my indebtedness to all who have directly or indirectly contributed to the successful completion of my industrial training.

ANKIT VASHISTH

014.CSE.204

(2014-2018)

## CONTENTS

ABSTRACT.....	
ORGANIZATIONAL PROFILE.....	
CERTIFICATE.....	
1. INTRODUCTION.....	9
1.1 OVERVIEW.....	9
1.2 TYPES OF SERVER.....	10
1.3 HISTORY.....	10
1.4 IMPLEMENTATION.....	11
2. OBJECTIVE AND SCOPE OF PROJECT.....	12
2.1 OBJECTIVE.....	12
2.2 SCOPE.....	13
3. REQUIREMENT ANALYSIS.....	14
3.1 IN BUISNESS.....	14
3.2 IN FILE SERVICES.....	15
3.3 IN PRINT SERVICES.....	16
3.4 FAX SERVICES.....	16
3.5 NETWORK AND POLICY ACCESS.....	17
4. METHODOLOGY.....	18
4.1 ACTIVE DIRECTORY DOMAIN CONTROLLER.....	18
4.1.1 ACTIVE DIRECTORIES.....	19
4.1.2 LOGICAL STRUCTURE.....	20
4.1.3 OBJECTS.....	21
4.1.4 FOREST,TREES AND DOMAINS.....	22

4.1.5 ORGANIZATIONAL UNIT.....	22
4.2 INSTALLING ACTIVE DIRECTORIES.....	23
4.3 CREATING ACTIVE DIRECTORIES.....	40
4.4 CONFIGURE STATIC DOMAIN.....	45
4.5 POLICY MANAGEMENT.....	46
4.6 STATIC IP CONFIGURE IN CLIENT.....	51
4.7 LOGIN TO USER.....	52
5. HARDWARE AND SOFTWARE USED.....	53
5.1 HARDWARE.....	54
5.1.1 PROCESSOR.....	53
5.1.2 RAM .....	54
5.1.3 HARD DISK.....	54
5.1.4 VIDEO.....	54
5.2 SOFTWARE.....	54
5.2.1 WINDOWS NT.....	55
5.2.1.1 FEATURES OF WINDOWS NT.....	57
5.2.1.2 ARCHITECTURE.....	60
5.2.2 WINDOWS SERVER 2008.....	70
5.2.3 VMWARE WORKSTATION.....	73
6. PROJECT DESIGN.....	74
BIBLIOGRAPHY.....	
APPENDIX.....	

## LIST OF FIGURES

1. LOGICAL STRUCTURE.....	21
2. WINDOWS NT ARCHITECTURE.....	60
3. HYPER-V.....	71
4. DECISION FLOW CHART.....	73

## ABSTRACT

In this project we will mainly focus on how to create active directories with the help of windows server 2008 and how to manage its policies. Firstly it is important for us to know some theoretical knowledge of project after that we will go on about its practical. All the important thing are described in the project which are actually implemented by a network administrator of a company or college

Windows Server 2008 R2 offers some exciting benefits, especially as Windows 7 deployments pick up steam. While your end-user population will benefit from many Windows Server 2008 R2 features, some new server features require Windows 7 desktops. You'll need to efficiently manage your Windows Server 2008 R2 infrastructure. The Server Manager console, introduced in the original release of Server 2008, offers a one-stop management experience for just about anything you'd need to do on a server. Several new concepts are described in this project like Hyper-V, virtualization and much more which are very important for us to us to know about. And lastly we can have our project design we surely remove all our doubts that we have regarding its design.

## **ORGANIZATIONAL PROFILE**

The Institute of Information Security is one of the most trusted sources of hands-on trainings in information security with Ethical Hacking, Web Application Security, Network Security, Penetration Testing and forensics trainings & certification courses in India, Middle East, Malaysia, Singapore and Africa. With the backing of our brilliant technical team providing consulting services for the past 11 years under the brand name of Network Intelligence India Pvt. Ltd., they are here not only to teach, but also mentor you for achieving great heights in this exciting field of information security. Our emphasis on hands-on practical training definitely gives our clients and students an edge to grow rapidly and advance professionally in their respective career.



# 1.

## Introduction

### 1.1 Overview

Windows Server is a brand name for a group of server operating systems released by Microsoft. It includes all Windows operating systems that are branded "Windows Server", but not any other Microsoft product. The first Windows server edition to be released under that brand was Windows Server 2003. However, the first server edition of Windows was Windows NT 3.1 Advanced Server, followed by Windows NT 3.5 Server, Windows NT 4.0 Server, and Windows 2000 Server; the latter was the first server edition to include Active Directory, DNS Server, DHCP Server, Group Policy, as well as many other popular features used today. Windows Server is generally capable of providing server-oriented services, such as the ability to host a website, user management, resource management across users and applications, messaging, security and authorization and many other server-focused services.

### 1.2 windows server types:

Windows Server software includes:

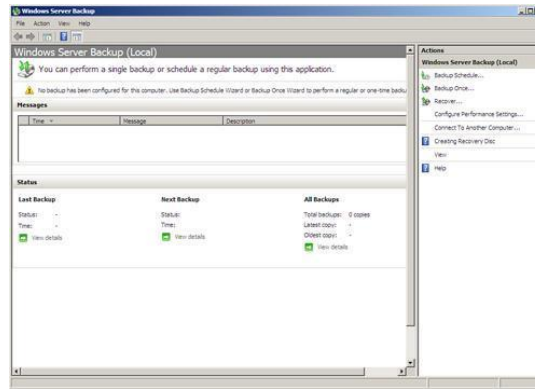
- Windows 2000 Server
- Windows Server 2003
- Windows Server 2008

- Windows HPC Server 2008
- Windows Server 2008 R2
- Windows Server 8
- Windows server 2012

### 1.3 History

Originally known as Windows Server Codename "Longhorn", Microsoft chairman Bill Gates announced its official title (Windows Server 2008) during his keynote address at WinHEC 16 May 2007. Beta 1 was released on 27 July 2005, Beta 2 was announced and released on 23 May 2006 at WinHEC 2006 and Beta 3 was released publicly on 25 April 2007.[6] Release Candidate 0 was released to the general public on 24 September 2007[7] and Release Candidate 1 was released to the general public on 5 December 2007. Windows Server 2008 was released to manufacturing on 4 February 2008 and officially launched on 27 February 2008. During the development cycle, Longhorn, now known as Windows Server 2008, incorporated the best of what was found in the Windows Server 2003 environment and also adapted some of the new bells and whistles that are also found in the Windows Vista operating system. Windows Server 2008 also provides a number of improvements over Windows Server 2003, while still providing a scalable enterprise networking platform that can be easily expanded as a company or organization grows.

In terms of features adopted from Windows Vista, you will find that Windows Server 2008 shares a number of similarities with Windows Vista, including the Start Menu, desktop, and Windows Control Panel. Thanks to Windows Vista, Windows Server 2008 also now provides a better native backup utility: the Windows Server Backup snap-in (see figure 1). This backup utility runs in the Microsoft Management Console and enables you to back up and restore server files to backup media including DVDs.



SCREEN SHOT:1(windows serVer backup snap in)

## 1.4 implementation

In general, a network utilizing Active Directory has more than one licensed Windows server computer. Backup and restore of Active Directory is possible for a network with a single domain controller, but Microsoft recommends more than one domain controller to provide automatic failover protection of the directory. Domain controllers are also ideally single-purpose for directory operations only, and should not run any other software or role.

Certain Microsoft products such as SQL Server and Exchange can interfere with the operation of a domain controller, necessitating isolation of these products on additional Windows servers. Combining them can make configuration or troubleshooting of either the domain controller or the other installed software more difficult.[38] A business intending to implement Active Directory is therefore recommended to purchase a number of Windows server licenses, to provide for at least two separate domain controllers, and optionally, additional domain controllers for performance or redundancy, a separate file server, a separate Exchange server, a separate SQL Server, and so forth to support the various server roles.

Physical hardware costs for the many separate servers can be reduced through the use of virtualization, although for proper failover protection, Microsoft recommends not running multiple virtualized domain controllers on the same physical hardware.

# 2.

## **OBJECTIVE AND SCOPE OF PROJECT**

### **2.1 Objective**

Our Main objective is to Understand Server portion of Windows Server Administration , Fundamentals certification , managing server domains and its policies & server security.

Other main services that we studied later are:

- Active directory certificate services
- Active directory domain services
- Active directory light weight services.
- Rights and policy management services
- Application server
- DNS server
- Hyper-v

### **2.2 scope**

As we know about our objectives lets talk about its scope, it normally includes that how we implement it and what is its use in future services. By now, the list of goals and objectives might be getting quite long. But when the myriad of business and technical objectives as well as the overall priorities start to become clear, the scope of work starts to take shape. A key question to ask at this point, to home in on the scope of the project, is whether the migration is primarily an operating system upgrade or an application upgrade. Often the answer to this question seems clear at first but becomes more complex as the different goals of the business units are discussed, so the scope of work that is created might be quite different than it appeared at first.

Specifically, a decision needs to be made whether the entire network operating system (NOS) needs to be upgraded or only a subset of it, and what other infrastructure components need to be changed or replaced.

Upgrading to the latest version of a key network application (CRM solution, document management system, or remote access solution) might require a network operating system upgrade, but it might need to involve only a limited portion of the network (perhaps only one server). However, if this application needs to be accessed by every member of the organization, in several offices, and requires upgrades to data storage solutions, tape backup software, antivirus software, remote access, and connectivity among offices, a full NOS upgrade might make more sense. An upgrade to Windows Server 2008 R2 enterprise wide can allow centralization of resources, consolidation of servers, enhanced management tools, and other features that can make a larger project more attractive.

Windows Server 2008 introduces over 1,000 new Group Policy Objects specific to Windows Server 2008 R2 and Windows 7, along with several new components that expand on the core capabilities of Group Policy management that have been part of Windows 2000/2003 Active Directory. The basic functions of Group Policy haven't changed, so the Group Policy Object Editor (gpedit) and the Group Policy Management Console (GPMC) are the same, but with more options and settings available.

As mentioned earlier, the Group Policy Management Console can either be run as a separate MMC tool, or it can be launched off the Features branch of the Server Manager console tree. Group policies in Windows Server 2008 R2 provide more granular management of local machines, specifically having policies that push down to a client that are different for administrator and non-administrator users. Windows Server 2008 R2 introduces new and revised performance and reliability monitoring tools intended to help network administrators better understand the health and operations of Windows Server 2008 R2 systems. Just like with the Group Policy Management Console, the new Reliability and Performance Monitor shows up as a feature in the Server Manager console. By clicking on the Performance Diagnostic Console, the tool shows up in the right pane.

File Server Resource Manager (FSRM) was a feature pack add-in to Windows 2003 R2 and has been significantly improved with the release of Windows Server 2008 R2. FSRM is a quota management system of files on network shares across an enterprise. Rather than allowing employees to copy the entire content of their laptop to a network, or potentially back up their MP3 audio files onto a network, FSRM provides the ability to not only limit the amount of

content stored on network shares, but also to set quotas on certain file types. So, a user could be limited to store 200GB of files on a network share, but of that limit, only 2GB can be allocated to MP3 files.

In Windows Server 8, Microsoft strives to deliver the full Windows experience wherever a user wants to connect, while offering superior access control and audit capabilities based on strong identity-verification frameworks and data classification features.

**Enable high availability while simplifying management.** When we start thinking of data centers and clouds, images that come to mind may include racks of headless machines and tons of networking equipment, and then the hundreds or thousands of virtual machines that you probably have running within that infrastructure.

Windows Server 2008 will expand the ability of the operating system to use commodity storage, networking and server infrastructure easily and efficiently, while using less power and increasing the ability to prevent failures from occurring and to recover from errors when they do happen. And management tools have been upgraded with new single-pane-of-glass views, PowerShell capabilities in full and exposed Web-service management endpoints that get you well on your way to full lights-out automation of your Windows Server infrastructure.

# 3.

## **REQUIREMENT ANALYSIS**

### 3.1 REQUIREMENT ANALYSIS FOR BUSINESS

We're often talking with small business owners about their business – to understand not only their needs and usage of technology, but also what's important to them as business owners. Not surprisingly saving time and money, all the while providing better and differentiated service to their customers is of key importance.

Windows Small Business Server 2008 (SBS 2008) is really a best kept secret that is a catalyst for small businesses to reduce costs, increase productivity and delight their customers because it really enables them to organize their business and communicate more effectively internally and with their customers.

SBS 2008 is an all in one server suite designed specifically for small businesses. It provides businesses with the technology to do the following:

- Organize and centralize information and data so everyone can find what they need.
- Share hardware such as printers and faxes.
- Back-up important data and restore files.
- Work remotely with easy and secure access to desktops, files, email and calendars from an internet connected PC or mobile phone.

- Share files more easily across PCs and mobile devices with a company intranet
- Run accounting or other business software on more than one pc.
- Easily set up new users, computers, and network access (or discontinue existing users and devices) as staffing levels fluctuate
- Look professional by consolidating email accounts with your own company hosted email
- Get better performance out of existing PC investments with centralized storage to free up memory on individual PCs.

SBS 2008 was designed specifically for businesses with 75 or fewer PCs or users – and many small businesses are benefiting from a server, even those with as few as 2 to 3 PCs. If you're interested you can try SBS 2008 today for free by visiting our product site.

SBS 2008 software can be purchased through a variety of channels such as Microsoft Small Business Specialists, retailers, or preinstalled on a server. Full solutions with server hardware can be purchased through a local system builder or major OEM (Original Equipment Manufacturer) such as Dell or HP for as little as \$1,299. You can visit our product site for more information on “How to Buy SBS 2008” or visit one of our partners directly.

## 2.2 In File Services:

Provides technologies for storage management, which includes control of the types of files stored on a server via file screens and powerful quotas, file replication, distributed namespace management, NFS, and support for UNIX clients.



## 2.3 For Print Services

It Enables the management of print servers and printers. A print server reduces administrative and management workload by centralizing printer management tasks. Also part of Print Services is the Print Management Console, which streamlines the management of all aspects of printer server management including the ability to remotely scan a subnet for printers and automatically create the necessary print queues and shares.

## 2.4 Fax Services

Sends and receives faxes, and allows you to manage fax resources such as jobs, settings, reports, and fax devices on this computer or on the network.

## 2.5 Network Policy and Access Services

Delivers a variety of methods to provide users with local and remote network connectivity, to connect network segments, and to allow network administrators to centrally manage network access and client health policies. With Network Access Services, you can deploy VPN servers, dial-up servers, routers, and 802.11 protected wireless access. You can also deploy RADIUS servers and proxies , and use Connection Manager Administration Kit to create remote access profiles that allow client computers to connect to your network.

# 4.

## **METHODOLOGY:**

To implement the above goals that we write above we need to implement the following methodology:

- Specify our needs like software used and hardware need and their architecture structure.
- Specifying the bindings between our different task that we perform either manually or with some designed tools.
- Specifying the port interconnection between the resources
- Analysis:

Extracting the data required for analysis and doing the analysis. It involves getting more and more information about the resources that we used and then implementing it the best way possible for us.

- Using the extra embedded tools for development

Structure of the system that we used are elaborate below as we go down in this project, it also includes its architectural information with its diagram and features.

### **4.1 Active directory and Domain Controller**

Let us know how to make a domain in windows server and managing its policies. Before that we should know about specific terms that is used in this method. we start with window domain and controller

A Windows domain is a form of a computer network in which all user accounts, computers, printers and other security principals, are registered with a central database located on one or more clusters of central computers known as domain controllers. Authentication takes place on domain controllers. Each person who uses computers within a domain receives a unique user account that can then be assigned access to resources within the domain. Starting with Windows 2000, Active Directory is the Windows component in charge of maintaining that central database. The concept of Windows domain is in contrast with that of a workgroup in which each computer maintains its own database of security principals.

On Microsoft Servers, a domain controller (DC) is a server computer that responds to security authentication requests (logging in, checking permissions, etc.) within a Windows domain. A domain is a concept introduced in Windows NT whereby a user may be granted access to a number of computer resources with the use of a single username and password combination.

#### 4.1.1 Active directory:

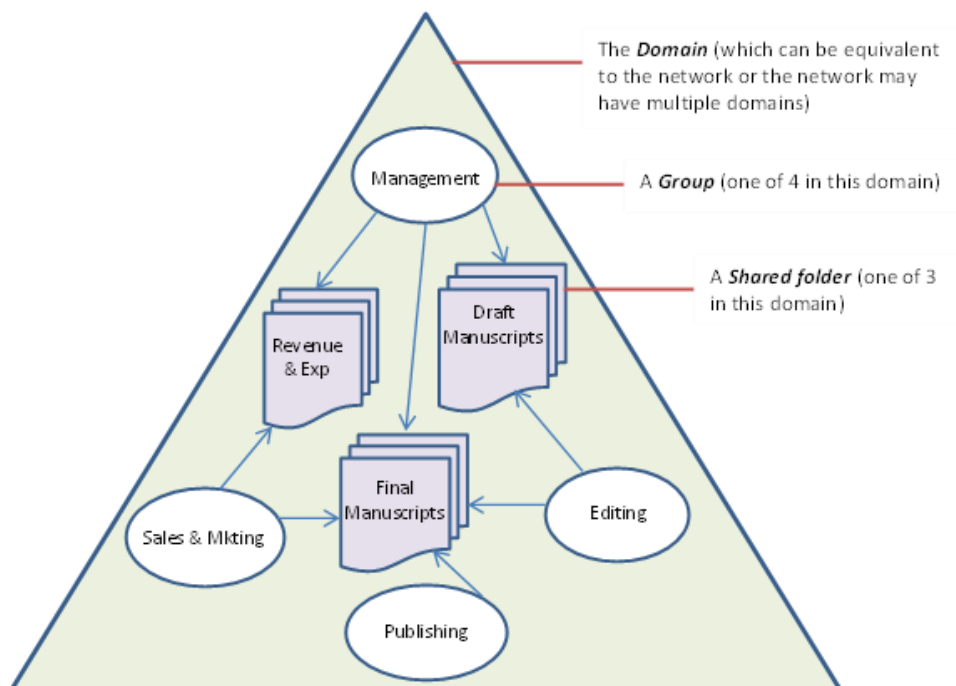
Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.

A server running Active Directory Domain Services (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services,

Federated Services, Lightweight Directory Services and Rights Management Services.

#### 4.1.2 Logical structure:

As a directory service, an Active Directory instance consists of a database and corresponding executable code responsible for servicing requests and maintaining the database. The executable part, known as Directory System Agent, is a collection of Windows services and processes that run on Windows 2000 and later. Objects in Active Directory databases can be accessed via LDAP, ADSI (a component object model interface), messaging API and Security Accounts Manager services.



**Figure 1:** A simplified example of a publishing company's internal network. The company has four groups with varying permissions to the three shared folders on the network.

### 4.1.3 Objects:

Active Directory structures are arrangements of information about objects. The objects fall into two broad categories: resources (e.g., printers) and security principals (user or computer accounts and groups). Security principals are assigned unique security identifiers (SIDs).

Each object represents a single entity—whether a user, a computer, a printer, or a group—and its attributes. Certain objects can contain other objects. An object is uniquely identified by its name and has a set of attributes—the characteristics and information that the object represents— defined by a schema, which also determines the kinds of objects that can be stored in Active Directory.

### 4.1.4 Forests, trees and domains

The Active Directory framework that holds the objects can be viewed at a number of levels. The forest, tree, and domain are the logical divisions in an Active Directory network.

Within a deployment, objects are grouped into domains. The objects for a single domain are stored in a single database (which can be replicated). Domains are identified by their DNS name structure, the namespace.

A domain is defined as a logical group of network objects (computers, users, devices) that share the same Active Directory database.

A tree is a collection of one or more domains and domain trees in a contiguous namespace, linked in a transitive trust hierarchy.

At the top of the structure is the forest. A forest is a collection of trees that share a common global catalog, directory schema, logical structure, and directory configuration. The forest represents the security boundary within which users, computers, groups, and other objects are accessible.

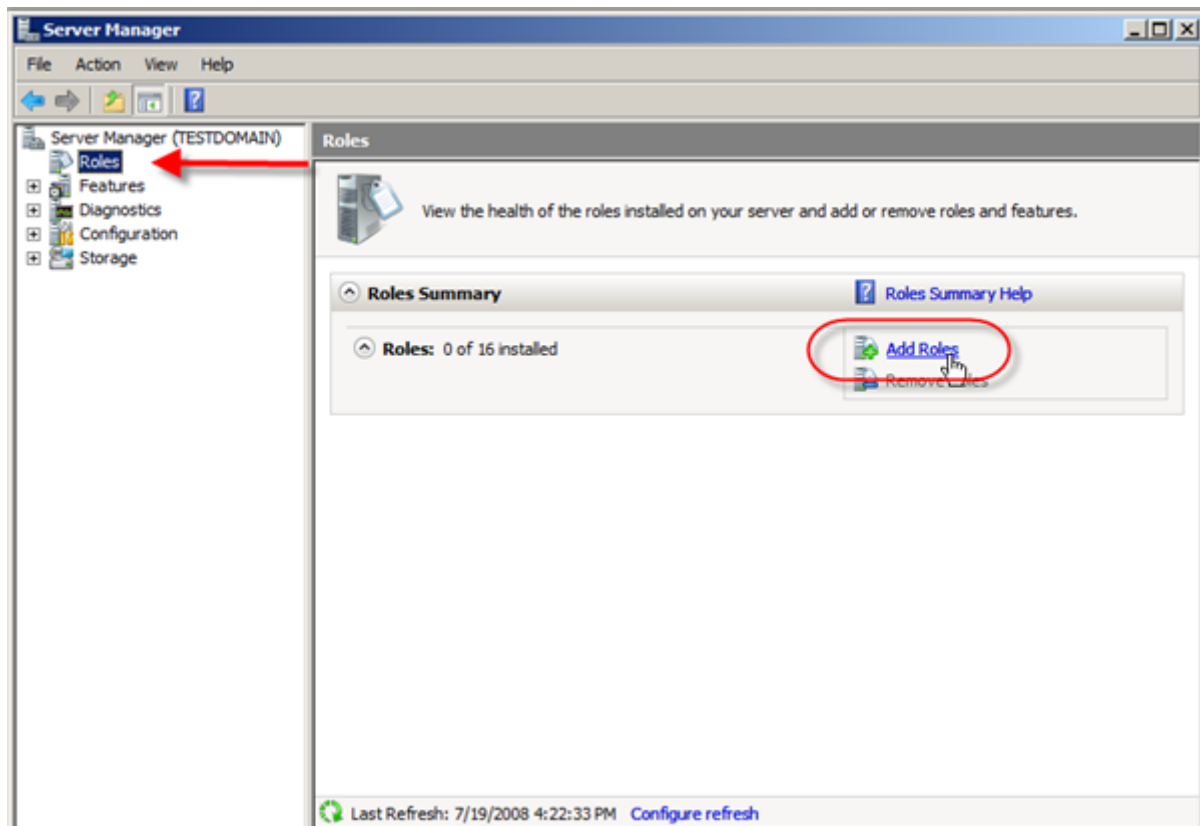
### 4.1.5 Organizational units

The objects held within a domain can be grouped into Organizational Units (OUs). OUs can provide hierarchy to a domain, ease its administration, and can resemble the organization's structure in managerial or geographical terms. OUs can contain other OUs—domains are containers in this sense. Microsoft recommends using OUs rather than domains for structure and to simplify the implementation of policies and administration. The OU is the recommended level at which to apply group policies, which are Active Directory objects formally named Group Policy Objects (GPOs), although policies can also be applied to domains or sites (see below). The OU is the level at which administrative powers are commonly delegated, but delegation can be performed on individual objects or attributes as well.

### 4.2 Lets know about how to install active directory

let's start by installing Active Directory through Server Manager. This is the most straight forward way, as a wizard will guide you through the steps necessary.

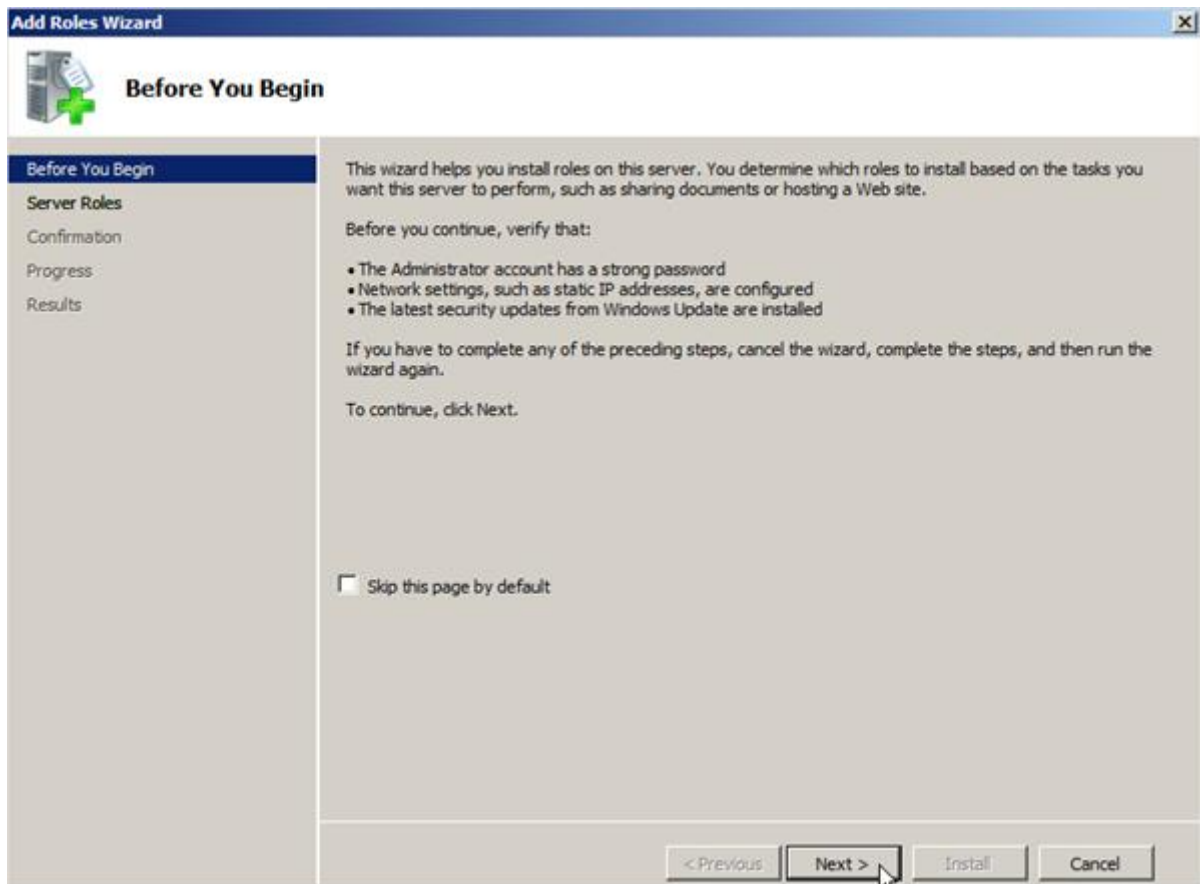
1. Start Server Manager.
2. Select Roles in the left pane, then click on Add Roles in the center console.



SCREENSHOT:2

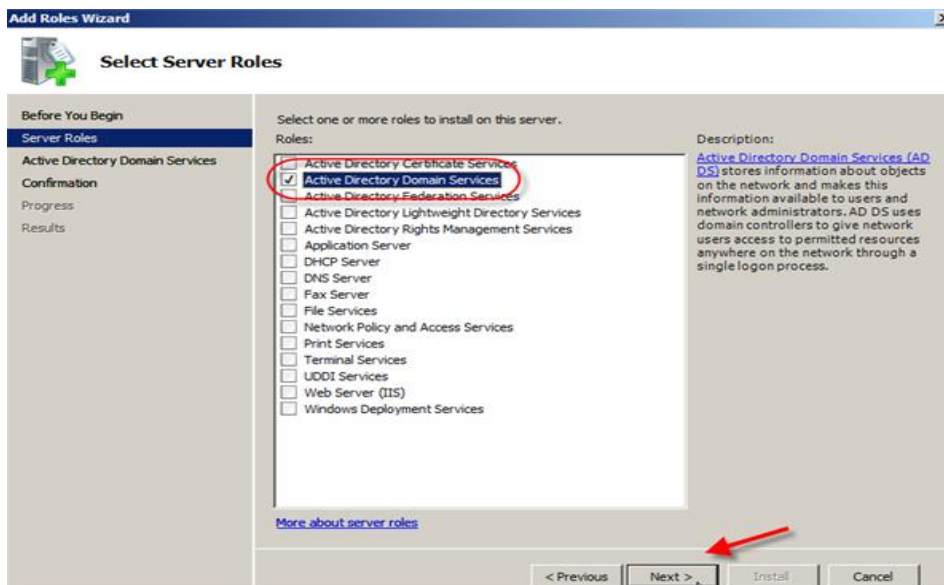
3. Depending on whether you checked off to skip the Before You Begin page while installing another service, you will now see warning pages telling you to make sure you have strong security, static IP, and latest patches before adding roles to your server.

If you get this page, then just click **Next**.



SCREENSHOT:3

4. In the **Select Server Roles** window we are going to place a check next to **Active Directory Domain Services** and click **Next**.

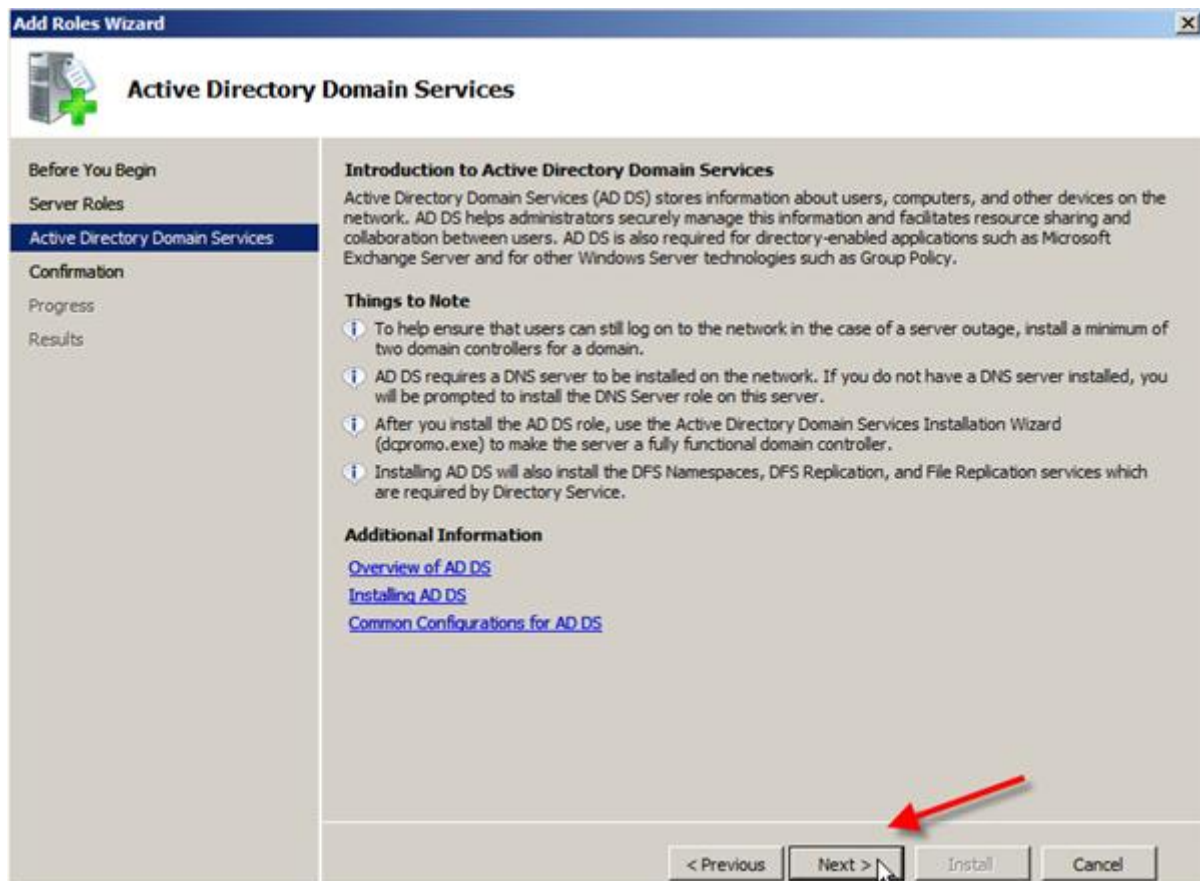


SCREENSHOT:4



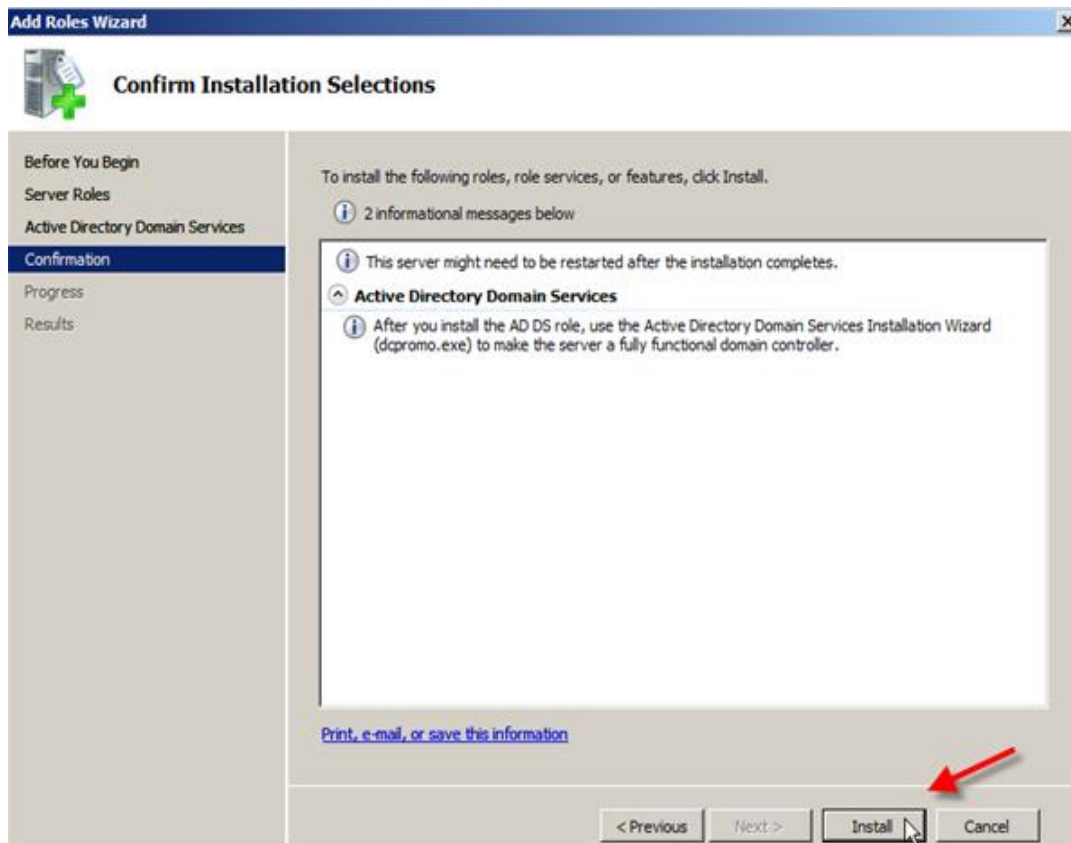
5. The information page on Active Directory Domain Services will give the following warnings, which after reading, you should click **Next**:

- Install a minimum of two Domain Controllers to provide redundancy against server outage (which would prevent users from logging in with only one)
- AD DS requires DNS which if not installed you will be prompted for
- After installing AD DS you must run dcpromo.exe to upgrade to a fully functional domain controller
- Installing AD DS will also install DFS Namespaces, DFS Replication, and File Replication services which are required by Directory Service.



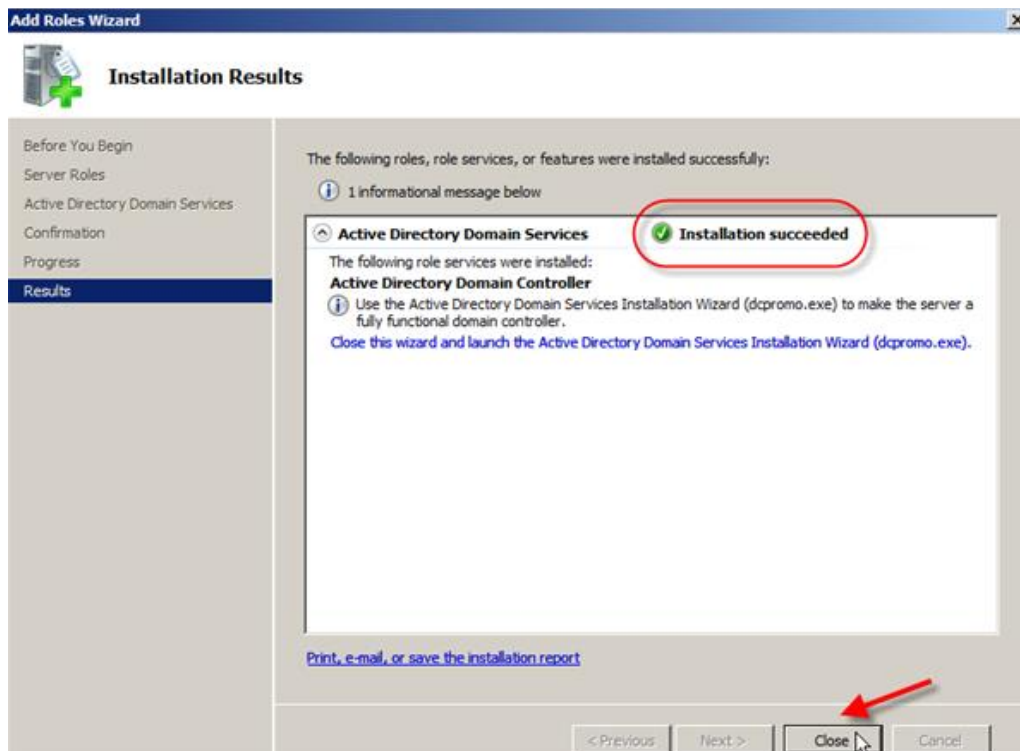
SCREENSHOT:5

6. The **Confirm Installation Selections** screen will show you some information messages and warn that the server may need to be restarted after installation. Review the information and then click **Next**.

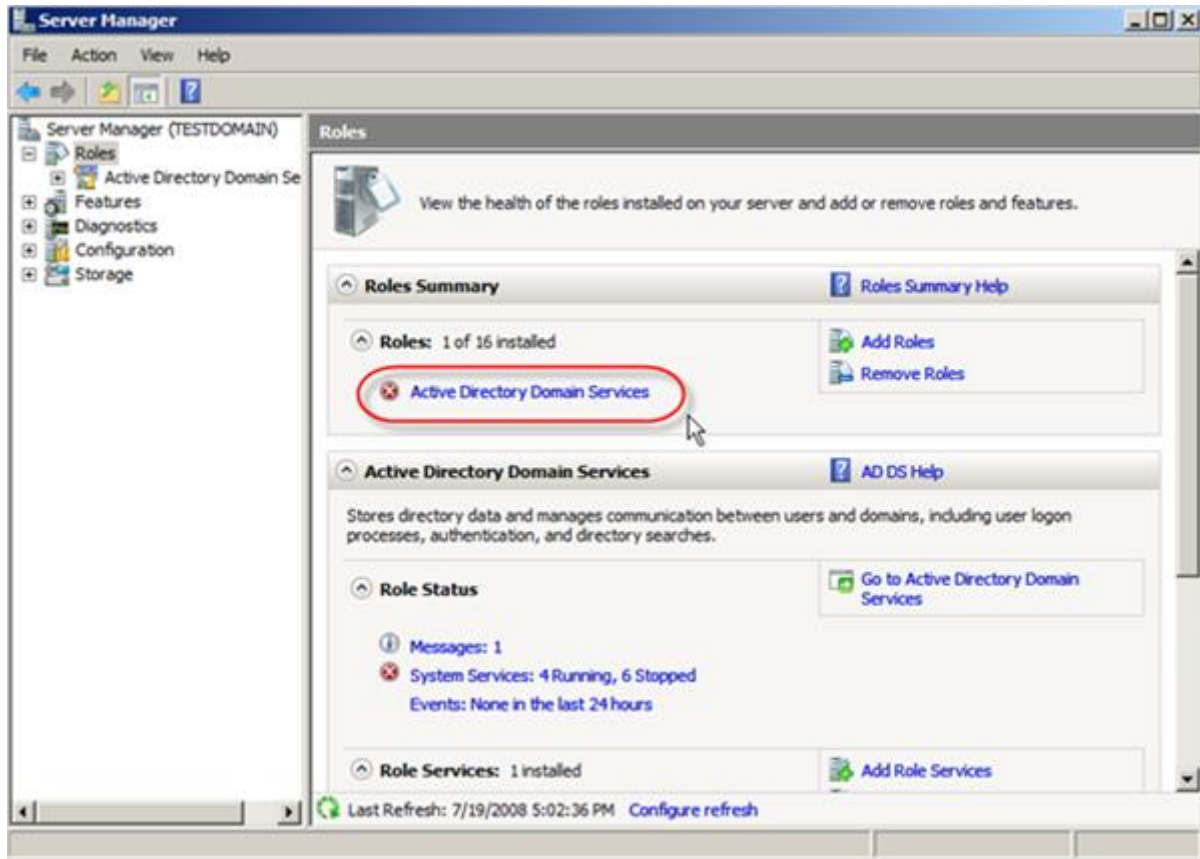


SCREENSHOT:6

7. The **Installation Results** screen will hopefully show **Installation Succeeded**, and an additional warning about running dcpromo.exe ( run dcpromo).

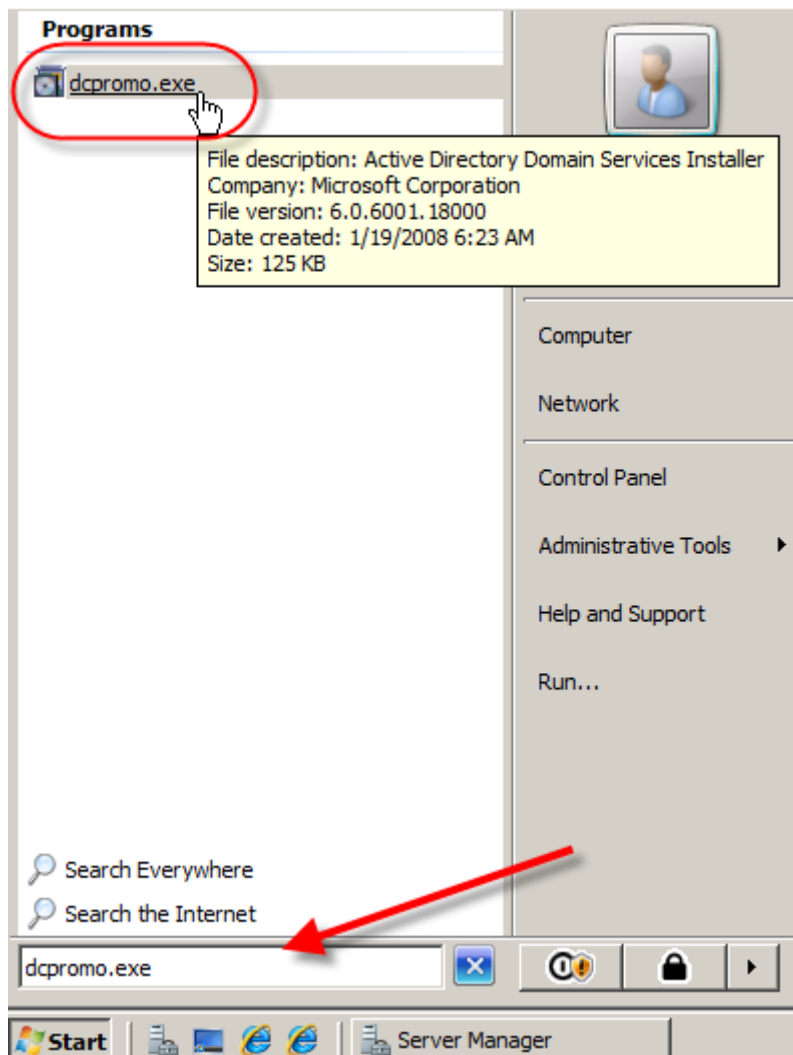


8. After the Installation Wizard closes you will see that server manager is showing that **Active Directory Domain Services** is still not running. This is because we have not run dcpromo yet.



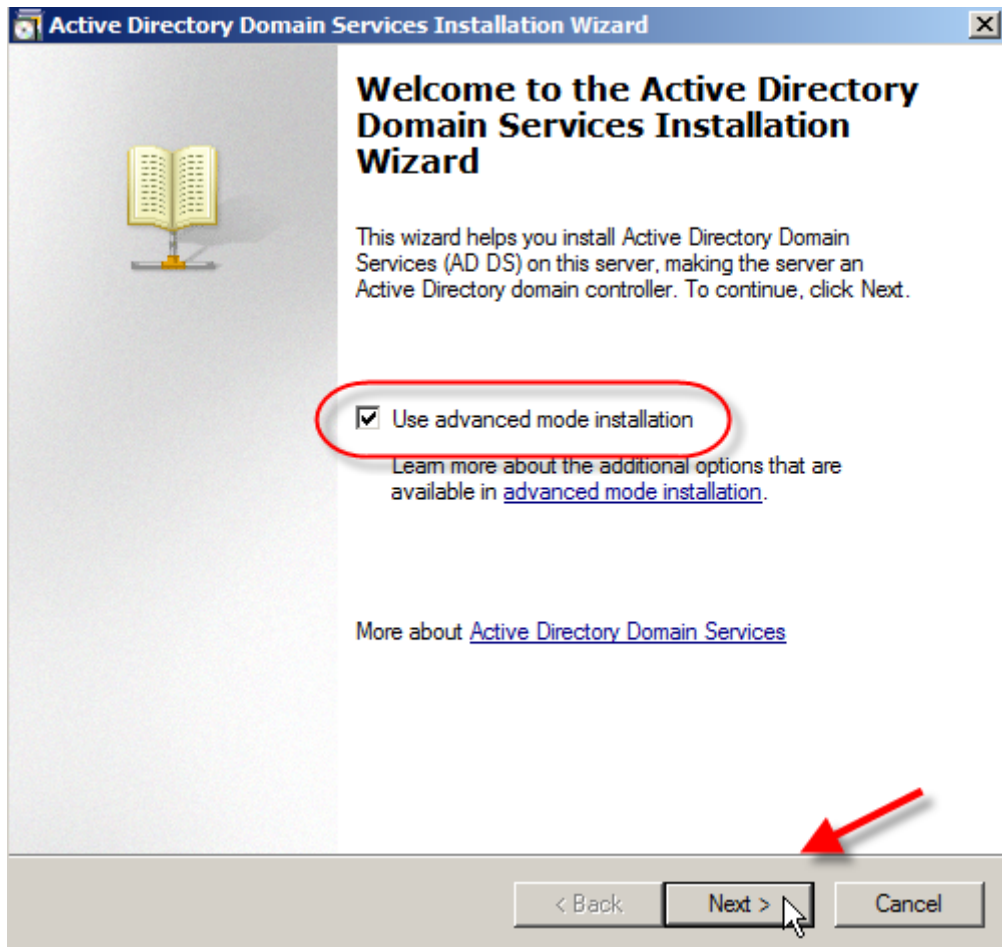
SCREENSHOT:8

9. Click on the **Start** button, type **dcpromo.exe** in the search box and either hit **Enter** or click on the search result.



SCREENSHOT:9

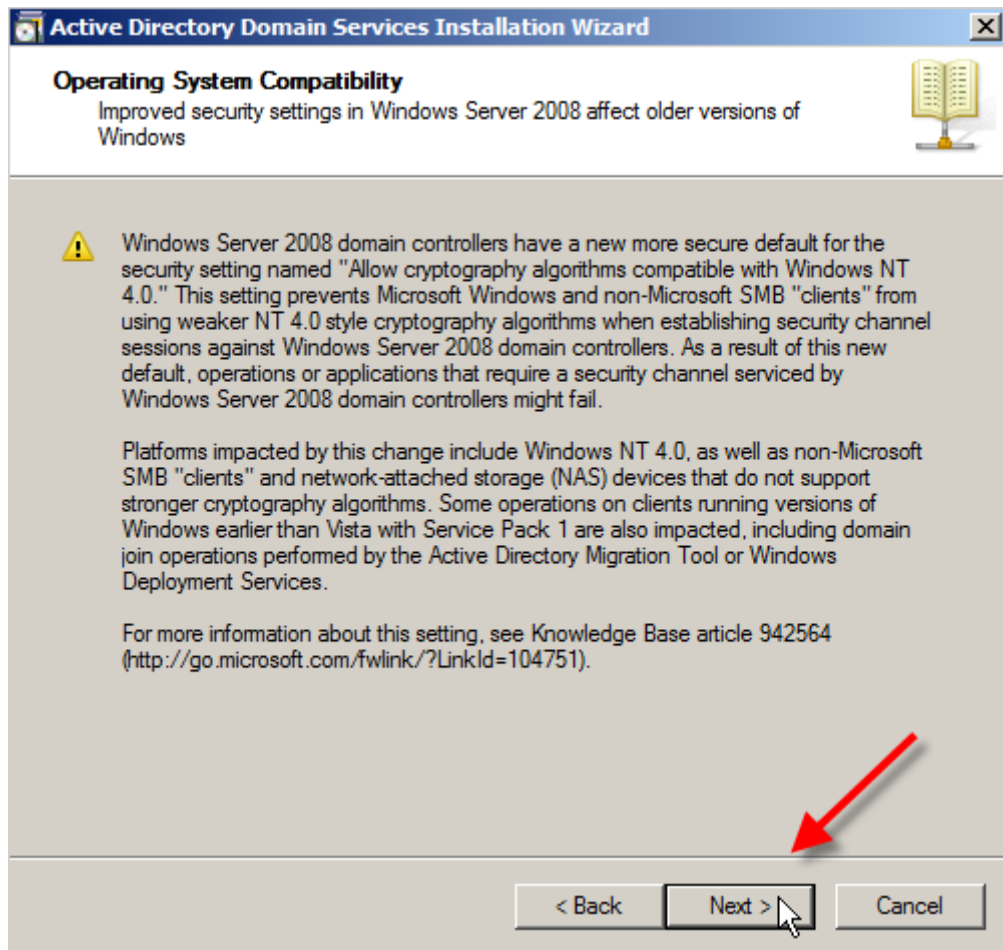
**10.** The **Active Directory Domain Services Installation Wizard** will now start. There are links to more information if you want to learn a bit more you can follow them or you can go ahead and click **Use advanced mode installation** and then click **Next**.



SCREENSHOT:10

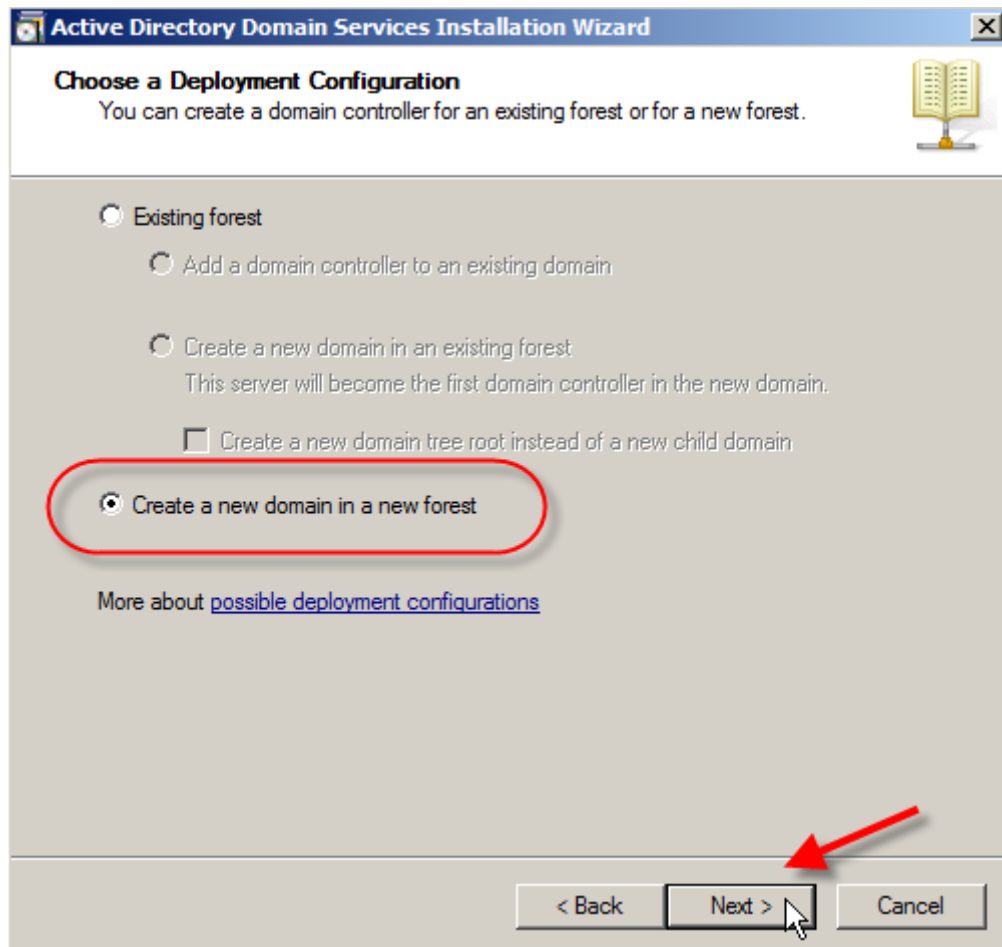
11. The next screen warns about some operating system compatibility with some older clients.

For more information you can view the support documentation from microsoft and after you have read through it go ahead and click **Next**.



SCREENSHOT:11

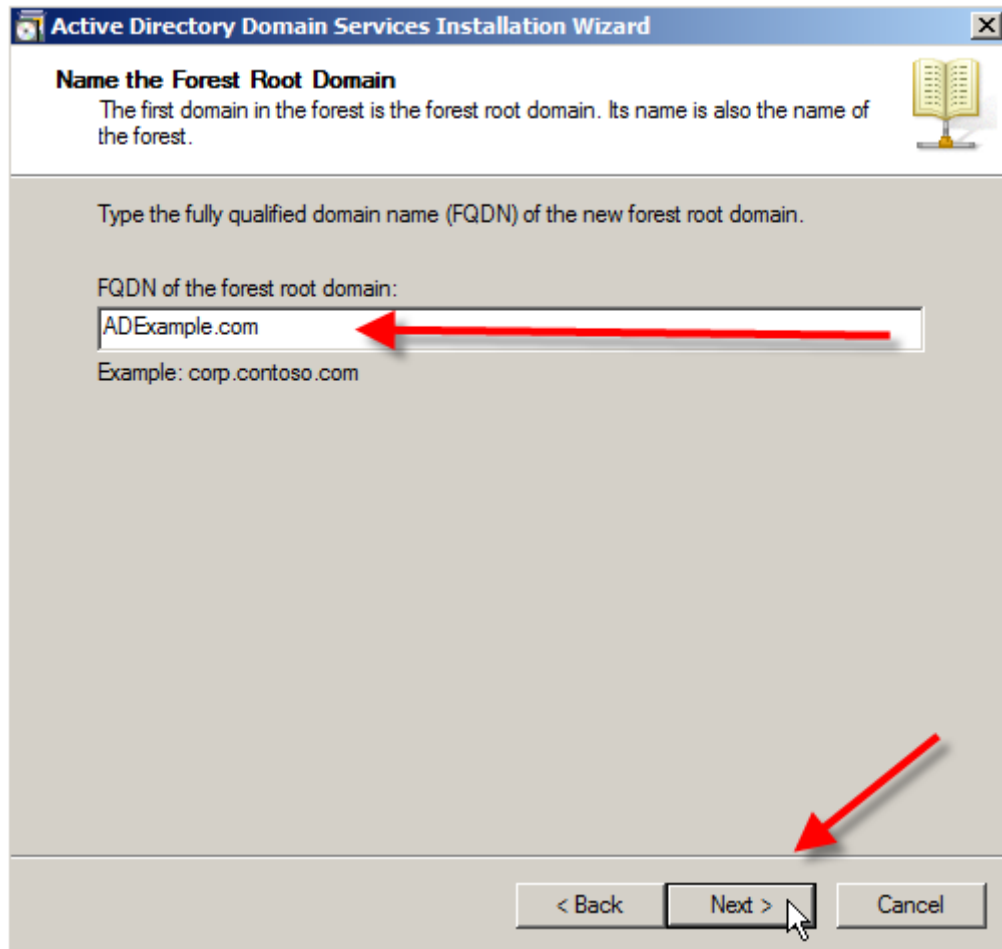
12. Next is the **Choose Deployment Configuration** screen and you can choose to add a domain to an existing forest or create a forest from scratch. Choose **Create a new domain in a new forest** and click **Next**.



SCREENSHOT:12

**13. The Name the Forest Root Domain** wants you to name the root domain of the forest you are creating.

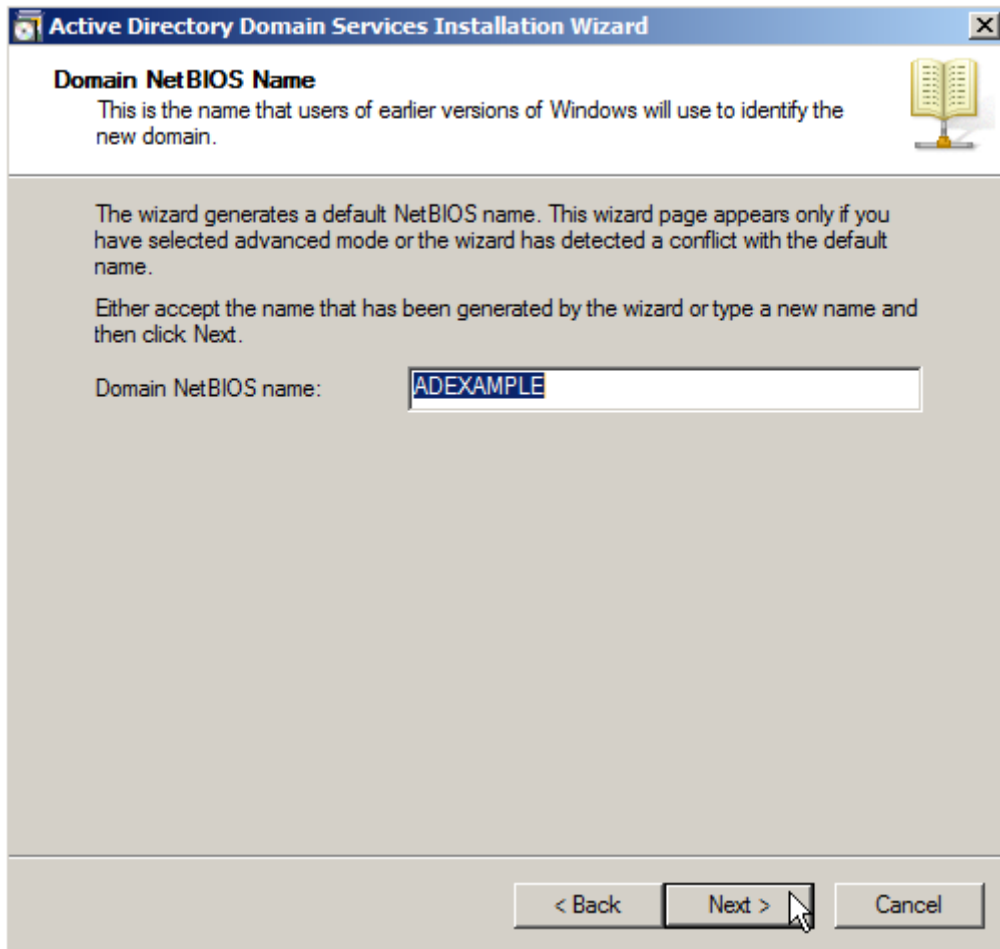
For the purposes of this test we will create **ADExample.com**. After typing that go ahead and click **Next**.



SCREENSHOT:13

**14.** The wizard will test to see if that name has been used, after a few seconds you will then be asked for the NetBios name for the domain. In this case I will leave the default in place of **ADEXAMPLE**, and then click **Next**.



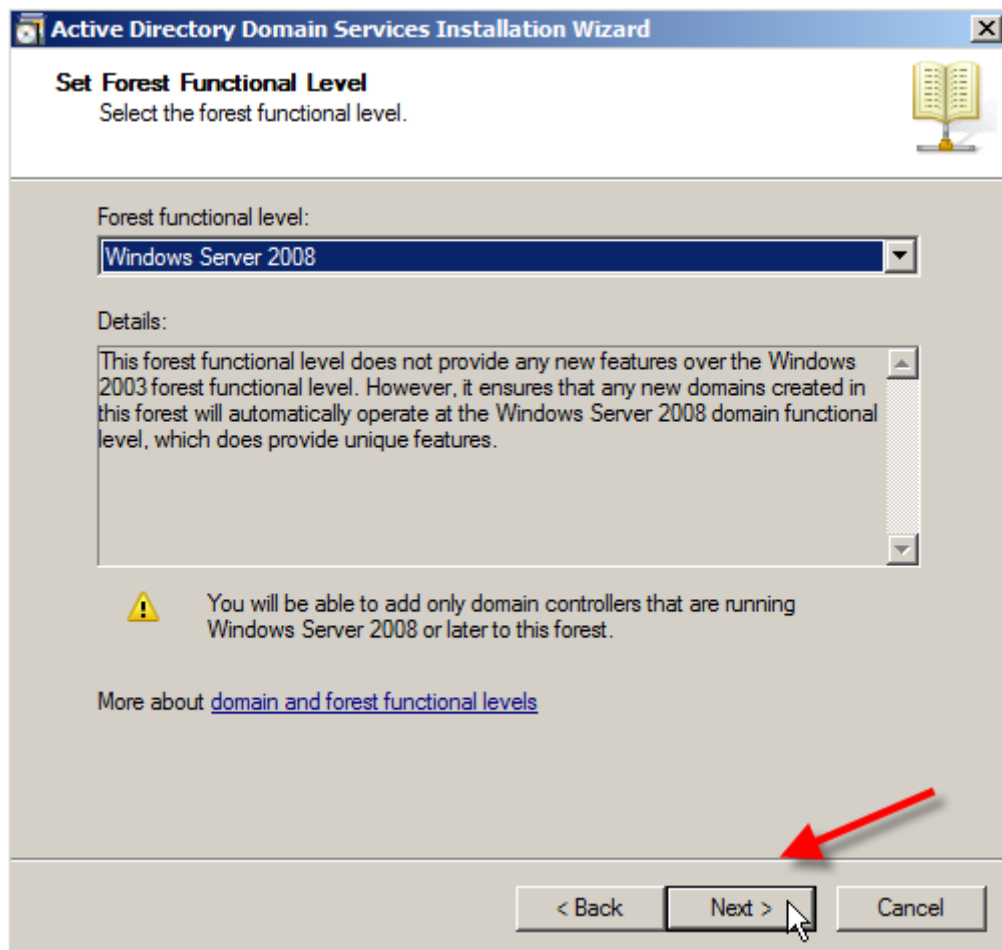


SCREENSHOT:14

**15.** The next screen is the **Set Forest Functional Level** that allows you to choose the function level of the forest.

Since this is a fresh install and a new forest with no additional prior version domains to worry about I am going to select Windows Server 2008. If you did have other domain controllers at earlier versions or had a need to have Windows 2000 or 2003 domain controllers (because of Exchange for example), then you should select the appropriate function level.

Select **Windows Server 2008** and then click **Next**.

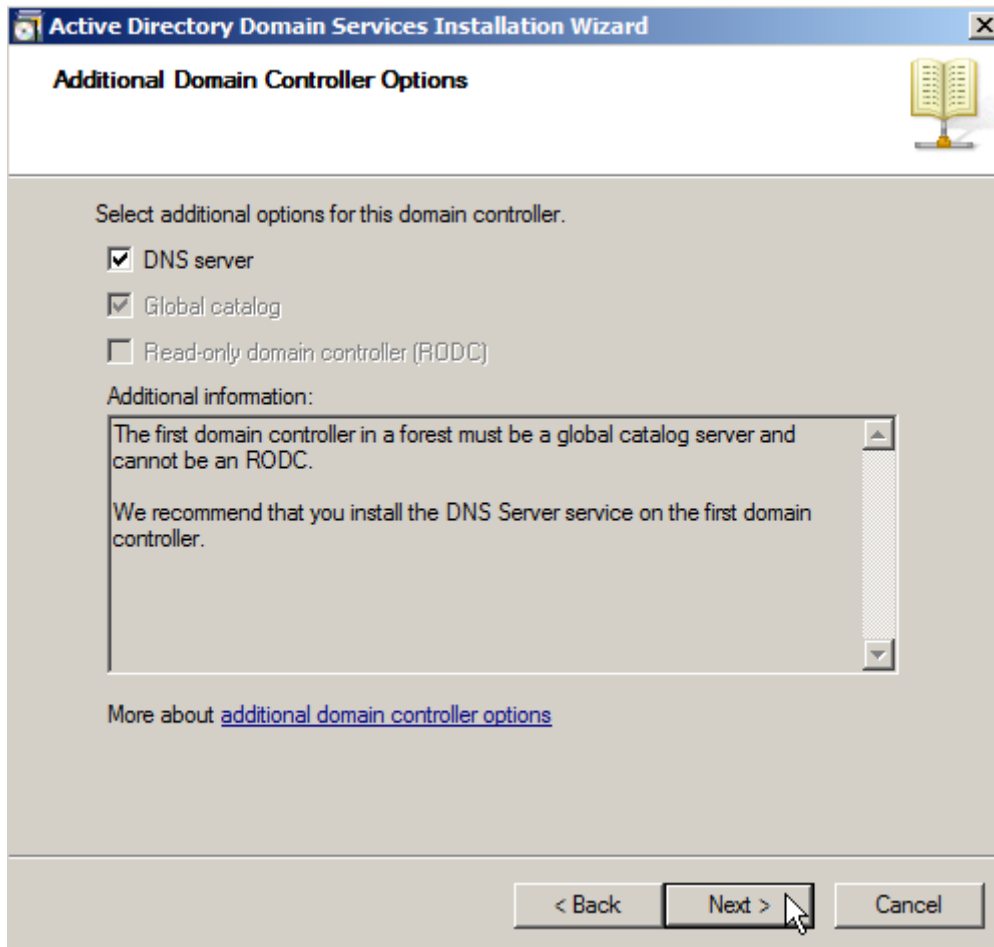


SCREENSHOT:15

**16.** Now we come to the **Additional Domain Controller Options** where you can select to install a DNS server, which is recommended on the first domain controller.

If this was not the first domain controller you would have the options of installing **Global Catalog** and/or setting this as a **Read-only Domain Controller**. Since it is the first domain controller, **Global Catalog** is mandatory, and a **RDOC** controller is not an available option.

Let's install the **DNS Server** by placing a check next to it and clicking **Next**.



SCREENSHOT:16

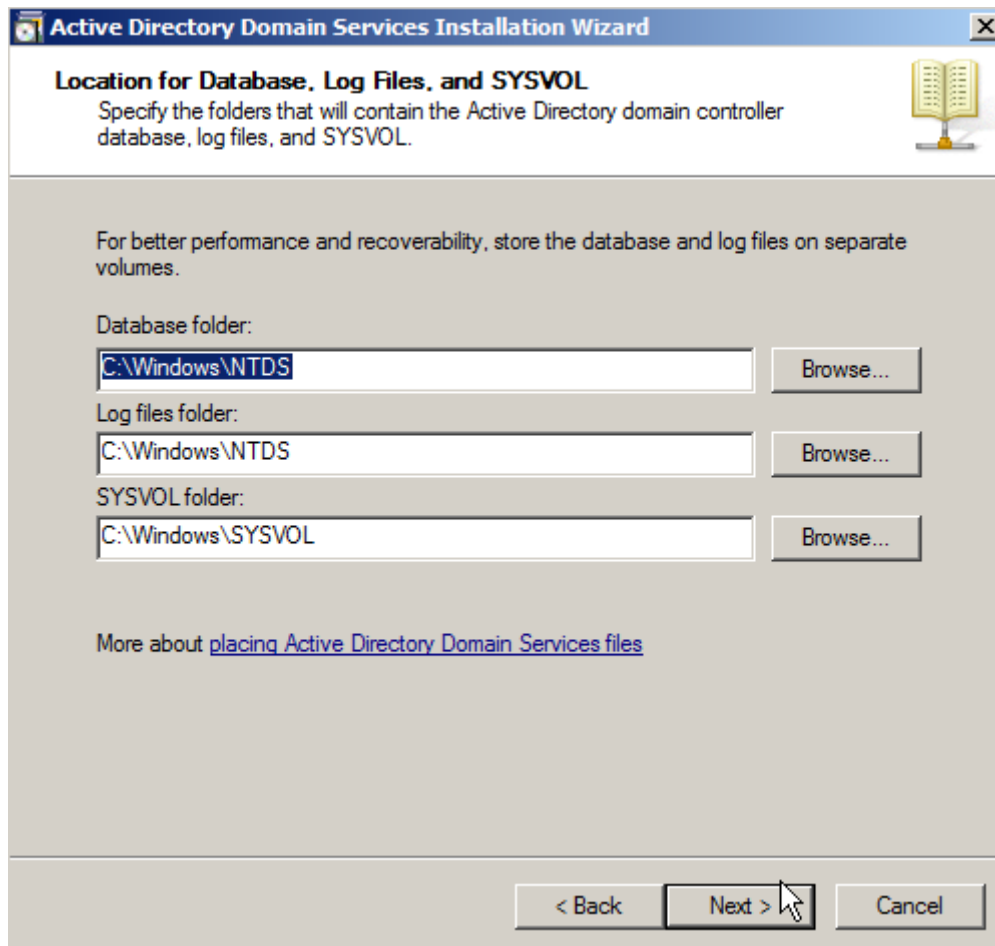
17. You will get a warning window about delegation for this DNS server cannot be created, but since this is the first DNS server you can just click **Yes** and ignore this warning.



SCREENSHOT:17

18. Next you can choose to place the files that are necessary for Active Directory, including the **Database, Log Files, and SYSVOL**.

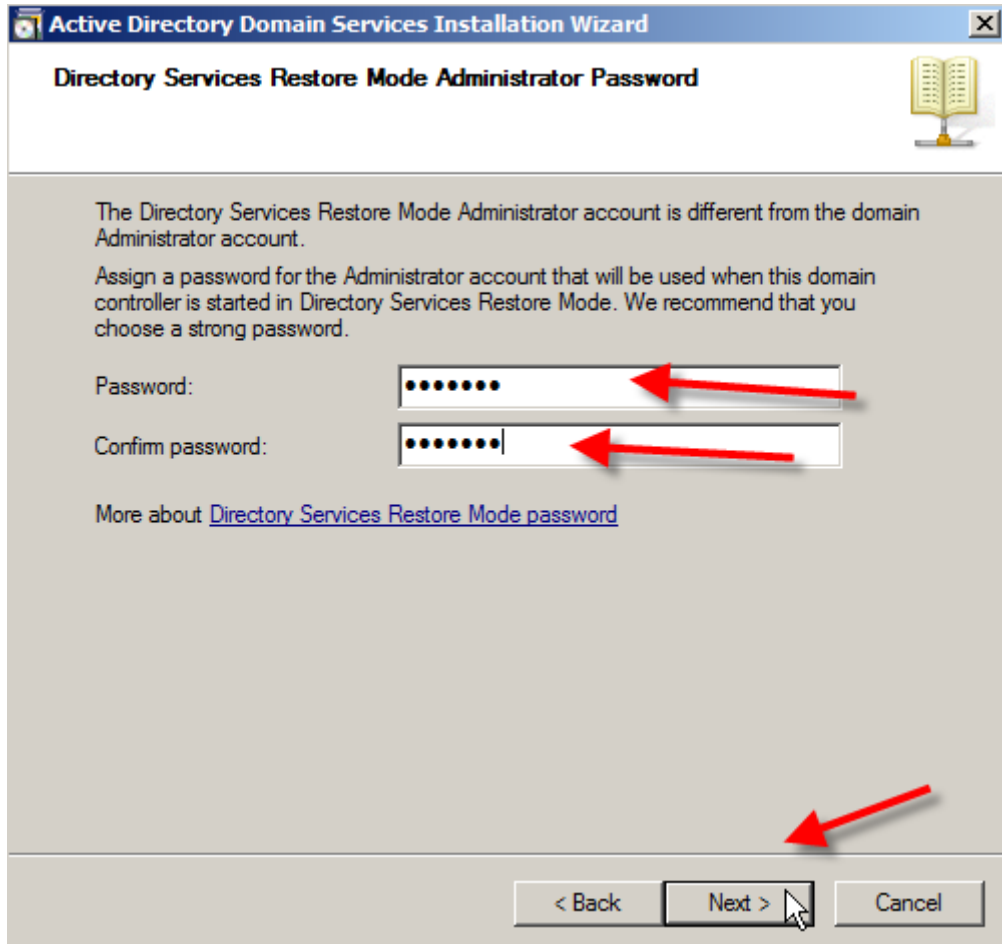
It is recommended to place the log files and database on a separate volume for performance and recoverability. You can just leave the defaults though and click **Next**.



SCREENSHOT:18

19. Now choose a password for **Directory Services Restore Mode** that is different than the domain password. Type your password and confirm it before hitting **Next**.

**Note:** You should use a **STRONG** password for this and will be warned if it doesn't meet criteria.



The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password:

Confirm password:

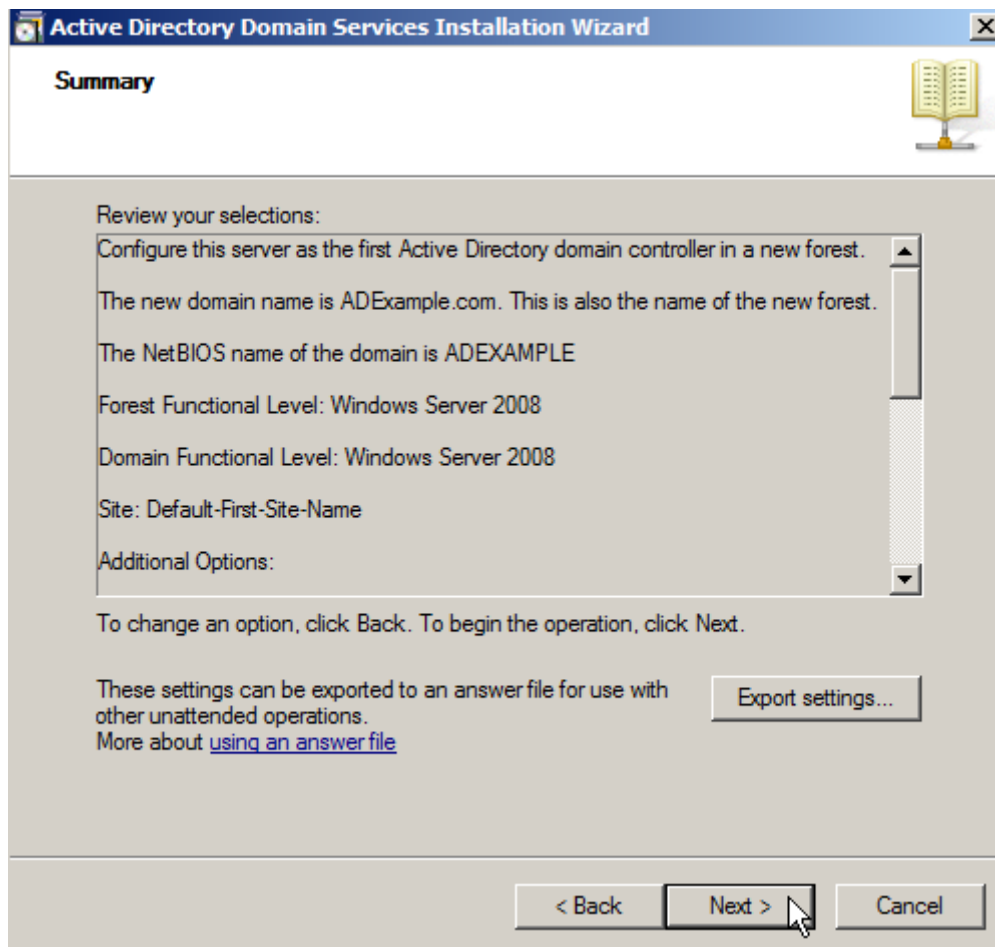
More about [Directory Services Restore Mode password](#)

< Back Next > Cancel

SCREENSHOT:19

20. Next you will see a summary of all the options you have went through in the wizard.

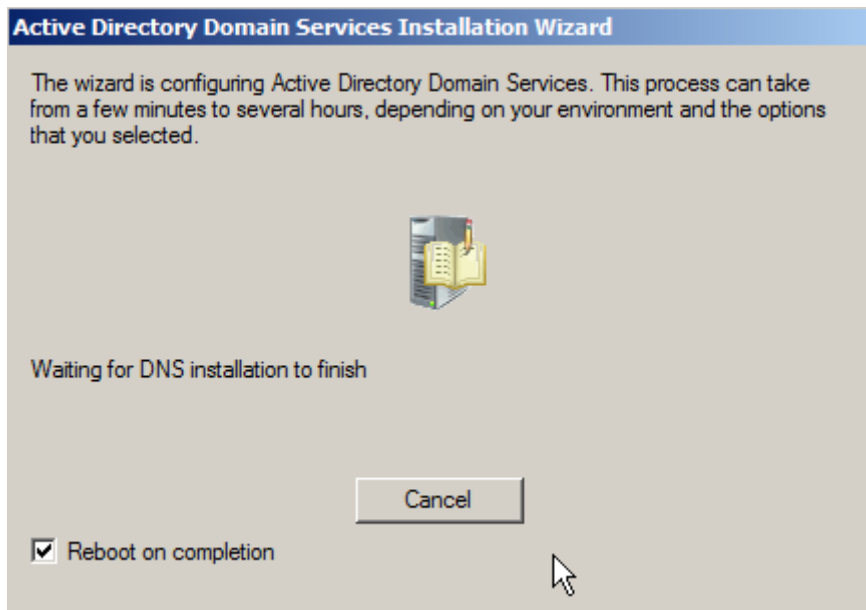
If you plan on creating more domain controllers with the same settings hit the **Export settings ...** button to save off a txt copy of the settings to use in an answer file for a scripted install. After exporting and reviewing settings click on **Next**.



SCREENSHOT:20

21. Now the installation will start including the DNS server option if selected. You will notice a box to **Reboot on completion** that you can check to reboot soon as everything is installed (A reboot is required you can do it manually or use this function to do it automatically).

**NOTE: This can be from a few minutes to several hours depending on different factors.**

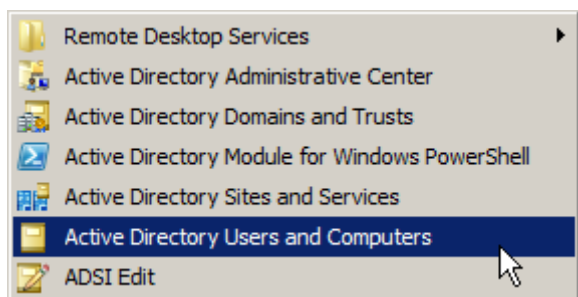


SCREENSHOT:21

### **4.3 Our next step is to create a user in active directory**

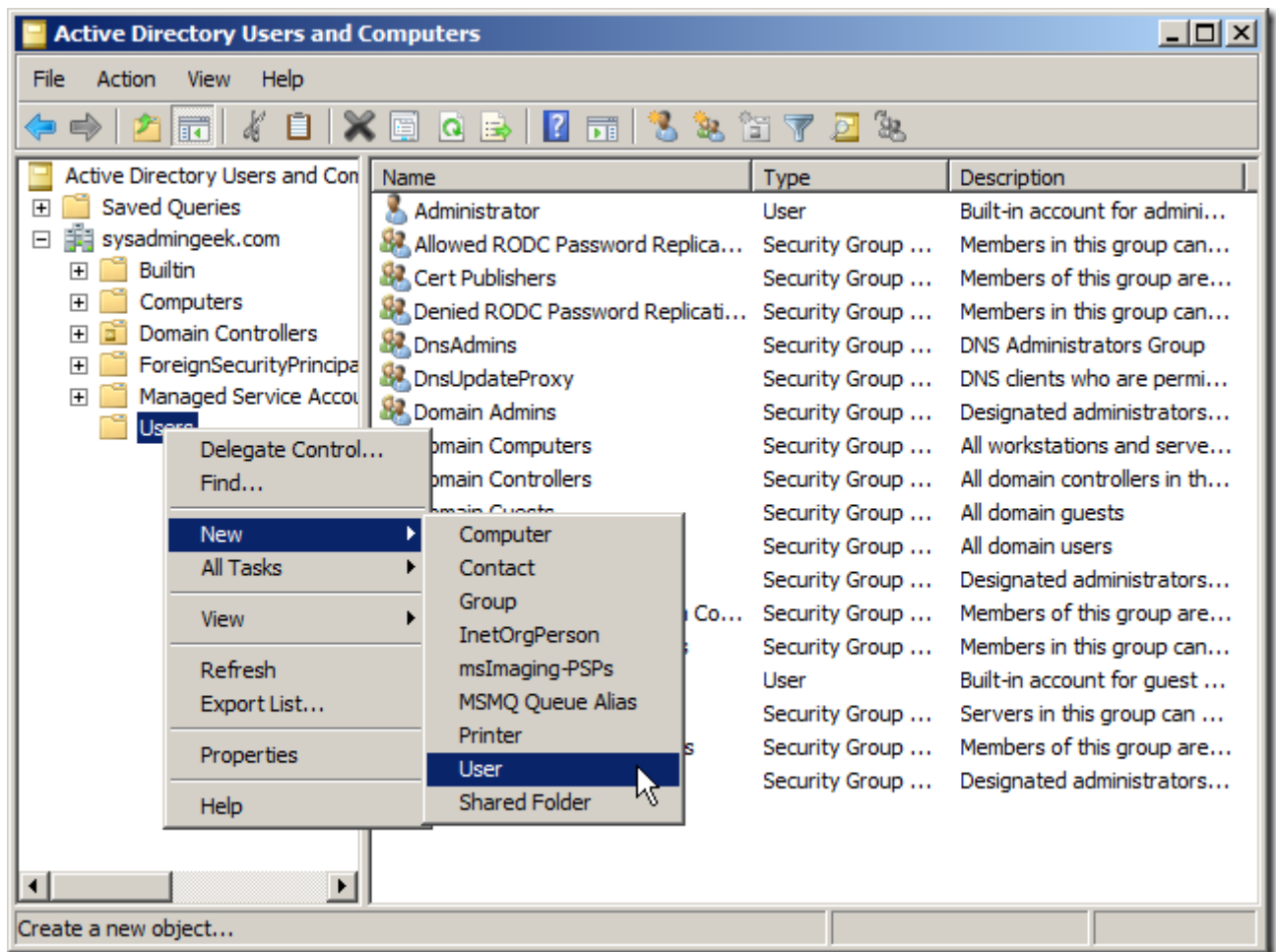
One of the first things to do in a new network is to create Users, also called User Objects. As long as you know the information about the user you need to create, the process will take no time at all.

This is a task we want to do from a Domain Controller, and you should have the Administrative Tools in your Start menu next to the Control Panel link. We'll choose the *Active Directory Users and Computers* snap-in.



SCREENSHOT:22

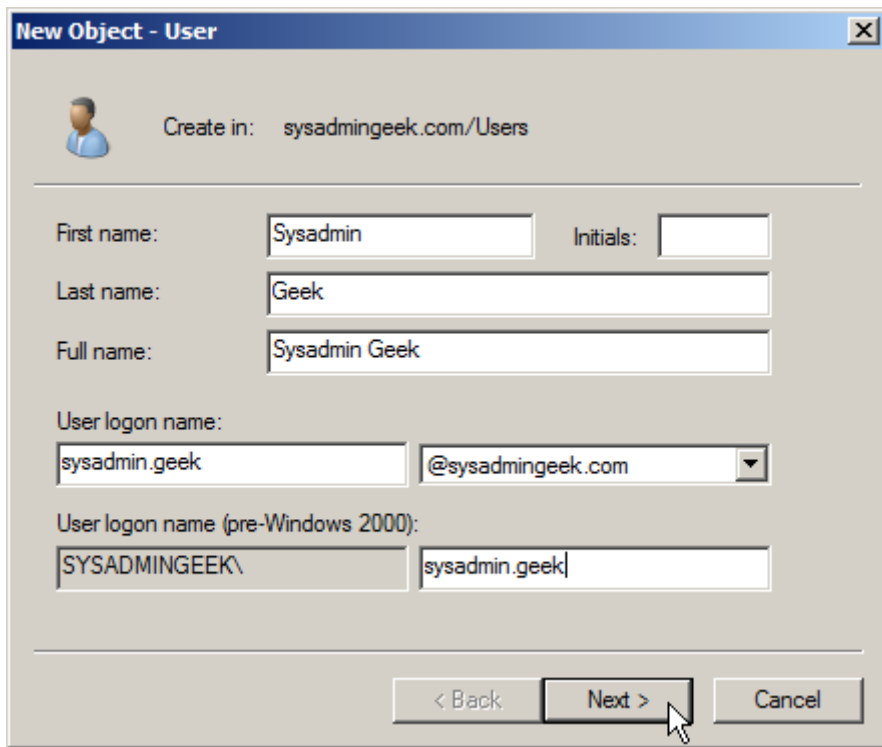
Once we're inside the *Active Directory Users and Computers* snap-in, we'll need to expand the domain in which we want to create the user, and right-click on the *userfolder*. We'll then select *New|User*.



SCREENSHOT:23

The *New Object – User* box will pop up and require you to put in the user's name and create the user logon. You'll need to use a standard method of creating user logon names, as this will cause much less confusion in the future. If you have a small network, you may want to just stick to using the first initial and last name because it's shorter. If you anticipate that your network will grow quite large, the standard advice is to use the full first and last name separated by a period, as we've done below.





**New Object - User**

Create in: sysadmingeek.com/Users

First name: Sysadmin Initials:

Last name: Geek

Full name: Sysadmin Geek

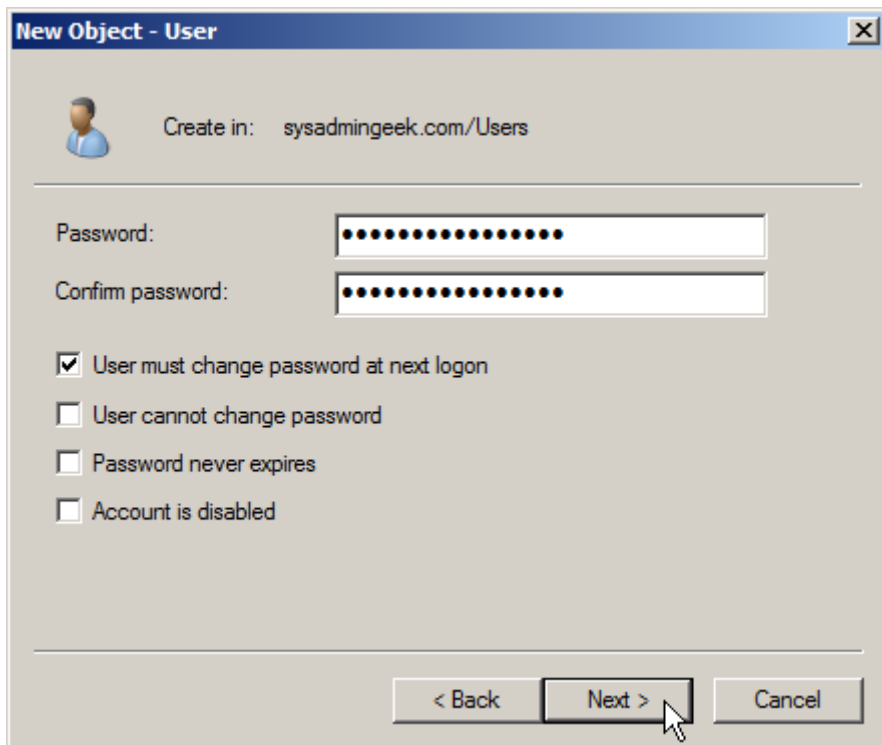
User logon name: sysadmin.geek @sysadmingeek.com

User logon name (pre-Windows 2000): SYSADMIN.GEEK\ sysadmin.geek

< Back Next > Cancel

SCREENSHOT:24

Next we'll give the user an initial password, and make sure to have them change it as soon as they first logon.



**New Object - User**

Create in: sysadmingeek.com/Users

Password:

Confirm password:

☒ User must change password at next logon

☐ User cannot change password

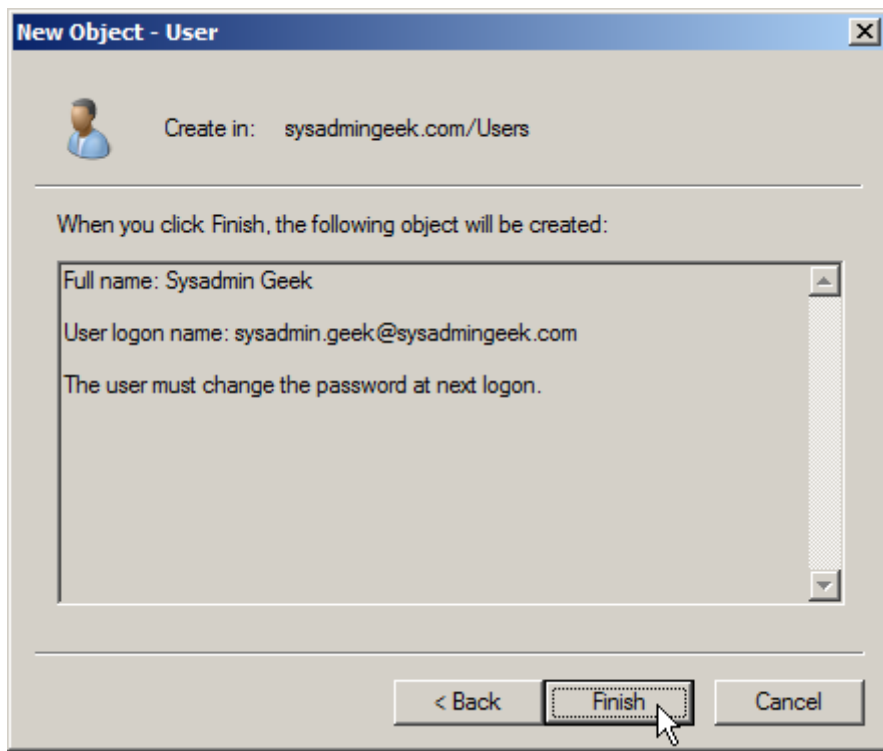
☐ Password never expires

☐ Account is disabled

< Back Next > Cancel

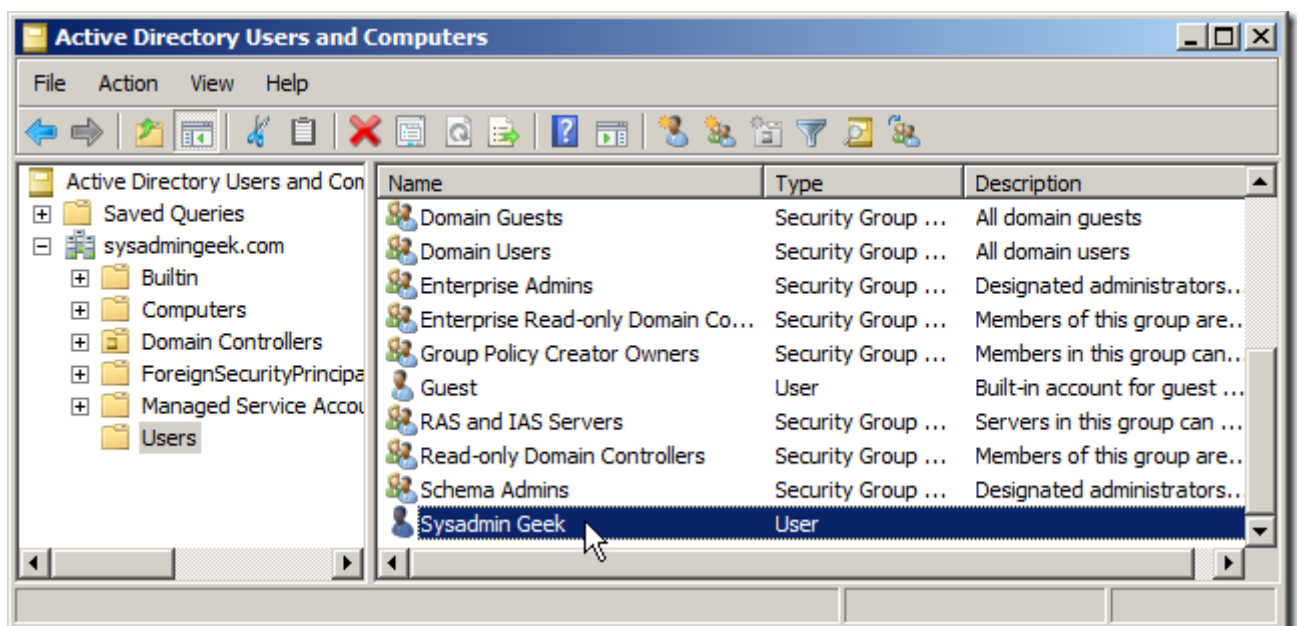
SCREENSHOT:25

When we're finished, we'll get a nice summary of our work.



SCREENSHOT:26

When we go back to the *Users* folder in the domain, we can see our newly created user.



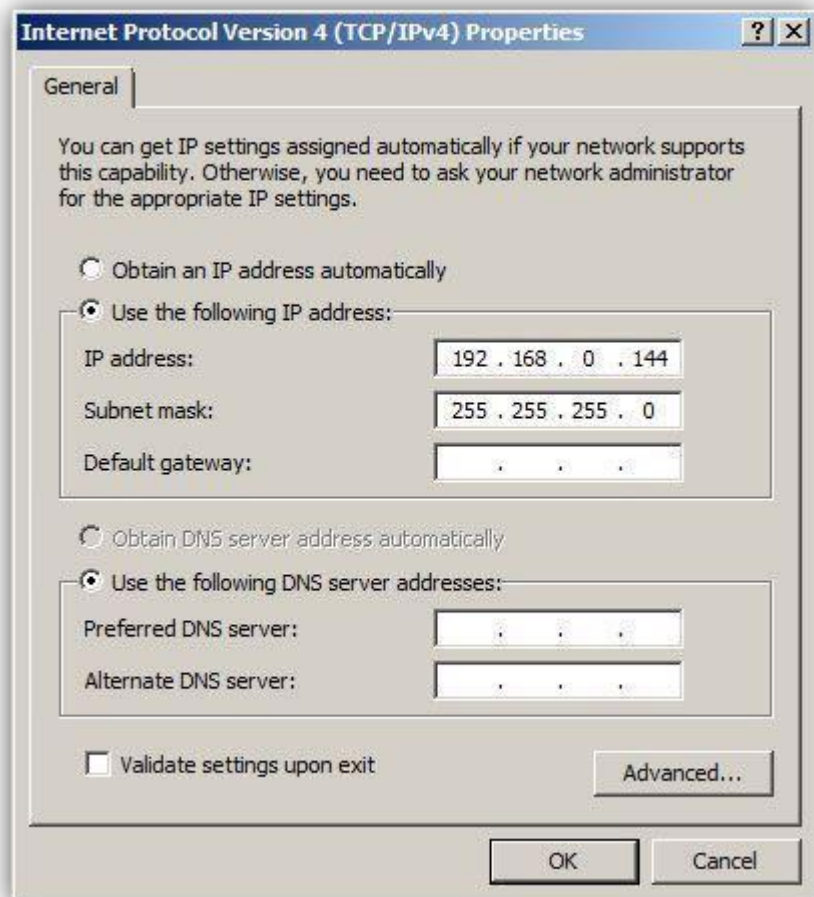
SCREENSHOT:27

Once we've created a user, there are many things that we'll need to do with them in order for them to be useful, like adding permissions and security groups, but at least the operation for spawning them is simple and straightforward.

## 4.4 CONFIGURING STATIC DOMAIN

Assigning a static IP address to a computer requires elevated privileges and therefore administrator account must be used to log on to Windows Server 2008 R2 computer while following the steps below:

1. Log on to Windows Server 2008 computer



with Administrator account. ( SCREENSHOT:28)

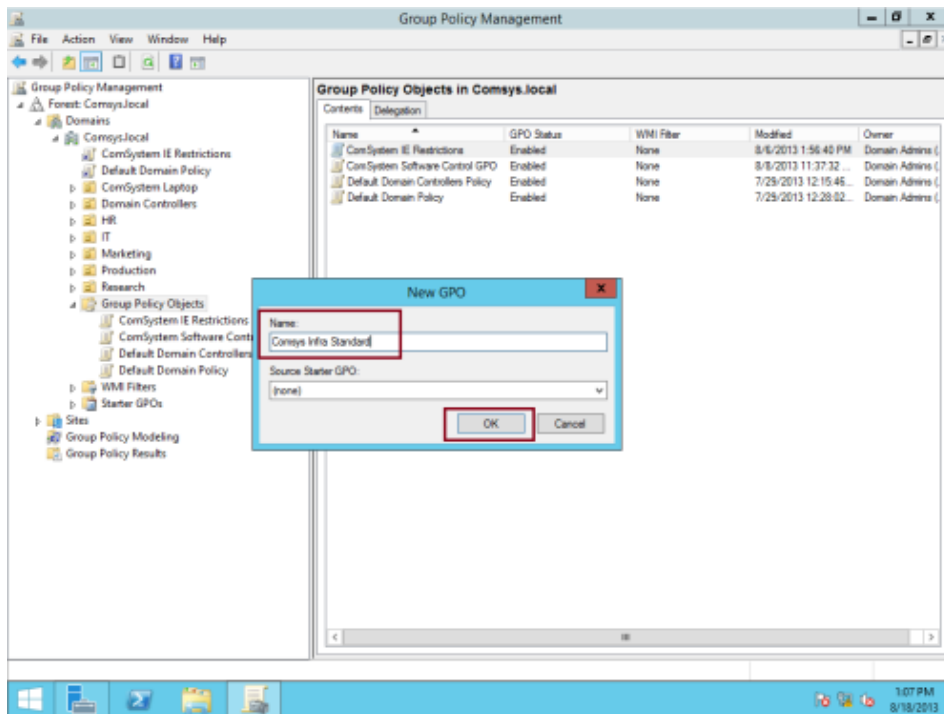
2. Click Start and then click Run from the menu.
3. In the opened Run command box type NCPA.CPL command and press Enter key.
4. On the opened window right-click on the NIC on which static IP address has to be assigned and from the available context menu click Properties.

5. On Local Area Network Properties box make sure that Networking tab is selected and from the available list of options in the middle box double-click Internet Protocol Version 4 (TCP/IPv4).
6. On Internet Protocol Version 4 (TCP/IPv4) Properties box make sure that General tab is selected and click to select Use the following IP address radio button.
7. Populate the enabled IP address and Subnet mask fields with appropriate values, i.e. IP address and subnet mask and click OK button. Enter ip address(192.168.1.169) subnet mask(255.255.255.0) and default gateway(192.168.1.1).
8. Back on Local Area Connection Properties box click OK to save the changes.

#### 4.4 policy Management

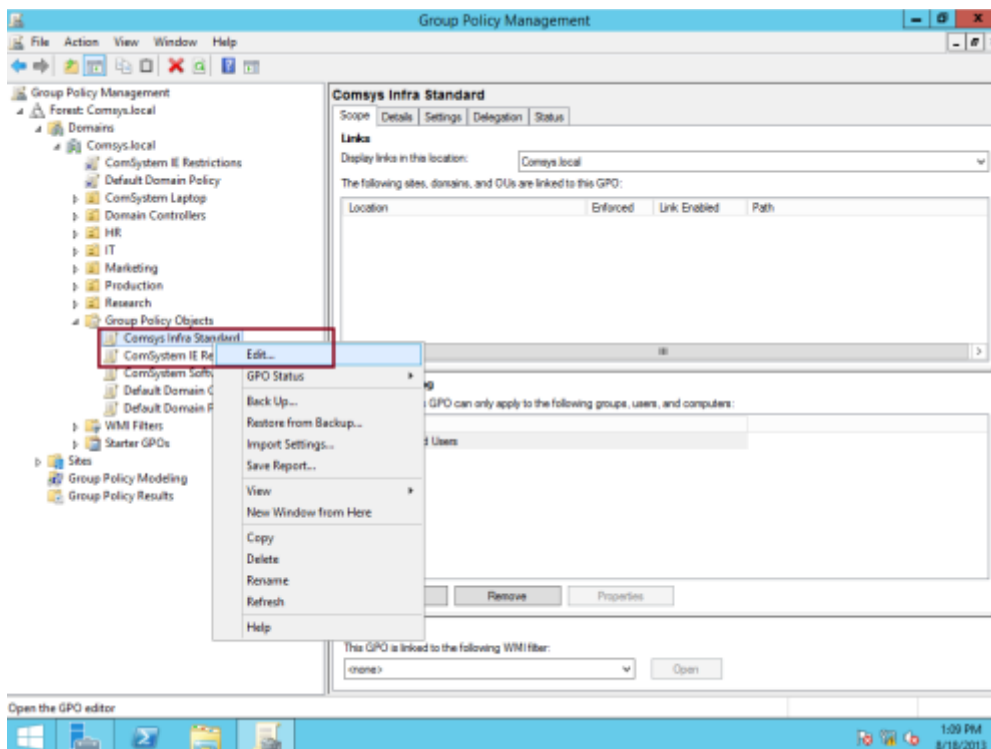
Next important thing is to put the policy on the user that we made. So, let know how to put policy in the user.

1 – As usual on the domain server, create a new GPO, in my case my new GPO will be Comsys Infra Standard...



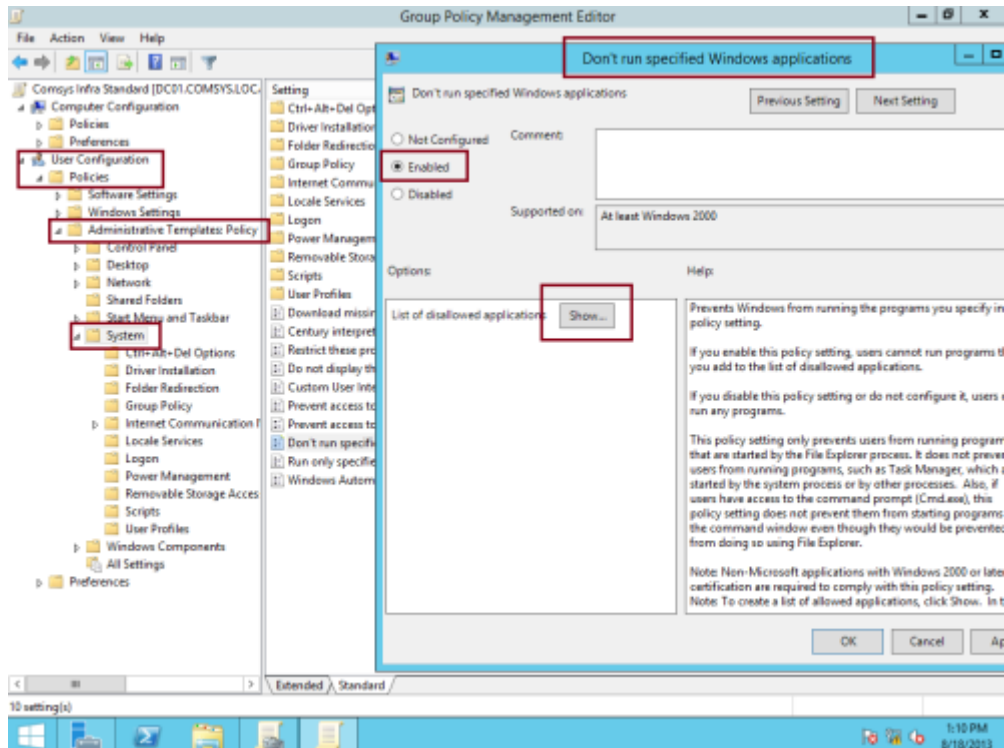
SCREENSHOT:29

2 – Next, right click Comsys Infra Standard GPO and click Edit...



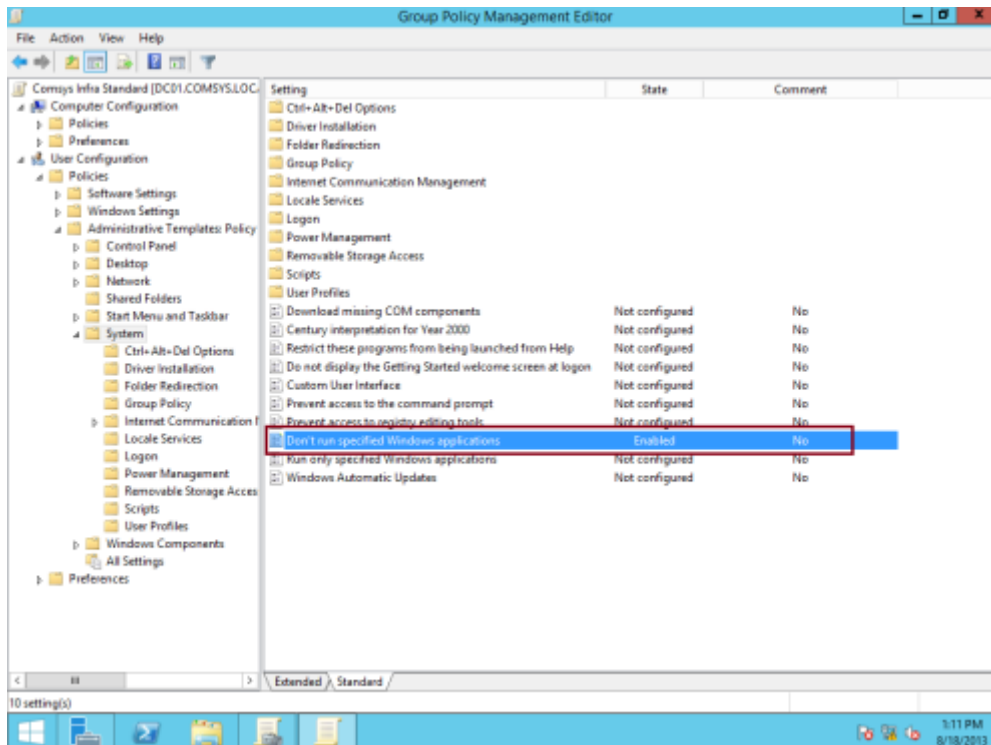
SCREENSHOT:30

3 – Next, on the Group Policy Management Editor, expand User Configuration, Policies, and Administrative Templates, and then click System, next double click Don't run specified Windows applications, click Enabled and click Show...



SCREENSHOT:31

4 – In the Show Contents box, in the Value list, type notepad.exe, Calc.exe and Paint.exe and then click OK...

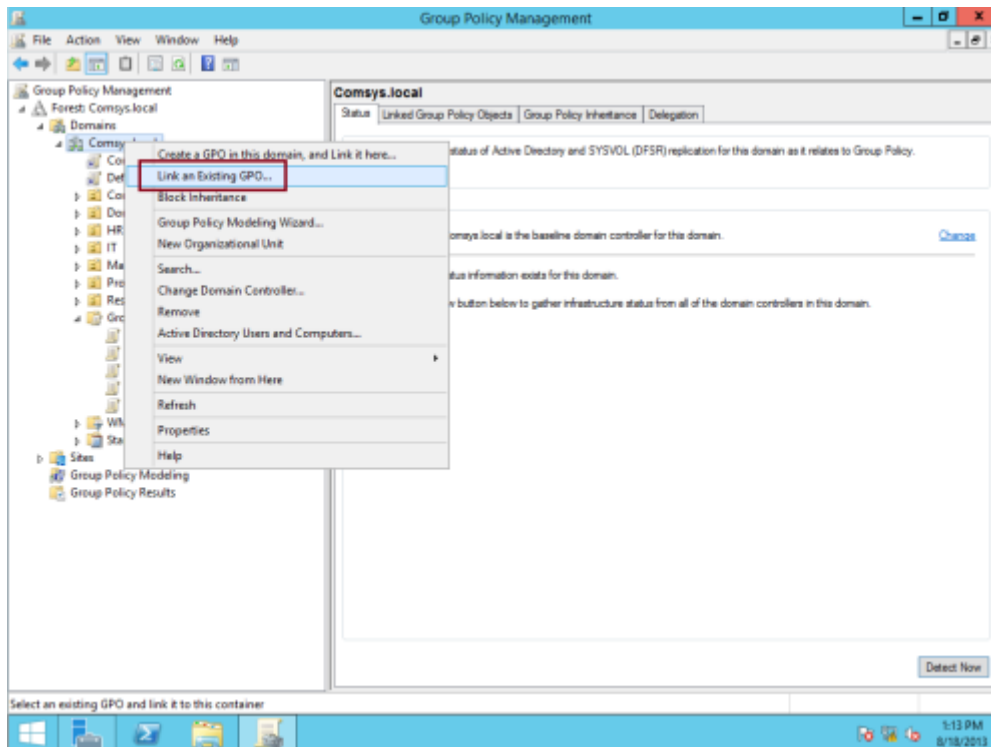


SCREENSHOT:32

5 – Next, click Control Panel, on the right pane, double click Prohibit access to Control Panel and PC Settings, then click Enabled and click OK...

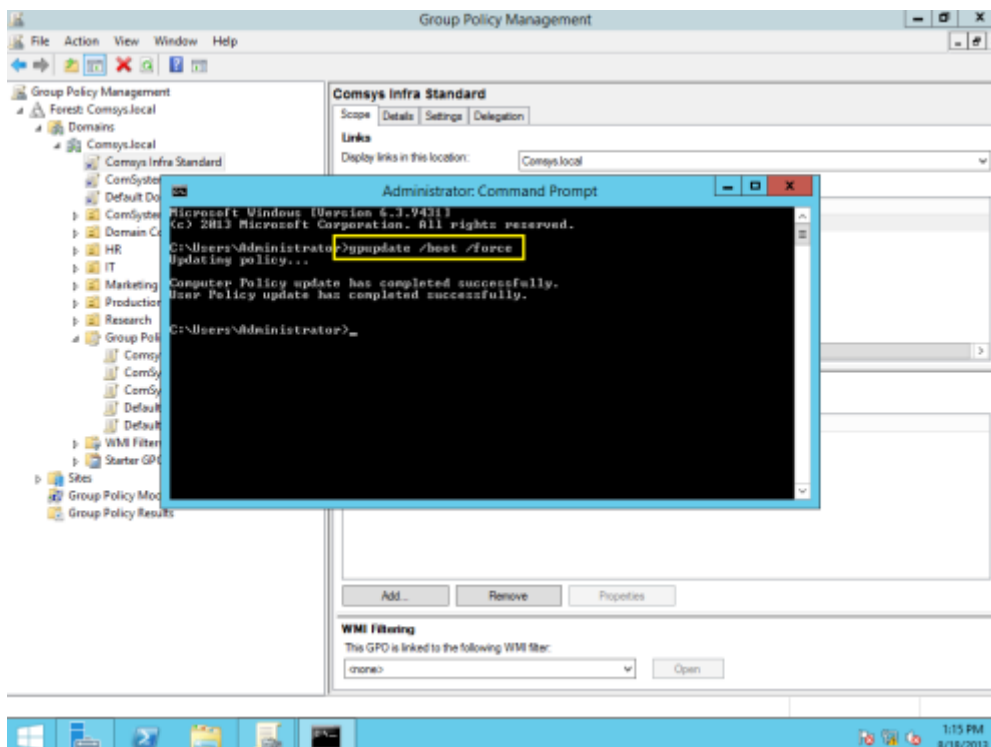
6 - Next, lets Link the Comsys Infra Standard GPO to our domain, right click Comsys.local and click Link an Existing GPO...

7 – On the Select GPO box, under Group Policy Object, click Comsys Infra Standard and then click OK to proceed...



SCREENSHOT:33

8 – Next, you can open CMD and type gpupdate /boot /force...



SCREENSHOT:34



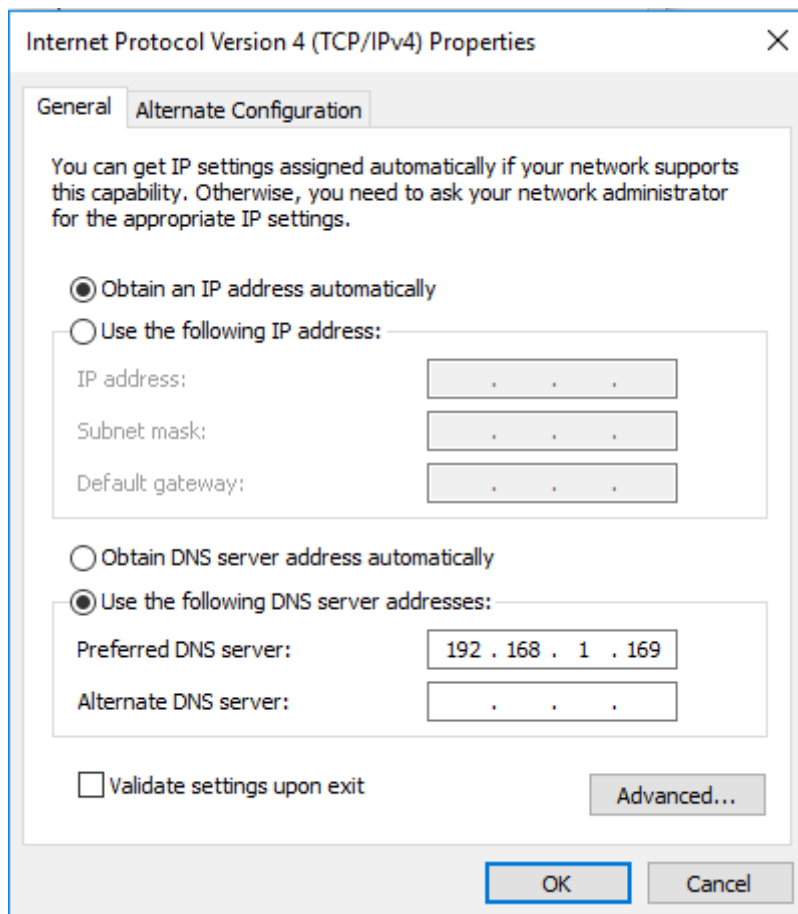
We are all done here , just reboot the system and our policies got apply on the user.

#### 4.5 Static IP Configuration In Client

Now next important thing is to login user in the other system (as we have use window 7 here)

For it we have to simply:

- First enter the lan setting in network and sharing manager and open ipv4 setting and change the DNS configuration to our server ip i.e 192.168.1.169



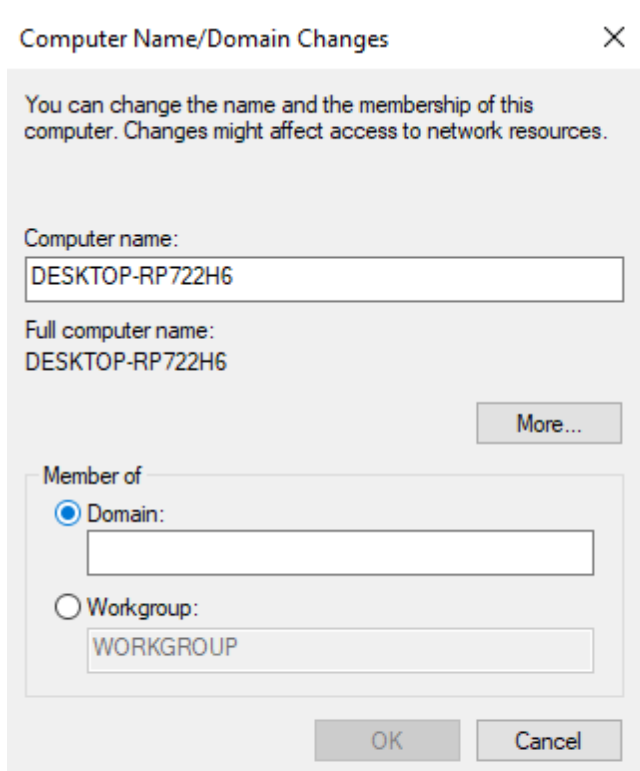
SCREENSHOT:35

And click ok to apply the setting .

## 4.6 Login Into User

As we configure the IP . client domain IP is connected to server IP so we can simply login into the user

1. Now open system properties.
2. Then click on change the domain.
3. Then click on domain and enter the name of domain that we make earlier i.e ADEXAMPLE.



SCREENSHOT:36

4. After that we need to login with administer and password of windows server.
5. After successful login , we need to start the pc and on login screen we login via the user and enter the password of it. That's it we are now in the user account with our security policies that we applied

# 5.

## Hardware and Software used

### 5.1Hardware:

<u>component</u>	<u>requirement</u>
processor	1 GHz (x86 CPU) or 1.4 GHz (x64 CPU)
RAM	2GB required; 8GB or higher recommended.
Hard Disk	10 GB required. 40 GB or more recommended.
Video	Super VGA or higher video card and monitor.
Hardware	Must be on the Windows 2008 Hardware Compatibility List.

**TABLE:4**

#### 5.1.1Processor:

Processor matters most when it comes to execution of program. Currently processor comes in x86,x64,x32 : where 86,64,32 means bits. Intel i7 currently is best processor when it comes to speed , i5 is also good. But we use AMD A8 for our project, it is 64 bit processor having four cores.

### 5.1.2 RAM:

The total ram in this is laptop is 8GB. As we have Vmware tool so we ave use distributed ram and gave approx. 3GB of ram to our server and windows 7, which is also higher than minimum requirement.

### 5.1.3 HARDDISK:

A size of 60GB is allocated to each O.S from a total of 1TB.

### 5.1.4 VIDEO:

AMD video graphics are used having capacity of 6GB.

NOTE: All the hardware are microsoft windows supported .

## 5.2 SOFTWARE USED:

We have used mainly three software which also includes O.S:

- Windows server 2008.
- Windows NT family O.S(windows 7).
- Vmware workstation for virtualization.

A brief summary of windows server 2008 with its architecture is described just below. We can conclude them from this what we want.

As comes to windows NT it is a family of operating systems produced by Microsoft, the first version of which was released in July 1993. It is a processor-independent, multiprocessing, multi-user operating system. "NT" formerly expanded to "New Technology" but no longer carries any specific meaning. Starting with Windows 2000, "NT" was removed from the product name and is only included in the product version string.

VMware Workstation is a hosted hypervisor that runs on x64 versions of Windows and Linux operating systems it enables users to set up virtual machines (VMs) on single physical machine, and use them simultaneously along with the actual machine.

---

### 5.2.1 WINDOWS NT:

---

Windows NT is a family of operating systems produced by Microsoft, the first version of which was released in July 1993. It is a processor-independent, multiprocessing, multi-user operating system.

The first version of Windows NT was Windows NT 3.1 and was produced for workstations and server computers. It was intended to complement consumer versions of Windows that were based on MS-DOS (including Windows 1.0 through Windows 3.1x). Gradually, the Windows NT family was expanded into Microsoft's general-purpose operating system product line for all personal computers, deprecating the Windows 9x family.

"NT" formerly expanded to "New Technology" but no longer carries any specific meaning. Starting with Windows 2000, "NT" was removed from the product name and is only included in the product version string.

NT was the first purely 32-bit version of Windows, whereas its consumer-oriented counterparts, Windows 3.1x and Windows 9x, were 16-bit/32-bit hybrids. It is a multi-architecture operating system. Initially, it supported several instruction set architectures, including IA-32, MIPS, DEC Alpha, PowerPC and later Itanium. The latest versions support x86 (more specifically IA-32 and x64) and ARM. Major features of the Windows NT family include Windows Shell, Windows API, Native API, Active Directory, Group Policy,

Hardware Abstraction Layer, NTFS, BitLocker, Windows Store, Windows Update, and Hyper-V.

It has been suggested that Dave Cutler intended the initialism "WNT" as a play on VMS, incrementing each letter by one.[4] However, the project was originally intended as a follow-on to OS/2 and was referred to as "NT OS/2" before receiving the Windows brand.[5] One of the original NT developers, Mark Lucovsky, states that the name was taken from the original target processor—the Intel i860, code-named N10 ("N-Ten"). A 1998 question-and-answer session with Bill Gates, reveal that the letters were previously expanded to "New Technology" but no longer carry any specific meaning.[7] The letters were dropped from the names of releases from Windows 2000 and later, though Microsoft described that product as being "Built on NT Technology".

Microsoft decided to create a portable operating system, compatible with OS/2 and POSIX and supporting multiprocessing, in October 1988. When development started in November 1989, Windows NT was to be known as OS/2 3.0,[17] the third version of the operating system developed jointly by Microsoft and IBM. To ensure portability, initial development was targeted at the Intel i860XR RISC processor, switching to the MIPS R3000 in late 1989, and then the Intel i386 in 1990. Microsoft also continued parallel development of the DOS-based and less resource-demanding Windows environment, resulting in the release of Windows 3.0 in May 1990. Windows 3 was eventually so successful that Microsoft decided to change the primary application programming interface for the still unreleased NT OS/2 (as it was then known) from an extended OS/2 API to an extended Windows API. This decision caused tension between Microsoft and IBM and the collaboration ultimately fell apart. IBM continued OS/2 development alone while Microsoft continued work on the newly renamed Windows NT. Though neither operating system would immediately be as popular as Microsoft's MS-DOS or Windows products, Windows NT would eventually be far more successful than OS/2.

Microsoft hired a group of developers from Digital Equipment Corporation led by Dave Cutler to build Windows NT, and many elements of the design reflect

earlier DEC experience with Cutler's VMS and RSX-11, but also an unreleased object-based operating system developed by Dave Cutler for DEC Prism. The operating system was designed to run on multiple instruction set architectures and multiple hardware platforms within each architecture. The platform dependencies are largely hidden from the rest of the system by a kernel mode module called the HAL (Hardware Abstraction Layer).

Windows NT's kernel mode code further distinguishes between the "kernel", whose primary purpose is to implement processor- and architecture-dependent functions, and the "executive". This was designed as a modified microkernel, as the Windows NT kernel was influenced by the Mach microkernel developed at Carnegie Mellon University, but does not meet all of the criteria of a pure microkernel. Both the kernel and the executive are linked together into the single loaded module `ntoskrnl.exe`; from outside this module there is little distinction between the kernel and the executive. Routines from each are directly accessible, as for example from kernel-mode device drivers.

API sets in the Windows NT family are implemented as subsystems atop the publicly undocumented "native" API; this allowed the late adoption of the Windows API (into the Win32 subsystem). Windows NT was one of the earliest operating systems to use Unicode internally.

#### 5.2.1.1 FEATURES OF WINDOWS NT

A main design goal of NT was hardware and software portability. Various versions of NT family operating systems have been released for a variety of processor architectures, initially IA-32, MIPS, and DEC Alpha, with PowerPC, Itanium, x86-64 and ARM supported in later releases. The idea was to have a common code base with a custom Hardware Abstraction Layer (HAL) for each platform. However, support for MIPS, Alpha, and PowerPC was later dropped in Windows 2000. Broad software compatibility was achieved with support for several API "personalities", including Windows API, POSIX,[9] and OS/2 APIs[10] – the latter two were phased out starting with Windows XP.[11] Partial MS-DOS compatibility was achieved via an integrated DOS Virtual Machine – although this feature is being phased out in the x86-64 architecture.[12] NT supported per-object (file, function, and role) access control lists allowing a rich set of

security permissions to be applied to systems and services. NT supported Windows network protocols, inheriting the previous OS/2 LAN Manager networking, as well as TCP/IP networking (for which Microsoft would implement a TCP/IP stack derived at first from a STREAMS-based stack from Spider Systems, then later rewritten in-house). Windows NT 3.1 was the first version of Windows to use 32-bit flat virtual memory addressing on 32-bit processors. Its companion product, Windows 3.1, used segmented addressing and switches from 16-bit to 32-bit addressing in pages.

Windows NT 3.1 featured a core kernel providing a system API, running in supervisor mode (ring 0 in x86; referred to in Windows NT as "kernel mode" on all platforms), and a set of user-space environments with their own APIs which included the new Win32 environment, an OS/2 1.3 text-mode environment and a POSIX environment. The full preemptive multitasking kernel could interrupt running tasks to schedule other tasks, without relying on user programs to voluntarily give up control of the CPU, as in Windows 3.1 Windows applications (although MS-DOS applications were preemptively multitasked in Windows starting with Windows 1.0). Notably, in Windows NT 3.x, several I/O driver subsystems, such as video and printing, were user-mode subsystems. In Windows NT 4, the video, server, and printer spooler subsystems were moved into kernel mode. Windows NT's first GUI was strongly influenced by (and programmatically compatible with) that from Windows 3.1; Windows NT 4's interface was redesigned to match that of the brand new Windows 95, moving from the Program Manager to the Windows shell design.

NTFS, a journaled, secure file system, was created for NT. Windows NT also allows for other installable file systems; starting with versions 3.1, NT could be installed on FAT or HPFS file systems.

Windows NT introduced its own driver model, the Windows NT driver model, and is incompatible with older driver frameworks. With Windows 2000, the Windows NT driver model was enhanced to become the Windows Driver Model, which was first introduced with Windows 98, but was based on the NT driver model. Windows Vista added native support for the Windows Driver Foundation, which is also available for Windows XP, Windows Server 2003 and to an extent, Windows 2000. Windows NT was one of the earliest operating systems to use Unicode internally.



## WINDOWS NT HARDWARE REQUIREMENT:

TABLE 1:

❖ <u>WINDOWS VERSION</u>	❖ <u>CPU</u>	❖ <u>RAM</u>	❖ <u>FREE DISK SPACE</u>
NT3.1	I386, 25 MHz	12MB	90MB
NT 3.1 SERVER	I386,25MHZ	16MB	90MB
NT 4.0 SERVER	i486, 25 MHz	12MB	124MB
2000 SERVER	PENTINUM,133MHZ	128MB	650MB
XP	PENTINUM,233MHZ	64MB	1.5GB
SERVER 2003	133MHZ	128MB	1.5GB
VISTA HOME BASIC	800MHZ	512MB	20GB
7 X64	1GHZ	1GB	20GB
8.1 FOR X64	1GHZ WITH NX BIT,SSE2,PAE	1GB	20GB
10 FOR X64	1GHZ WITH NX BIT,SSE2,PAE	2GB	20GB

### 5.2.1.2 WINDOWS NT ARCHITECTURE:

The architecture of Windows NT, a line of operating systems produced and sold by Microsoft, is a layered design that consists of two main components:

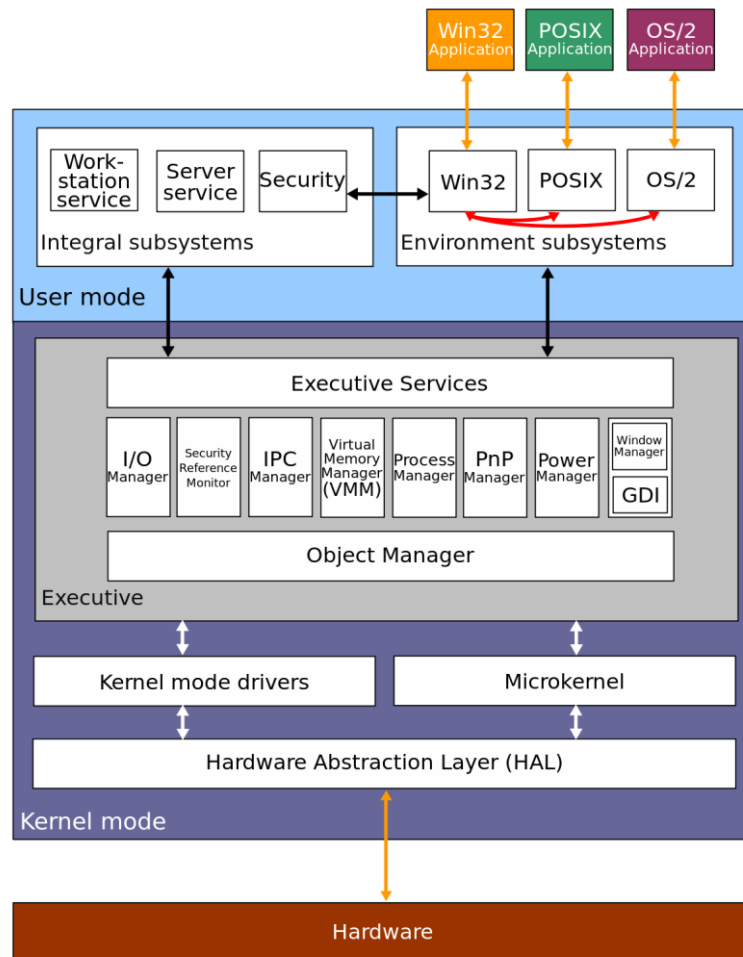
- USER MODE
- KERNEL MODE

It is a preemptive, reentrant operating system, which has been designed to work with uniprocessor and symmetrical multi processor (SMP)-based computers. To process input/output (I/O) requests, they use packet-driven I/O, which utilizes I/O request packets (IRPs) and asynchronous I/O. Starting with Windows XP, Microsoft began making 64-bit versions of Windows available; before this, these operating systems only existed in 32-bit versions.

Programs and subsystems in user mode are limited in terms of to what system resources they have access, while the kernel mode has unrestricted access to the system memory and external devices. The Windows NT kernel is known as a hybrid kernel. The architecture comprises a simple kernel, hardware abstraction layer (HAL), drivers, and a range of services (collectively named Executive), which all exist in kernel mode.

User mode in Windows NT is made of subsystems capable of passing I/O requests to the appropriate kernel mode [device drivers](#) by using the I/O manager. The user mode layer of Windows NT is made up of the "Environment subsystems," which run applications written for many different types of operating systems, and the "Integral subsystem," which operates system specific functions on behalf of environment subsystems. Kernel mode in Windows NT has full access to the hardware and system resources of the computer. The kernel mode stops user mode services and applications from accessing critical areas of the operating system that they should not have access to. The Executive interfaces, with all the user mode subsystems, deals with I/O, object management, security and process management. The kernel sits between the Hardware

Abstraction Layer and the Executive to provide multiprocessor synchronization, thread and interrupt scheduling and dispatching, and trap handling and exception dispatching.



**FIGURE :2(WINDOWS NT ARCHITECTURE)**

### USER MODE:

User mode is made up of various system-defined processes and DLLs.

The interface between user mode applications and operating system kernel functions is called an "environment subsystem." Windows NT can have more than one of these, each implementing a different API set. This mechanism was designed to support applications written for many different types of operating

systems. None of the environment subsystems can directly access hardware; access to hardware functions is done by calling into kernel mode routines.

There are four main environment subsystems: the Win32 subsystem, an OS/2 subsystem, the Windows Subsystem for Linux and a POSIX subsystem.

The Win32 environment subsystem can run 32-bit Windows applications. It contains the console as well as text window support, shutdown and hard-error handling for all other environment subsystems. It also supports Virtual DOS Machines (VDMs), which allow MS-DOS and 16-bit Windows (Win16) applications to run on Windows NT. There is a specific MS-DOS VDM that runs in its own address space and which emulates an Intel 80486 running MS-DOS 5.0. Win16 programs, however, run in a Win16 VDM. Each program, by default, runs in the same process, thus using the same address space, and the Win16 VDM gives each program its own thread on which to run. However, Windows NT does allow users to run a Win16 program in a separate Win16 VDM, which allows the program to be preemptively multitasked, as Windows NT will preempt the whole VDM process, which only contains one running application. The Win32 environment subsystem process (csrss.exe) also includes the window management functionality, sometimes called a "window manager". It handles input events (such as from the keyboard and mouse), then passes messages to the applications that need to receive this input. Each application is responsible for drawing or refreshing its own windows and menus, in response to these messages.

The OS/2 environment subsystem supports 16-bit character-based OS/2 applications and emulates OS/2 1.x, but not 32-bit or graphical OS/2 applications as used with OS/2 2.x or later, on x86 machines only. To run graphical OS/2 1.x programs, the Windows NT Add-On Subsystem for Presentation Manager must be installed. The last version of Windows NT to have an OS/2 subsystem was Windows 2000; it was removed as of Windows XP.

The POSIX environment subsystem supports applications that are strictly written to either the POSIX.1 standard or the related ISO/IEC standards. This subsystem has been replaced by Interix, which is a part of Windows Services for UNIX. This was in turn replaced by the Windows Subsystem for Linux.

The security subsystem deals with security tokens, grants or denies access to user accounts based on resource permissions, handles login requests and initiates login authentication, and determines which system resources need to be audited by Windows NT.[citation needed] It also looks after Active Directory.[citation needed] The workstation service implements the network redirector, which is the client side of Windows file and print sharing; it implements local requests to remote files and printers by "redirecting" them to the appropriate servers on the network. Conversely, the server service allows other computers on the network to access file shares and shared printers offered by the local system.

### KERNEL MODE:

Windows NT kernel mode has full access to the hardware and system resources of the computer and runs code in a protected memory area. It controls access to scheduling, thread prioritization, memory management and the interaction with hardware. The kernel mode stops user mode services and applications from accessing critical areas of the operating system that they should not have access to; user mode processes must ask the kernel mode to perform such operations on their behalf.

While the x86 architecture supports four different privilege levels (numbered 0 to 3), only the two extreme privilege levels are used. Usermode programs are run with CPL 3, and the kernel runs with CPL 0. These two levels are often referred to as "ring 3" and "ring 0", respectively. Such a design decision had been done to achieve code portability to RISC platforms that only support two privilege levels, though this breaks compatibility with OS/2 applications that contain I/O privilege segments that attempt to directly access hardware.

Kernel mode consists of executive services, which is itself made up of many modules that do specific tasks: kernel drivers, a kernel, and a Hardware Abstraction Layer (HAL).

## Object Manager

The Object Manager (internal name Ob) is an executive subsystem that all other executive subsystems, especially system calls, must pass through to gain access to Windows NT resources—essentially making it a resource management infrastructure service.[11] The object manager is used to reduce the duplication of object resource management functionality in other executive subsystems, which could potentially lead to bugs and make development of Windows NT harder.[12] To the object manager, each resource is an object, whether that resource is a physical resource (such as a file system or peripheral) or a logical resource (such as a file). Each object has a structure or object type that the object manager must know about.

Object creation is a process in two phases, creation and insertion. Creation causes the allocation of an empty object and the reservation of any resources required by the object manager, such as an (optional) name in the namespace. If creation was successful, the subsystem responsible for the creation fills in the empty object.[13] Finally, if the subsystem deems the initialization successful, it instructs the object manager to insert the object, which makes it accessible through its (optional) name or a cookie called a handle.[14] From then on, the lifetime of the object is handled by the object manager, and it's up to the subsystem to keep the object in a working condition until being signaled by the object manager to dispose of it.

Handles are identifiers that represent a reference to a kernel resource through an opaque value. Similarly, opening an object through its name is subject to security checks, but acting through an existing, open handle is only limited to the level of access requested when the object was opened or created.

Object types define the object procedures and any data specific to the object. In this way, the object manager allows Windows NT to be an object-oriented operating system, as object types can be thought of as polymorphic classes that define objects. Most subsystems, though, with a notable exception in the I/O Manager, rely on the default implementation for all object type procedures.

Each instance of an object that is created stores its name, parameters that are passed to the object creation function, security attributes and a pointer to its object type. The object also contains an object close procedure and a reference count to tell the object manager how many other objects in the system reference that object and thereby determines whether the object can be destroyed when a close request is sent to it. Every named object exists in a hierarchical object namespace.

### Cache Controller

Closely coordinates with the memory Manager , I/O

Manager and I/O drivers to provide a common cache for regular file I/O. The Windows Cache Manager operates on file blocks (rather than device blocks), for consistent operation between local and remote files, and ensures a certain degree of coherency with memory-mapped views of files, since cache blocks are a special case of memory-mapped views and cache misses a special case of page faults.

### Configuration Manager

Implements the Windows Registry.

### I/O Manager

Allows devices to communicate with user-mode subsystems. It translates user-mode read and write commands into read or write IRPs which it passes to device drivers. It accepts file system I/O requests and translates them into device specific calls, and can incorporate low-level device drivers that directly manipulate hardware to either read input or write output. It also includes a cache manager to improve disk performance by caching read requests and write to the disk in the background.

### Local Procedure Call (LPC)

Provides inter-process communication ports with connection semantics. LPC ports are used by user-mode subsystems to communicate with their clients, by Executive subsystems to communicate with user-mode subsystems, and as the basis for the local transport for Microsoft RPC.

## Memory Manager

Manages virtual memory, controlling memory protection and the paging of memory in and out of physical memory to secondary storage, and implements a general-purpose allocator of physical memory. It also implements a parser of PE executables that lets an executable be mapped or unmapped in a single, atomic step.

Starting from Windows NT Server 4.0, Terminal Server Edition, the memory manager implements a so-called session space, a range of kernel-mode memory that is subject to context switching just like user-mode memory. This lets multiple instances of the kernel-mode Win32 subsystem and GDI drivers run side-by-side, despite shortcomings in their initial design. Each session space is shared by several processes, collectively referred to as a "session".

To ensure a degree of isolation between sessions without introducing a new object type, the association between processes and sessions is handled by the Security Reference Monitor, as an attribute of a security subject (token), and it can only be changed while holding special privileges.

The relatively unsophisticated and ad-hoc nature of sessions is due to the fact they weren't part of the initial design, and had to be developed, with minimal disruption to the main line, by a third party (Citrix Systems) as a prerequisite for their terminal server product for Windows NT, called WinFrame. Starting with Windows Vista, though, sessions finally became a proper aspect of the Windows architecture. No longer a memory manager construct that creeps into user mode indirectly through Win32, they were expanded into a pervasive abstraction affecting most Executive subsystems. As a matter of fact, regular use of Windows Vista always results in a multi-session environment.

## Process Structure

Handles process and thread creation and termination, and it implements the concept of Job, a group of processes that can be terminated as a whole, or be placed under shared restrictions (such a total maximum of allocated memory, or CPU time). Job objects were introduced in Windows 2000.



## PnP Manager

Handles plug and play and supports device detection and installation at boot time. It also has the responsibility to stop and start devices on demand—this can happen when a bus (such as USB or IEEE 1394 FireWire) gains a new device and needs to have a device driver loaded to support it. Its bulk is actually implemented in user mode, in the Plug and Play Service, which handles the often complex tasks of installing the appropriate drivers, notifying services and applications of the arrival of new devices, and displaying GUI to the user.

## Power Manager

Deals with power events (power-off,stand-by,hibernate, etc) and notifies affected drivers with special IRPs.

## Security Reference Monitor (SRM)

The primary authority for enforcing the security rules of the security integral subsystem. It determines whether an object or resource can be accessed, via the use of access control lists (ACLs), which are themselves made up of access control entries (ACEs). ACEs contain a Security Identifier (SID) and a list of operations that the ACE gives a select group of trustees—a user account, group account, or login session—permission (allow, deny, or audit) to that resource.

## GDI

The Graphics Device Interface is responsible for tasks such as drawing lines and curves, rendering fonts and handling palettes. The Windows NT 3.x series of releases had placed the GDI component in the user-mode Client/Server Runtime Subsystem, but this was moved into kernel mode with Windows NT 4.0 to improve graphics performance.

## Kernel

The kernel sits between the HAL and the Executive and provides multiprocessor synchronization, thread and interrupt scheduling and dispatching, and trap handling and exception dispatching; it is also responsible for initializing device drivers at bootup that are necessary to get the operating system up and running. That is, the kernel performs almost all the tasks of a traditional

microkernel; the strict distinction between Executive and Kernel is the most prominent remnant of the original microkernel design, and historical design documentation consistently refers to the kernel component as "the microkernel".

The kernel often interfaces with the process manager. The level of abstraction is such that the kernel never calls into the process manager, only the other way around (save for a handful of corner cases, still never to the point of a functional dependence).

### Kernel-mode drivers

Windows NT uses kernel-mode device drivers to enable it to interact with hardware devices. Each of the drivers has well defined system routines and internal routines that it exports to the rest of the operating system. All devices are seen by user mode code as a file object in the I/O manager, though to the I/O manager itself the devices are seen as device objects, which it defines as either file, device or driver objects. Kernel mode drivers exist in three levels: highest level drivers, intermediate drivers and low level drivers. The highest level drivers, such as file system drivers for FAT and NTFS, rely on intermediate drivers. Intermediate drivers consist of function drivers—or main driver for a device—that are optionally sandwiched between lower and higher level filter drivers. The function driver then relies on a bus driver—or a driver that services a bus controller, adapter, or bridge—which can have an optional bus filter driver that sits between itself and the function driver. Intermediate drivers rely on the lowest level drivers to function. The Windows Driver Model (WDM) exists in the intermediate layer. The lowest level drivers are either legacy Windows NT device drivers that control a device directly or can be a PnP hardware bus. These lower level drivers directly control hardware and do not rely on any other drivers.

### Hardware abstraction layer

The Windows NT hardware abstraction layer, or HAL, is a layer between the physical hardware of the computer and the rest of the operating system. It was designed to hide differences in hardware and provide

a consistent platform on which the kernel is run. The HAL includes hardware-specific code that controls I/O interfaces, interrupt controllers and multiple processors.

However, despite its purpose and designated place within the architecture, the HAL isn't a layer that sits entirely below the kernel, the way the kernel sits below the Executive: All known HAL implementations depend in some measure on the kernel, or even the Executive. In practice, this means that kernel and HAL variants come in matching sets that are specifically constructed to work together.

In particular hardware abstraction does not involve abstracting the instruction set, which generally falls under the wider concept of portability.

---

## 5.2.2 WINDOWS SERVER 2008:

---

Windows Server 2008 is the second major release of the Windows Server family of operating systems for server computers. Developed by Microsoft, it was released to manufacturing on February 4, 2008, and reached general availability on February 27, 2008. It is the successor of Windows Server 2003, released nearly five years earlier.

Windows Server 2008 is built from the same code base as Windows Vista; therefore, it shares much of the same architecture and functionality. Since the code base is common, it automatically comes with most of the technical, security, management and administrative features new to Windows Vista such as the rewritten networking stack (native IPv6, native wireless, speed and security improvements); improved image-based installation, deployment and recovery; improved diagnostics, monitoring, event logging and reporting tools; new security features such as BitLocker and ASLR (address space layout randomization); improved Windows Firewall with secure default configuration; .NET Framework 3.0 technologies, specifically Windows Communication Foundation, Microsoft Message Queuing and Windows Workflow Foundation; and the core kernel, memory and file system improvements. Processors and memory devices are modeled as Plug and Play devices, to allow hot-plugging of these devices. This allows the system resources to be partitioned dynamically using Dynamic Hardware Partitioning; each partition has its own memory, processor and I/O host bridge devices independent of other partitions.

Windows Server 2008 includes a variation of installation called Server Core. Server Core is a significantly scaled-back installation where no Windows Explorer shell is installed. All configuration and maintenance is done entirely through command-line interface windows, or by connecting to the machine remotely using Microsoft Management Console. However, Notepad and some control panel applets, such as Regional Settings, are available. Server Core does not include the .NET Framework, Internet Explorer, Windows PowerShell or many other features not related to core server features. A Server Core machine can be configured for several basic roles: Domain controller/Active Directory

Domain Services, AD LDS (ADAM), DNS Server, DHCP server, file server, print server, Windows Media Server, IIS 7 web server and Hyper-V virtual server. Server Core can also be used to create a cluster with high availability using failover clustering or network load balancing.

### Active Directory roles:

Active Directory roles are expanded with identity, certificate, and rights management services. Active Directory, until Windows Server 2003, allowed network administrators to centrally manage connected computers, to set policies for groups of users, and to centrally deploy new applications to multiple computers. This role of Active Directory is being renamed as Active Directory Domain Services (AD DS).[11] A number of other additional services are being introduced, including Active Directory Federation Services (AD FS), Active Directory Lightweight Directory Services (AD LDS), (formerly Active Directory Application Mode, or ADAM), Active Directory Certificate Services (AD CS), and Active Directory Rights Management Services (AD RMS). Identity and certificate services allow administrators to manage user accounts and the digital certificates that allow them to access certain services and systems. Federation management services enable enterprises to share credentials with trusted partners and customers, allowing a consultant to use his company user name and password to log in on a client's network. Identity Integration Feature Pack is included as Active Directory Metadirectory Services. Each of these services represents a server role.

### Self-healing NTFS:

In Windows versions prior to Windows Vista, if the operating system detected corruption in the file system of an NTFS volume, it marked the volume "dirty"; to correct errors on the volume, it had to be taken offline. With self-healing NTFS, an NTFS worker thread is spawned in the background which performs a localized fix-up of damaged data structures, with only the corrupted files/folders remaining unavailable without locking out the entire volume and needing the server to be taken down. The operating system now features S.M.A.R.T. detection techniques to help determine when a hard disk may fail.

## Hyper-v:

Hyper-V is hypervisor-based virtualization software, forming a core part of Microsoft's virtualization strategy. It virtualizes servers on an operating system's kernel layer. It can be thought of as partitioning a single physical server into multiple small computational partitions. Hyper-V includes the ability to act as a Xen virtualization hypervisor host allowing Xen-enabled guest operating systems to run virtualized. A beta version of Hyper-V shipped with certain x86-64 editions of Windows Server 2008, prior to Microsoft's release of the final version of Hyper-V on 26 June 2008 as a free download. Also, a standalone version of Hyper-V exists; this version supports only x86-64 architecture. While the IA-32 editions of Windows Server 2008 cannot run or install Hyper-V, they can run the MMC snap-in for managing Hyper-V.

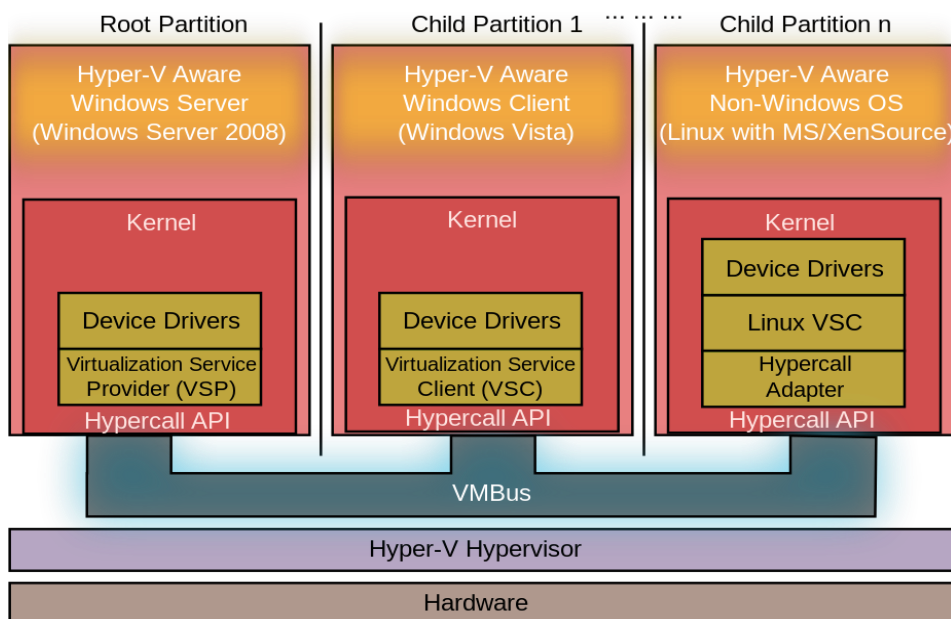


Figure:3(hyper-v)

---

## 5.2.3 VMWARE WORKSTATION

---

VMware Workstation is a hosted hypervisor that runs on x64 versions of Windows and Linux operating systems (an x86 version of earlier releases was available);[3] it enables users to set up virtual machines (VMs) on a single physical machine, and use them simultaneously along with the actual machine. Each virtual machine can execute its own operating system, including versions of Microsoft Windows, Linux, BSD, and MS-DOS. VMware Workstation is developed and sold by VMware, Inc., a division of Dell Technologies. There is a free-of-charge version, VMware Workstation Player, for non-commercial use. An operating systems license is needed to use proprietary ones such as Windows. Ready-made Linux VMs set up for different purposes are available from several sources.

VMware Workstation supports bridging existing host network adapters and sharing physical disk drives and USB devices with a virtual machine. It can simulate disk drives; an ISO image file can be mounted as a virtual optical disc drive, and virtual hard disk drives are implemented as .vmdk files.

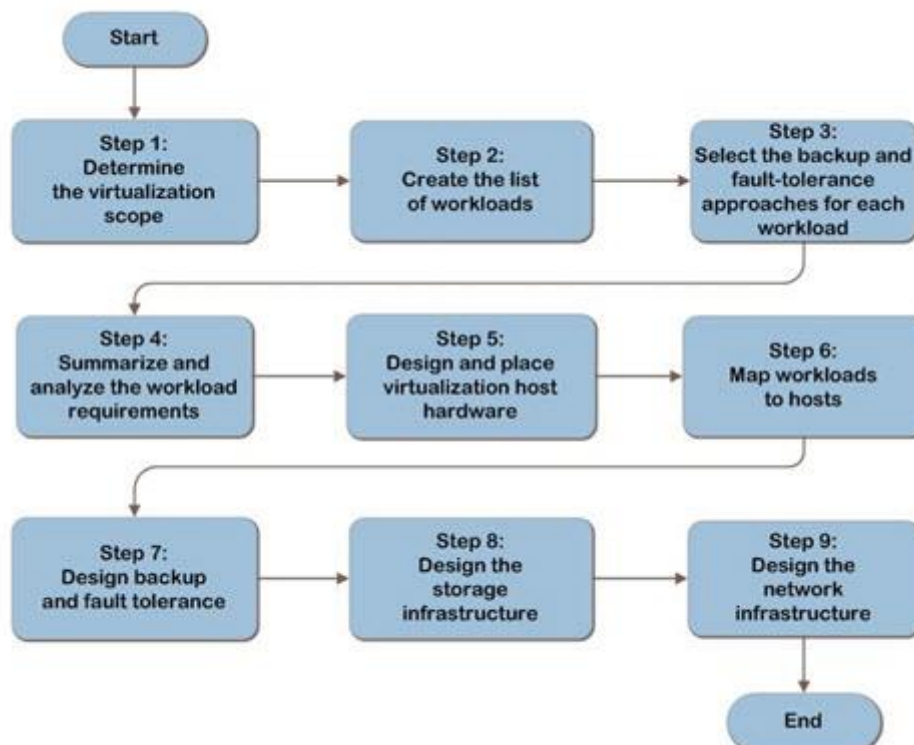
VMware Workstation Pro can save the state of a virtual machine (a "snapshot") at any instant. These snapshots can later be restored, effectively returning the virtual machine to the saved state, as it was and free from any post-snapshot damage to the VM.

VMware Workstation includes the ability to group multiple virtual machines in an inventory folder. The machines in such a folder can then be powered on and powered off as a single object, useful for testing complex client-server environments.

# 6.

## PROJECT DESIGN

The Windows Server Virtualization guide, updated to reflect the features and functionalities of Windows Server 2008 , outlines the critical infrastructure design elements that are crucial to a successful implementation of Windows Server virtualization (WSv). The reader is guided through the nine-step process of designing components, layout, and connectivity in a logical, sequential order. Identification of the Microsoft Hyper-V server hosts required is presented in simple, easy-to-follow steps, helping the reader to design and plan virtual server data centers.





**Figure 4 : Decision flow chart**

*The Infrastructure Planning and Design for Windows Server*

*Virtualization* includes the following nine-step process:

Step 1: Determine the Virtualization Scope. The goal of this step is to define the scope of the infrastructure that will be virtualized.

Step 2: Create the List of Workloads. This step involves identifying the total resource requirements for all of the workloads that the organization's virtual infrastructure will host.

Step 3: Select the Backup and Fault-Tolerance Approaches for Each Workload. This step involves selecting the backup approach for the virtualized workloads that will be used in the design of the host system, its storage, and network infrastructure. Also, the most appropriate fault-tolerance approach is selected for each workload that will be virtualized.

Step 4: Summarize and Analyze the Workload Requirements. This step involves analyzing the previously gathered information to summarize the overall requirements for the solution.

Step 5: Design and Place Virtualization Host Hardware. The goal of this step is to determine the most appropriate type of virtualization host hardware on which to deploy the virtual machines.

Step 6: Map Workloads to Hosts. The purpose of this step is to determine which workloads will be placed on which physical hosts and how many of those hosts will be required.

Step 7: Design Backup and Fault Tolerance. The purpose of this step is to determine the backup and fault-tolerance approaches that virtualization host

servers will use to meet the workload requirements that were defined in step 3.

Step 8: Design the Storage Infrastructure. This step involves planning the I/O performance and capacity requirements of the VMs that will run on each virtualization server.

Step 9: Design the Network Infrastructure. This step involves determining the host connectivity and network throughput requirements of the virtual machines that will run on each virtualization server.

## **BIBLIOGRAPHY**

Main sources of information for this project are:

- <https://msdn.microsoft.com/en-us/library/bb897507.aspx>
- [https://en.wikipedia.org/wiki/Windows\\_Server](https://en.wikipedia.org/wiki/Windows_Server)
- <https://www.google.com/>
- [https://en.wikipedia.org/wiki/Group\\_Policy](https://en.wikipedia.org/wiki/Group_Policy)
- Book: Introduction to windows server 2008 (CHARLIE RUSSEL and CRAIG ZACKER).
- Book: windows server 2008 administration (AGATHA KIM).

## **APPENDIX A**

Lets get detail about windows server 2008 on vmware workstation:

### **Installation Instructions**

You can install the Windows Server 2008 R2 in a virtual machine using the corresponding Windows Server 2008 R2 distribution CD.

#### **Prerequisites**

Before you begin, verify that the following tasks are complete:

- Read General Installation Instructions for All VMware Products.
- Read the Microsoft System Requirements for the recommended storage and memory values.
- Create and configure a new virtual machine, with the appropriate virtual storage and virtual memory to support the intended workload.

#### **Installation Steps**

1. Insert the Windows Server 2008 R2 CD in the CD-ROM drive.
2. Power on the virtual machine to start installing Windows Server 2008 R2.
3. (Optional) If you are using VMware Paravirtual as the default SCSI controller, you can install Windows Server 2008 R2 64-bit using the pvscsi-windows2008.flp driver.
4. Follow the prompts to complete the installation.
5. Install VMware Tools.

### **VMware Tools in an Windows Server 2008 R2 Guest**

For information on VMware Tools, see Knowledge base article 1014294, General VMware Tools installation instructions, at <http://kb.vmware.com/kb/1014294>.

### **Knowledge Base Articles for Windows Server 2008 R2**

The following link refers to knowledge base articles on operating system specific issues. See VMware Knowledge Base for a list of known issues about the operating system.

## **VMware Compatibility Guide**

The VMware Compatibility Guide Web site lists supported guest and host operating systems and provides related support information.