Career Essentials in System Administration

1) Operating Systems: Installing, updating, and maintaining OSs :-

* Servers and Clients:

=> Managing servers:

- Main server types
- Windows
- Linux
- Unix and others

=> Directory services:

- Active Directory Domain Services
- OPen LDAP
- Thivd - party products

* Active Directory:

=> stores information about objects on network and allow others to find and use.

* System center suite:

=> A comprehensive suite of management tools developed by microsoft to help IT administrators manage and monitor enterprise level IT infrastructure.

* Intune :

⇒ A cloud based service that focuses on mobile device management and mobile application management.

⇒ Used to securely manage devices and apps.

2) Servers: Managing, Configuring, Maintaining and monitoring :-

* Commercial administration monitoring tools :

- Solar winds
- Manage Engine

* Built-in Windows monitoring tools :

- Performance Monitor
- Task Manager
- Best Practices Analyzer

3) Identity and Authentication services :-

* On- premises and cloud identity services :

- Identity services → Authentication
  → Authorization

* Azure AD and directory services:

- Azure entra ID hybrid (simple signing)
- Azure entra ID native

* Multi factor Authentication :

⇒ A process in which users are prompted during sign-in process for identification.

* Group creation and management:

- Powershell
- On- premises AD

* Shared folder security:

- sharing tab – network level access
- security tab – NTFS permission

- Simple sharing - accessed via folders
  - limited controls
  - read / write / remove are the available options
- Advanced sharing - can change name
  - set user limits
  - Can modify permissions

* Security in modern era:

- Multiple defense mechanisms like MFA, firewalls, etc.
- Follow (RBAC) role-based access control.
- Minimal necessary access (least privilege)
- Use Just-in-time (JIT)
- Use DLP
- Use cameras, locks for physical security.

4) Basic Networking :-

* What runs over internet protocols
  - Transmission control protocol:
    - connection oriented
    - ensures data
    - secure and reliable

- User datagram protocol:
  - connectionless, faster
  - less reliable
  - Doesn't ensure
  - real time applications
- Internet control message protocol:
  - used for network diagnostics
  - Helps to detect if devices are reachable
- Generic routing encapsulation:
  - tunneling protocol
  - used in VPNs

* The OSI model:-
  - Has 7 layers

(1) Physical layer
- deals with physical hardware
- transmits raw bits

(2) Data link layer
- Handles MAC addresses
- transmits data as frames
- Adds header and trailer to datas.

(3) Network layer

- Deals with IP address and routing.
- Transmits data as packets
- Moves data btw diff networks

(4) Transport layer

- Manage end-to-end connection
- Uses TCP and UDP protocols

(5) Session layer

- Manages sessions or connections
- Supports duplex or simplex communi
- Manages tunnel in VPNs.

(6) Presentation layer

- Translates data into a form of readable
- Handles encryption / decryption, compression, character encoding.

(7) Application layer

- Closest to end user
- Provides network services

* IP structure:

- Also known as 4th version of IP (IPV4).
- It's a core protocol for routing.
- Uses 32-bit addressing
- Allows 4billion unique IPs
- Made up of 4 octets (32 bits)

* Routing tools:

- Ping - tests connectivity to a host
- arp - displays arp tables
- route print - displays routing table
- Powershell - alternative view of table
- tracert - traces each hop
- Path ping - combines ping + tracert

* VLANS and subnets:

- subnets - separate networks from hosts by adding or subtracting numbers from 'L' to 'R'.
- It is represented by using binary and CIDR notations.
- Improves network segmentation and security.
- Reduce broadcast traffic
- Enable ACLs to restrict comminications.

* Static and dynamic routing:

- Static routing
  - Manually configured routes to specific networks.
  - remains until deleted
- Dynamic routing
  - Automatically discovers and maintains routes
  - Uses protocols like RIP
  - uses bandwidth for updates

5) Virtualization :-

* Virtualization:

- Uses software to create virtual versions of computer hardware.
- Allows one physical computer to run multiple virtual machines.
- Hypervisors => Bare metal
  - runs directly on hardware
  - faster, stable

=> Hosted

- runs on top of OS
- slower, more prone to crash

* Windows - Hyper-V

• A virtualization platform built into windows server

• Allows to create and manage virtual machines directly on a windows server.

6) Cloud Administration:-

* cloud administration:

• It manages cloud computing services for an organization.

• Identify and migrate suitable resources to cloud

• Maintain and monitor cloud infrastructure

• Patch and updates virtual machines and systems.

* Virtualization in cloud:

• It's the creation of virtual versions of resources such as servers, storage, OS.

- It enables multiple virtual machines to run on a single physical machine using a hypervisor.

- It efficiently allocates resources
- Runs multiple customer's workloads.

* Overview of Azure portal and services:

- Contains 100 + services
- Best compatibility with windows networks and AD
- Supports both windows, linux virtual machines.

7) Security and Monitoring :-

* Email security from phishing attacks:

- Phishing attacks - Emails designed to trick victims into clicking links that lead to malware or fake sites, to steal credentials or money.

* Overview of backup solutions:-

• A backup is a server that stores copies of data, files, applications, database etc.

+ It combines hardware x software for store and restore.

* Cloud restores can take long time
* Local restores are faster and cheaper

* Different backup types for different types of organizations:

• Full Backup - copies all data
- for small business with manageable data sizes.

• Incremental backup - Back ups only files changed since last backup.
- for organizations with limited storage.

• Differential backups - Backup files changed since last full backup.
- for mid sized business balancing backup time and recovery.

- Daily backup - Backs up based on file modification date, not archive bit
  - for very small business or legacy systems.
- Copy backup - copies files regardless of archive bit, overwrites existing data
  - for one time migrations or simple scheduled backup.