Week 1

A concise guide to essential Active Directory concepts, server management, and security best practices for apprentices.

Core Concepts & Installation

Active Directory Fundamentals

Domain: A security boundary; a group of computers that share a common directory database.

Forest: A collection of one or more domains that share a common schema, configuration, and global catalog.

Tree: A hierarchical grouping of domains within a forest, linked by trusts.

Organizational Unit (OU): A container within a domain used to organize users, groups, and computers for easier administration and GPO application.

Domain Controller (DC): A server that runs Active Directory Domain Services (AD DS) and authenticates users and computers.

LDAP (Lightweight Directory Access Protocol): The protocol used to access and modify directory data.

Installing a Domain Controller

1. **Install AD DS Role:** Use Server Manager to add the Active Directory Domain Services role.
2. **Promote to Domain Controller:** Run the Active Directory Domain Services Configuration Wizard (dcpromo).
3. **Choose Deployment Option:** Create a new forest, add to an existing domain, or create a new domain in an existing forest.
4. **DNS Configuration:** Integrate DNS with Active Directory for automatic name resolution.
5. **Set Directory Services Restore Mode (DSRM) Password:** This is crucial for recovery.

Essential Server Roles

DHCP Server:	Automatically assigns IP addresses, subnet masks, default gateways, and DNS server addresses to client computers.
DNS Server:	Translates domain names to IP addresses, enabling users to access resources using friendly names.
IIS (Internet Information Services):	A web server used to host websites and web applications.

User & Group Management

User Account Management

Creating Users: Use Active Directory Users and Computers (ADUC) or PowerShell (`New-ADUser`).

Account Attributes: Set username, password, group memberships, profile path, home directory, etc.

Password Management: Enforce password complexity, age, and lockout policies via GPO.

Account Disabling/Deletion: Disable accounts for temporary leaves, delete when no longer needed.

User Authentication: Active Directory uses Kerberos for authentication.

Group Management

Security Groups: Used to assign permissions to resources (files, folders, printers, etc.).

Distribution Groups: Used for email distribution lists.

Group Scope: *Domain Local*, *Global*, and *Universal*. Understand the differences for effective group strategy.

Adding Users to Groups: Use ADUC or PowerShell (`Add-ADGroupMember`).

Best Practice: AGDLP (Accounts-Global-Domain Local-Permissions) for permission assignment.

GPO Essentials

GPO (Group Policy Object):	A set of rules that control the working environment of user and computer accounts.
Linking GPOs:	Apply GPOs to domains, OUs, or sites. Inheritance is a key concept.
GPO Processing Order:	Local, Site, Domain, OU (LSDOU). Last applied wins.
GPUpdate:	Force a GPO refresh on a client (`gpupdate /force`).

Security & Hardening

Securing Active Directory

Principle of Least Privilege: Assign users only the permissions they need to perform their job.

Tiered Administration: Separate administrative accounts based on the level of access required (Tier 0, Tier 1, Tier 2).

Account Auditing: Regularly audit user accounts, group memberships, and permissions.

Password Policies: Enforce strong password complexity, length, and expiration rules.

Multi-Factor Authentication (MFA): Implement MFA for privileged accounts.

Server Hardening

Remove Unnecessary Roles and Features: Reduce the attack surface.

Firewall Configuration: Configure the Windows Firewall to allow only necessary traffic.

Patch Management: Regularly apply security updates and patches.

Antivirus/Antimalware: Install and maintain antivirus/antimalware software.

Disable Unnecessary Services: Stop and disable services that are not required.

Secure Remote Access: Use VPNs or other secure methods for remote administration.

ADFS (Active Directory Federation Services)

Purpose:	Enables single sign-on (SSO) for web applications across organizational boundaries.
Components:	Federation servers, web application proxies, and AD FS proxies.
Use Cases:	Allowing users to access cloud applications using their Active Directory credentials.

Networking & Automation

TCP/IP Fundamentals

IP Address: A unique numerical identifier for a device on a network.
Subnet Mask: Defines the network portion of an IP address.
Default Gateway: The IP address of the router that allows a device to communicate with networks outside its own.
DNS Server: Translates domain names to IP addresses.
Common Ports: 80 (HTTP), 443 (HTTPS), 25 (SMTP), 53 (DNS), 389 (LDAP), 636 (LDAPS).

Trust Relationships

Trust: A logical link between two Active Directory domains that allows users in one domain to access resources in another domain.
Types: *One-way*, *Two-way*, *Transitive*, *Non-transitive*.
Authentication Flow: Users authenticate in their home domain, and the trust allows access to resources in the trusting domain.

Automation with PowerShell

Get-ADUser:	Retrieve user account information (`Get-ADUser -Identity 'username'`).
New-ADUser:	Create new user accounts (`New-ADUser -Name 'FullName' -SamAccountName 'username'`).
Set-ADUser:	Modify user account attributes (`Set-ADUser -Identity 'username' -Description 'New Description'`).
Get-ADGroupMember:	List members of a group (`Get-ADGroupMember -Identity 'GroupName'`).