Active Directory Basics

▼ What is Active Directory?

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is used for managing and organizing resources, such as computers, users, and services within a network.

- **Core Function:** AD allows administrators to manage permissions and access to network resources.

▼ Key Components of Active Directory:

- Domains: A domain is a collection of objects (users, computers, etc.) that share the same AD database. It acts as a boundary for security policies and administrative tasks.
- Organizational Units (OUs): OUs are containers within a domain that organize users, groups, computers, and other OUs. They help to structure the AD environment and apply policies at different levels.
- Domain Controllers (DCs): These are servers that store the AD database and handle authentication requests from users and computers within the domain.
- Forest: A forest is a collection of one or more AD domains that share a common schema and configuration. The first domain created in a forest is called the "forest root domain."
- Trees: A tree is a collection of one or more domains in a contiguous namespace, which is part of a single forest.
- Global Catalog: This is a distributed data repository that contains information about every object in the AD forest. It speeds up search and login processes.

3. User and Group Management:

- Users: In AD, user accounts represent people or services that need to access network resources. These accounts are used for authentication and authorization.

- Groups: Groups are collections of user accounts, and they can be used to simplify permission management. Common types are:
- Security Groups: Used to assign permissions to resources.
- Distribution Groups: Used for email distribution lists.

4. Group Policy:

- Group Policy Objects (GPOs): These are collections of settings that control the working environment of user accounts and computer accounts. GPOs can be applied to OUs, domains, or entire forests.
- Examples of GPOs: Password policies, software installation, security settings, and user environment configurations.

5. Authentication and Authorization:

- Kerberos: The primary authentication protocol used by AD. It provides secure authentication over non-secure networks.
- LDAP (Lightweight Directory Access Protocol): Used to access and manage directory information within AD.

6. AD Schema:

- The schema is a blueprint that defines the structure of the AD database, including the types of objects (e.g., users, computers) and the attributes they can have.

7. Common Administrative Tasks:

- Creating Users and Groups: Adding new users and placing them in appropriate groups for access control.
- Managing OUs: Organizing users and computers into OUs for easier management.
- Applying GPOs: Configuring and applying GPOs to enforce policies across the network.
- Monitoring and Troubleshooting: Regularly checking logs, monitoring performance, and troubleshooting issues.

8. AD Tools:

- Active Directory Users and Computers (ADUC): A common tool for managing users, groups, and computers.
- Active Directory Administrative Center (ADAC): An advanced tool for managing AD that provides a more modern interface.
- PowerShell: Used for automating AD tasks with scripts.

▼ Active Directory

The core of any Windows Domain is the **Active Directory Domain Service (AD DS)**s.

> ### *Users*

Users are one of the most common object types in Active Directory. Users are one of the objects known as **security principals**, meaning that they can be authenticated by the domain and can be assigned privileges over **resources** like files or printers. You could say that a security principal is an object that can act upon resources in the network.

Users can be used to represent two types of entities:

- **People:** users will generally represent persons in your organisation that need to access the network, like employees.
- **Services:** you can also define users to be used by services like IIS or MSSQL. Every single service requires a user to run, but service users are different from regular users as they will only have the privileges needed to run their specific service.

> ### *Machines*

For every computer that joins the Active Directory domain, a machine object will be created. Machines are also considered "security principals" and are assigned an account just as any regular user.

The machine accounts themselves are local administrators on the assigned computer, they are generally not supposed to be accessed by anyone except the computer itself, but as with any other account, if you have the password, you can use it to log in.

> **Note:** Machine Account passwords are automatically rotated out and are generally comprised of 120 random characters.

The machine account name is the computer's name followed by a dollar sign. For example, a machine named `DC01` will have a machine account called `DC01$`.

Security Groups

If you are familiar with Windows, you probably know that you can define user groups to assign access rights to files or other resources to entire groups instead of single users. This allows for better manageability as you can add users to an existing group, and they will automatically inherit all of the group's privileges. Security groups are also considered security principals and, therefore, can have privileges over resources on the network.

Groups can have both users and machines as members. If needed, groups can include other groups as well.

Several groups are created by default in a domain that can be used to grant specific privileges to users.

Security Group	Description
Domain Admins	Users of this group have administrative privileges over the entire domain. By default, they can administer any computer on the domain, including the DCs.
Server Operators	Users in this group can administer Domain Controllers. They cannot change any administrative group memberships.
Backup Operators	Users in this group are allowed to access any file, ignoring their permissions. They are used to perform backups of data on computers.
Account Operators	Users in this group can create or modify other accounts in the domain.
Domain Users	Includes all existing user accounts in the domain.
Domain Computers	Includes all existing computers in the domain.
Domain Controllers	Includes all existing DCs on the domain.

You can obtain the complete list of default security groups from the Microsoft documentation.

Organizational Units (OUs)

Which are container objects that allow you to classify users and machines. OUs are mainly used to define sets of users with similar policing requirements.

These containers are created by Windows automatically and contain the following:

- **Builtin:** Contains default groups available to any Windows host.
- **Computers:** Any machine joining the network will be put here by default. You can move them if needed.
- **Domain Controllers:** Default OU that contains the DCs in your network.
- **Users:** Default users and groups that apply to a domain-wide context.
- **Managed Service Accounts:** Holds accounts used by services in your Windows domain.

Security Groups vs OUs

You are probably wondering why we have both groups and OUs. While both are used to classify users and computers, their purposes are entirely different:

- **OUs** are handy for **applying policies** to users and computers, which include specific configurations that pertain to sets of users depending on their particular role in the enterprise. Remember, a user can only be a member of a single OU at a time, as it wouldn't make sense to try to apply two different sets of policies to a single user.
- **Security Groups**, on the other hand, are used to **grant permissions over resources**. For example, you will use groups if you want to allow some users to access a shared folder or network printer. A user can be a part of many groups, which is needed to grant access to multiple resources.

Managing Users in AD

- **Delegation**

  One of the nice things you can do in AD is to give specific users some control over some OUs. This process is known as **delegation** and allows you to grant users specific privileges to perform advanced tasks on OUs without needing a Domain Administrator to step in.

- **Reset Any User Password:**

```
PS C:\Users\phillip> Set-ADAccountPassword sophie -Reset
New Password: ************
VERBOSE: Performing the operation "Set-ADAccountPassword
"CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
```

- **To Force User To Reset Password On Next Logon:**

  ```
  PS C:\Users\phillip> Set-ADUser -ChangePasswordAtLogon $
  VERBOSE: Performing the operation "Set" on target "CN=Sc
  PS C:\Users\phillip>
  ```

▼ Managing Computers in AD

> By default, all the machines that join a domain (except for the DCs) will be put in the container called "Computers".

In general, you'd expect to see devices divided into at least the three following categories:

1. Workstations

Workstations are one of the most common devices within an Active Directory domain. Each user in the domain will likely be logging into a workstation. This is the device they will use to do their work or normal browsing activities. These devices should never have a privileged user signed into them.

2. Servers

Servers are the second most common device within an Active Directory domain. Servers are generally used to provide services to users or other servers.

3. Domain Controllers

Domain Controllers are the third most common device within an Active Directory domain. Domain Controllers allow you to manage the Active Directory Domain. These devices are often deemed the most sensitive devices within the network as they contain hashed passwords for all user accounts within the environment.

▼ Group Policies

Group Policy Objects (GPO) are a feature of Microsoft Windows that allows administrators to manage the configuration and settings of users and computers in an Active Directory (AD) environment. GPOs are used to enforce specific policies, settings, and security rules across an organization.

▼ Key Concepts of GPO:

1. **Group Policy**: A system that controls the working environment of user accounts and computer accounts in an Active Directory. Group Policies can configure settings such as password policies, software installation, desktop settings, and more.
2. **Objects (GPOs)**: These are the containers where group policies are defined. Each GPO can contain multiple settings, which can apply to users or computers.
3. **Scope of GPOs**:
   - **Domain**: GPOs can be applied to an entire domain, affecting all users and computers within that domain.
   - **Organizational Units (OUs)**: GPOs can be targeted to specific OUs within a domain, allowing for more granular control.
   - **Site**: GPOs can be applied to specific AD sites, which are collections of well-connected IP subnets.
4. **Types of Settings in GPOs**:
   - **Computer Configuration**: These settings apply to computers, regardless of who logs on to them. They include security settings, startup scripts, software installation, etc.
   - **User Configuration**: These settings apply to user accounts, regardless of which computer they log on to. They include settings like login scripts, folder redirection, and software policies.
5. **Inheritance and Precedence**: GPOs are processed in a specific order, and policies can be inherited from parent containers (e.g., from a domain down to an OU). However, GPOs linked directly to an OU have higher precedence over those linked to the parent domain.
6. **Local Group Policy**: A GPO that applies to a single computer. It is useful for settings that need to be enforced on standalone machines not connected to a domain.

Benefits of Using GPOs:

- **Centralized Management**: Administrators can manage multiple users and computers from a central location.
- **Security Enforcement**: GPOs can enforce security settings across an organization, such as password complexity requirements and software restrictions.

- **Automation**: Tasks like software installation, updates, and scripts can be automated through GPOs, reducing manual effort.

▼ GPO Distribution

GPOs are distributed to the network via a network share called `SYSVOL`, which is stored in the DC. All users in a domain should typically have access to this share over the network to sync their GPOs periodically. The SYSVOL share points by default to the `C:\Windows\SYSVOL\sysvol\` directory on each of the DCs in our network.

Once a change has been made to any GPOs, it might take up to 2 hours for computers to catch up. If you want to force any particular computer to sync its GPOs immediately, you can always run the following command on the desired computer:

```
PS C:\> gpupdate /force
```

▼ Authentication Methods

When using Windows domains, all credentials are stored in the **Domain Controllers**. Whenever a user tries to authenticate to a service using domain credentials, the service will need to ask the Domain Controller to verify if they are correct. Two protocols can be used for network authentication in windows domains:

1. **Kerberos:** Used by any recent version of Windows. This is the default protocol in any recent domain.
2. **NetNTLM:** Legacy authentication protocol kept for compatibility purposes.

▼ 1. Kerberos Authentication

Kerberos is a secure, robust, and efficient authentication protocol used in Active Directory environments. It was designed to provide strong authentication for client-server applications by using secret-key cryptography. Here’s a detailed explanation of how Kerberos works:

Key Components:

- **Key Distribution Center (KDC):** The core of Kerberos, consisting of two services:
    - **Authentication Service (AS):** Verifies users and issues Ticket Granting Tickets (TGTs).
    - **Ticket Granting Service (TGS):** Issues service tickets for accessing specific services.

- **Ticket Granting Ticket (TGT):** A ticket used to request service tickets from the TGS.
- **Service Ticket:** A ticket that allows access to a particular service on the network.
- **Client and Server:** The user or device requesting access (client) and the resource or service being accessed (server).

Steps in Kerberos Authentication:

1. **Initial Login and TGT Request:**
   - The user logs in by entering their credentials (username and password).
   - The client encrypts the credentials with a key derived from the user's password and sends them to the KDC’s Authentication Service (AS).
   - The AS verifies the credentials and, if valid, generates a TGT, which includes the user’s ID and is encrypted with the KDC’s secret key.
   - The TGT is sent back to the client along with a session key (encrypted with the user’s password-derived key).
2. **Service Ticket Request:**
   - When the user tries to access a specific service (e.g., file server), the client sends the TGT to the KDC’s Ticket Granting Service (TGS).
   - The TGS decrypts the TGT using its secret key, verifies the user’s identity, and generates a service ticket.
   - The service ticket, along with a session key (specific to the service), is sent back to the client.
3. **Service Access:**
   - The client presents the service ticket to the server hosting the requested resource.
   - The server decrypts the service ticket using its secret key and verifies the client’s identity.
   - If the ticket is valid, the server grants access to the resource.
4. **Mutual Authentication (Optional):**
   - Kerberos can also provide mutual authentication, where the server proves its identity to the client using the service ticket.

Security Features of Kerberos:

- **Mutual Authentication:** Both the client and server can authenticate each other.
- **Replay Protection:** Kerberos tickets have timestamps and limited validity, preventing replay attacks.
- **No Password Transmission:** Passwords are not transmitted over the network; instead, encrypted tickets are used.

▼ 2. NTLM Authentication

NTLM (NT LAN Manager) is an older authentication protocol primarily used for compatibility with systems and applications that do not support Kerberos. NTLM uses a challenge-response mechanism for authenticating users.

Key Components:

- **Client:** The user or device requesting access.
- **Server:** The resource or service being accessed.
- **Domain Controller (DC):** Holds the user's credentials and is responsible for verifying them (in a domain environment).

Steps in NTLM Authentication:

1. **Initial Request:**
    - The client sends a request to the server to access a resource.
2. **Server Challenge:**
    - The server responds with a challenge, which is a random number (nonce).
3. **Challenge-Response:**
    - The client computes a response by encrypting the challenge with the user's password hash.
    - The encrypted response is sent back to the server.
4. **Server Verification:**
    - In a standalone environment:
        - The server compares the received response with its own computed response using the stored password hash.
    - In a domain environment:

    - The server forwards the challenge and response to the domain controller (DC).
    - The DC verifies the response using the stored password hash and sends the result back to the server.

5. **Access Granted/Denied:**
    - If the response is correct, the server grants access to the resource.
    - If the response is incorrect, access is denied.

Security Issues with NTLM:

- **Pass-the-Hash Attack:** Since NTLM relies on password hashes, if an attacker captures the hash, they can use it to authenticate without knowing the actual password.
- **Relay Attack:** Attackers can capture the NTLM challenge-response and relay it to authenticate with other services.
- **Lack of Mutual Authentication:** NTLM does not provide mutual authentication, meaning the client cannot verify the server’s identity.

▼ Trees, Forests and Trusts

In Active Directory (AD), the concepts of Trees, Forests, and Trusts are fundamental to understanding how the directory service organizes and manages multiple domains and their relationships. These concepts help in designing scalable, secure, and manageable AD environments, especially in large organizations. Let's break them down:

▼ 1. Active Directory Trees

An Active Directory **Tree** is a collection of one or more domains that are logically grouped together. Domains within a tree share a common namespace, meaning that they have a hierarchical relationship.

Key Characteristics:

- **Common Root Domain**: The first domain created in a tree is the root domain, and it forms the base of the namespace. For example, if the root domain is `example.com`, a child domain might be `sales.example.com`.
- **Domain Hierarchy**: Additional domains added to the tree are child domains, which are subdomains of the root or other domains within the tree.

- **Namespace Continuity**: All domains in a tree share a contiguous namespace, meaning they are part of the same DNS hierarchy.

Example:

If `example.com` is the root domain:

- A child domain might be `sales.example.com`.
- Another child domain could be `marketing.example.com`.

These domains form a tree with a single, shared DNS namespace (`example.com`).

▼ 2. Active Directory Forests

An Active Directory **Forest** is the topmost logical container in an AD environment. It consists of one or more trees that do not necessarily share a common namespace. Forests represent the boundary of security, trust, and administration in Active Directory.

Key Characteristics:

- **Multiple Trees**: A forest can contain multiple trees, each with its own unique namespace. For example, one tree might be `example.com`, and another tree in the same forest might be `contoso.com`.
- **Common Schema**: All trees in a forest share a common schema, which defines the classes and attributes within the AD database.
- **Global Catalog**: The forest contains a Global Catalog, a partial replica of all objects in the forest, which allows for searching across domains.
- **Single Configuration Partition**: All trees in the forest share a single configuration partition, which contains information about the forest-wide structure.
- **Security Boundary**: Forests are security boundaries. Administrative permissions do not cross forest boundaries unless explicitly defined by trust relationships.

Example:

A forest could contain:

- A tree with the root domain `example.com`.
- Another tree with the root domain `contoso.com`.

- Both trees are part of the same forest but have distinct namespaces (`example.com` and `contoso.com`).

▼ 3. Active Directory Trusts

Trusts are relationships established between domains and forests that allow users in one domain or forest to access resources in another. Trusts enable communication and resource sharing across domains and forests, even if they do not share a common namespace.

Types of Trusts:

1. **Within a Forest:**
    - **Parent-Child Trust**: Automatically created when a new child domain is added. It is a two-way transitive trust, meaning that if Domain A trusts Domain B, and Domain B trusts Domain C, then Domain A automatically trusts Domain C.
    - **Tree-Root Trust**: Automatically created between the root domains of two trees within the same forest. It is also a two-way transitive trust.
2. **Between Forests:**
    - **External Trust**: A one-way or two-way non-transitive trust between domains in different forests. It allows access to resources but does not extend beyond the trusted domains.
    - **Forest Trust**: A transitive trust between two forests, allowing users in one forest to access resources in another. It is more comprehensive than an external trust and can cover multiple domains within the forests.
    - **Shortcut Trust**: A manually created trust between two domains in the same forest or different forests to speed up access. It is often used when there is frequent communication between two domains in a complex hierarchy.
3. **Special Trusts:**
    - **Realm Trust**: Used to integrate AD with non-Windows Kerberos realms, such as UNIX or Linux environments.
    - **Cross-Link Trust**: Similar to a shortcut trust but used specifically to create a trust between child domains in different trees within the same forest.

Trust Properties:

- **Transitive Trust**: Automatically extends the trust relationship to other domains or forests in a chain. For example, if Domain A trusts Domain B, and Domain B trusts Domain C, then Domain A trusts Domain C.
- **Non-Transitive Trust**: Limited to the specific domains or forests that the trust is directly established between.

> Author : @Sneckey0Day