Course Material No. 2

ITP111– System Administration and Maintenance

Joseph D. Cartagenas
Course Instructor

Operating System Installation and Configuration

2

LEARNING OUTCOMES

At the end of this module the student be able to:

1. Define the requirements for installing different operating systems.
2. Demonstrate how to partition disks and allocate storage space for different operating systems.
3. Identify how they manage user groups and the significance of group membership.
4. Understand the concept of system services and daemons and their roles in the operating system.

RESOURCES NEEDED

For this lesson, you would need the following resources:

Panek, C. (2020). Windows Operating System Fundamentals.
Phillips, H. L. (2012). Microsoft Windows 7 for Power Users : Advanced.

MODULE CONTENTS

PLANNING AND PERFORMING OS INSTALLATION

Operating System Installation and Configuration is a fundamental process in setting up and optimizing computer systems. This crucial stage involves planning and performing OS installations, managing disk partitions and file systems, configuring initial system settings, handling user and group management, and managing essential system services. A well-executed installation and configuration process ensures a stable, secure and efficient operating system environment laying the groundwork for seamless software deployment and reliable computing experiences.

Operating system installation starts with careful planning. It involves determining the appropriate OS version for the specific hardware and user requirements. Different operating systems may be chosen depending on factors such as compatibility, functionality, security features, and support. Once the OS is selected, the installation process begins. This can be done using installation media like DVDs, USB drives, or over a network.

During the installation, users are prompted to make decisions such as the language, keyboard layout, time zone and installation type (fresh install or upgrade). A fresh install wipes out existing data while an upgrade maintains data and applications while updating the OS version.

Performing the operating system installation is a critical phase in the setup of a computer system. It involves careful consideration of hardware and software requirements. Below are the details of installation process:

1. **Hardware and Software Requirements:** Before proceeding with the installation, it is essential to review the hardware and software requirements of the chosen operating system. Different OS versions have specific hardware prerequisites, such as minimum RAM, processor speed, disk space, and graphics capabilities. Ensuring that the hardware meets or exceeds these requirements is vital to achieving optimal performance and avoiding compatibility issues. Additionally, it's essential to verify that all necessary drivers for

hardware components are available and compatible with the chosen OS. Drivers are software that enables the OS to communicate with hardware devices effectively.

2. **Operating System Selection:** Choosing the appropriate operating system is a significant decision based on various factors. Different operating systems offer different features, functionalities, and compatibility with software applications. Some common operating systems include Windows, macOS, Linux distributions (such as Ubuntu, Fedora, and CentOS), and others. Considerations for selecting an OS include user requirements, the purpose of the system (e.g., personal use, server deployment, scientific research), compatibility with required software, security features, and support options.

3. **Backup and Data Management:** Before initiating the OS installation, it is essential to back up all critical data. The installation process may require formatting or repartitioning the hard drive, which can lead to data loss. Creating backups on an external storage device or cloud storage ensures that valuable data is not lost during the installation.
4. **Installation Media:** The installation media is the physical or digital medium through which the OS installation files are accessed. It can be a DVD, USB drive, or an ISO image downloaded from the internet. For older systems, the installation media might be in the form of floppy disks. The choice of installation media depends on the system's hardware and available boot options.
5. **Installation Process:** The installation process varies depending on the chosen operating system. Generally, it begins by booting the computer from the installation media. This is usually achieved by changing the boot order in the BIOS/UEFI settings or selecting the boot device manually during startup.

The user is guided through a series of prompts once the system boots from the installation media to set up the language, keyboard layout, time zone, and other system-specific settings. The user then selects the installation type, which can be a fresh install or an upgrade from an existing OS.

During a fresh install, the installer formats the specified partition(s) and copies the OS files to the designated location. In the case of an upgrade, existing system files are replaced or updated without affecting personal data and applications.

6. **Post-Installation Setup:** There are usually additional setup steps to finalize the system configuration after the OS installation is complete. These steps may include creating user accounts, setting up passwords and configuring network settings. Installing essential drivers, such as graphics, audio, and network drivers, is also crucial for optimal hardware functionality.
7. **Software and Security Updates:** Once the OS is installed it is essential to apply software updates and security patches promptly. Operating systems regularly release updates to address security vulnerabilities, improve stability and introduce new features. Keeping the OS up to date and ensures a more secure and reliable computing environment.

DISK PARTITIONING AND FILE SYSTEM MANAGEMENT

Disk partitioning and file system management are crucial aspects of setting up a computer system and organizing data on storage devices. Disk partitioning involves dividing the physical hard drive into separate sections, while file system management involves choosing the appropriate file system to control data storage and retrieval within those partitions.

1. Disk Partitioning:

Disk partitioning is the process of dividing a physical hard drive into logical segments, each acting as an independent storage unit. Each partition is treated as a separate entity with its file system, allowing for better data organization, improved performance, and enhanced security. Here are some key points related to disk partitioning:

a. **Purpose of Disk Partitioning:** Partitioning helps in segregating different types of data and system files, reducing the risk of data corruption and improving data recovery options. It also allows for the installation of multiple operating systems on the same hard drive, facilitating dual-boot setups.

b. **Types of Partitions:** Common partitions on a typical computer system include:

- Root Partition (/): This is the primary partition where the operating system and system files are installed.

- Swap Partition: Used for virtual memory, particularly on Linux systems, to improve system performance.
- /home Partition: This partition stores user data, documents, and settings, providing a clear separation between the OS and user data.
- Data Partitions: Additional partitions may be created for specific data storage needs, such as media files, databases, or backup data.

c. Master Boot Record (MBR) and GUID Partition Table (GPT): These are two partitioning schemes used on hard drives. MBR is the older standard and supports up to four primary partitions or three primary partitions and one extended partition. The GPT scheme, introduced later, allows for an almost unlimited number of partitions and is more suited for modern systems with large storage capacities.

d. Partitioning Tools: Operating systems often come with built-in partitioning tools, like Disk Management on Windows and Disk Utility on macOS. Additionally, third-party partitioning software is available for more advanced partition management tasks.

2. File System Management:

File system management involves choosing the appropriate file system for each partition created during disk partitioning. The file system is responsible for organizing and managing files and directories, controlling how data is stored, retrieved, and secured on the storage device. Common file systems include:

a. NTFS (New Technology File System): Used primarily on Windows operating systems, NTFS supports advanced features like file and folder permissions, encryption, disk quotas, and journaling, which helps with data recovery after a system crash.

b. ext4: Commonly used on Linux distributions, ext4 is an evolution of the earlier ext3 file system and provides better performance and reliability. It supports large file sizes and partitions.

c. APFS (Apple File System): Developed by Apple, APFS is the default file system on macOS. It offers features like snapshots, cloning, and space sharing, optimizing performance on flash storage.

d. FAT32 (File Allocation Table): An older file system used for compatibility with various devices, especially USB drives, cameras, and gaming consoles. However, it has limitations, such as supporting only file sizes up to 4GB.

e. exFAT (Extended File Allocation Table): A newer file system designed to overcome FAT32 limitations, supporting larger file sizes and improved compatibility across different platforms.

Choosing the appropriate file system depends on the operating system, hardware compatibility and intended usage of the partition. For example, Windows usually requires NTFS for system partitions, while Linux may use ext4 for both system and data partitions.

Disk partitioning and file system management are crucial components of setting up an efficient and well-organized computer system. Properly dividing the hard drive into partitions allows for better data management and improves system performance, while selecting the appropriate file system ensures data integrity, security, and compatibility with the chosen operating system. Careful consideration of partitioning schemes and file system options is essential for creating a reliable and scalable storage infrastructure.

CONFIGURATION AND SETUP OF OPERATING SYSTEM

Initial configuration and setup of operating systems is a critical phase in the deployment of a computer system. It involves configuring various settings and options to optimize the system's performance, security, and usability. This phase takes place right after the operating system installation and before users start using the system. Let's delve into the details of this process:

1. **Language, Time Zone, and Keyboard Layout:** During the initial setup, users are prompted to select their preferred language, time zone, and keyboard layout. These choices determine the system's display language, date, and time settings, as well as

keyboard input settings. Accurate settings are essential for proper system operation and user convenience.

2. **Network Configuration:** Configuring the network settings is a crucial step, especially for systems connected to the internet or local networks. The setup includes assigning IP addresses (either manually or through DHCP), configuring DNS settings, and setting up network interfaces. Proper network configuration ensures seamless internet connectivity and access to local resources.
3. **Updating System Packages and Drivers:** After the OS installation, it is essential to update the system packages and drivers to the latest versions available. This process helps fix bugs, improve stability, and address security vulnerabilities. Updating system packages also ensures compatibility with the latest software and hardware.
4. **Firewall Configuration:** Configuring the system's firewall is essential for securing the system from unauthorized access and potential threats. Firewalls control network traffic based on predefined rules, allowing or denying access to specific ports or services. By setting up firewall rules, administrators can control which applications and services can communicate over the network.
5. **User Account Setup:** Creating user accounts and assigning appropriate permissions is crucial for managing user access and security. Administrative accounts with elevated privileges are usually created during the initial setup to perform system-level tasks. Regular user accounts are set up for everyday use, limiting their access to sensitive system files and settings.
6. **Password Policies:** Implementing strong password policies is vital for enhancing system security. Password policies often include requirements for password length, complexity (uppercase, lowercase, numbers, and special characters), and periodic password changes. By enforcing strong passwords, the system is better protected against unauthorized access and potential security breaches.
7. **Time Synchronization:** Ensuring accurate time synchronization is crucial for various system functions, such as log management, scheduled tasks, and network authentication. Systems can be synchronized with internet time servers or local time sources to maintain consistent time across the network.

8. **Disk Encryption:** On systems that handle sensitive data or are subject to security regulations, enabling disk encryption provides an additional layer of protection. Disk encryption encrypts the data stored on the hard drive, making it inaccessible without the correct encryption key or passphrase.
9. **Display and Theme Settings:** Customizing display settings, such as screen resolution, wallpaper, and theme, allows users to personalize their computing experience. While this aspect is more user-oriented, administrators might pre-configure default settings to ensure uniformity across multiple systems in an organization.
10. **Software Installation and Configuration:** Installing and configuring essential software applications (e.g., web browsers, office suites, media players) during the initial setup can save time for users and ensure a productive environment from the start. Organizations often use automated deployment tools or pre-configured system images to streamline this process.

The initial configuration and setup of operating systems are crucial for establishing a functional, secure, and user-friendly computing environment. It involves configuring language and regional settings, network connectivity, firewall rules, user accounts, password policies, and time synchronization. Additionally, administrators can enhance security by enabling disk encryption and ensure a consistent user experience by configuring display settings and installing necessary software applications. A well-planned and executed initial setup lays the foundation for a stable and efficient operating system environment.

USER AND GROUP MANAGEMENT

User and group management is a fundamental aspect of operating system administration that involves creating, managing, and organizing user accounts and groups to control access to resources and enhance security. This process plays a vital role in maintaining the integrity and confidentiality of data and ensuring proper user privileges within a computing environment. Let's examine into the details of user and group management:

1. **User Accounts:** User accounts represent individual users who interact with the operating system and various applications. Each user account has a unique username and associated

security credentials, such as a password or passphrase. Here are the key aspects of user account management:

a. **User Creation:** Administrators can create user accounts for individuals or employees. Each user is assigned a username and, optionally, other information such as full name, contact details, and user role.

b. **Password Management:** Passwords are crucial for securing user accounts. Administrators can enforce password policies, such as complexity requirements, length restrictions, and periodic password changes, to enhance security.

c. **User Privileges:** User accounts can be assigned different levels of privileges based on the principle of least privilege. Regular users typically have limited access to system resources, while administrative accounts have elevated privileges to perform critical system tasks.

d. **User Deactivation and Removal:** When users leave an organization or no longer require access to the system, their accounts should be deactivated or removed to prevent unauthorized access.

2. **Group Management:** Groups are collections of user accounts that share common permissions and access rights. Group management allows administrators to apply permissions and security settings collectively, simplifying access control. Here are the main aspects of group management:

a. Group Creation: Administrators can create groups based on organizational roles or project teams. Each group is given a unique name and an optional description.

b. Group Membership: User accounts can be added or removed from groups as needed. Group membership grants the users the permissions associated with that group.

c. Resource Access Control: Permissions can be assigned to groups on specific resources, such as files, folders, and applications. This simplifies access control, as administrators can apply permissions to groups instead of individual users.

d. Nesting Groups: In some cases, groups can be nested within other groups, creating a hierarchical structure. This allows for easier management of permissions and access rights.

3. **Access Control Lists (ACLs):** Access Control Lists are a more granular way to control resources and allowing administrators to set specific permissions for individual users or groups on a particular resource. ACLs are used in addition to the traditional file permissions offering fine-grained access control.
4. **Multi-factor Authentication (MFA):** MFA is an additional security layer that requires users to provide multiple forms of identification before gaining access to the system. This can include something they know (password), something they have (smartphone or security token), or something they are (biometric data).
5. **Auditing and Monitoring:** User and group management often involves auditing and monitoring activities. Logs are maintained to track user account creation, changes in group membership, and other critical events to maintain accountability and detect any unauthorized activities.
6. **Directory Services:** User and group management is often facilitated in larger organizations through directory services like Active Directory (used in Windows environments) or LDAP (Lightweight Directory Access Protocol). Directory services centralize user and group information making management more efficient across multiple systems and domains.

User and group management is essential for maintaining a secure and well-organized computing environment. Properly managing user accounts, assigning appropriate privileges, and controlling access to resources through groups and permissions contribute to data integrity, confidentiality, and system stability. By implementing effective user and group management practices, administrators can ensure that users have the necessary access they need while minimizing potential security risks.

MANAGING SYSTEM SERVICE AND DAEMON

Managing system services and daemons is a crucial task in operating system administration. System services and daemons are background processes that run continuously to handle various tasks and functions on the computer system. These processes range from managing hardware devices, network services, and system resources to providing essential functionality for user applications. Efficiently managing these services and daemons is essential for system performance, security, and stability. Let's explore this topic in detail:

1. Understanding Services and Daemons:

Services and daemons are background processes that start automatically when the operating system boots and run continuously in the background, waiting to perform specific tasks or respond to requests. They operate independently of user interaction and are often critical for the system's proper functioning.

Services are primarily used in Windows environments, while daemons are commonly associated with Unix-like systems (Linux, macOS, etc.).

2. Starting and Stopping Services and Daemons:

Administrators can start, stop, restart, or reload services and daemons to manage their behavior. Starting a service/daemon makes it active and ready to execute its tasks, while stopping it suspends its operation. Restarting or reloading services/daemons is useful when changes to their configurations or settings need to take effect without requiring a full system restart.

3. Configuration Files and Parameters:

Services and daemons often have configuration files that determine their behavior and settings. Administrators can modify these configuration files to customize the services' functionality according to specific requirements. Careful management of configuration files is essential to avoid errors and security vulnerabilities.

4. Enabling and Disabling Services and Daemons:

Enabling or disabling services/daemons controls whether they start automatically during system boot. Enabling essential services ensures they are available when needed, while disabling unnecessary ones reduces system resource consumption and potential security risks.

5. **Monitoring and Logging:**

Monitoring services and daemons is crucial for detecting issues, performance bottlenecks, or potential security breaches. Many operating systems provide built-in tools to monitor service status and resource usage. Additionally, logging helps track service activities, system events, and error messages, which can be used for troubleshooting and auditing purposes.

6. **Dependency Management:**

Services and daemons can have dependencies on other services or system resources. Administrators must consider these dependencies when managing services to avoid conflicts and ensure that all required components are available for proper functionality.

7. **Security Considerations:**

Managing services and daemons is critical for security. Unnecessary or unused services may present potential attack vectors, making the system more vulnerable to security threats. Regularly reviewing and disabling unnecessary services helps minimize the system's attack surface.

8. **Managing Services and Daemons in the Cloud:**

In cloud environments, the management of services and daemons is often performed using cloud-specific tools and services. Cloud providers offer ways to deploy, scale, and manage various services without direct interaction with the underlying operating system.

9. **Automation and Orchestration:**

In modern IT environments, automation and orchestration tools play a significant role in managing services and daemons. Tools like Ansible, Puppet, and Chef allow administrators to define and automate service configurations and deployments across multiple systems, ensuring consistency and reducing manual intervention.

Managing system services and daemons is a critical task for maintaining a stable, secure, and high-performance computing environment. Administrators must be familiar with the services and daemons running on their systems, understand their configurations, and apply best practices to optimize system performance and enhance security. Regular monitoring, configuration management, and security considerations are key aspects of efficiently managing services and daemons on any operating system.

SUMMARY

We covered various topics related to IT infrastructure and system administration. We began by exploring the role and responsibilities of a system administrator, highlighting their crucial tasks in managing and maintaining computer systems and networks within organizations. We provided an overview of operating systems, focusing on Windows, Linux, and macOS. Each system offers distinct features and capabilities, and system administrators work with these platforms to ensure smooth operations and user experiences.

Networking fundamentals for system administrators were thoroughly explained including an introduction to network models like the OSI and TCP/IP models, essential networking protocols, and various networking devices such as routers, switches, and firewalls. We also covered common troubleshooting techniques to address connectivity issues and monitor network traffic.

Lastly, we examine into the world of virtualization technologies. Virtualization allows for the creation of virtual environments such as virtual machines and containers which offer benefits like server consolidation, resource utilization and simplified disaster recovery. We mentioned popular virtualization platforms such as VMware vSphere, Microsoft Hyper-V, KVM, VirtualBox and Docker.

Overall, this discussion provided comprehensive insights into essential topics for aspiring system administrators and anyone interested in understanding the backbone of IT infrastructure, networking and virtualization technologies. By mastering these fundamental concepts system administrators can effectively manage complex IT environments and contribute to the efficiency and security of modern organizations.

KEY TERMS

Containers
OSI Model
TCP/IP Model
Networks
VMWare vSphere
RAM
ISO Image
Daemon

POSTTEST

True or False. Read the question and the corresponding provided statement and determine whether the statement is true or false.

_____ 1. Operating System Installation and Configuration is an optional process in setting up and optimizing computer systems.

_____ 2. During operating system installation, an upgrade maintains existing data and applications while updating the OS version.

_____ 3. Multi-factor Authentication (MFA) is not related to user and group management.

_____ 4. File system management involves choosing the appropriate file system for each partition created during disk partitioning.

_____ 5. Disk partitioning is not essential for data organization and improving system performance.

_____ 6. Services and daemons are foreground processes that require user interaction to function properly.

_____ 7. Monitoring and logging are not important aspects of managing system services and daemons.

_____ 8. Enabling unnecessary services and daemons enhances system security.

_____ 9. Dependency management is not a consideration when managing services and daemons.

_____ 10. In cloud environments, the management of services and daemons is related to traditional operating system practices.

REFERENCES

Textbook:

al., M. E. (2019). CSS and Networking Guide for CCNA and CSS. Unlimited Books Library Services & Publishing Inc.

Barnes, R. (2020). Understanding Operating Systems. Lanrye International.

Holcombe, J., & Holcombe, C. (2020). Survey of Operating System. McGraw Hill Education.

Jang, M., & Messier, R. (2017). Security Strategies in Linux Platforms and Applications. Jones & Bartlett.

Lee, G. (2014). Cloud Networking. Elseviers Inc.

Messier, R. (2014). Collaboration with Cloud Computing. Elsevier.

Panek, C. (2020). Windows Operating System Fundamentals. Sybex.

E-Book

Andrews, D. W. (2020). CompTIA A+ Core 2 Exam: Guide to Operating Systems and Security.

Ciampa. (2022). CompTIA Security+ Guide to Network Security Fundamentals.

West. (2021). CompTIA Cloud+ Guide to Cloud Co.