**Module: 14 Identity with Windows Server**

**Active directory domain services**

1. **what is domain controller?**

* A domain controller is a server that responds to security authentication requests within a computer network domain. It is a network server that is responsible for allowing host access to domain resources. It authenticates users, stores user account information and enforces security policy for a domain.

1. **describe forest, domain, tree, schema, OU, container, site, subnet,**

* **Forest**:
  + A **forest** is a collection of one or more **Active Directory domains** that share a common logical structure, directory schema, configuration, and global catalog.
  + It represents the highest level of organization within AD.
  + Forests allow multiple domains to be managed together.
  + Each forest has a unique **forest-wide schema** and **configuration partition**.
  + Example: If an organization has two separate domains (e.g., example.com and subsidiary.example.com), they can be part of the same forest.
* **Domain**:
  + A **domain** is a logical grouping of network objects (such as computers, users, and resources) within AD.
  + Domains have their own security policies, user accounts, and group policies.
  + Each domain has a unique **domain-wide schema** and **configuration partition**.
  + Example: The domain “example.com” could include all resources and users within that organization.
* **Tree**:
  + A **tree** is a grouping of one or more domains within a contiguous namespace.
  + Domains in a tree share a common naming structure.
  + Example: If “sales.example.com” and “hr.example.com” are part of the same tree, they share the “example.com” namespace.
* **Schema**:
  + The **schema** defines the structure of objects within AD.
  + It specifies the classes of objects (e.g., users, groups, computers) and their attributes (e.g., name, email, phone number).
  + The schema is replicated across all domain controllers in the forest.
* **Organizational Unit (OU)**:
  + An **OU** is a container within a domain used to organize and manage objects.
  + OUs allow delegation of administrative tasks.
  + Example: An OU named “Sales” could contain user accounts, computers, and other resources related to the sales department.
* **Container**:
  + A **container** is similar to an OU but is not an object class in itself.
  + Containers are used to organize objects within AD.
  + Example: The “Computers” container holds computer objects.
* **Site**:
  + A **site** represents a physical location within the network.
  + Sites help optimize replication and communication between domain controllers.
  + Example: If an organization has offices in New York and London, they can create separate sites for each location.
* **Subnet**:
  + A **subnet** defines a range of IP addresses within a network.
  + Subnets are associated with sites to optimize traffic flow.
  + Example: A subnet with IP addresses 192.168.1.0/24 could be associated with the New York site.

1. **partition, trust relationship**

* Partitioning a trust fund refers to splitting the fund between the income and capital beneficiaries. This will terminate the trust. This guidance note looks at how and when a trust can be partitioned and the tax effects of this. Partitioning a trust should be done by deed.

1. **what is active directory?**

* Active Directory (AD) is Microsoft's proprietary directory service. It runs on Windows Server and enables administrators to manage permissions and access to network resources

1. **what is global catalog server?**

* The global catalog is a feature of Active Directory (AD) that allows a domain controller (DC) to provide information on any object in the forest, regardless of whether the object is a member of its domain. Domain controllers with the global catalog feature enabled are referred to as global catalog servers.

1. **what is ADC AND RODC?**

* Active Directory (AD) is Microsoft's directory service that authenticates and authorizes all users and computers in a Windows domain network, assigning and enforcing security policies for all computers and installing or updating software. An RODC is a type of domain controller in Windows Server that holds a read-only copy of the Active Directory database. Unlike a traditional DC, an RODC does not store any user passwords locally.

1. **what is operation master role?**

* Operation Master Roles, also known as Flexible Single Master Operations (FSMO) roles, are specific responsibilities within an Active Directory (AD) domain. These roles are essential for the proper functioning of the AD environment

1. **type of operation master role and describe all role.**

* At the forest level, there is the Schema Master and Domain Naming Master. At the domain level, the 3 other operational roles are Infrastructure Master, PDC Emulator and RID Master. The Schema Master determines the structure and thus what can be stored in Active Directory.

1. **difference between transferring and seizing role**

* Transferring makes the old DC know that it does not own the role(s) any more. If the DC is broken (e. g. hardware defect) and will never come back again, then you can seize the role on a remaining DC

1. **password policy**

* A password policy is a set of rules and requirements that dictate how passwords are created, used, and managed within an organization's IT environment. These policies are crucial for enhancing security and mitigating the risk of unauthorized access. Here's a brief overview of components typically included in a password policy:

1. **what id profile and type of profile?**

* In the context of user accounts and permissions management, a profile typically refers to a set of personalized settings, preferences, and configurations associated with a user account. These profiles are used to customize the user experience and ensure consistency across different sessions or devices.

1. **group nesting and scope, type of group**

* Nested groups inherit the permissions and privileges of the group they are put under, and hence this makes privilege administration easier. However, not all groups can be nested within other groups, and this depends on the types of groups in AD, and their scope of nesting.

**Practical**

1. **install ADDS and create a new forest**

* YES

1. **give membership of pc to domain**

* YES

1. **create a ADC**

* YES

1. **create RODC and password replication**

* YES

1. **create a new site**

* **YES**

1. **create a new child domain**

* YES

1. **create a new tree**

* **YES**

1. **create a new user with GUI and CLI**

* YES

1. **create roaming profile**

* YES

**10. create OU and give delegation**

* YES

**11. create a group**

* YES

1. **transfer roles—PDC, RID , schema master ,**

* YES

1. **Doamin name master—**

* YES

1. **GUI and ntdsutil**

* YES

1. **IFM**

* YES

**Advance feature**

1. **describe account policy**

* The account policy must be defined in the default domain policy or in a new policy that is linked to the root of the domain and given precedence over the default domain policy, which is enforced by the domain controllers in the domain.

1. **describe account lockout policy**

* An account lockout policy is a security feature implemented by organizations to protect against unauthorized access to user accounts. It helps mitigate the risk of brute-force attacks and unauthorized access attempts by enforcing restrictions on login attempts

1. **what is trust relationship**

* In the context of computer networks and systems, a trust relationship refers to the establishment of mutual authentication and authorization between two domains or systems. This relationship allows users in one domain to access resources in another domain, typically in a secure and controlled manner.

1. **type of trust relationship describe all trust**

* In the context of Active Directory and network environments, there are several types of trust relationships that facilitate communication and resource sharing between domains or forests.

1. **what is site and subnet ?**

* A site is made up of one or more internet protocol subnets that are linked by high – speed and reliable connections

**Practical**

1. **manage active directory offline**

* **YES**

1. **restore object of active directory from AD Recycle bin**

* YES

1. **backup active directory**

* YES

1. **manage active directory replication---repadmin DcDiag**

* YES

1. **create multiplae UPN suffix multidomain enviourment**

* YES

1. **configure trust between forest check with login**

* YES

1. **configure ADDS sites and subnet**

* YES

**Group Policy**

1. **what is group policy?**

* Group Policy is a feature in Microsoft Windows operating systems that allows administrators to centrally manage and configure the settings of user accounts and computer systems in an Active Directory environment. It provides a powerful tool for enforcing security policies, implementing administrative controls, and customizing the user experience across a network of Windows-based computers.

1. **what is default policy? Default Domain and domain controller**

* In the context of Microsoft Active Directory, the "Default Domain Policy" and "Default Domain Controllers Policy" are predefined Group Policy Objects (GPOs) that are automatically created when a new Active Directory domain is established.

1. **what is user configuration and computer configuration**

* User Configuration" and "Computer Configuration" are two distinct sections where administrators can define and apply settings that affect users and computers, respectively. These configurations help administrators manage the behavior and settings of user accounts and computer systems within an Active Directory environment.

1. **what is GPO?**

* GPO stands for Group Policy Object. In the context of Microsoft Windows operating systems and Active Directory environments, a Group Policy Object (GPO) is a collection of settings and configurations that define how a computer system or user account behaves within an organization's network. GPOs are a key component of Group Policy, which allows administrators to centrally manage and enforce policies across multiple computers and users.

1. **define software setting, windows setting, and administrative templates**

* In the context of Group Policy in Microsoft Windows environments, "Software Settings," "Windows Settings," and "Administrative Templates" are three distinct categories of settings and configurations that administrators can define and apply using Group Policy Objects (GPOs).

1. **link GPO**

* Linking a Group Policy Object (GPO) involves associating the GPO with Active Directory containers such as domains, organizational units (OUs), or sites. This linking process determines which users, groups, or computer objects within the specified Active Directory container(s) will receive and apply the settings configured in the GPO.

1. **delegation GPO management**

* Delegating Group Policy Object (GPO) management allows administrators to assign specific permissions to other users or groups, enabling them to create, edit, link, and manage GPOs within a domain or organizational unit (OU). Delegation of GPO management is useful for distributing administrative tasks and responsibilities, ensuring efficient management of Group Policy settings across an organization

1. **inheritance policy**

* Inheritance in the context of Group Policy refers to the hierarchical propagation of policy settings from higher-level Active Directory containers (such as domains or organizational units) down to lower-level containers, such as child OUs or individual objects (users or computers). Group Policy settings are inherited by default, meaning that settings applied at higher levels in the Active Directory hierarchy will be passed down to child objects unless explicitly blocked or overridden.

1. **filtering**

* In the context of Group Policy in Microsoft Windows environments, "filtering" refers to the process of selectively applying Group Policy settings to specific users, groups, or computers within the scope of a Group Policy Object (GPO). By default, Group Policy settings apply to all users and computers within the scope of the GPO. However, filtering allows administrators to target specific subsets of users, groups, or computers, providing greater flexibility and control over policy application.

1. **script, templates**

* Both scripts and templates are widely used in IT and software development, but they serve different purposes and are used in different contexts:

**Practical**

1. **backup restore import and copy GPO**

* YES

1. **force group policy command**

* YES

1. **check group policy settings**

* YES

1. **configure folder redirection**

* YES

1. **software installation ---assign and publish**

* YES

1. **drive map through policy**

* YES

**Certification services**

1. **purpose of certification**

* A professional certification is a credential that verifies someone's knowledge, skills and abilities to perform a specific job. Certifications are typically awarded by a professional association after a candidate completes an assessment of some kind.

1. **certificate service and its role service –certificate authority, certificate enrolment policy web service**

* Certificate services, often referred to as Certificate Authorities (CAs), are an integral part of public key infrastructure (PKI) systems. They are responsible for issuing, managing, and revoking digital certificates used to authenticate users, devices, and services in secure communications.

1. **standalone v/s enterprise CA**

* Standalone and Enterprise Certification Authorities (CAs) are two deployment options for implementing Certificate Services in Microsoft's Active Directory Certificate Services (AD CS).

1. **root CA and subordinate CA**

* A Root Certification Authority (CA) and a Subordinate Certification Authority (CA) are two types of Certification Authorities within a Public Key Infrastructure (PKI) hierarchy.

1. **describe certificate templates and how to use it**

* Certificate templates are predefined configurations or templates that specify the characteristics and properties of digital certificates issued by a Certification Authority (CA) within a Public Key Infrastructure (PKI). These templates define the key usage, cryptographic algorithms, validity periods, and other attributes of the certificates issued by the CA

**Practical**

1. **install certiface services ---certifacte authority and web enrolment**

* YES

1. **issue certificate through web enrolment and make secure web site**

* YES

1. **self-signed certificate**

* YES

1. **mange certificate---using template and issue certificate for computer**

* YES

1. **backup CA**

* YES

**ADFS**

1. **what is federation services**

* Active Directory Federation Services (AD FS) is a Windows Server feature that provides Federated Identity and Access Management. It allows secure sharing of digital identity and entitlement rights across different security and enterprise boundaries. AD FS facilitates single sign-on (SSO) to give users access to multiple systems after just one login, extending this convenience to internet-facing applications. [This helps streamline the user experience for customers, partners, and suppliers when accessing an organization’s web-based applications](https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/understanding-key-ad-fs-concepts)

1. **ADFS service component**

* **Active Directory Federation Services (ADFS)** is a **Single Sign-On (SSO)** solution created by Microsoft. [As a component of Windows Server operating systems, it provides users with authenticated access to applications that are not capable of using **Integrated Windows Authentication (IWA)** through Active Directory (AD)](https://www.okta.com/uk/blog/2018/06/what-is-adfs/)

1. **ADFS requirement**

* When deploying **Active Directory Federation Services (ADFS)**, there are several requirements you need to consider

1. **multifactor authentication**

* Multifactor authentication is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login.

1. **web application proxy**

* **Web Application Proxy** is a role service of the **Remote Access** role in Windows Server.
* Its primary purpose is to enable **secure access** for end users outside a specified network to their published web applications.

**Practical**

**1. Install ADFS service and configure between two trusted organizations (relay party trust)**

* YES

**2. multifactor authentication**

* YES

**ADRMS**

1. **what is ADRMS**

* Active Directory Rights Management Services (AD RMS), previously known as Rights Management Services (RMS) before Windows Server 2008, is a server software for information rights management that comes with Windows Server. It’s designed to help protect digital information from unauthorized use, both inside and outside of your organization.

**2. how to secure data and type of security 3 what is service account**

.Securing data involves a variety of strategies and practices to protect information from unauthorized access, corruption, or theft. Here are some key methods to secure data:

* [**Back up regularly**: Ensure you have multiple copies of your data in case one version is lost or corrupted1](https://www.techrepublic.com/article/how-to-protect-and-secure-data/).
* [**Update software**: Keep all systems and applications updated to protect against known vulnerabilities1](https://www.techrepublic.com/article/how-to-protect-and-secure-data/).
* [**Use strong passwords**: Implement a strict password policy to prevent unauthorized access1](https://www.techrepublic.com/article/how-to-protect-and-secure-data/).
* [**Employ a VPN**: Use a Virtual Private Network to encrypt data transmission, especially when using public networks1](https://www.techrepublic.com/article/how-to-protect-and-secure-data/).
* [**Install antivirus software**: Protect your systems from malware and other threats](https://www.techrepublic.com/article/how-to-protect-and-secure-data/)

**Practical**

1. **install ADRMS and secure data (different security apply)**

* YES