IT412 - System Administration and Maintenance

1. Introduction to System Administration

1.1 Overview of system administration roles and responsibilities

Who is a System Administrator?

- A professional who oversees and maintains computer systems, servers, and networks for a client or within an organization.
- Understands the requirements of their clients and recommends or curates computer system designs for them.
- They do a lot of servicing tasks, but mostly they maintain software updates and the hardware conditions of systems, and some bits of identifying cybersecurity threats and ensure the security of their clients' systems.
- They ensure the smooth operation of IT services.

Core duties of a sys admin

- Installation and configuration

1.2 Understanding system architecture

What is system architecture?

- It is an abstract reflection of how a system interacts with other systems in a similar environment.
- Since system architecture is usually an abstract concept, the way to visualize it is through diagrams.
- A well designed system architecture is crucial for:
  - Scalability: ability to grow and manage increased loads
  - Reliability: ensuring systems are dependable and available
  - Performance: optimizing system resources for efficient operation
  - Security: structuring systems to protect against threats

- User management
- System monitoring
- Backup and recovery
- Security management

2. Computer Server Fundamentals: Types of Servers and their Roles

Computer Server - a powerful computer or system designed to provide resources, data, or services to other computers.

Key characteristics of a server:

- Powerful Hardware - equipped with high performance components to handle heavy tasks
- Reliability - built for 24/7 operation
- Scalability - can grow with demand
- Specialized operating systems - uses platforms like Windows Server, Unix, or Linux

Types of Servers:

- File server - stores and manages files, which users on network can access
- Web server - hosts websites and serves web pages
  - *Apache*
  - *Nginx*
  - *Microsoft Internet Information Services*
- Database server - manages database and handles client requests
  - *MySQL*
  - *Microsoft SQL Server*

    - *Oracle Database*
- Application server - runs applications and serves functionalities
    - *WebLogic*
    - *JBoss*
    - *Tomcat*
- Mail server - manages and stores emails
    - *Microsoft Exchange Server*
    - *Postfix*
- Print server - manages printers on a network
- Domain Name Server (DNS) - translates human-readable domain names into IP addresses
- Proxy Server - acts as an intermediary between clients and other servers, often used for security, content filtering, or caching
- Virtual server - a virtual instance of a server that runs on a physical server using virtualization technology

Functions of a server:

- Resource sharing - allows multiple clients in the same network to share resources
- Data management - stores, manages, and protects data, ensures that it is accessible only to authorized users
- Service provision - provides specific services (depends on the type of server)
- Network management - can manage network resources (e.g., authentication, permissions, security policies)

3. Operating Systems Fundamental

What is an OS?

The most important software that runs on a computer, managing computer's memory and processes, and other software and hardware components.

Types of OS

- Batch operating systems → executes a series of jobs without user interaction
  - Examples: Early mainframe systems like IBM's OS/360
- Time-sharing systems → allow multiple users to access the computer resources simultaneously via allocating *time slices* to each user.
  - Examples: UNIX
- Distributed operating systems → manages a group of independent computers and present them to users as a single, coherent system. Enables resource sharing across multiple machines.
  - Examples: Google's Android OS
- Real-time operating systems → designed to process data as it comes in, typically used in environments where timing is critical.
  - Examples: VxWorks is an RTOS used in embedded systems, which are found in aerospace and automotive applications
- Network operating systema → provides services to computers connected over a network
  - Examples: Microsoft Windows Server
- Mobile operating systems → designed specifically for mobile devices
  - Examples: iOS and Android

Installation Basics

1. Preparation
   a. Ensure that hardware meets the requirements for an OS
   b. Backup any important data, as installation may overwrite existing data
2. Booting from installation media
   a. Use installation media like USB drives or DVD to boot the computer. This media contains the OS installation files.
3. Partitioning the disk

a. During installation, you may need to partition the hard drive to allocate space for the OS and other data

4. Post-installation configuration
    a. After installation, configure system settings, install drivers, and update the OS to ensure optimal performance and security

4. Active Directory Administration

What is **Active Directory Administration?**

A critical component of Windows Server environments, provides centralized location for managing users, computers, and other resources within a network. Setting up Active Directory involves understanding various networking concepts, including IP addressing and subnetting.

Setting up Active Directory in Windows Server 2008

1. Prerequisites
    a. Windows Server 2008 is installed and properly configured on the server
    b. Verify that the server has a static IP address assigned, as dynamic addresses can lead to connectivity issues in an Active Directory environment.
2. Install Active Directory Domain Services (AD DS)
    a. Open the server manager from the start menu.
    b. Click on **Roles** and then **Add Roles**
    c. Select **Active Directory Domain Services** and follow the prompts to install the role
3. Promote the Server to a Domain Controller
    a. After installing AD DS, you will need to promote the server to a domain controller
    b. In Server Manager, click on the notification flag and select **Promote this server to a domain controller**

c. Choose to create a new domain in a new forest, and provide a domain name (e.g., “example.local”)

d. Configure the Domain Controller options, including the Directory Services Restore Mode (DSRM) password

4. Configure DNS

   a. During promotion process, the server will also configure DNS. Ensure that the DNS server is set up correctly, as Active Directory relies heavily on DNS for locating resources

   b. Verify that the DNS settings are correct by checking the DNS manager after the installation process

5. Complete the installation

   a. Follow the remaining prompts to complete the installation. The server will restart, and upon reboot, it will be functioning as a domain controller

6. Create Organizational Units (OUS)

   a. After setting up the Active Directory, you can create Organizational Units to organize users, groups, and computers logically

7. Add users and groups

   a. Use the Active Directory Users and Computers (ADUC) console to create user accounts and groups

IP ADDRESS

A unique identifier for each device on a network. In an Active Directory environment, it is crucial to assign static IP addresses to domain controllers to ensure consistent connectivity.

SUBNET MASK

Subnetting involves dividing a larger network into smaller, manageable sub-networks. This helps improve network performance and security.

5. User and Group Management

User and Group Management **Main Concepts**

- Important in environments that involve Active Directory (AD)
- Essential for maintaining security, ensures appropriate access to resources, and facilitating collaboration within an organization

Permissions

- Defines what actions users and groups can perform
- Common permissions are read, write, modify, delete

Access Control Lists (ACLs)

- Used to define permissions for users and
  groups on specific resources.
- **User Accounts:** individual profiles
- **Group Accounts:** Collections of user accounts

Types of Groups

- **Security Group:** assigns permissions to shared resources
- **Distribution Group:** normally has no permissions, used for information distribution like emails

Practice: Which Group?

- Payroll Access → Secure
- Email all employees → Distribution
- Shared marketing folder → Secure

6. File Systems and Storage Management

File System Types/Formatting

- A **file system** is a structure used by the operating system to organize and manage files on storage devices (HDD, SSD, USB, etc.).
- It defines **how data is stored, accessed, and organized**.
- A file system must be created before information can be written to a drive.
- The chosen file system must be **compatible with the operating system**.
- Ideally, the file system should allow the OS to **easily read and write files**.
- Some operating systems support **multiple file systems**, while others can only read from **specific ones**.

Common File Systems

FAT (File Allocation Table)

- One of the oldest, simplest file systems.
- Used in early OS such as **MS-DOS, Windows 95/98/ME**; still used in **removable storage** (USBs, memory cards, cameras).
- Uses a **table to track file locations** on disk (clusters linked as files).
- **Lacks advanced features** (e.g., permissions, journaling).
- Still supported by **Windows, macOS, Linux** for compatibility.

ext4 (Fourth Extended File System)

- Standard file system for **Linux**.
- Features: **journaling, high performance, large file/partition support, reliability**.
- Used in: **Linux distros** (Ubuntu, Debian, Fedora, etc.) and **Android OS**.

FAT32

- An improved version of FAT, introduced with **Windows 95 OSR2 (1996)**.
- Supports **volume sizes up to ~2 TB** and **files up to 4 GB**.
- A file system defines how data is **stored, organized, and managed** with names and permissions.

NTFS (New Technology File System)

- Default Windows file system since **Windows NT (1993)** through **Windows 11**.
- Features: **permissions, encryption, compression, journaling, large file/partition support**.
- **Best for modern storage devices** due to advanced capabilities.
- **Compatibility:** Fully supported on Windows; limited on **macOS/Linux** (read-only by default, write requires tools).

- **Disk Management** → a built-in Windows utility that allows users to perform advanced operations on their computer's storage devices, such as:
  - Initializing new drives
  - Creating and deleting partitions
  - Formatting drives
  - Changing drive letters

- **Partitioning** → the process of dividing a physical disk into separate, logical sections

7. System Monitoring and Performance Tuning

- **System Monitoring →** Observing, collecting, and reporting key performance metrics over time. Helps to detect issues, track trends, ensure system health.
- **Performance Tuning →** Taking actions (configuration, code changes, hardware adjustments) to improve the system based on monitoring data.

Performance Metrics in System Monitoring

- **CPU Usage:** % of processor in use; high usage = heavy resource load.
- **Memory Usage:** RAM in use; low memory = slowdowns/disk swapping.
- **Disk I/O:** Speed of disk reads/writes; high I/O = possible bottlenecks.
- **Network Traffic:** Data sent/received; high traffic = congestion/slow responses.

Performance Tuning Techniques

Why Important?

- Avoid downtime
- Improve responsiveness / user experience
- Better resource usage → cost savings
- Scalability

Various Tools in System Monitoring

Windows Tools:

- Task Manager for quick process overview
- Performance Monitor for detailed counters
- Event Viewer for system logs

Linux Tools:

- top/htop for CPU and process activity.
- vmstat for memory and system statistics.
- iostat for disk performance.
- netstat/ss for network traffic and connections.

- **Establish Baselines:** Define normal performance to detect issues.
- **Identify Bottlenecks:** Identify problem areas (CPU, memory, disk, network).
- **Config Tuning:** Adjust system/database settings for efficiency.
- **Hardware Scaling:** Add RAM, SSDs, CPUs, or load balancing.
- **App Optimization:** Improve queries, caching, and reduce blocking.
- **Resource Isolation:** Use virtualization/containers to separate workloads.

Performance Tuning Processes

- **Monitor:** Gather performance data with tools.
- **Analyze:** Spot unusual patterns or changes.
- **Identify:** Find exact bottlenecks.
- **Fix:** Adjust configs, upgrade hardware, or optimize apps.
- **Validate:** Compare results to baseline.
- **Repeat:** Continuously tune and document.

8. Backup and Recovery Strategies

Importance of Data Backup

- Regular backups are essential to avoid unwanted data loss
- Ex: A company that relies on customer databases must have a backup strategy to prevent data loss in case of a server crash.

Types of Backups

- Full Backup → complete copy of all data at a specific timeframe. Can be comprehensive, but time-consuming and memory-hogging.

Backup Storage Solutions

- **On-site Storage:** Local storage devices such as external hard drives or network-attached storage (NAS) devices.
- **Off-site Storage:** Remote locations or cloud storage solutions that provide additional protection against local disasters.

Recovery Procedures

- **Recovery Time Objective (RTO):** The maximum acceptable time to

- Incremental Backup → Only backup the data that has been changed over time. Faster and consumes less memory than full backup, but can complicate the process.

restore data after a failure.

- **Recovery Point Objective (RPO):** The maximum acceptable amount of data loss
measured in time.
- Ex: A company may set an RTO of 4 hours and an RPO of 1 hour, meaning they
aim to restore data within 4 hours and can tolerate losing up to 1 hour of data.

9. Security Fundamentals

System Security

- Involves protecting computer systems and networks from threats such as malware, unauthorized access, and data breaches.
- Implements measures to safeguard hardware, software, and data.

Common Security Threats

- **Malware:** Malicious software designed to harm or exploit systems. *Ex. viruses, worms, ransomware, and spyware.*
- **Phishing:** A social engineering attack where attackers impersonate legitimate entities to trick users into revealing sensitive information, such as passwords or credit card numbers.

Best Practices for System Security

- Regular software updates
- Strong password policies
- User education and awareness

Security Audits

- A systematic evaluation of an organization's security policies, procedures, and controls.
- Helps identify vulnerabilities and assess the effectiveness of security measures.
- *Ex: An organization conducts a security audit to evaluate its network security, access controls, and incident response procedures.*

- **Unauthorized Access:** Gaining access to systems or data without permission, often through weak passwords or exploiting vulnerabilities.