Active Directory Basics

- a **Windows domain** is a group of users and computers under the administration of a given business.
- The main idea behind a domain is to centralise the administration of common components of a Windows computer network in a single repository called **Active Directory (AD)**.
- The core of any Windows Domain is the **Active Directory Domain Service (AD DS)**.
- The server that runs the Active Directory services is known as a **Domain Controller (DC)**.

The main advantages of having a configured Windows domain are:

- **Centralised identity management:** All users across the network can be configured from Active Directory with minimum effort.
- **Managing security policies:** You can configure security policies directly from Active Directory and apply them to users and computers across the network as needed.

Active Directory Domain Service (AD DS).

This service acts as a catalogue that holds the information of all of the "**objects**" that exist on your network such as **users, groups, machines, printers, shares and many others.**

Users (security principals)

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. This account has somewhat limited rights within the domain itself.
- 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.
- Identifying machine accounts is relatively easy. They follow a specific naming scheme. 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

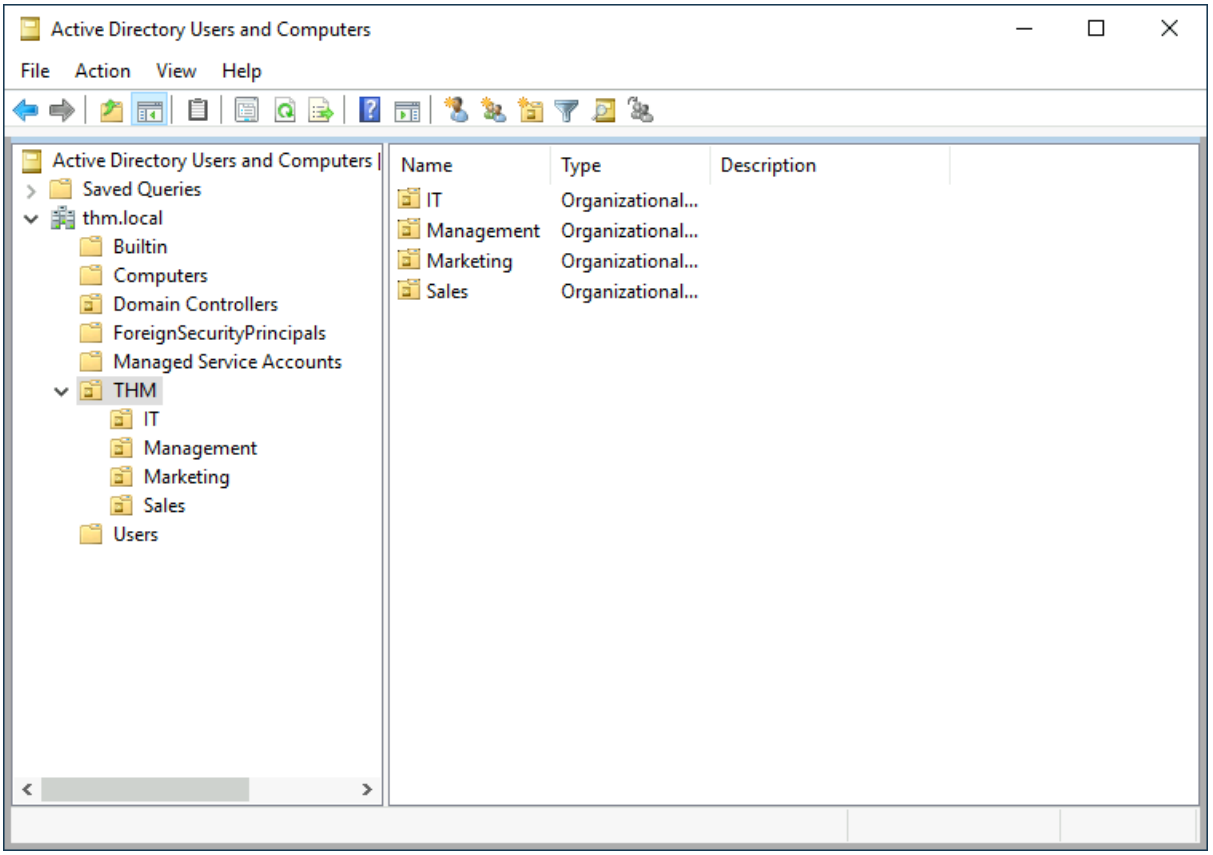
- you can define user groups to **assign access rights to files or other resources to entire groups instead of single users.**
- Security groups are also considered security principals and, therefore, can have privileges over resources on the network.
- **Groups can have both users and machines as members**. 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. As an example, here are some of the most important groups in a domain:

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.
Domain Controllers	Includes all existing DCs on the domain.
Server Operators	Users in this group can administer Domain Controllers. They cannot change any administrative group memberships.
Domain Users	Includes all existing user accounts in the domain.
Domain	Includes all existing computers in the domain.

Computers	
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.

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.**
- The people in the Sales department of your organisation are likely to have a different set of policies applied than the people in IT, for example. Keep in mind that **a user can only be a part of a single OU at a time.**
- you can create an organization unit inside of an organization unit
- 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.
    - **Managed Service Accounts:** Holds accounts used by services in your Windows domain.
    - **Users:** Default users and groups that apply to a domain-wide context.

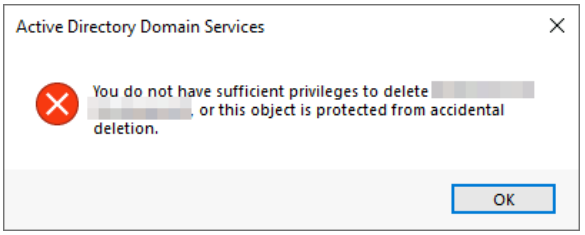


Security Groups vs OUs

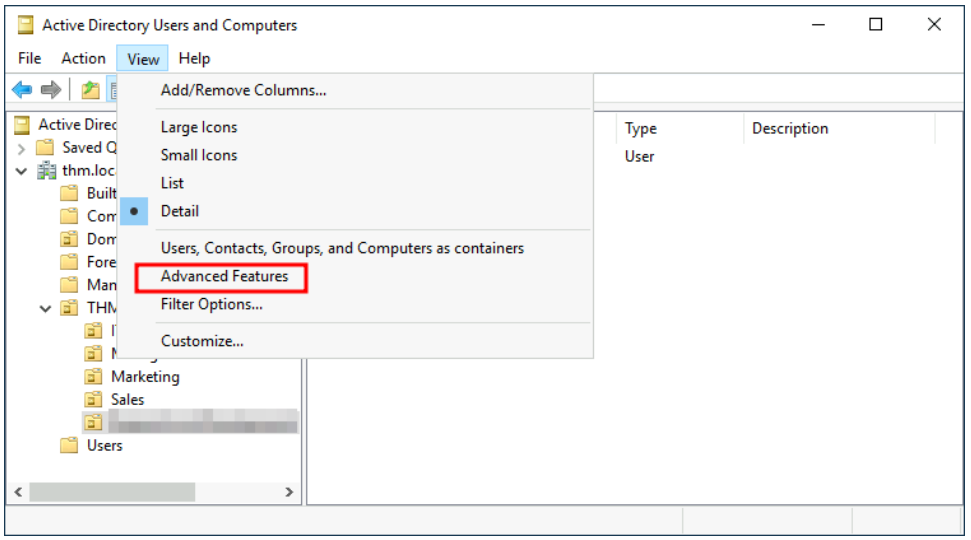
- **OUs** are handy for **applying policies** to users and computers, which include **specific configurations** that pertain to sets of users depending on their particular role in the enterprise. Remember, **a user can only be a member of a single OU at a time**, as it wouldn't make sense to try to apply 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.

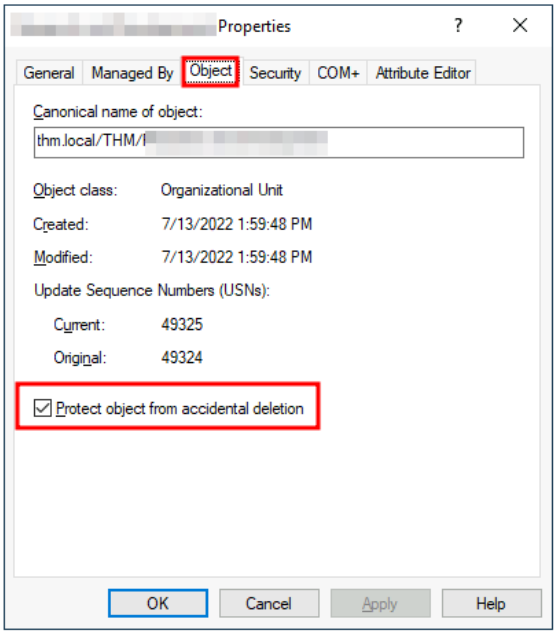
Managing users in AD

- to delete OU it will refuse because By default, OUs are protected against accidental deletion



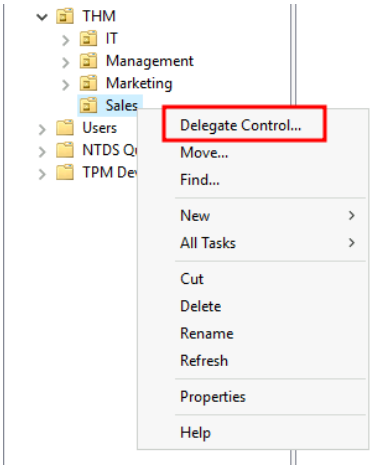
- To delete the OU, we need to enable the **Advanced Features** in the View menu then **disable the accidental deletion protection.**

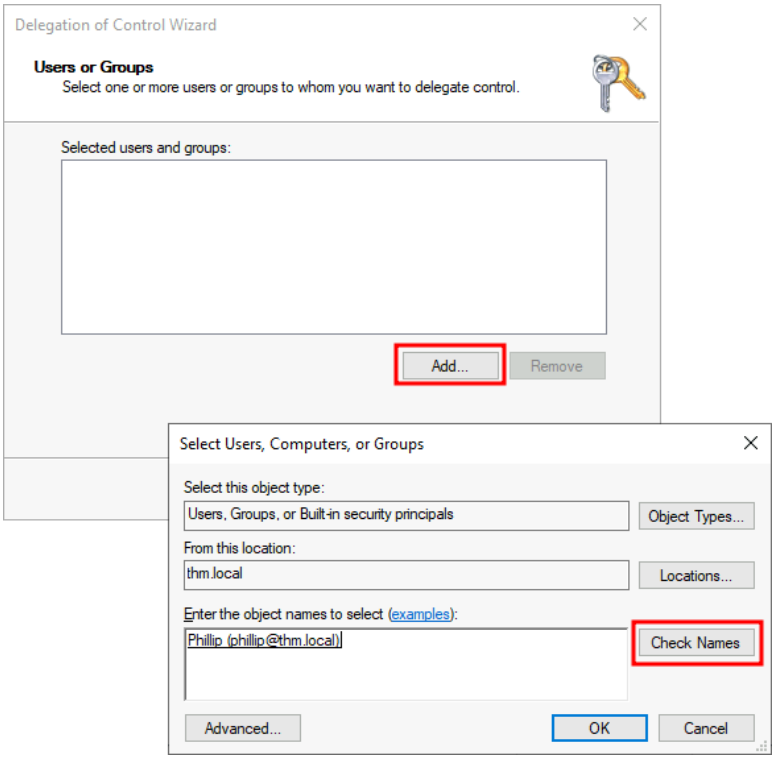


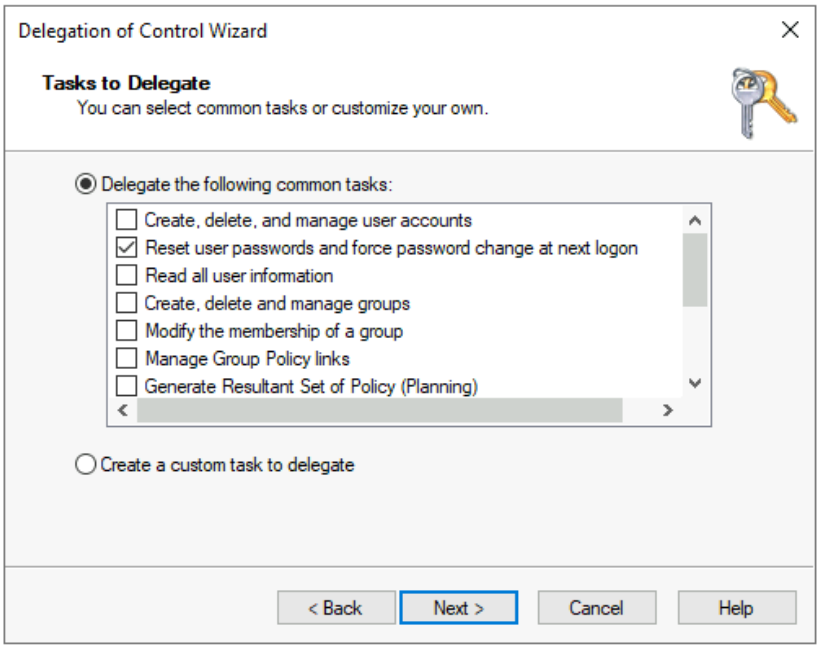


Delegation(تفويض)

allows you to grant users specific privileges to perform advanced tasks on OUs without needing a Domain Administrator to step in.

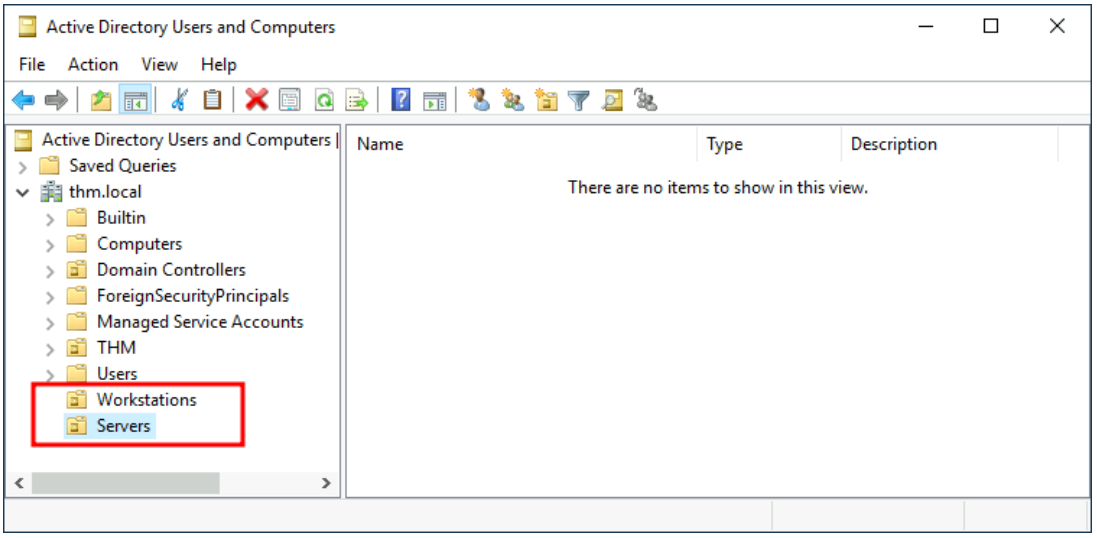

THM
IT
Management
Marketing
Sales
Users
NTDS Q
TPM De
Delegate Control...
Move...
Find...
New
All Tasks
Cut
Delete
Rename
Refresh
Properties
Help


Delegation of Control Wizard
Users or Groups
Select one or more users or groups to whom you want to delegate control.
Selected users and groups:
Add...
Remove
Select Users, Computers, or Groups
Select this object type:
Users, Groups, or Built-in security principals
Object Types...
From this location:
thm.local
Locations...
Enter the object names to select (examples):
Phillip (phillip@thm.local)
Check Names
Advanced...
OK
Cancel



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". If we check our DC, we will see that some devices are already there:
- you can Create different OUs to contain different kinds of computers, Doing so will allow us to configure policies for each OU later.
- for example
  - Workstations > to contain PCs and laptops
  - Servers > to contain servers



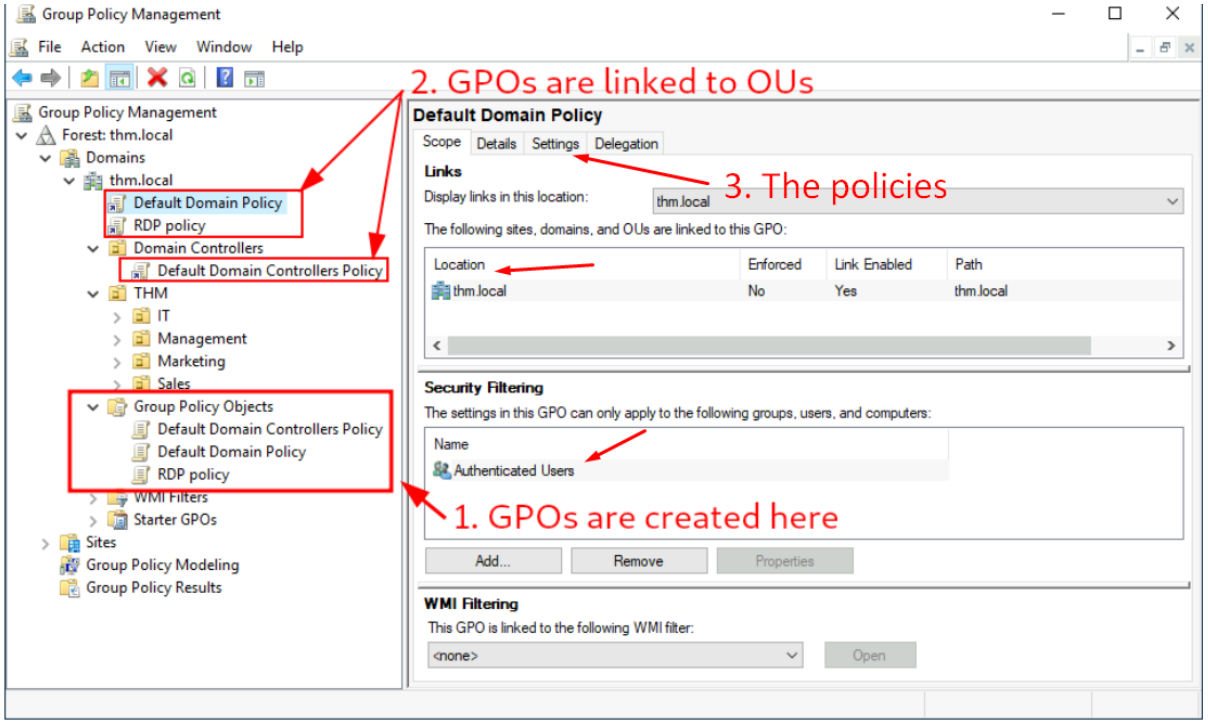
Domain Policies Overview

- You can think of **domain policies like domain groups**, except instead of permissions they **contain rules**, and instead of only applying to a group of users, the policies **apply to a domain as a whole.**
- They simply act as a rulebook for Active Directory that a domain admin can modify and alter as they deem necessary to keep the network running smoothly and securely. Along with the very long list of default domain policies, domain admins can choose to add in their own policies not already on the domain controller, for example: if you wanted to disable windows defender across all machines on the domain you could create a new group policy object to disable Windows Defender.
- The options for domain policies are almost endless and are a big factor for attackers when enumerating an Active Directory network. I'll outline just a few of the many policies that are default or you can create in an Active Directory environment:
- **Disable Windows Defender** - Disables windows defender across all machine on the domain
- **Digitally Sign Communication (Always)** - Can disable or enable SMB signing on the domain controller

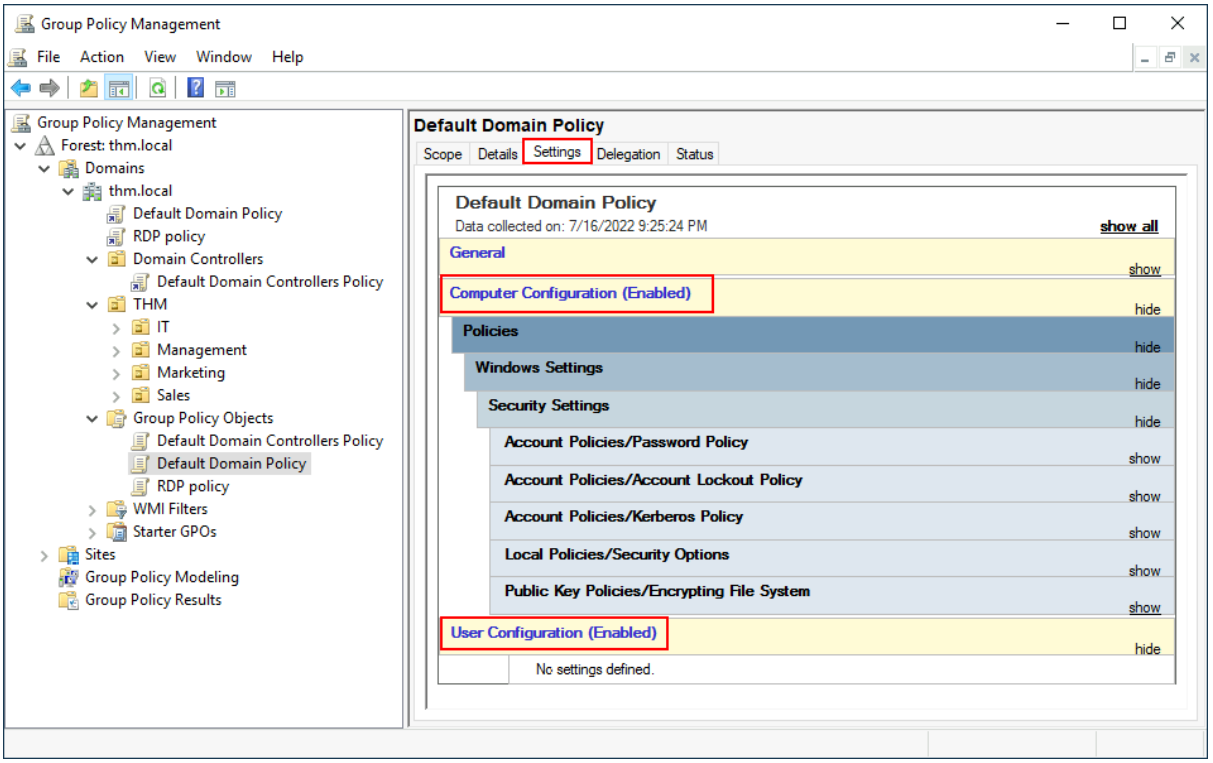
Group Policies

- Windows manages such policies through **Group Policy Objects (GPO).**

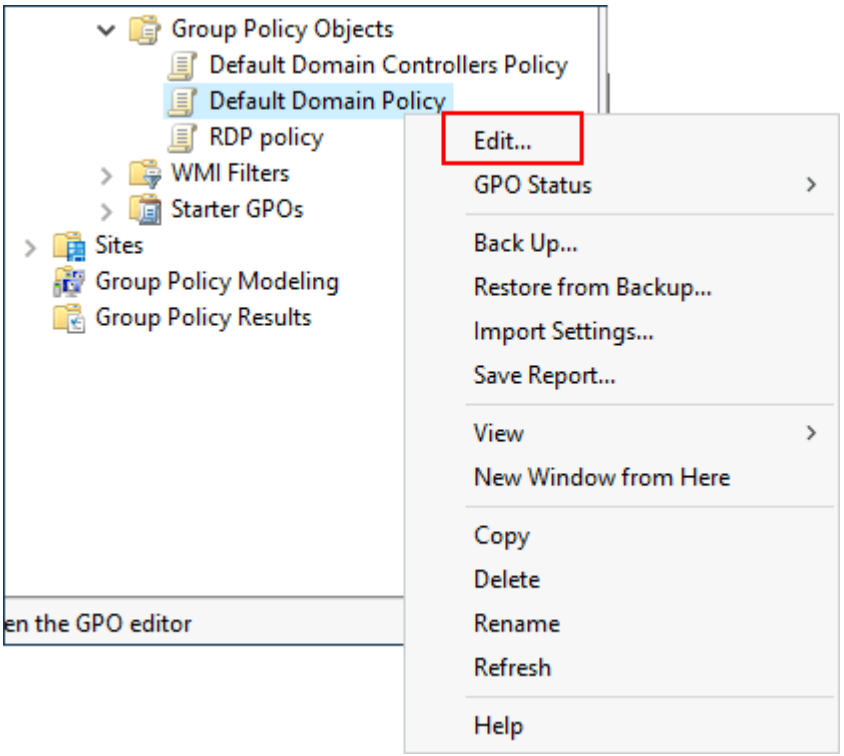
- GPOs are simply a collection of settings that can be applied to OUs.
- GPOs can contain policies aimed at either users or computers, allowing you to set a baseline on specific machines and identities.
- To configure GPOs, you can use the **Group Policy Management** tool.

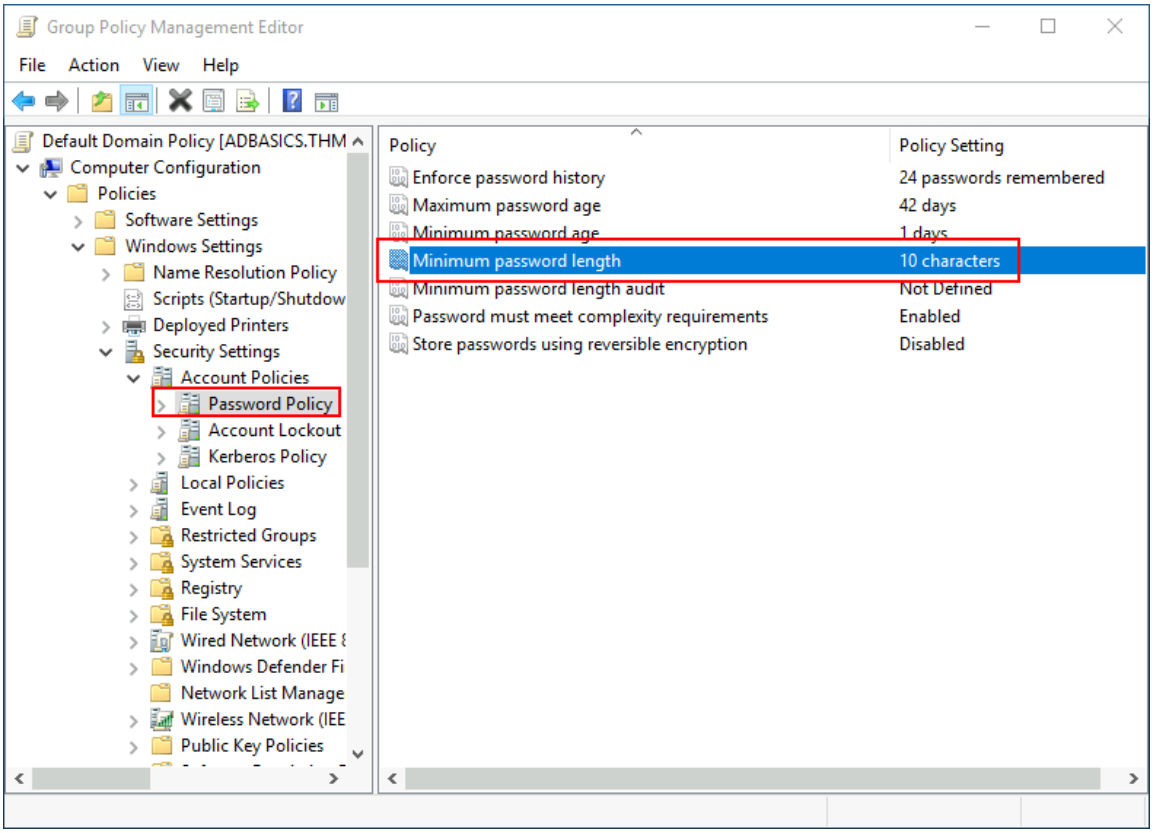


- Something important to have in mind is that any GPO will apply to the linked OU and any sub-OUs under it.
- For example, the `Sales` OU will still be affected by the `Default Domain Policy`.
- The first tab you'll see when selecting a GPO shows its **scope**, which is where the GPO is linked in the AD.
- you can also apply **Security Filtering** to GPOs so that they are only applied to specific users/computers under an OU. By default, they will apply to the **Authenticated Users** group, which includes all users/PCs.
- The **Settings** tab includes the actual contents of the GPO and lets us know what specific configurations it applies



- we can create , edit , copy , del ,….. group policies





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.

Domain Services Overview -

Domain Services are exactly what they sound like. They are services that the domain controller provides to the rest of the domain or tree. There is a wide range of various services that can be added to a domain controller; however, in this room we'll only be going over the default services that come when you set up a Windows server as a domain controller. Outlined below are the default domain services:

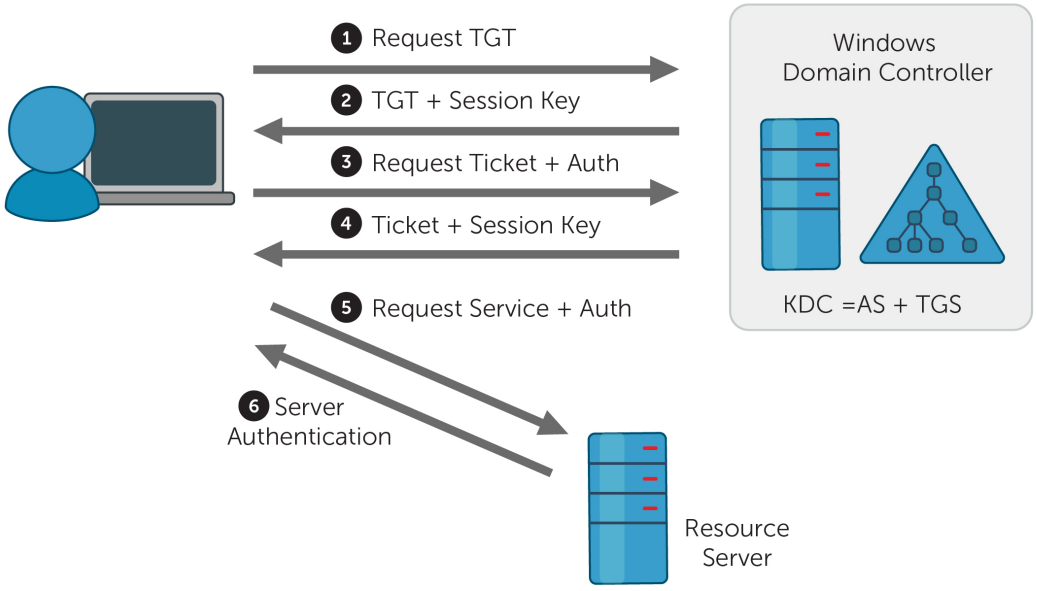
- **LDAP** - Lightweight Directory Access Protocol; **provides communication between applications and directory services**
- **Certificate Services** - allows the domain controller to create, validate, and revoke public key certificates
- **DNS**, **LLMNR**, **NBT-NS** - Domain Name Services for identifying IP hostnames

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

Kerberos

Kerberos authentication is the default authentication protocol for any recent version of Windows.



Terms :

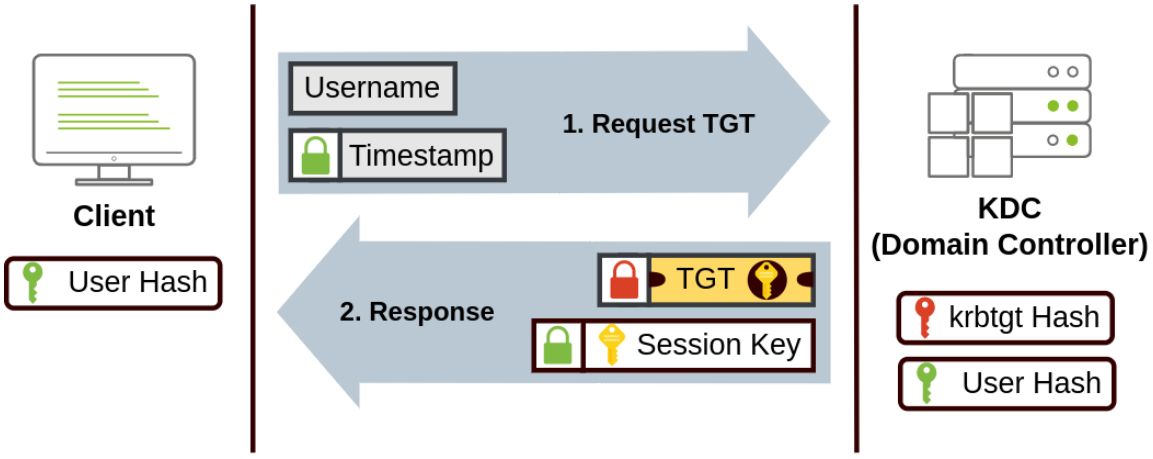
- **Key Distribution Center (KDC) :** a service usually installed on the Domain Controller in charge of creating Kerberos tickets on the network, it contatins 2 servers

- **Authentication Server (AS)**
- **Ticket Granting Service (TGS) :** tickets that allow connection only to the specific service they were created for.

- **Ticket Granting Ticket (TGT) :** a ticket that will allow the user to request additional tickets to access specific services. The need for a ticket to get more tickets without passing their credentials every time they want to connect to a service
  Session Key : an encryption and decryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between two computers
  Service Principal Name (SPN) : a unique identifier of a service instance.
- **Timestamp :** a sequence of different characters or information that has been encoded to help in the identification of the time an event will occur.

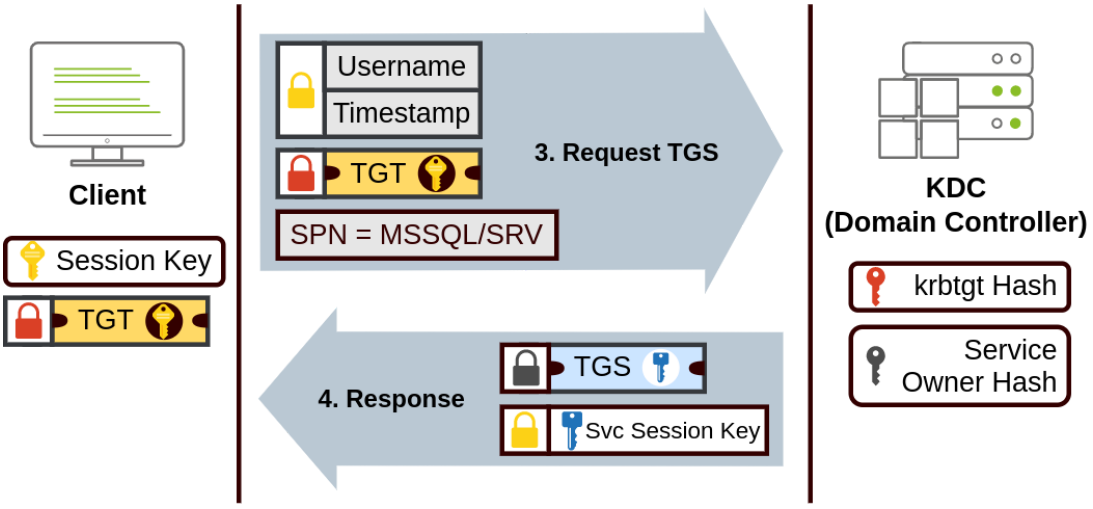
When Kerberos is used for authentication, the following process happens:

1. The user sends their username and a timestamp encrypted using a key derived from their password to the **Key Distribution Center (KDC)**
2. The KDC will create and send back a **Ticket Granting Ticket (TGT),**Along with a **Session Key**
   a. Notice the TGT is encrypted using the **krbTGT** account's password hash, and therefore the user can't access its contents

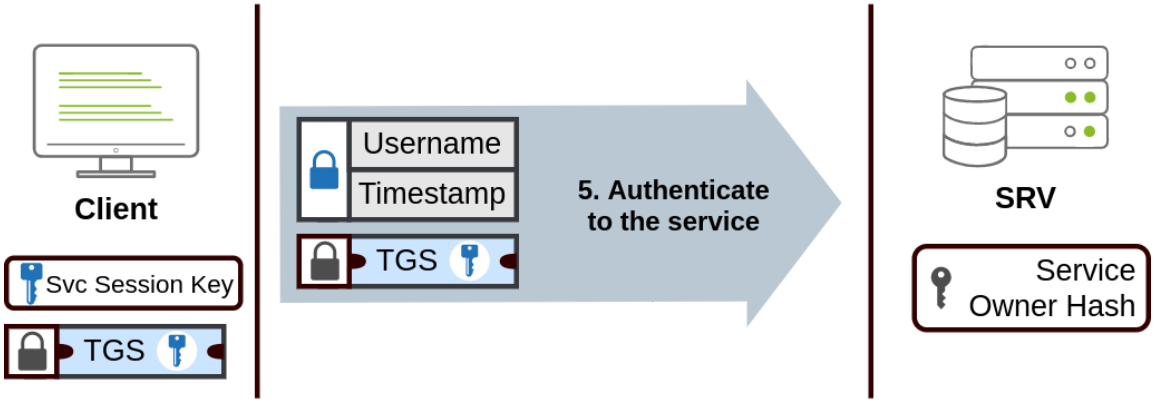


3. When a user wants to connect to a service on the network like a share, website or database, they will use their TGT to ask the KDC for a **Ticket Granting Service (TGS),**

4. the user will send their username and a timestamp encrypted using the Session Key, along with the TGT and a **Service Principal Name (SPN)**
5. the KDC will send us a **TGS** along with a **Service Session Key**, which we will need to authenticate to the service we want to access.
    a. Notice that The TGS is encrypted using a key derived from the **Service Owner Hash**
    b. The TGS contains a copy of the Service Session Key on its encrypted contents so that the Service Owner can access it by decrypting the TGS.



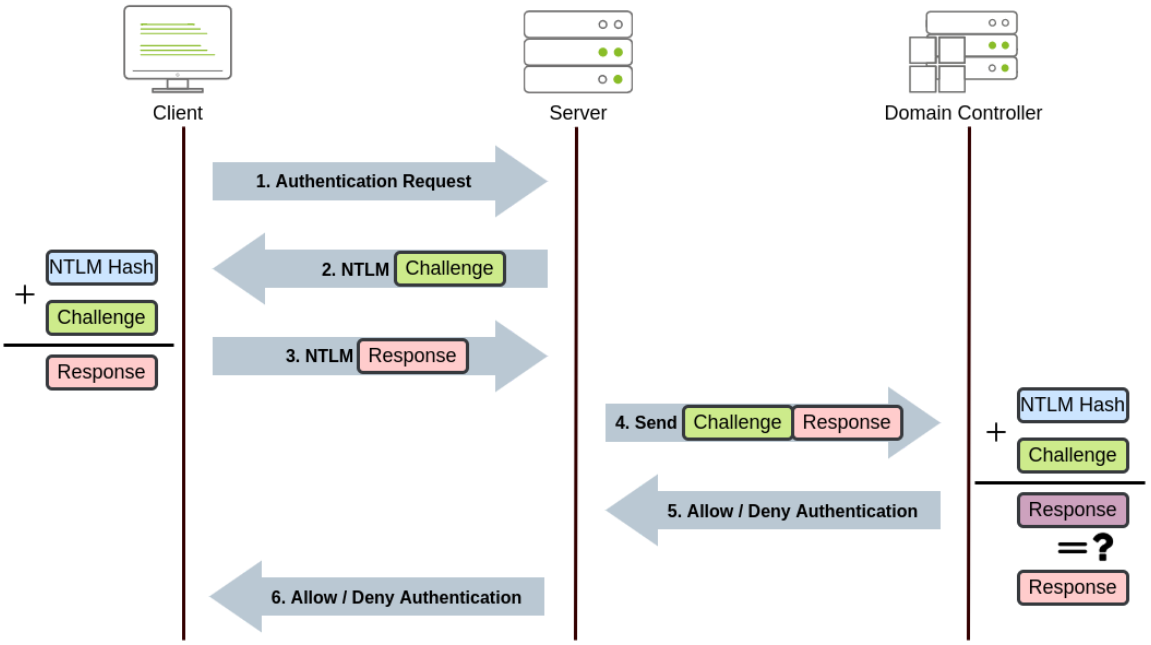
6. The TGS can then be sent to the desired service to authenticate and establish a connection
7. The service will use its configured account's password hash to decrypt the TGS and validate the Service Session Key.



NetNTLM Authentication

NetNTLM works using a challenge-response mechanism. The entire process is as follows:

1. The client sends an authentication request to the server they want to access.
2. The server generates a random number and sends it as a challenge to the client.
3. The client combines their NTLM password hash with the challenge (and other known data) to generate a response to the challenge and sends it back to the server for verification.
4. The server forwards the challenge and the response to the Domain Controller for verification.
5. The domain controller uses the challenge to recalculate the response and compares it to the original response sent by the client. If they both match, the client is authenticated; otherwise, access is denied. The authentication result is sent back to the server.
6. The server forwards the authentication result to the client.

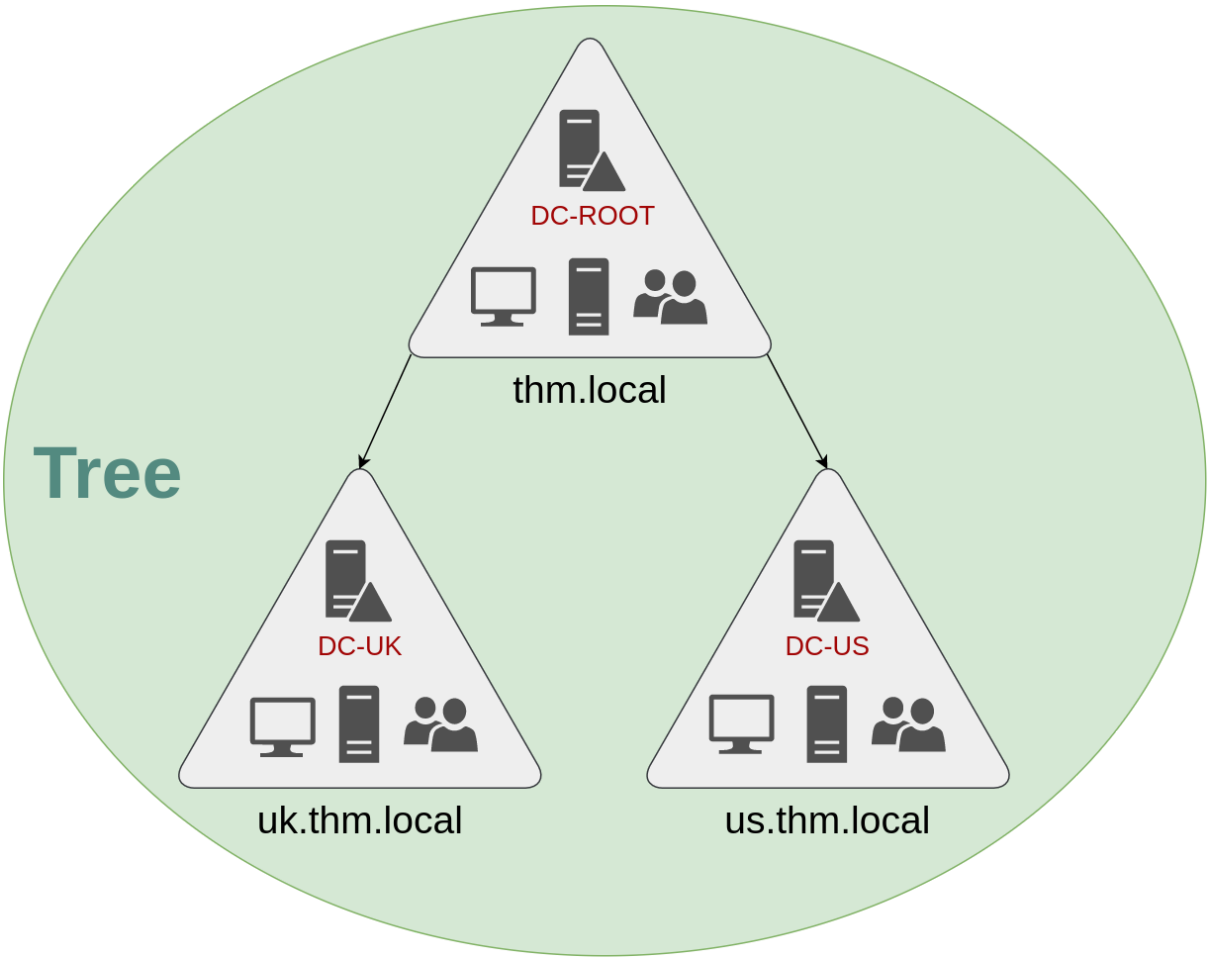


Note that the user's password (or hash) is never transmitted through the network for security.

Tree

A tree or domain tree is a **collection of domains.** Moreover, a tree follows a parent domain, child domain tree structure. When a domain is under a specific domain, that

domain is called the child domain while the main domain is called the parent domain.



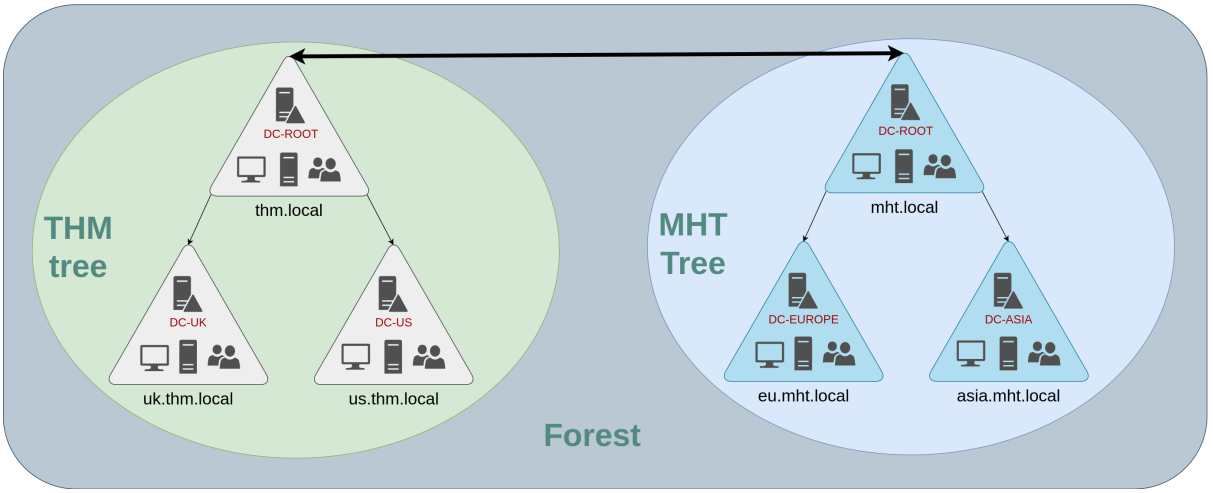
Forest

A forest is a **collection of trees** or domain trees which provides the highest level of security boundary. It is also a complete active directory instance. Moreover, objects within the same forest can communicate with each other. If an object in one forest needs to exchange information with an object in another forest, the two forests should have forest level trust.

The Forest consists of these parts which we will go into farther detail with later:

- Trees — A hierarchy of domains in Active Directory Domain Services
- Domains — Used to group and manage objects
- Organizational Units (OUs) — Containers for groups, computers, users, printers and other OUs
- Trusts — Allows users to access resources in other domains
- Objects — users, groups, printers, computers, shares

- Domain Services — DNS Server, LLMNR, IPv6
- Domain Schema — Rules for object creation



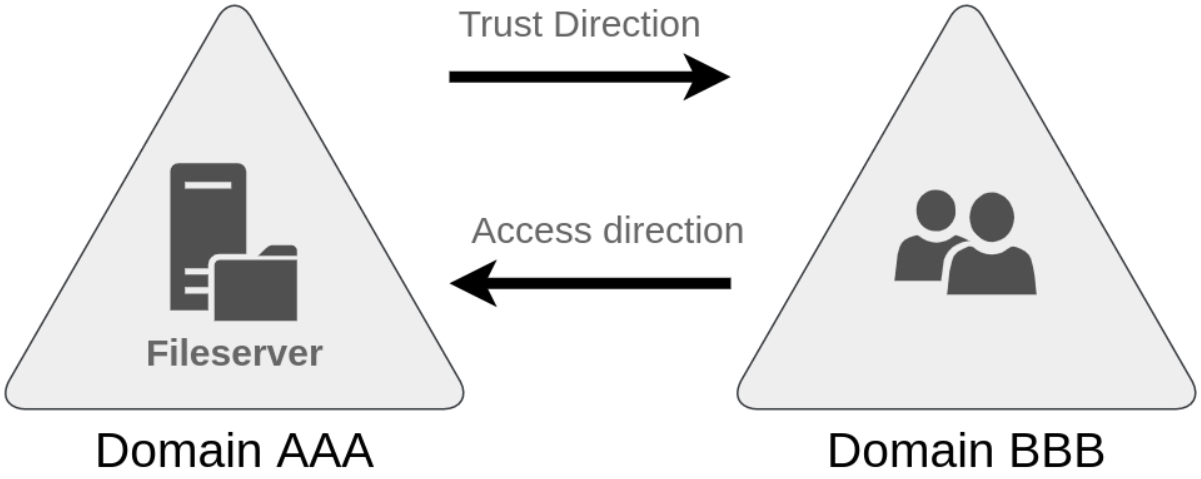
Trust Relationships

In simple terms having a trust relationship between domains allows you to authorise a user from domain `THM UK` to access resources from domain `MHT EU`

The simplest trust relationship that can be established is a **one-way trust relationship**. In a one-way trust, if `Domain AAA` trusts `Domain BBB`, this means that a user on BBB can be authorised to access resources on AAA:

Two-way trust relationships
 can also be made to allow both domains to mutually authorise users from the other. By default, joining several domains under a tree or a forest will form a two-way trust relationship.

Transitive - The trust relationship expands beyond just two domains to include other trusted domains



- The type of trusts put in place determines how the domains and trees in a forest are able to communicate and send data to and from each other when attacking an Active Directory environment you can sometimes abuse these trusts in order to move laterally throughout the network.

AD DS Data Store -

The Active Directory Data Store holds the databases and processes needed to store and manage directory information such as users, groups, and services. Below is an outline of some of the contents and characteristics of the AD DS Data Store:

- Contains the **NTDS.dit** - a database that contains all of the information of an Active Directory domain controller as well as password hashes for domain users
- Stored by default in **%SystemRoot%\NTDS**
- accessible only by the domain controller

Default Security Groups -

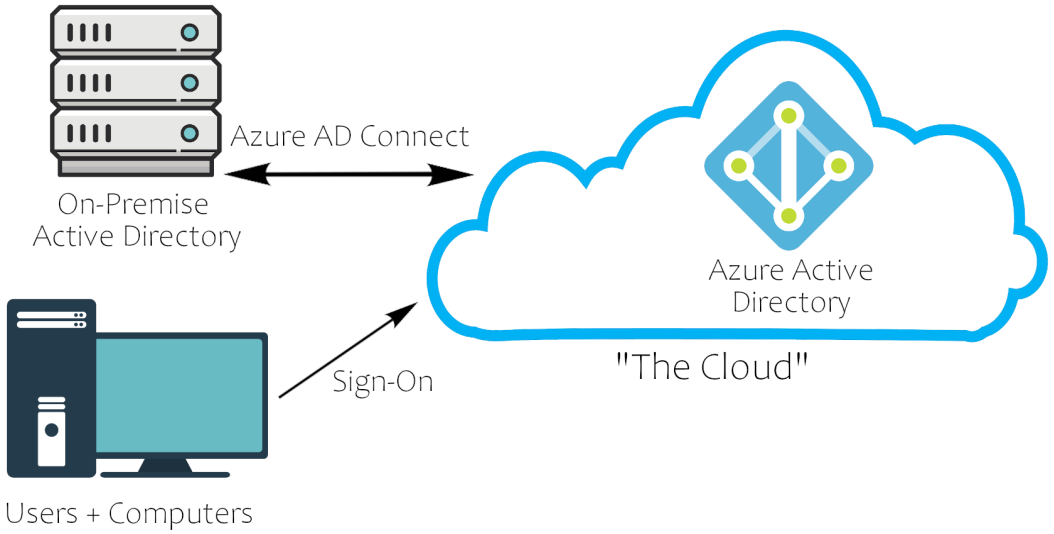
There are a lot of default security groups so I won't be going into too much detail of each past a brief description of the permissions that they offer to the assigned group. Here is a brief outline of the security groups:

- Domain Controllers - All domain controllers in the domain
- Domain Guests - All domain guests
- Domain Users - All domain users
- Domain Computers - All workstations and servers joined to the domain

- Domain Admins - Designated administrators of the domain
- Enterprise Admins - Designated administrators of the enterprise
- Schema Admins - Designated administrators of the schema
- DNS Admins - DNS Administrators Group
- DNS Update Proxy - DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).
- Allowed RODC Password Replication Group - Members in this group can have their passwords replicated to all read-only domain controllers in the domain
- Group Policy Creator Owners - Members in this group can modify group policy for the domain
- Denied RODC Password Replication Group - Members in this group cannot have their passwords replicated to any read-only domain controllers in the domain
- Protected Users - Members of this group are afforded additional protections against authentication security threats. See http://go.microsoft.com/fwlink/?LinkId=298939 for more information.
- Cert Publishers - Members of this group are permitted to publish certificates to the directory
- Read-Only Domain Controllers - Members of this group are Read-Only Domain Controllers in the domain
- Enterprise Read-Only Domain Controllers - Members of this group are Read-Only Domain Controllers in the enterprise
- Key Admins - Members of this group can perform administrative actions on key objects within the domain.
- Enterprise Key Admins - Members of this group can perform administrative actions on key objects within the forest.
- Cloneable Domain Controllers - Members of this group that are domain controllers may be cloned.
- RAS and IAS Servers - Servers in this group can access remote access properties of users

Azure AD Overview -

Azure acts as the middle man between your physical Active Directory and your users' sign on. This allows for a more secure transaction between domains, making a lot of Active Directory attacks ineffective.



Cloud Security Overview -

The best way to show you how the cloud takes security precautions past what is already provided with a physical network is to show you a comparison with a cloud Active Directory environment:

Windows Server AD	**Azure AD**
LDAP	Rest APIs
NTLM	OAuth/SAML
Kerberos	OpenID
OU Tree	Flat Structure
Domains and Forests	Tenants
Trusts	Guests