LECTURE 1: SYSTEM ADMINISTRATION

COMPUTER SYSTEM ADMINISTRATOR

- The first-point-of-contact for an organization's network users when they experience technical problems.
- To ensure the performance and security of the computers they manage meet the needs of the network users, without exceeding the company's budget

SERVER ADMINISTRATOR

- Maintains the operating system of the servers, such as the mail services, the web services, etc.
- In charge in troubleshooting any hardware, operating system or application-related protocol

NETWORK ADMINISTRATOR

- Maintains the network infrastructure, such as the routers and switches, and troubleshoots networks-related problems

IMPLEMENTATION

- Installing and configuring networking software and application software
- Laying out and connecting cables between servers and nodes
- Establishing user accounts
- Installing wireless transmitters and receivers
- Installing storage area networks

MANAGEMENT

- Training new users
- Updating network application and security softwares
- Maintaining user accounts and access privilege
- Monitoring daily servers traffic and system usage
- Maintaining network logs
- Perform schedules tests and backups
- Assisting with special projects
- And writing user documentation

TROUBLESHOOTING

- Responding to user reports about service interruptions
- Analyzing network logs, and applying appropriate solutions.

SELF-EDUCATION

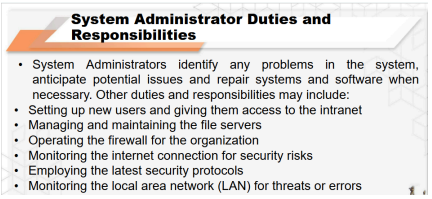
- Researching hardware and software upgrades
- Reading trade publications to keep abreast of new networking technology,
- Recommending purchases
- Helping with planning and designing special projects.

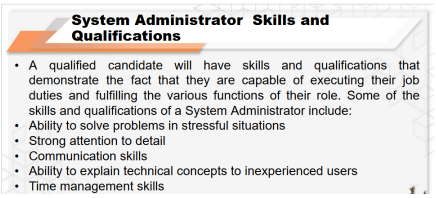
DATABASE ADMINISTRATOR

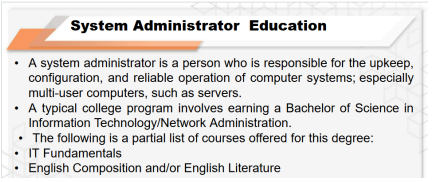
- Maintains the database system used by the company or organization
- Plan security measures, making sure that data is secure from unauthorized access
- Responsible for backing up systems in case of a power outage or other disasters
- Ensure integrity of the database, guaranteeing the data

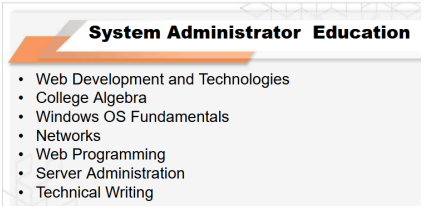
SECURITY SYSTEMS ADMINISTRATOR

- Maintains the daily operation of security systems:
  - Monitoring, running regular backups, setting up, deleting, and maintaining individual user accounts and developing organizational security procedures









LECTURE 2: ADMINISTRATOR ADMINISTRATIVE ACTIVITIES

CONTENT MANAGEMENT SYSTEMS

- Application that is used to manage web content, allowing multiple contributors to create, edit, and publish
- Software package that provides some level of automation for the taste required to effectively manage content
- Usually server-based, multiuser software that interacts with content stored in a repository
- allows us to get control of our content, which is something you'll understand well if your content is out of control.
- Keeps track of content

  CORE CONTROL FUNCTIONS:
  - Permission
  - State management and workflow
  - versioning
  - Dependency management
  - Search and organization

TYPES OF CONTENT MANAGEMENT SYSTEMS

WEB CONTENT MANAGEMENT

- Intended for mass delivery via a website
- Excels as separating content from presentation and publishing to multiple channels

ENTERPRISE CONTENT MANAGEMENT

- The management of general business content
- Excels in collaboration, access control and file managements

DIGITAL ASSET MANAGEMENT

- Management and manipulation of rich digital assets such as image, audio, and video for usage in other media
- Excels at metadata and renditioning

RECORDS MANAGEMENT

- Management of transactional information and other records that are created as a byproduct of business operations
- Excels at retention and access control

COMPONENT CONTENT MANAGEMENT SYSTEMS

- Management of extremely fine-grained content, often to assemble documentation or highly technical content

LEARNING MANAGEMENT SYSTEMS

- Management of learning resources and student interaction

PORTALS

- Used for management, presentation, and aggregation of multiple streams of information into a unified system

CONTENT DEPLOYMENT STRATEGIES

FILE SYSTEM

- Is a process of managing how and where data on a storage disk

EXAMPLE OF FILE SYSTEMS

FILE ALLOCATION TABLE (FAT / 1977)

- Used for 12 or 16 bits for each and every cluster access into the file allocation table

GLOBAL FILE SYSTEM (GFS)

- Has the ability to make enable multiple computers to act as an integrated machine
- Developed at the University of Minnesota

HIERARCHICAL FILE SYSTEM (HFS)

- Used on a Macintosh computer for creating a directory at the time hard disk is formatted

NT FILE SYSTEMS (NTFS)

- Stores and retrieves files on Windows NT, 2000, XP, 7, and 10.

UNIVERSAL DISK FORMAT (UDF / 1995)

- Developed by OSTA (OPTICAL STORAGE TECHNICAL ASSOCIATION)
- Ensuring consistency among data written to several optical media

TYPES OF FILE SYSTEMS

DISK FILE SYSTEM

- Has the ability to randomly address data within a few amounts of time
- Includes the anticipation that led to the speed of accessing data

FLASH FILE SYSTEM

- Responsible for restrictions, performance, and special abilities of flash memory

TAPE FILE SYSTEM

- Hold files on the tape as it is a tape format and file system

DATABASE-BASED FILE SYSTEM

- Another method for file management
- Files are recognized by their characteristics rather than hierarchical structured management

TRANSACTIONAL FILE SYSTEM

- Some programs require one or more changes to fail for any reason or need several file system changes but do not make any changes.

NETWORK FILE SYSTEM

- Offers access to files on a server

SHARED-DISK FILE SYSTEM

- Allows the same external disk subsystem to be accessed by multiple machines.

MINIMAL FILE SYSTEM

- Cheaper basic data storage data systems

FLAT FILE SYSTEM

- It contains only directory, and all files are held in a single directory

FILE SYSTEM PLANNING AND STRUCTURE

ACTIVE DIRECTORY(AD)

- Is a directory service that runs on Microsoft WIndows Server
- Enable administrators to manage permissions and control access to network resources

WINDOWS SERVER 2003 FILE SYSTEMS

FILE ALLOCATION TABLE

- Small partition on your disk next to NTFS

FILE ALLOCATION TABLE 32

- Backward compatibility and multiple boot partitions

WINDOWS NEW TECHNOLOGY SYSTEM 5

- Is more robust and the one you want to deploy whenever planning for AD

SERVER MANAGEMENT

- Is the process of monitoring and maintaining servers to operate at peak performance
- Also encompasses the management of hardware, software. And security backups

PRIMARY GOALS:

- Minimize(eliminate) servers slowdown and downtime
- Build secure server environments
- Ensure servers continue to meet the needs of an organization as it evolves.

VIRTUAL SERVERS

VIRTUALIZATION

- Is a major trend in today's server environments

VIRTUAL SERVERS

- Also known as virtual machines – can help increase efficiency by enabling more to be done with less hardware

SERVER MANAGEMENT

- Basics include management of hardware, software, security, and backups

USER AND GROUP MANAGEMENT

USER MANAGEMENT

- Describes the ability for administrators to manage user access to various IT resources like systems, devices, applications, storage systems, networks and more
- Enables admin control user access and on-board and off-board users to and from IT resources

GROUPS

- Administrative structures that organize assets so that you can locate an asset quickly to perform operations on all assets of the same type
- Can contain any number of assets, and assets can be members of more than one group

BACKUP MANAGEMENT

- Is an application that schedules, manages and operates data backup processes on a computer, server or network device
- Integrated application for extracting backup data copies from a source computer or IT environment to a remote storage facility

FIVE KINDS OF BACKUP MANAGEMENT:

THE FULL BACKUP

- Saves all of your data

THE INCREMENTAL BACKUP

- Only new and edited data is saved, and added to the full backup

THE DIFFERENTIAL BACKUP

- Files are saved individually

THE MIRRORED BACKUP

- Are clones of the data

THE VIRTUAL BACKUP

- Can provide almost uninterrupted access to data and applications through a virtual system in the event of a breakdown

INFORMATION SECURITY MANAGEMENT SYSTEM

- Is a framework of policies and controls that manage security and risks systematically and across your entire enterprise — information security.

PENETRATION TESTS

- Are designed to identify vulnerabilities in a company's computer network

VULNERABILITY MANAGEMENT

- allow threats such as spyware and malware to gain entry into a company's network

ENDPOINT SECURITY

- involves protecting an organization's computer network by protecting the remote devices that are bridged to it

PHISHING AND INDENTITY THEFT

- is a tactic used by criminals to steal someone’s identity

DISASTER RECOVERY

- is an organization’s method of regaining access and functionality to its IT infrastructure after events