

Chapter Objectives

At the end of this chapter, the students will be able to:

- Learn the foundation of network and system administration
- Know the scope, duties and responsibilities of network and system administrator
- Know the network operation system that support system administration
- Distinguish the support of each network operating system

1.1. Introduction

Networking is the technology of interconnecting computing devices of all types so information can flow between them. This includes activities as simple as topology design to those as complex as the configuration of services and protocols to enable an entire intranet and the support of that environment.

While all that data eventually gets to the user, it spends most of its time on hundreds of interconnected servers. Systems administration is the design, installation, configuration, operation, and support of these servers. Networking professionals must be knowledgeable in considering when to use physical or virtual servers, when to use a public or private cloud, and other key performance, reliability, and security issues.

In today's information-rich environment, computer systems exist at the heart of nearly every organization and are critical to the organization's success. Upon graduation, students can work in nearly any industry as a valuable part of the team helping to ensure their organization's products and services are always available.

Network and system administration is a branch of engineering that concerns the operational management of human–computer systems. It is unusual as an engineering discipline in that it addresses both the technology of computer systems and the users of the technology on an equal basis. It is about putting together a network of computers (workstations, PCs and supercomputers), getting them running and then keeping them running in spite of the activities of users who tend to cause the system to fail.

1.2. Philosophy of System Administration and Network Administration

System Administration is the design, installation, configuration, operation, and support of these servers to support the operation need of information technology infrastructure of an organization. Generally it is planning, installing, and maintaining computer systems involving servers and clients that work together in a network environment using operation system like Windows 2008 Server or Linux platform.

1.2.1. Network Administration

Network administration involves a wide array of operational tasks that help a network to run smoothly and efficiently. Without network administration, it would be difficult for all but the smallest networks to maintain network operations.

The main tasks associated with network administration include:

- Design, installation and evaluation of the network
- Execution and administration of regular backups
- Creation of precise technical documentation, such as network diagrams, network cabling documents, etc.
- Provision for precise authentication to access network resources
- Provision for troubleshooting assistance
- Administration of network security, including intrusion detection

1.2.2. System Administration

A **system administrator** or **sysadmin** is a person who is responsible for the upkeep, configuration and reliable operation of computer systems; especially multi-user computers, such as servers.

The system administrator seeks to ensure that the uptime, performance, resources, and security of the computers he or she manages meet the needs of the users, without exceeding the budget.

To meet these needs, a system administrator may acquire, install, or upgrade computer components and software; provide routine automation; maintain security policies; troubleshoot; train and/or supervise staff; or technical support in projects.

The terms *network administration* and *system administration* exist separately and are used both variously and inconsistently by industry and by academics.

System administration is the term used traditionally by mainframe and UNIX engineers to describe the management of computers whether they are coupled by a network or not.

To this community, network administration means the management of network infrastructure devices (routers and switches).



Figure 1. Computers connecting in Server using Network.

1.3. Scope, Goals and Duties

1.3.1. Applying technology in an environment

A key task of network and system administration is to build hardware configurations; another is to configure software systems. Both of these tasks are performed for users. Each of these tasks presents its own challenges, but neither can be viewed in isolation. Hardware has to conform to the constraints of the physical world; it requires power, a temperate (usually indoor) climate, and a conformance to basic standards in order to work systematically. The type of hardware limits the kind of software that can run on it.

Software requires hardware, a basic operating system infrastructure and a conformance to certain standards, but is not necessarily limited by physical concerns as long as it has hardware to run on. Modern software, in the context of a global network, needs to inter-operate and survive the possible hostilities of incompatible or inhospitable competitors. Today the complexity of multiple software systems sharing a common Internet space reaches almost the level of the biological. In older days, it was normal to find proprietary solutions, whose strategy was to lock users into one company's products. Today that strategy is less dominant, and even untenable, thanks to networking.

Today, there is not only a physical environment but a technological one, with a diversity that is constantly changing. Part of the challenge is to knit apparently disparate pieces of this community into a harmonious part.

System Administrator

A system administrator, or sysadmin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers.

The system administrator seeks to ensure that the uptime, performance, resources, and security of the computers he or she manages meet the needs of the users, without exceeding the budget.

To meet these needs, a system administrator may acquire, install, or upgrade computer components and software; provide routine automation; maintain security policies; troubleshoot; train and/or supervise staff; or technical support in projects.

Network Administrator

A network administrator is an individual that is responsible for the maintenance of computer hardware and software systems that make up a computer network including the maintenance and monitoring of active data network or converged infrastructure and related network equipment.

Network administrators are generally mid-level support staff within an organization and do not typically get involved directly with users. Network administrators focus upon network components within a company's LAN/WAN infrastructure ensuring integrity. Depending on the company and its size, the network administrator may also design and deploy networks.

The actual role of the network administrator will vary from place to place, but will commonly include activities and tasks such as network address assignment, management and implementation of routing protocols such as ISIS, OSPF, BGP, routing table configurations and certain implementations of authentication (e.g.: challenge response, etc.). It can also include maintenance of certain network servers: file servers, VPN gateways, intrusion detection systems, etc.

In smaller organizations, network administrators may also be technically involved in the maintenance and administration of servers, desktop computers, printers, routers, switches, firewalls, and phones, IP Phones, personal digital assistants, smartphones, software deployment, security updates and patches as well as a vast array of additional technologies inclusive of both hardware and software.

Duties of a system administrator

The duties of a system administrator are wide-ranging, and vary widely from one organization to another. Sysadmins are usually charged with installing, supporting, and maintaining servers or other computer systems, and planning for and responding to service outages and other problems. Other duties may include scripting or light programming, project management for systems- related projects.

The system administrator is responsible for following things:

- User administration (setup and maintaining account)
- Maintaining system
- Verify that peripherals are working properly
- Quickly arrange repair for hardware in occasion of hardware failure
- Monitor system performance
- Create file systems
- Install software
- Create a backup and recovery policy
- Monitor network communication
- Update system as soon as new version of OS and application software comes out
- Implement the policies for the use of the computer system and network
- Setup security policies for users. A sysadmin must have a strong grasp of computer security (e.g. firewalls and intrusion detection systems)
- Documentation in form of internal wiki
- Password and identity management
- Install patches
- Review system logs
- Report malicious or suspicious activity on systems to ISO immediately
- Report sensitive information stored on systems to ISO
- Maintain user access administration
- Disaster recovery planning
- Physical security
- Disable unnecessary services on servers
- Generate/Retain system backups

- Identify secondary system administrator(s)
- Comply with password requirements
- Access control
- Environmental protection (i.e., protection from possible exposure to water damage, excessive heat, etc.)
- Security training will be required every three (3) years
- System audit logging
- Maintain minimum security standards for systems
- Monitoring of system activity
- Designate a secondary administrator

1.3.2. What is so special about the system administrator account?

The root account has full (unrestricted) access, so he/she can do anything with system. For example, root can remove critical system files. In addition, there is no way you can recover file except using tape backup or disk based backup systems.

Many tasks for system administration can be automated using Perl/Python or shell scripts. For example:

- Create new users
- Resetting user passwords
- Lock/unlock user accounts
- Monitor server security
- Monitor special services etc

1.3.3. Additional skills of system and network administrator

The subject matter of system administration includes computer systems and the ways people use them in an organization. This entails knowledge of operating systems and applications, as well as hardware and software troubleshooting, but also knowledge of the purposes for which people in the organization use the computers.

Perhaps the most important skill for a system administrator is problem solving frequently under various sorts of constraints and stress. The sysadmin is on call when a computer system goes down or malfunctions, and must be able to quickly and correctly diagnose what is wrong and how best to fix it. They may also need to have team work and communication skills; as well as being able

to install and configure hardware and software.

System administrators are not software engineers or developers. It is not usually within their duties to design or write new application software. However, sysadmins must understand the behavior of software in order to deploy it and to troubleshoot problems, and generally know several programming languages used for scripting or automation of routine tasks.

Particularly when dealing with Internet-facing or business-critical systems, a sysadmin must have a strong grasp of computer security. This includes not merely deploying software patches, but also preventing break-ins and other security problems with preventive measures. In some organizations, computer security administration is a separate role responsible for overall security and the upkeep of firewalls and intrusion detection systems, but all sysadmins are generally responsible for the security of computer systems.

1.3.4. Ethical issues

Because computer systems are human–computer communities, there are ethical considerations involved in their administration. Even if certain decisions can be made objectively, e.g. for maximizing productivity or minimizing cost, one must have a policy for the use and management of computers and their users.

Some decisions have to be made to protect the rights of individuals. A system administrator has many responsibilities and constraints to consider. Ethically, the first responsibility must be to the greater network community, and then to the users of our system. An administrator’s job is to make users’ lives bearable and to empower them in the production of real work.

1.3.5. Education requirements of System and Network Administrator

Unlike many other professions, there is no single path to becoming a system and network administrator. Many system administrators have a degree in a related field: computer science, information technology, computer engineering, information systems, or even a trade school program. On top of this, nowadays some companies require an IT certification. Other schools have offshoots of their Computer Science program specifically for system administration.

1.3.7 Five reasons to consider a career in System and Network Administration

Though system and network administration isn't for everyone, it offers plenty of rewarding and profitable challenges for those who can soak up technical knowledge and put it to practical use. Industries across the career spectrum and around the world depend on computer networking to keep employees connected and business flowing. And these networks need administrators - Hardworking men and women who know their way around a computer and aren't afraid to take a hands-on approach to troubleshooting.

Though network administration isn't for everyone, it offers plenty of rewarding and profitable challenges for those who can soak up technical knowledge and put it to practical use. Here are five of the biggest reasons why it could be just the career path you're looking for.

A. You'll learn as you go

Job descriptions in fields like network administration and network engineering tend to lean heavily on buzzwords and phrases like "high-level management," "hardware evaluation," and "network configuration." In truth, though, no two corporate networks are quite alike, and most of a company's network procedures will have been ironed out through a long-term tailoring process. This means that most of a particular job's specifics will be covered in on-site training, as one company's qualifications - elaborate though they may be - aren't likely to translate directly to another company's networking needs.

"A lot of today's networking technology is packaged under a nice user interface," says Misha Hanin, a senior solutions architect at Compugen in Winnipeg, Canada; "but if you really want to become an expert, you have to know what's going on under the hood - and that's where the real fun starts." In other words, the learning curve at a new job will be steep at first - but in the end, the most valuable traits for a network administrator are a head for analytical problem-solving and a drive to dig into the details.

B. You'll be in demand, and demand keeps growing

The United States Bureau of Labor Statistics pegs the 2012 median annual wage for network administrators at \$74,270. But network administrators don't just pull in a wage well above the national median - they're a necessary part of any large company, which means their hiring rate is on an upward curve, even throughout the global recession. The U.S. Department of Labor estimates that 96,600 new network administration posts will open up between 2010 and 2020, in

addition to more than 300,000 such jobs already out there. In short, if you're looking to break into an industry with long-term growth potential, network administration is a solid bet.

C. It's an inroad to nearly any industry

Networks are integral to the functioning of almost any large business, from manufacturing to food service to science and nonprofit activism. Once you've proven yourself as a dependable administrator, you'll be able to market yourself as a useful asset in any form of business that sparks your curiosity. In fact, developing nations are also expressing more interest than ever at building up their technological infrastructure - which means network administration could be your ticket to visit exotic lands across the globe, contributing real-world impact everywhere you go.

D. It opens up new career branches

With a few years of network administration experience under your belt, you'll be better equipped than ever to consider becoming a freelance field technician, a systems analyst, or a network engineer. If you like the security of regular paychecks and health benefits, there will be plenty of needs to fill - but you may also be in a position to consider working from home, setting your own hours, and maybe even charging a consultation fee just for providing your technological expertise. As more businesses come to depend on networks, your options will continue to broaden.

E. It's a challenge worthy of your skill

Though years of computer-science training aren't necessary for an entry-level network administration position, each day offers new opportunities to bring out-of-the-box thinking to tough problems. As you earn the right to be trusted with more responsibility, your technical skills will continue to grow, increasing your confidence - and your value as an intellectual worker. Besides, Hanin says, "our users are sometimes even smarter than we are - they come up with all kinds of funny tricks we'd never have thought of."

Network administration may not be the most glamorous job on the planet, but it offers you a chance to prove to the world how smart you really are, in a way that brings practical benefits to yourself and your co-workers. It's not just any field that can make that claim and back it up.

1.4. What is a Network Operating System?

Unlike operating systems, such as Windows, which are designed for single users to control one computer, network operating systems (NOS) coordinate the activities of multiple computers across a network. The network operating system acts as a director to keep the network running smoothly.

Network operating system refers to software that implements an operating system of some kind that is oriented to computer networking. For example, one that runs on a server and enables the server to manage data, users, groups, security, applications, and other networking functions. The network operating system is designed to allow shared file and printer access among multiple computers in a network, typically a local area network (LAN), a private network or to other networks.

Network operating systems can be based on a client/server architecture in which a server enables multiple clients to share resources. Client/server network operating systems allow the network to centralize functions and applications in one or more dedicated file servers. The server is the center of the system, allowing access to resources and instituting security. The network operating system provides the mechanism to integrate all the components on a network to allow multiple users to simultaneously share the same resources regardless of physical location.

1.4.1. The Client

The client is the end user of the network and needs to be secured the most. The client end usually exposes data through the screen of the computer. Client connections to server should be secured through passwords and upon leaving their workstations clients should make sure that their connection to the server is securely cut off in order to make sure that no hackers or intruders are able to reach the server data. Not only securing the workstations connection to the server is important but also securing the files on the workstation (client) is important as it ensures that no hackers are able to reach the system. Another possibility is that of introducing a virus or running unauthorized software on the client workstation thus threatening the entire information bank at the server (Exforsys Inc., 2007).

The users themselves could also be a security threat if they purposely leave their IDs logged in or use easy IDs and passwords to enable hacking. Users may also be sharing their passwords in order to give the hackers access to confidential data (Wilson, Lin, & Craske, 1999). This can be overcome by giving passwords to each client and regularly asking clients to change their passwords. Also passwords should be checked for guess ability and for their strength and uniqueness.

1.4.2. The Network

The network allows transmission of data from the clients to the server. There are several points on the network where a hacker could eavesdrop or steal important packets of information. These packets may contain important confidential data such as passwords or company details. It is important that these networks are secured properly to keep unauthorized professionals away from all the data stored on the server. This can be done by encrypting important data being sent on the network. However, encryption may not be the only possible way of protecting networks as hackers can work their way around encryption. Another method could be conducting security audits regularly and ensuring identification and authorization of individuals at all points along the network. This should discourage potential hackers (Wilson, Lin, & Craske, 1999). Making the entire environment difficult to impersonate also makes sure that the clients are reaching the true files and applications on the server and that the server is providing information to authorized personnel only.

1.4.3. The Server

The server can be secured by placing all the data in a secure, centralized location that is protected through permitting access to authorized personnel only. Virus protection should also be available on server computers as near vast amounts of data can be infected. Regular upgrades should be provided to the servers as the software and the applications need to be updated. Even the entire body of data on a server could be encrypted in order to make sure that reaching the data would require excessive time and effort (Wilson, Neal, & Craske, 1999).

1.5. Network Operating System Software

The following links include some of the more popular peer-to-peer and client/server network operating systems.

- Macintosh OS X
- Microsoft Windows Server
- UNIX/Linux

1.5.1. Server Operating Systems

Overview

The primary server operating systems at Stanford are Linux (with a preference for Debian) and Windows Server. Central IT applications all run on those two platforms. Mac OS is supported through CRC (Computer Resource Consulting) for departmental servers. IT Services' ability to be an effective supplier of server hosting services depends on being able to support the platforms required by the customers; providing excellent reliability at an affordable cost.

For Linux:

Debian Lenny is the preferred operating system for Linux systems, with some Debian Etch. Red Hat 5 is only used as needed per vendor specifications, with some remaining Red Hat 4. Ubuntu Hardy is used for servers running the Timeshare service. Centralized build systems that are more flexible and capable than any other on campus, and are used by other departments. IT Services provides leadership in Puppet configuration management best practices. This work has inspired the community and driven product improvement, and Stanford's expertise has been sought by many other institutions.

Figure 2. Linux Ubuntu Server Logo



For Windows:

Windows 2000 Server, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, and Windows Server 2008 R2 are supported. Most hosting providers have moved to Windows Server 2012 or Windows Server 2012 R2 to take advantage of improvements in server management and scalability. The base operating system installation is fully automated, but applications are usually installed manually. Firewalls and other critical system settings are controlled by Group Policy.



Figure 3. Microsoft Windows Server

For Mac OS X Server:

Servers run OS 10.4 to 10.9. A minimum of 10.5 is recommended, and upgrades are planned for all current servers to meet this minimum recommendation. Some managed servers are part of a central directory system, while some servers are not.



Figure 4. Mac OS X Server

1.5.2. The difference between Windows, Linux and Macintosh

A. What is Windows?

- The Windows is a operating system. This allows people to manage files and run software programs on desktop and laptop computers.
- The Windows operating system is developed and maintained by Microsoft, the company founded by Bill Gates. The first version was released in 1985. Since then, it has grown significantly, and it now dominates the market.
- Windows uses a graphical user interface (GUI) to make it easier for people to use their computers. The primary ways that people navigate are through icons on the desktop and the Start menu.
- Some of the popular Windows editions are Win 98, Win 2000, , Win Me, Win 2003, Win XP, Win Vista etc.
- All Flavors of Windows Come from Microsoft.

B. What is LINUX?

- Linux stands for Linus' Unix
- Linux is the kernel of an operating system.
- Linux was built on the Unix tradition. Linux was originally developed by Linus Torvalds of Finland, who currently owns the Linux trademark.
- Using the open source code of the Linux kernel, people have been developing operating systems based on the Linux kernel. These are called the "Linux distributions." Also known as Linux Operating System.
- The various distributions of Linux come from different companies.(i.e. Lindows, Lycoris, Red Hat, SuSe, Mandrake, Knopping, Slackware)
- NASlite is one of version of Linux that runs off a single floppy disk and converts an old computer into file server. This ultra-small edition of Linux is capable of networking, file sharing and being a web server.

C. What is Macs?

- Mac OS is the original primary operating system of Apple Computer's line of personal computers.
- The first version was released with the original —Thin Macintosh (i.e., the Macintosh 128K) in 1984, and until the release of Mac OS X, the Mac OS remained Apple's flagship operating system.

- Mac OS is characterized by a user-friendly graphical user interface (GUI), single- button moussing, and nearly universal plug-and-play support.
- In the spring of 2001, Apple transitioned from its original code base to Mac OS X, a very different operating system based on UNIX and the Mach microkernel. Like its predecessor, Mac OS X maintains the traditional Mac OS ease of use, but with substantially improved stability.

Summary of the difference between Windows, LINUX and Macintosh

- Windows, Macintosh, and Linux are the three most popular operating systems. All three provide a way for computers to store, launch, and organize programs and files.
- Windows it the most popular of the three operating systems. Estimates vary, but approximately 85% to 90% of personal computers use Windows. Because of its popularity, software and hardware add-ons for Windows computers are widely available.
- In contrast to the large market share enjoyed by Windows, Macintosh is used by fewer people. Although the software and hardware add-ons for Macintosh computers are limited in comparison to Windows add-ons, popular Windows applications like Microsoft Office have Macintosh equivalents.
- Macintosh also regulates the design of software and hardware add-ons more rigidly than Microsoft, so the software and hardware added to a Mac is less likely to fail.
- Linux is the third of the popular operating systems available. Linux is based on Unix, an operating system used for more than three decades that now powers about 90% of Web sites. In sharp contrast to both Windows and Macintosh, Linux is an open source project.
- As such, anyone can modify the Linux code, and Linux is free to use and distribute. Although Linux offers greater security and flexibility than other operating systems, it requires some technical knowledge to install and use.
- Linux is an open source operating system that, until fairly recently, was only used on servers. Now it is used on Mac OS X computers, and more people are starting to use it on computers that aren't servers.
- Linux is Customizable in a way that Windows is not.
- For desktop or home purpose, Linux is very cheap or free, Windows is expensive. For server use, Linux is very cheap compared to Windows. Microspft allows single copy of Windows to be used on only one computer. Starting with Windows XP, they use software to enforce this rule (activation).

- In contrast, once you have purchased Linux, you can run it on any number of computers for no additional charges.
- Every computer printer ships with drivers for the last few versions of windows (at the time it was work. Still, this is far better situation than Linux i.e. which doesn't support as many printers as Windows. Home users of Linux however, will no doubt suffer from the relatively poor support for printers.
- Windows allows programs to store user information (files and settings) anywhere. This makes it impossibly hard for the users to backup user data files and settings and to switch to a new computer. In contrast, Linux stores all user data in the home directory making it much easier to migrate from an old computer to a new one. If home directories are segregated in their own partition, you can even upgrade from one version of Linux to another without having to migrate user data and setting.
- Linux has a reputation for fewer bugs than Windows. In general, Linux is very secure, efficient and flexible than Windows and Macintosh. The software and hardware add-ons for Windows computers are widely available. The software and hardware added to a Mac is less likely to fail. Linux requires some technical knowledge to install and use whereas Windows doesn't requires and Mac requires a little. Windows supports the printers very well than Linux.

Chapter-2

Installation of Windows Server and
Active Directory Domain
Service(AD DS)

Installing Windows Server 2012 and Configuring the Local server

Minimum hardware requirements

- The minimum requirements to install windows server 2012 are:
 - Processor speed: 1.4 GHz
 - Memory (RAM): 512 MB
 - Disk space: 32 GB
- Then to install windows server on a virtual machine, you have to first install the virtual machine, then you install the windows server in the virtual machine environment.
- Refer to the note about the steps on how to install windows server 2012

Installing Windows Server 2012

- After we finish installing the server and every time it loads, it takes us to the server manager by default
- The server manager is where we manage the server/s
- For the first time, click on Configure this local server or click on Local Server link on the left pane (they are the same)

Server Manager

Server Manager ▸ Dashboard

Manage Tools View Help

Dashboard

Local Server

All Servers

File and Storage Services ▸

WELCOME TO SERVER MANAGER

QUICK START

WHAT'S NEW

LEARN MORE

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

Hide

ROLES AND SERVER GROUPS

Roles: 1 | Server groups: 1 | Servers total: 1

File and Storage Services 1

Manageability

Events

Performance

BPA results

Local Server 1

Manageability

1 Events

Services

Performance

BPA results

All Servers 1

Manageability

1 Events

Services

Performance

BPA results

4/1/2016 6:10 AM 4/1/2016 6:10 AM

Configuring the Local Server

- Then we are on the Local Server properties page.
- The first thing we see is the Computer Name (having a random name)
- Click on the computer name to change the name of the server
 - Then click on Change button (shown on next slide)
 - Type the name of the server on the Computer Name text box, for this case name the server as AU-DC-1
 - Click ok, it then restarts.

Dashboard

Local Server

All Servers

File and Storage Services

PROPERTIES

For WIN-AHMF7G04DS2


System Properties

Computer Name

Hardware

Advanced

Remote

 Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

Full computer name: WIN-AHMF7G04DS2

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

Change...

OK

Cancel

Apply

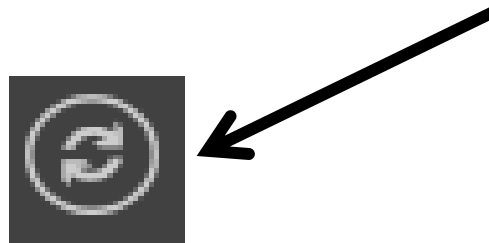
12 R2 Standard Platform

SERVER Name ID Severity Source

WIN-AHMF7G04DS2 8198 Error Microsoft-Windows-Security-SPP

Configuring the Local Server

- Go to the local server again, then click on Windows Firewall, because this server is for demonstration purpose, turn the windows firewall off (for both public and private networks)
 - This is not recommended on real working environment
- You may see it is not off immediately on the local server, but it will be changed after some moments, or click on the refresh button on top



Configuring the Local Server

- Remote management is enabled by default, leave it enabled
 - With that we may not be at the physical computer, but we can manage it remotely using commands in a domain environment
 - Uses the winrm command
- Then enable Remote Desktop
 - Disabled by default, so click on it, then click on “Allow remote connections to this computer” option, click ok on the dialog box, we can then select users of remote desktop, but for now we have no users, so click ok.
 - Remote desktop enables us to work on the server remotely

Configuring the Local Server

- The next is NIC Teaming, this is about bringing multiple Network Interface Cards together to function as one network connection (if we have more than 1 network adapters)
 - We only have one NIC now, so leave it
- The next is Ethernet, by default it takes IP address from a DHCP server, but we don't want that since we will make this machine a domain controller, so click on the link (IPV4 address...)
 - Then right click on the network adapter, properties, select Internet Protocol version 4 (TCP/IPv4), then click on properties, and select "Use the following IP address" option, and give the IP address.

Configuring the Local Server

- Click on Windows update, then click on Turn on automatic update
 - It will update if you have Internet connection.
- Then leave all the rest as default but change the time zone appropriately

Active Directory Domain Services(AD DS)

What is active Directory Domain Services(AD DS)?

- The AD DS database stores information on user identity, computer, groups, services and resources.
- AD DS domain controllers also host the services that authenticate user and computer accounts when they log on to the domain .

Purpose of Active Directory

- It provides user logon and authentication services using Kerberos protocol.
- To centralize and decentralize the resources management.
- To centrally organize and manage:
 - user accounts, computers, Groups, Network resources.

Enable authorized user to easily locate network resources.

Cont...

- Active Directory Domain Services (AD DS) is the server service for security and permissions in a windows environment.
 - Used to set up computers and security policy for those computers on the network
 - Users sign in to a network, then all the policy set up on you will apply, like some things are available, some are not available to you by that single sign up
- AD is the brain of a windows server network
 - If we don't have AD, what we have is called workgroup, and that is not centrally managed.
 - Useful for only for networks with few computers, like less than 10 to 20.
- AD is a database that keeps track of a huge amount of stuff and gives us a centralized way to manage all our network machines, users, and resources.
- There are three primary types of items in AD:
 - Users and groups
 - Services (like email, etc)
 - Resources (like printers, shared folders, etc)
- All these items are objects in the Active Directory database.

Domain

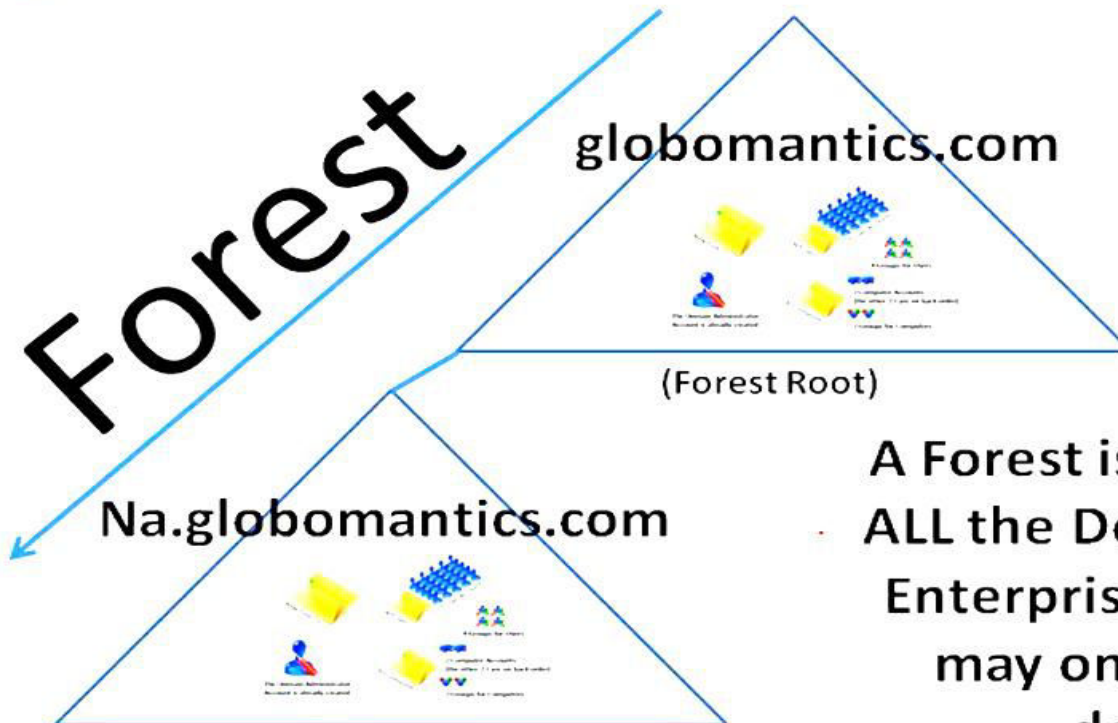
- Domain is a logical grouping of user, computer and groups objects for the purpose of management and security .
- Creating the initial domain controller in a network also creates the domain- you cannot have a domain without at least one domain controller.
- Each domain identifies by a DNS domain name.



- A windows server domain is a logical group of computers running versions of the Microsoft windows operating system that share a central directory database.
- The machines are all named with part of a domain name like “AU.EDU.ET” (also called suffix) and are registered in the active directory database so they can be managed
 - E.g. AU-DC-1.au.edu.et, CL1.au.edu.et, CL2.AU.edu.et, etc
 - All these names are said to be part of a **namespace**
- Users are also part of the namespace:
 - e.g. john@au.edu.et (if we have an email server)

Domain

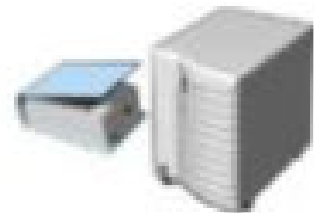
- Assume we have a domain named globomantics.com:



A Forest is comprised of ALL the Domains in your Enterprise. Your Forest may only have one domain!

What is Domain controller(DC)

- A domain controller is a server that is configured to store a copy of the AD DS directory database (NTDS.DIT) and a copy of the SYSVOL folder.
- All domain controller except RODCs stores a read/write copy of both NTDS.DIT and the SYSVOL folder.
- NTDS.DIT is the database itself, the SYSVOL folder contains all the templates setting for GPOs.
- A domain controller is a windows server machine that runs AD domain services.
- They hold the active directory database files.
- We can have multiple domain controllers that all have copies of the same active directory database.
 - When changes occur, they inform each other about it, in a process called replication.



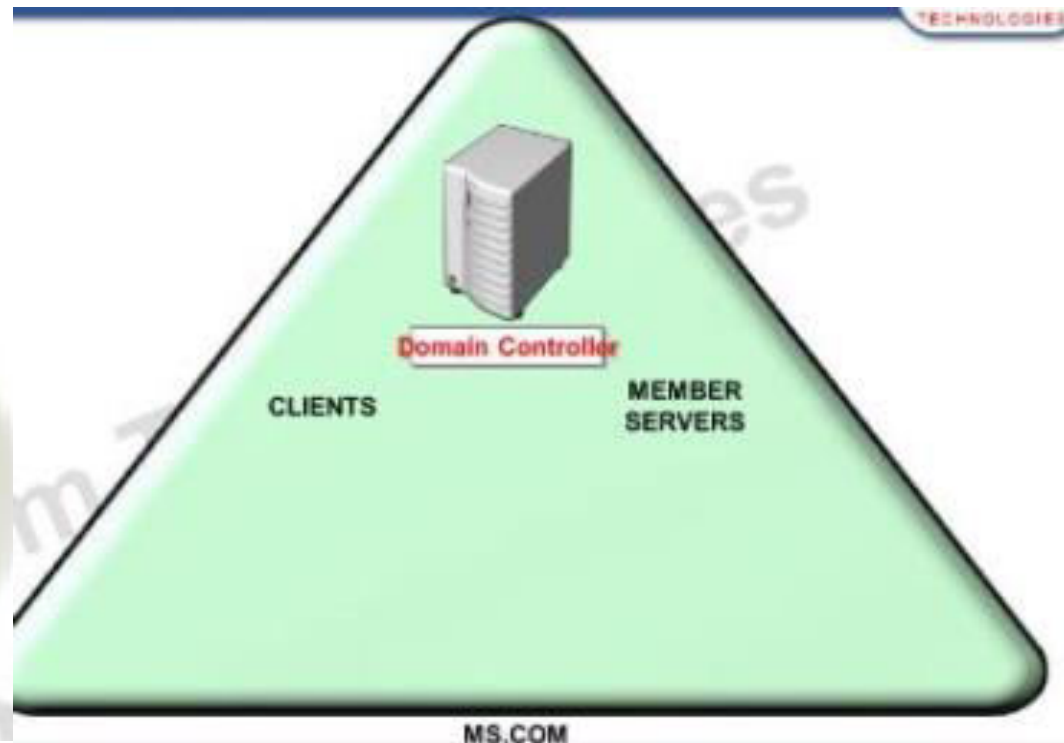
Clients and member servers.

Clients

A computer joined in the domain with client operating system. Client operating system like. Windows -8, windows-7, windows XP professional,...

Member servers.

A computer joined in the domain with server operating system. Server operating. window system like : window server 2012, windows server 2008, windows server 2003.



Server Roles

- A server role is a major job that a server can perform.
 - E.g. active directory domain services (ADDS)
- It is recommended that a server not have too many roles.
- A domain controller usually has only two roles:
 - Active directory domain services, and
 - DNS
 - DNS is a service provided by a server that allows you to find other computers in your network.
 - DNS allows us to type a friendly name of a machine instead of its IP address, allowing our client to get the IP address from the DNS server and go find the resource.
 - Without DNS, active directory will not work

Installing Active Directory Domain Services

- To install an active directory on the server, get to the server manager and click on the dashboard, then click on Add Roles and Features
- The page that comes can be eliminated not to come in future by clicking at the checkbox down (skip this page by default), and press next.
- Select “Role-based....” the default one, click next.
- Select the server, in this case “AU-DC-1”, and click next
- From the coming window, select Active Directory Domain Services
- Then comes additional roles and features wizard, click on Add Features, and click Next
- What is required is automatically checked for you, so click next

Installing Active Directory Domain Services

- Again click next, check on restart if required checkbox, and click on install
- Then click on the link “Promote this server to a domain controller”
- Here, we have to choose among 3 options
 - Add a DC to an existing domain
 - Add a new domain to an existing forest
 - Add a new forest

Installing Active Directory Domain Services

- Because this DC is the very first one we are installing, we select the last option (**add a new forest**)
 - Name it as “au.local”, and click next
- Then set functional levels based on how far we install and support previous operating systems.
 - i.e. what is the oldest DC in the entire forest or in this domain that we have to support
 - For this case, we don’t have any previous server, so choose the default (Windows Server 2012 R2).
- It is a good idea to have an Active Directory integrated DNS for many reasons, so keep the default checked DNS server

Installing Active Directory Domain Services

- Then type the directory services restore mode password
 - Which will be used in backup and recovery
- Click next, you get a warning about delegation for this DNS server cannot be created... this is because in this example we used the .local domain, it is saying that it can't find a DNS server with .local domain, just click next.
- It then finds the NetBIOS domain name (for this case AU), and click next
- Then it tells you the path where the database and log files will be stored
 - For production environments, better to separate the database and log files locations to different hard disks for a better performance.

Installing Active Directory Domain Services

- Click next, and comes the review options.
- Here, if you click on the View Script button, you see the actual PowerShell commands to make this all happen.
 - You can copy and save it for creating similar AD DC (another forest), by changing the domain and domain NetBIOS, using it as a script.
- Then click next, and it makes a pre-requisite check.
 - If you get an error, you have to follow its recommendation and solve it and re-run this check again
 - E.g. if your user account doesn't have a password, it shows you error, so solve that and come back again

Installing Active Directory Domain Services

- Then click install. It installs and restarts finally.
- When it restarts, login as the domain administrator, [domain name]\[user name]
 - E.g. AU\administrator
- Now we have installed active directory domain controller, you see that on the dashboard, we have the installed roles shown.

Installing Active Directory Domain Services

- We can add another domain controller for backup purposes, if one DC fails, the other functions.
 - In production environments, it is recommended to have more than one domain controller.
- Install another windows server to act as a second domain controller, name it as **AU-DC-2**
- Here, the important things we change are:
 - The IP address: give it another IP from same network
 - AU-DC-1: 192.168.0.10
 - AU-DC-2 : 192.168.0.11
 - Set the DNS server of the later domain controller (AU-DC-2) as the IP address of the first domain controller because we made AU-DC-1 a DNS server (in addition to making it a DC)
 - Do this together with when configuring the IP address

Installing Active Directory Domain Services

- Then go to the dashboard of AU-DC-2 and add active directory role
 - Following the same steps as in AU-DC-1 to install Active Directory Domain Services
- When you promote the server to a domain controller, this time select “Add a domain controller to an existing domain” – the default
- To specify the domain information, click on the “Select” button.
 - Put credentials given in the domain and click Ok
 - Select the domain from the retrieved ones
- Click next, and select DNS server, and also Global catalog
 - You can also make it a read only domain controller (for security reasons), but here just make it read write (the default)
 - Give the DSRM password
- Click next, for Replicate from, you can choose the nearest DC if you have multiple DCs, but now leave the default
- Click install, and then done.

Chapter Three

User Management

User Account

- User Account is an object in AD DS which controls the authentication and access to resources, and contains many attributes about a user on your network.
- In other terms, a user account in the AD represents actual user or actual person, who is going to access resource on the network.

Local user and Domain User

Local user

- A user account created in a local database of a computer.
- A local user are generally used in WORKGROUP model.
- Local user can login only on the perspective computer.

Domain user

- A user account created in ACTIVE DIRECTORY database.
- A domain user are used in domain model.
- Domain user can logon to any computer in the DOMAIN.

Traditional AD Management Tools

Tool	Description
Active Directory Users and Computers	Used for typical day to day management of Active Directory objects such as users, groups, computers, and OUs
Active Directory Sites and Services	Used to manage sites, replication, network topology, and related services
Active Directory Domains and Trusts	Used to manage trust relationships and forest functional level
Active Directory Schema	Used to manage the schema, and is not installed by default
Command Line Tools	A collection of tools which can be used for command line management and basic scripting

New Active Directory Management Tools

Tool	Description
Active Directory Administrative Center	A GUI built upon Windows PowerShell with an enhanced interface allowing you to perform object management using task-oriented navigation
Windows PowerShell	Used to create and manage objects and provides flexible scripting capabilities

Creating User Accounts on a DC

- Go to Server Manager, click on Tools menu (right side), and click on *Active Directory Users and Computers*
- On the window that comes, on the left column, under Active Directory Users and Computers, you see Saved Queries and the Domain Name you created earlier (in this case au.local)
- Expand the domain name (click on the small triangle before the name)

Creating User Accounts on a DC

- There you see the default containers
 - ✓ Builtin
 - ✓ Computers
 - ✓ Domain Controllers
 - ✓ ForeignSecurityPrincipals
 - ✓ Managed Service Accounts
 - ✓ Users
- Click on each of these to see what they have
 - ✓ The Domain Controllers for examples show you the DC servers you set up

Creating User Accounts on a DC

- Click on Users (the last one), and you see many security groups and 2 or 3 users (including Administrator and Guest-which is disabled by default)
 - ✓ Disabled accounts show small little down arrow symbols with them, like on the guest account
- To create a user account, right click on User, go to New, click on User
- This takes you to New Object – User wizard

Creating User Accounts on a DC

- Then fill the fields like First name, Last name, etc.
 - ✓ Assume you have a user named John Doe, to create a user account for this person type John as First name, and Doe as Last name, you see his full name is given by itself
- For User logon name, you should first have to plan on what format user logon names should have
 - ✓ In this case for user logon name we will follow First name and the first letter of last name, with no spaces
 - E.g. JohnD

Creating User Accounts on a DC

- Then click next
- Here you type password for this user
- You see the options “user must change password at next logon”, “user cannot change password”, “password never expires”, “account is disabled”.
 - ✓ For this case, select password never expires, since this is a test environment
- Click next, and then finish

User Properties

- After creating the user, you see the new user in the list of users
- Right click on the newly created user, and click on Properties
- There you see many tabs, including the General tab, Account tab, etc.
- Click on the Account tab, here you see options like setting the logon hours for the user, the computers he is allowed to logon etc.
- For temporary users, we can set the account expire date also.

User Template

- User templates are used to create other users based on same properties in the future
- To create a user template, right click on Users, then New > User
 - ✓ User templates are still a real user accounts, but let us give first name: `_Sales_User`, last name: `_Template`
 - ✓ Give sample user logon name, like `_sales_user_template`
 - Assuming we are creating user account template for future sales department staff members
 - We use the underscore (`_`) just to make the template appear first alphabetically (not a must)
 - ✓ Click next, give appropriate password, and password never expires (or the other option also possible)
 - ✓ **Select “Account is disabled”**, click next and finish.

User Template

- To create users based on the template, right click on the user template account, and click “copy”
- Then enter the real user name, logon name, click next, give password and de-select “account is disabled”
- The advantage of using template instead of directly creating the user is it copies all the properties from the template, like the logon ours, member of (the group this user belongs to), the privileges, etc.
 - ✓ This saves time and effort if we have many users.

Common Administrative Processes

- You can reset the password of users
 - ✓ Right click on the user, click on Reset password
 - ✓ There you can type in the new password, and also unlock the account (if it is locked for trying many times with wrong username password)
- You can also unlock an account (not reset the password) by right clicking on the user account name, properties, and then click on Account tab, there click on Unlock account checkbox
- To disable an account (like if the user leaves the organization), right click on the account, then click on Disable account
- We can also delete an account by right clicking on it

Common Administrative Processes

- We can also rename user accounts, like when you want to change the full name or logon name
 - ✓ To do so, right click on the User account, and click rename

Group Account Management

Group Account

- A Group Account is an object in AD DS which is used to help manage the permissions assigned to the users on your network.
- Instead of individually give or deny privileges to individual users, we assign them to groups and we manage the group.
 - ✓ It simplifies the management of permissions assigned to the users in the network.
 - ✓ Assume we have different users, they all work for the same department, and if it is true that they should have the same access to the same resources on a network, then group account management becomes important.

Group Account

- It enables us to give permissions to a group, and every user account which is a member of that group will inherit those permissions.

Types of Groups

- There are two types of groups:
 - ✓ Security groups
 - Used for the management of permissions
 - We will see this in this course
 - ✓ Distribution group
 - Used for activities like email distribution groups and the like
 - In exchange environment for e.g. we setup distribution groups, and email to the group other than typing all the individual users

Group Scopes

- On a domain based network, we have 3 types of group scopes
 - ✓ Domain local
 - ✓ Global
 - ✓ Universal
- Domain Local Groups:
 - ✓ Used for the direct assignment of access permissions on files, printer queues, and other such resources.

Group Scopes

- Global groups
 - ✓ Provide domain-centric membership, place all user accounts into Global groups.
 - ✓ Specific to one domain in the forest
- Universal groups
 - ✓ Used for the gathering of users and groups from multiple domains throughout the forest
 - ✓ Typically, organizations using WANs should use Universal groups only for relatively static groups in which memberships change rarely.

In reality, what we mostly deal with is the global group, and the rest are not practiced

Creating Group Accounts

- To create a group, open Active Directory Users and Computers, on the containers list, right click on users, then new, then select Group.
- You get the New Object-Group wizard.
- You put the group name (e.g. Sales Users)
 - ✓ The group scope is global
 - ✓ Group type is security
 - Just the default
- Then click ok. The security group is created.

Make Users Member of a Group

- There are more than one ways to make users of a domain be member of a group.
- One way is, right click on the group name, select properties, then click on Members tab.
- There, type the Add button, then type the user name, and click on Check Names button.
- From the populated list, select the right one and click Ok.

Make Users Member of a Group

- The other way to make users be member of a group is go to the user in the Active Directory Users and Computers, right click on it > properties > click on the Member Of tab, then click on the Add button.
- Then type the group name, and click on Check Names, then click ok (with the correct group names populated)

Make Users Member of a Group

- To add multiple users be members of a group, go to Active Directory Users and Computers, click on Users container, then press the Control (Ctrl) key and click on the multiple user accounts.
- Then right click on the selected users, select Add to Group
- Then type the group name, and click on the check names button
- Then with the appropriate group populated, click Ok.

Remove Users from a Group Membership

- To remove users membership of a group, one way is to right click on the Group, Properties, then click on the Members tab
- Then click on the member tab, and click on Remove button, click Ok.
- This does not deletes the user account, but it only removes its membership from that group

Group Account

- Using the Active Directory users and Computers or the GUI, there is not much more to do with managing groups
- But we can use PowerShell to manage our groups using scripts, or at more enterprise level we use AD Administrative Center.

Computer Account Management

Computer Account Management

- So far, we saw other ADDS objects, specifically – user accounts and group accounts.
- Computer accounts is also another type of ADDS object.
- First, go to Active Directory Users and Computers, and click on the Computers container
 - ✓ Because we did not add any computer object so far, the container is empty

Computer Account Management

- First have a client computer
 - ✓ In a VMware environment, install a client operating system (like windows 7)
 - ✓ On a physical environment, have a PC and connect it physically to the network.
- On the client computer, give it appropriate name (e.g. WIN8-client1), give an IP address from same address pool, for the DNS server of the client computer, fill the IP address of one of the Domain Controllers

Joining a Computer to a Domain

- Usually, a computer account is created when a client computer joins a domain.
- To make a computer join a domain, as an example on a windows 8.1 PC, after giving the appropriate IP address as stated on the previous slide, right click on My Computer, on the system properties, click on Change Settings, under the Member of, click on Domain, and type the domain name (in our case au.local), click Ok

Joining a Computer to a Domain

- On the coming screen, enter either the AD Administrator credentials, or any created user account on the AD as user name and password.
- It then should well come you to the domain, and allow it to restart.

Joining a Computer to a Domain

- On the Domain controller, go to the Active Directory Users and Computers, and if you click on the Computers container, you see the newly joined computer name listed.
- That is typically how computer accounts are created.
- You can also create a computer account before the computer actually joins the domain
 - ✓ This is called pre-staging or manually creating a computer account
 - ✓ To do so, right click on the Computers container > new > computer ... (try this by yourself)
 - ✓ Usually used when you want to mass create computer accounts in advance

Computer Account Management

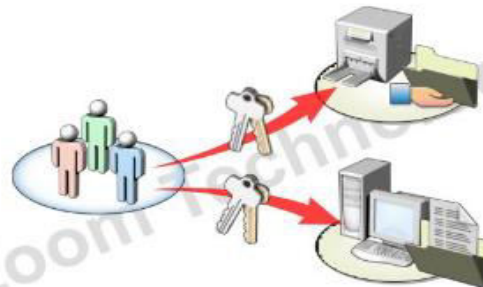
- Computer accounts are important for auditing
 - ✓ i.e. to know who did what from which computer
- If you go to the client computer and see it full computer name, it puts the domain name as suffix to the computer name
 - ✓ E.g. WIN7-Client1.au.local
 - If the computer name is WIN7-Client

Permission and group policy

What are Permissions?

- Permissions define the type of access granted to a user, group or computer to access resources.
- Permissions can be applied to resources such as files ,folders, and printers. like privilege to read a file, delete a file or to create a new file in folder.

What are Permissions?



Types of permissions

- Types of permissions
 - Security level permissions.
 - Share level permissions.
- Security level permissions
 - ✓ can be implemented only on NTFS partitions.
 - ✓ Security or NTFS permissions can be set on drives, folders and files
 - ✓ By default ,security permissions will be inherited from its parent drive or folder.
 - ✓ File permissions override folder permissions.
 - ✓ Creator of file and folder are their owner.
 - ✓ Different security permissions are :Full control, modify, read and execute, write, read, list folder contents.

Lab-Security level permissions.

Steps.

1. Open computer->goto any NTFS partitions and create a folder (DATA) along with some files in it.
2. Right click the folder(DATA) and select properties and click security tab-> click advanced tab->click edit->click disable inheritance.
3. Click remove->apply->ok->ok.
4. Click edit
5. Add administrator and allow full control permission.
6. Then add the users(user1) and all read permission.
7. Click apply->ok->ok.

Verification.

1. Login as user(user1) on the same computer, and open computer icon and verify the respective permissions by accessing the folder.
2. The user can just read the files and folders.

Share level permissions

- ¥ It can be implemented on NTFS and FAT partitions.
- ¥ It can be set on drives and shared folders but not files.
- ¥ What are shared folders?
- ¥ shared folders can be accessed from a network.
- ¥ When you copy or move a shared folder, the folder will no longer be shared.
- ¥ To hide a shared folder, include \$ after the name of the shared folder and user access hidden shared folder by typing the NUC path.
- ¥ Different share permissions are : **read, read/write**

Lab-share level permission

Steps.

1. Logon to a computer as administrator, open computer->open any drive and create a folder(sales) along with some files in it.
2. Right click the folder(sales) and select share.
3. Select the drop down arrow mark and select Find->enter the user name(user1)->click ok->select the user(user1) and assign permissions(EX read/write)->click share->click done.

Verification.

Access the shared folder.

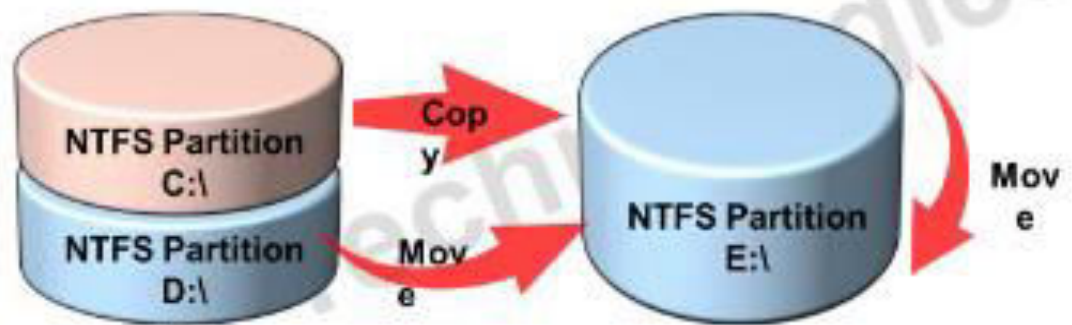
1. Logon the member or client as user(user1)->open network.
2. Open system name in which the shared folder is present.
3. Access the shared folder(sales)verify the permissions by creating some files.

Accessing shared folders using UNC path

1. Logon to member server or client as a user.
2. Click start ->click run and type the syntax \\servername\\sharename.
Example \\sys1\\sales

Effects on NTFS permissions when copying or moving files and folders

- When you copy files and folders within the same partitions or different partitions they inherit the permissions of the destination folder.
- When you move files and folders to a different partitions, they inherit the permissions of the destination folder.
- When you move files and folders within the same partition, they retain their previous permissions.



Working on organizational unit(OU)

- It is a logical container which contain active directory object(user, group,OU and other objects)
- It is also called as SBTREE
- Is used for minimizing administrative tasks.
- Is used for organizing and managing the active directory objects.
- It is used for delegating the control to one or more users.

What is Organizational Unit (OU)

- Organizational Unit (OU) is a container object in AD DS which is primarily used to help with group policy application and the delegation of permissions of other AD DS objects.
 - ✓ It is an object designed to be a container of other objects.
 - ✓ In windows explorer terms, it is like a folder..
- We use OU in domains with too many objects in the AD to organize these objects
 - ✓ Because it is difficult to manage them if they are too many and kept in simple alphabetical order.

What is Organizational Unit (OU)

- There are two other reasons why we use OUs
 - ✓ To help with group policy application
 - Group policy is applied to the various users and computers based on what container they are in.
 - ✓ For the delegation of permissions over AD DS objects
 - The OUs don't actually give the permissions, they just help us with the management of those permissions

Creating OUs

- Go to the Domain Controller and open Active Directory Users and Computers
 - ✓ Click on the top level container (the domain name)
 - ✓ You see Domain Controllers are OUs, but the rest are containers
 - ✓ OU objects has a little icon on them (different from containers)

Creating OUs

- To create your own containers, right click on the domain name (on the left pane of the AD Users and Computers window) > New > Organizational Unit
- Then give it a name
 - ✓ Leave the checked Protect container from accidental deletion on, and click Ok.
- Usually, our top level containers are expected to be static (i.e. do not change frequently), like locations
 - ✓ E.g. city of our branch office
 - ✓ For our example, name the OU as Addis.

Creating OUs

- Then we organize all our AD objects inside the OU
- We can put all the users inside the new OU
- To do so, you can drag (or cut and paste) the users you want from the Users or Computers containers to the new OU.
- It is just like creating folders and sub folders, so you can create sub OUs under OUs
 - ✓ Under the OU Addis, you can have two OUs named Addis Users and Addis Computers, and then put the appropriate objects inside them

Creating OUs

- You can decide what OUs to have and the sub OUs to organize objects in appropriate way based on three main things
 - ✓ Application of Group Policy Objects
 - How are our group policy objects going to be applied (we will see about group policy in coming chapters)
 - ✓ Delegation of Control
 - ✓ Organization
 - What is the best way to organize objects to easily find things in your company AD?
- Decide which one is most important (from the three) and do based on that.

Deleting OU

- If you delete an OU, everything inside it will be deleted.
- The 'Protect container from accidental deletion' option makes follow additional steps to delete an OU
- To delete an OU, if you right click on it and select delete, you see a warning that informs you it is not possible
- To change that and delete it, click on View menu (of the AD Users and Computers), click on Advanced Features.
- Then right click on the OU > Properties > click on the Object tab > then uncheck the Protect object from accidental deletion check box, and click ok.
 - ✓ Now you can delete the OU
 - ✓ But go to view menu and uncheck the Advanced Features

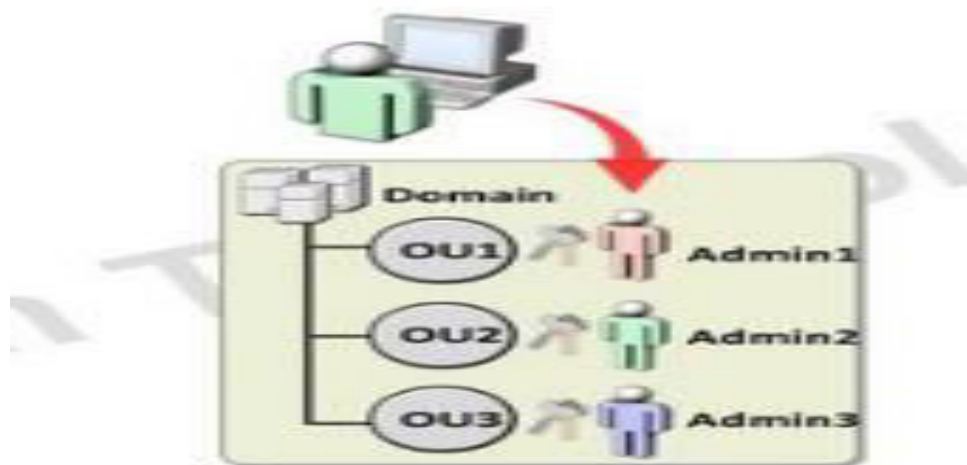
Lab on creating an organizational unit(OU)

Steps

1. press window key to go to start, select active directory user and computers.
2. Right click Domain Name->new->organizational Unit.
3. Enter the name for OU(Ex.sales1) and click Ok.
4. Create users in the sales OU(Ex. s1,s2,s3)

What is delegation of control?

- The process of decentralizing management of organizational units.
- Assigning management of an organization unit to another user or group
- Eases administration by distributing routine administrative tasks to another user or group.



Delegation of Control

- The delegation of control wizard helps us to assign specific privileges to any user, even he/she is not a member of the administrators group
- As an example, we want John Doe to reset passwords of users
 - ✓ He is **not** an administrator who can do everything but he can only reset passwords

Delegation of Control

- To delegate a user on an OU, right click the OU, select Delegate Control
- Click next on the wizard
- Then click Add to find the user who will be delegated
- Type the name of the user to be delegated and click on Check Names
- Click next and select the task that this user will be able to do
 - ✓ E.g. Reset user passwords and force password change at next logon
- Then next, and finish

Delegation of Control

- To undo the delegation for a user, make sure the Advanced Features is selected at the View menu, then right click on the container (OU), click Properties
- Click on security tab, click advanced button.
- There in the list, find the person you delegated, and double click on it or click on the edit button
- Then you uncheck the check boxes, or down click on clear all, and click ok.

Lab-on delegation of control

- Step.
- 1. got to active directory users and computers->right click OU->select delegate control
- 2. click Next.
- 3. click add->add the user(User1)
- 4. Check the box create,delete and manage user account and next.
- 5. Click finish.

Verification.

Logon to DC s user(User1),create user in OU.

Groups

- It is an object of active Directory used for applying permissions and distribution of emails to its members.

Types of groups

1. security group.
2. Distribution group.

Lab- on Creating groups

Steps.

1. Logon as administrator on a domain controller.
2. Go to start, select active directory users and computers.
3. Right click users->select New->group.
4. Mention the group name and select the Group scope as Domain local and Group type as security.
5. Group will be created successfully.
6. To add any user to this group, right click on user account and select add to a group.
7. Mention the group name as TVTI_user->click ok.
8. Add to Group operation was successfully completed.

Verification.

Go to active directory users and computer->right click on Group->select properties->select members tab->verify for the user.

Group policy

- Group policy Is a collection of setting which can be applied on computer and users
- With group policy administrator can centrally mange the computer and users.
- Eases administration using group policy.

Group Policy

Desktop Settings

Computer Icon
Recycle Bin Icon
Internet Explorer

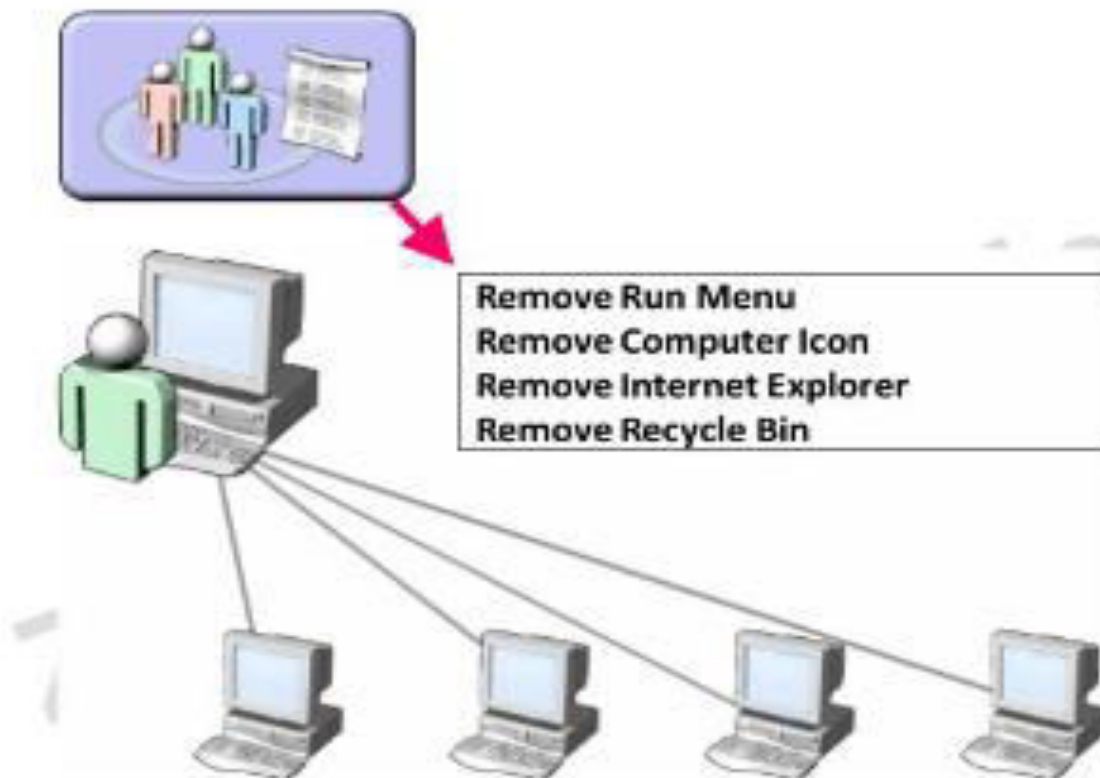
Allow or Deny

Start Menu Settings

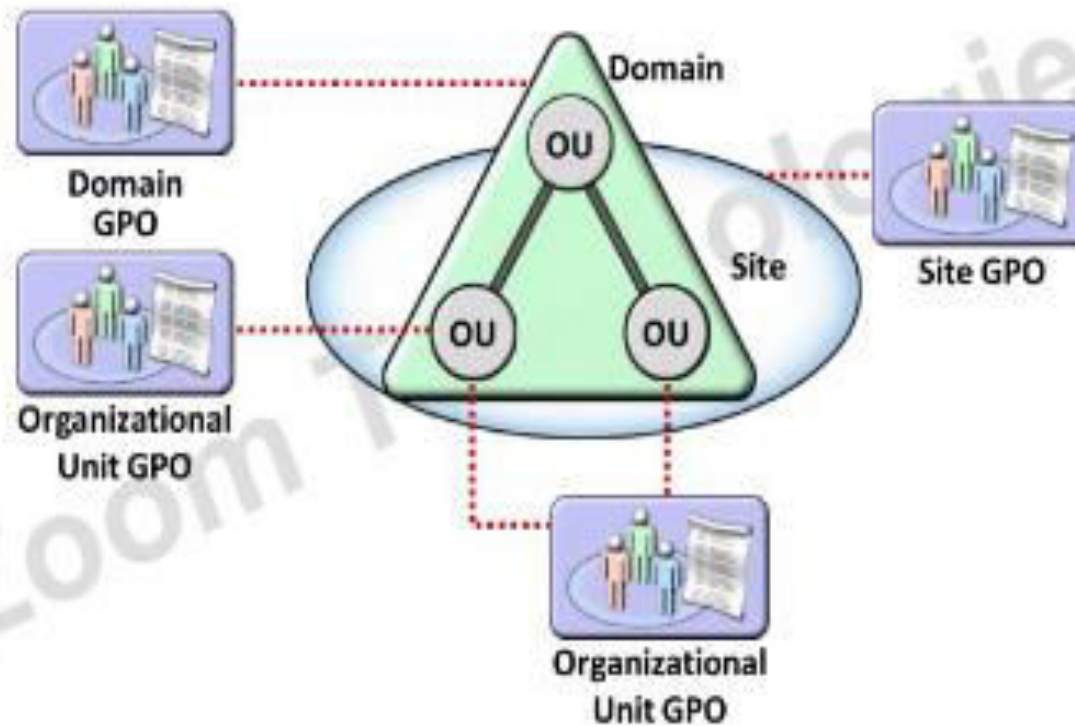
Help
Search
Run Menu

Hide or Show

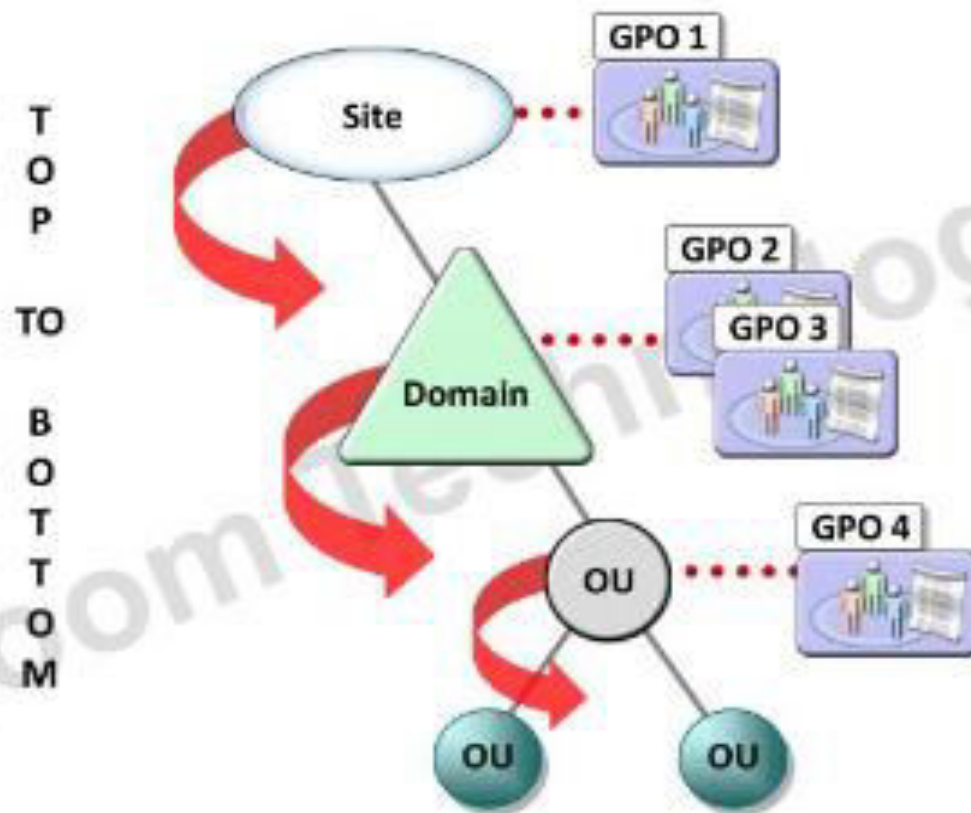
Group Policy



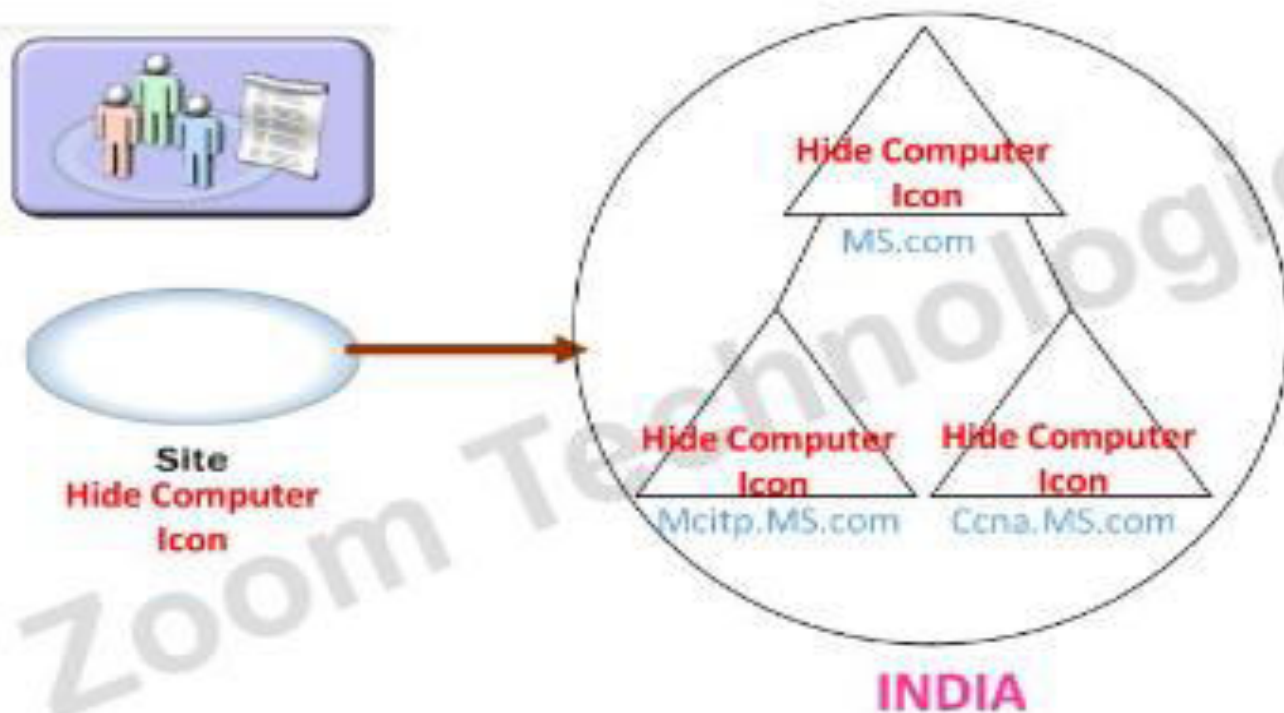
Scopes of Group Policy



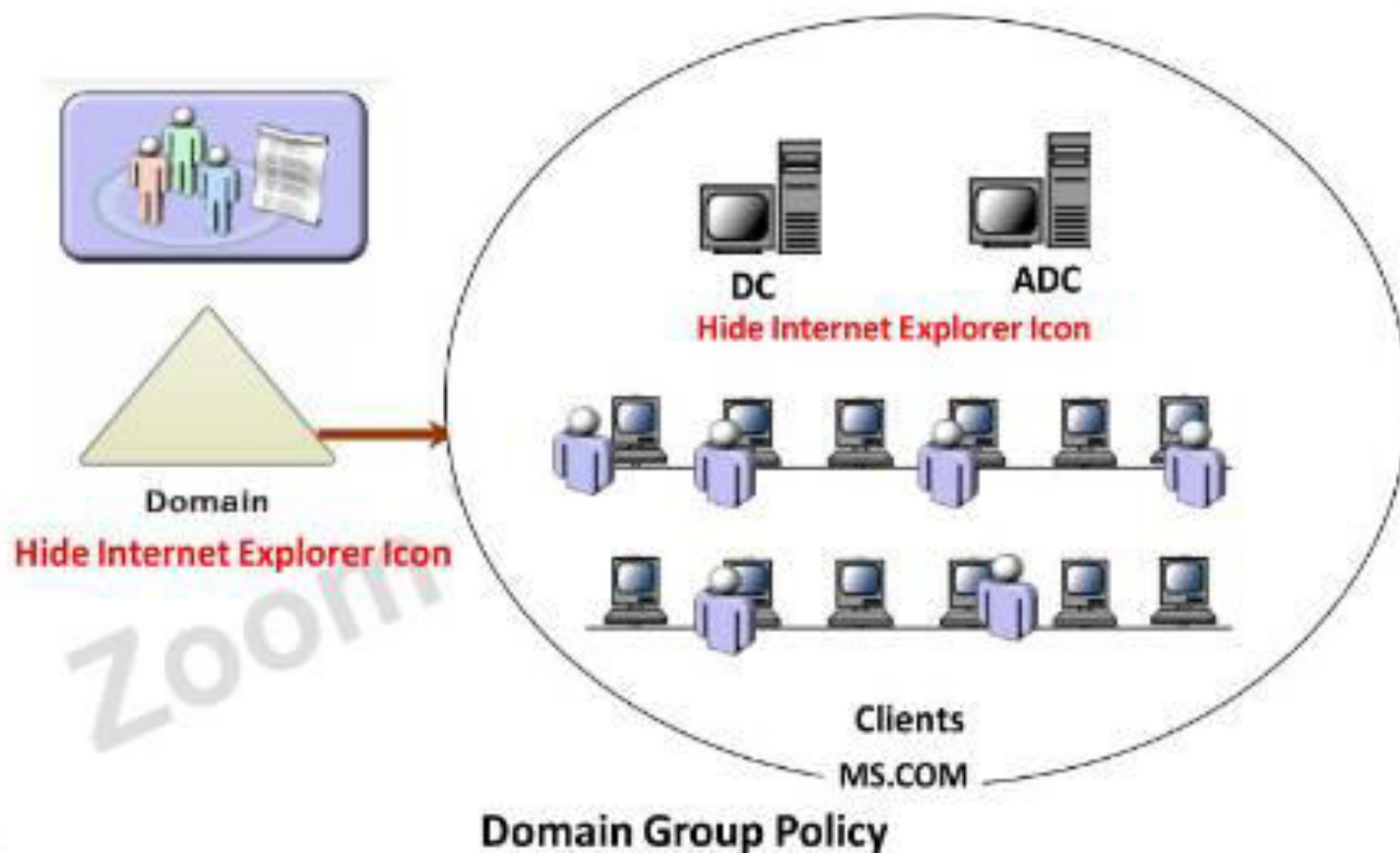
Hierarchy of Group Policy



Site Group Policy



Domain Group Policy



OU Group Policy



Lab-Applying group policy on organizational unit level

Steps.

1. Press window key to go to start, select group policy management.
2. Right click OU(sales)-create a GPO in in this domain and link it here.
3. Enter name to GPO link(ex. remove computer icon) and click ok.
4. Right click created GPO link->edit.
5. In Group policy management editor window, go to user configuration->policies ->administrative templates->desktop
6. Select policy(remove computer icon on the desktop) on right side of the screen, right click and select properties.
7. Select enabled option and click apply and ok.

Verification.

Logon to client system as sales OU user(s1) and verify the changes because of the policy.

Lab-Applying group policy on domain level.

Steps.

1. press window key to go to start ,select group policy management.
2. Right click domain name(tvti.local) and select create a GPO in this domain and link it here.
3. Enter New GPO link name ex. remove network icon and click ok.
4. Select the created GPO->right click created GPO->select edit.
5. In the Group policy management editor window ,go to user configuration->policies->administrative templates->control panel
6. Select a policy(prohibit access to control panel and pc setting) right side of the screen, right click and select properties.
7. Select enabled option and click apply and ok.

Verification

1. Logon as user(s1) to client or member server and try to access control panel.

Software deployment

- It is to deploy software(application) on all the computer in the domain from one central location by applying the group policies
- Support the deployment of “.MSI” but not “.EXE” applications.