CHAPTER 1: INTRODUCTION TO SAM

SAM – It is the processes and activities involved in managing and keeping a computer system or network infrastructure running smoothly and efficiently.

SYSTEM ADMINISTRATOR, SYSADMIN – A professional responsible for managing and maintaining computer systems and networks within an organization.

TYPES OF SYSTEM ADMINISTRATORS

1. **Network Administrator** – Specializes in managing and maintaining the organization's network infrastructure, including routers, switches, and network protocols.
2. **Systems Administrator** – Responsible for the installation, configuration, and maintenance of operating systems, software applications, and hardware devices (handle day-to-day tasks).
3. **Database Administrator** – Focuses on managing and maintaining databases, including installation, configuration, performance tuning, backup and recovery, and ensuring data integrity and security.
4. **Security Administrator** – Concentrates on implementing and maintaining security measures to protect the organization's systems and data.
5. **Cloud Administrator** – Specializes in managing and maintaining cloud-based infrastructures, such as virtual machines, storages, ad networking services provided by cloud service providers.
6. **Web Administrator** – Manages and maintains web servers, web applications, and related services.

SYSTEM ADMINISTRATOR ROLES

SYSTEM ADMINISTRATION – The practice of managing, configuring, and maintaining computer systems, servers, networks, and related IT infrastructure to ensure optimal performance, security, and availability.

PURPOSE:

- To keep IT systems running smoothly and free from technical issues.
- To manage resources efficiently so that business processes are not interrupted.
- To secure data and systems against threats such as cyberattacks and unauthorized access.
- To support users by troubleshooting problems and providing technical assistance.

SIGNIFICANCE:

- Business Continuity: Ensures critical systems remain operational, minimizing downtime.
- Data Protection: Implements backups, disaster recovery, and security measures.
- Operational Efficiency: Optimizes performance, enabling faster and more reliable services.
- Adaptability: Supports the integration of new technologies and system upgrades.

SYSADMIN RESPONSIBILITIES

1. **Monitoring & Alerting** – Sysadmin is in charge of monitoring and alerting across applications and infrastructure.
2. **Administering User Permissions & Administration** – Sysadmin can assign

user roles and manage the entire organization’s IT stack, allowing everyone the access they need to certain applications and services in a secure way.

3. **Managing SS0 & Passwords** – Sysadmin is tasked with managing passwords and single-sign-on policies and practices across the company.
4. **Managing Files** – Sysadmin will place policies and procedures around the way files are organized and shared within the organization to ensure data organization and consistency.
5. **Defining System Usage Policies & Procedures** – Sysadmin will need to define best practices for working within the organization’s systems.
6. **Installing & Maintaining Software** – Sysadmin’s job is to put policies and procedures in places to keep up with the software installation and updates (should be able to detect issues and fix them).
7. **Planning for Redundancies, Rollovers, & Recoveries** – Sysadmin should have active, updated plans for redundancies, rollovers, and incident recovery.
8. **Security** – It should be the top-of-mind across everything a sysadmin works on.
9. **Managing Documentation & Runbooks** – Sysadmin is often tasked with maintaining documentation and keeping runbooks up to date.
10. **Detecting & Remediating Incidents** – Sysadmins can’t simply throw their IT and security environment together rather they need to build it with visibility and speed in mind.

SYSADMIN SKILLS & TECHNOLOGIES

1. Configuration Management and Automation
2. Cloud Infrastructure
3. Git and Other Version Control Forms
4. Server and Network Upkeep
5. Scripting and Programming

CHAPTER 2: OVERVIEW OF LINUX OS

LINUX – It is a community of open-source Unix like operating systems that are based on the Linux kernel.

LINUS TORVALDS – Linux creator

SEPTEMBER 17, 1991 – Linux was released

LINUX – It is a free and open-source operating system and the source code can be modified and distributed to anyone commercially or noncommercially under the GNU.

LINUX – It was initially created for personal computers and gradually used in other machines like servers, mainframe computers, supercomputers, etc.

ANDROID – The biggest success of Linux that is based on the Linux kernel that is running on smartphones and tablets.

EVENTS LEADING TO LINUX CREATION

1. **Unix** – An OS developed by Bell Labs in the late 1960s and early 1970s (used in science and research).
2. **Minix** – An OS developed by comsci professor Andrew S. Tanenbaum in the early 1980s (used as an educational tool).
3. **Linux** – An OS developed by a 21-year-old student Linus Torvalds in 1991.
4. **Linux 0.01** – The first version of Linux that was released in September 1991 (CLI).

5. **Linux Community Development** – Developers began to form around Linux, contributing to the development of the OS by writing code, filing bug reports, and providing feedback.
6. **Enterprise Adoption** – In the late 1990s and early 2000s, the open-source nature of Linux made it more flexible, cost-effective, and more secure than proprietary OS making it popular choice for enterprises and businesses.
7. **Linux Distribution Growth** – As Linux became more popular, various groups of developers began creating their own versions of the OS (distributions) (RedHat, Debian, Ubuntu).
8. **Linux in the Enterprise** – Linux is now widely used as an OS for servers, mainframes, supercomputers, embedded systems, mobile devices, and IoT.
9. **Linux in the Consumer Market** – Linux has also entered the consumer market with the advent of Linux-based mobile devices, smart TVS, and other consumer electronics.

LINUX DISTRIBUTIONS

LINUX DISTRIBUTION – It is an operating system that is made up of a collection of software based on Linux kernel.

600+ Linux Distributions (MX Linux, Manjaro, Linux Mint, Elementary, Ubuntu, Debian, Solus, Fedora, openSUSE, Deepin)

IMPORTANT FACTORS TO CONSIDER

1. Usage
   - Ubuntu (for new Linux user)
   - Pop_OS! (for engineers and general users)
   - Arch Linux (for complete control of their machines)
   - Fedora (for enterprises, small businesses, sysadmins)
   - Kali Linux (for ethical hackers and security professionals)
2. Hardware Requirement
   - ARM-based Processors
   - 32bit and 64bit PCs
   - Less than 1GB RAM
   - 8GB Disk Space
   - *Minimum hardware requirements to install*
3. Software Support
   - RHEL (widely used by enterprises)
   - Ubuntu (offers software support In exchange for a service fee)
   - Zorin OS (pay a fee for the Pro version of the OS)
4. Stability
   - Debian (only release s version that are tested and stable)
   - ArchLinux (constantly releasing new software updates during the course of the year)
   - *Bleeding-edge distros are perfect if you want the latest features for testing purposes.*
5. Documentation and Community
   - Installation
   - Set-up
   - General Tutorials
   - *The bigger the community, the better.*
6. Previous Experience with Linux

- Zorin OS
- LinuxMint
- elementary OS

LINUX ADVANTAGES

1. Open Source (source code is easily available)
2. Security (not completely safe but less vulnerable than others)
3. Free (free to use, easy to download, no need to buy the license)
4. Lightweight (requirements are less than other)
5. Stability (doesn't require to reboot the system to maintain performance level)
6. Performance (capable of handling a large number of users simultaneously)
7. Flexibility (can be used for desktop apps, embedded systems, server apps)
8. Software Updates (are in user control)
9. Distribution/Distros (there are various options available in the market)
10. Live CD/USB (to run the OS without installing it)
11. Graphical User Interface (CLI-Based OS but provides an interactive user interface)
12. Suitable for Programmers (supports almost all of the most use programming languages)
13. Community Support (can find various support from various sources)
14. Privacy (it never takes much private data from the user)
15. Networking (client-server systems can be easily set)
16. Compatibility (supports almost all file formats)
17. Installation (takes less time)
18. Multiple Desktop Support (can be selected during installation)
19. Multitasking (can run multiple tasks simultaneously)
20. Heavily Documented for Beginners (available on the internet)

LINUX – It is an extremely versatile, powerful, and reliable operating system.

CHAPTER 3: GETTING STARTED

LINUX – It represents a philosophy, a community, and a revolution in the world of computing.

LINUX – It can be installed using USB stick and CD-ROM.

LINUX COMMANDS – List are on index card.

NAVIGATION – It is based on the concepts of paths.

ABSOLUTE PATH – It is a complete path to a resource, beginning at the file system's root /.

RELATIVE PATH – It may vary by user locations in the filesystem.

COMMANDS TO NAVIGATE FILESYSTEM

pwd – displays the present working directory

tree – displays file system information in a similar manner to a graphical interface

cd (change directory) – moves to the specified directory

. (present working directory)

.. (parent directory)

~ (home directory)

/ (root directory)

WORKING WITH FILES IN THE TERMINAL

ls: used to list the contents of a directory

cd: used to change the current working directory

pwd: used to display the current working directory

touch: used to create a new empty file

cat: used to display the contents of a file

cp: used to copy a file

mv: used to move or rename a file

rm: used to delete a file

MANAGING DIRECTORIES

mkdir: used to create a new directory

rmdir: used to delete an empty directory

rm -r: used to delete a directory and its content

mv: used to move or rename directories

cp -r: used to copy a directory and its content

CHAPTER 4: FS MANAGEMENT

LINUX FILESYSTEM – It is like a meticulously organized library, categorizing files and directories in a structured manner.

LINUX FILESYSTEM – It ensure the logical organization and easy retrieval of system and user data.

FILESYSTEM HIERARCHY STANDARD – It is a set of rules for Unix-like operating systems, including Linux.

FHSs GOAL – To establish a consistent and logical layout, simplifying the location and data sharing across systems.

ROOT DIRECTORY – It is the main entrance to the Linux filesystem, /.

ROOT DIRECTORIES SUBDIRECTORIES

- **/bin**: essential command binaries
- **/boot**: boot-related files
- **/dev**: device files that represent devices
- **/etc**: system-wide configuration files
- **/home**: user home directory
- **/lib**: library files for command binaries
- **/root**: admin home directory
- **/root** /sbin: essential system binaries
- **/tmp**: temporary storage area for files
- **/usr**: user-related files and directories
- **/var**: temporary files

THE /USR DIRECTORY

- **/usr**: contains user-related files and directories
- **/usr/bin**: contains executable programs that are used by the users
- **/user/include**: contains C and C++ header files that are used by the system's development tools
- **/usr/lib**: contains library files that are used by the programs in the /usr/bin and /usr/sbin directories
- **/usr/sbin**: contains executables that re userd for system maintenance
- **/usr/share**: contains sharable data that is used by programs
- **/usr/src**: contains source code for the operating system and other software package

THE /VAR DIRECTORY

- **/var**: houses files and directories anticipated to undergo changes as the system runs
- **/var/cache**: holds cashed data that enhances the system's speed and efficiency

- **/var/lib**: essential data files for applications (DB, package manner repo)
- **/var/log**: archives the log files created by system and software
- **/var/run**: runtime data (PID files, sockets)
- **/var/spool**: holds data queued for subsequent processing (print jobs, mail queues)
- **/var/tmp**: provisional storage space for files utilized by software

THE /ETC DIRECTORY

- **/etc**: houses configuration files and directories that apply to the entire system
- **/etc/init.db**: contains scripts that are used to start and stop system services
- **/etc/X11**: contains configuration files for the X Window System
- **/etc/cron.d**: contains cron job configuration files
- **/etc/network**: contains network configuration files (interfaces, routing tables)
- **/etc/security**: contains security-related configuration files (PAM, SELinux Policies)

THE HOME DIRECTORY

- **/home**: the main repository of the users; personal spaces
- **Desktop**: houses the files and directories located on the user's desktop
- **Download**: houses the files downloaded by the user
- **Documents**: houses the user's personal documents and files
- **Music**: houses user's collection of music tracks
- **Pictures**: houses user's photos and related imagery
- **Videos**: houses user's video content

THE /BOOT AND /LIB DIRECTORIES

- **/boot**: essential boot-related components (Linux kernel, initramfs, bootloader's settings)
- **/lib**: library files for command binaries found in the /bin and /sbin directories
- **/boot**: lies in its storage of the system booting elements
- **Linux Kernel** – It manages system resources and hardware instructions.
- **Initramfs** – It is an early-stage root filesystem, utilized by the kernel to launch the primary root filesystem.
- **/lib**: storing library files vital for /bin ad /sbin command binaries

/USR – It contains many of the programs and libraries that are used by the system and its users.

/VAR – It contains many of the files and directories that are needed for the operation of the system and its applications.

/ETC – It contains many of the configuration files and directories needed for the operation of the system and its applications.

/BOOT AND /LIB – It safeguards the necessary files and libraries for optimal booting and system operations

FILESYSTEM BEST PRACTICES

1. Keep the filesystem organized
2. Use separate partitions for crucial directories
3. Maintain a clean filesystem
4. Regular examine and mend the filesystem

FILE SYSTEM MANAGEMENT – It is a foundational aspect of operating system functionality, ensuring data is stores, accessed, ad managed effectively and efficiently.

- Proper Organization
- Regular Maintenance
- Adherence to Best Practices

CHAPTER 5: USER AND GROUP MNGMNT

USER ADMINISTRATION – It refers to the processes, tools, and protocols used to manage user accounts on a system.

SIGNIFICANCE OF UA

1. Ensures only authorized users can access the system.
2. Grant users only the resources they need.
3. Provide audit trails for monitoring and compliance.

FUNCTIONS OF UA

1. **User Account Creation** – setting up new accounts with usernames, password, and attributes
2. **Role & Permissions Assignment** – defining what users can or cannot do
3. **Password Management** – enforcing policies, resets, and authentication
4. **Account Maintenance** – updating, modifying, or deleting accounts as roles change
5. **Auditing and Security** – tracking user activities for anomalies and security

CHALLENGES

1. **Scalability** – managing accounts in growing organizations
2. **Security** – protecting against cyberattacks through strong policies (MFA)
3. **Compliance** – ensuring adherence to laws and industry standards

INTEGRATION WITH GM

- Groups simplify administration by assigning permissions collectively.
- Makes managing users with shared responsibilities more efficient.

FUTURE OUTLOOK

- AI and machine learning will enhance User Administration with predictive analytics, role suggestions, and early threat detection.

GROUP ADMINISTRATION – It is a key component of User and Group Management, focusing on organizing users into groups for easier control and security within digital systems.

IMPORTANCE OF GA

1. **Efficiency** – permissions can be assigned once to a group instead of individually
2. **Security** – ensures only the right groups access sensitive resources

3. **Simplicity** – easier onboarding and role changes by simply adding/removing users from groups

CORE FUNCTIONS OF GA

1. **Group Creation** – build groups by role, department, or project
2. **Assigning Users** – add or remove users from groups
3. **Setting Permissions** – define what a group can access
4. **Monitoring & Auditing** – track group activities to prevent misuse
5. **Group Deletion** – remove groups that are obsolete

CHALLENGES

1. **Scalability** – more users and groups increase complexity
2. **Overlapping Permissions** – avoid conflicting or excessive access
3. **User Mobility** – changing roles may cause users to accumulate unnecessary permissions

GROUP ADMINISTRATION – It provides a structured, secure, and efficient way of managing users, ensuring consistency and easier control in any digital system.

UM AND GM BEST PRACTICES

USER AND GROUP MANAGEMENT – It is essential for maintain security, efficiency, and system integrity in IT environments.

KEY BEST PRACTICES

1. **Principle of Least Privilege (POLP)** – It grants only the minimum access users need to perform tasks.

- **Importance**: It minimizes potential damage in cases of breaches, reduces errors, and ensures that users aren't overwhelmed with unnecessary permissions.
- **Implementation**: Regularly audit user permissions, ensuring that no user has more access than they acquire.

2. **Regular Audits and Reviews** – It routinely check and update user and group permissions.

- **Importance**: Regular audits ensure that users who have changed roles or left the organization don't retain unnecessary access.
- **Implementation**: Employ automated tools that schedule and flag irregularities during audits.

3. **User Group Policies** – It manage access through groups instead of individual accounts.

- **Importance**: Streamlines the process of user management, makes mass changes more efficient, and reduces the chance of errors.
- **Implementation**: Define groups based on departments, roles, or tasks. Assign rights to groups rather than individuals.

4. **Multi-Factor Authentication** – It strengthen login security with multiple verification steps.

- **Importance**: Increases security by requiring multiple forms of verification, reducing the risk of unauthorized access.
- **Implementation**: Integrate MFA tools into login processes, especially for users with elevated privileges.

5. **Onboarding & Offboarding Procedures** – It ensures proper access setup for new users and timely revocation for departing ones.

- **Importance**: Ensures that users are setup with the right permissions from the start and that access is promptly revoked when no longer needed.
- **Implementation**: Collaborate with HR to get timely updates on joiners and leavers. Use automated tools for provisioning and de-provisioning users.

6. **User Education and Training** – It teach users about security practices and safe access protocols.

- **Importance**: Informed users are less likely to make errors, fall for phishing attacks, or misuse their privileges.
- **Implementation**: Regular training sessions, sending updates on new security protocols, and running mock drills.

7. **Role-Based Access Control (RBAC)** – It assigns access based on organizational roles for consistency.

- **Importance**: Simplifies management, ensures consistent access permissions for users with similar roles, and allows for easy modifications.
- **Implementation**: Define roles within your organization, assign required permissions to each role, and then assign users to those roles.

8. **Logging and Monitoring** – It tracks user activity to detect suspicious behavior and maintain accountability.

- **Importance**: Helps in detecting suspicious activities, aids in audits, and provides accountability.
- **Implementation**: Employ security information and event management (SIEM) tools that offer real-time monitoring and alerts.

9. **Backup and Recovery Plans** – It protects against errors and breaches with regular backups and recovery protocols.

- **Importance**: Ensure business continuity, reduces downtime, ad protects against data loss.
- **Implementation**: Regular backups of configurations, use of cloud services for redundancy, and define recover protocols.

EFFECTIVE USER AND GROUP MANAGEMENT – It is a continuous, adaptive process. By applying these best practices, organizations can:

- Strengthen Security
- Reduce Risks
- Enhance Efficiency
- Build a Scalable IT Infrastructure for the Future.

Most Popular Linux Distribution

- RedHat
- Debian
- Ubuntu

Some Popular Linux Distribution

- MX Linux
- Manjaro
- Linux Mint
- Elementary
- Ubuntu
- Debian
- Solus
- Fedora
- openSUSE
- Deepin

Some Great Linux Server Distribution

- RHEL
- UbuntuServer
- Fedora
- Debian
- CentOS
- OracleLinux

Lightweight Linux Distribution

- Tiny CoreLinux
- Xubuntu
- AlpineLinux
- Lubuntu

More Emphasis on Stability than Others

- Debian
- openSUSE
- LinuxMint
- RHEL

Bleeding-Edge Linux Distribution

- Arch Linux
- openSUSETumbleweed
- Debian

Easy for OS Transition

- Zorin OS
- LinuxMint
- elementary OS

For Beginners

- Ubuntu
- LinuxMint

For Proficient and Programmers

- Debian
- Fedora

Linux Communities

- Ubuntu
- Reddit
- StackOverflow