Active Directory Basics - Tryhackme

Windows Domains

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

Advantages of having a configured windows domain:

1. **Centralized Identity Management:** All users across the network can be configured from Active Directory with minimum effort.
2. **Managing Security Policies:** We can configure security policies directly from Active Directory and apply them to users and computers across the network as needed.

Active Directory

- The core of any Windows domain is Active Directory Domain service (AD DS).
- This service acts as a catalogue that holds the information of all the objects that exists on our network.
- For example- We have users, group, machines, printers, shares and many others.

Users

- They are the most common object types in AD.
- They are knows as security principals.
- They can be authenticated by the domain and assigned privileges over resources like files and printers.
- They can be used to represent 2 types of entities:
  - **People:** Generally represent persons in an organization that need to access the network, like employees.
  - **Services:** Users can be defined to be used by services such as IIS or MSSQL.

Machines

- For every computer that joins the AD domain, a machine object is created.
- They are also considered “security principals” and assigned an account just as any regular user.
- Machine accounts themselves are local administrators on the assigned computer.
  - Machine Account passwords are automatically rotated out and are generally comprised of 120 random characters.
- For identifying machine accounts- 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 name `DC01$`.

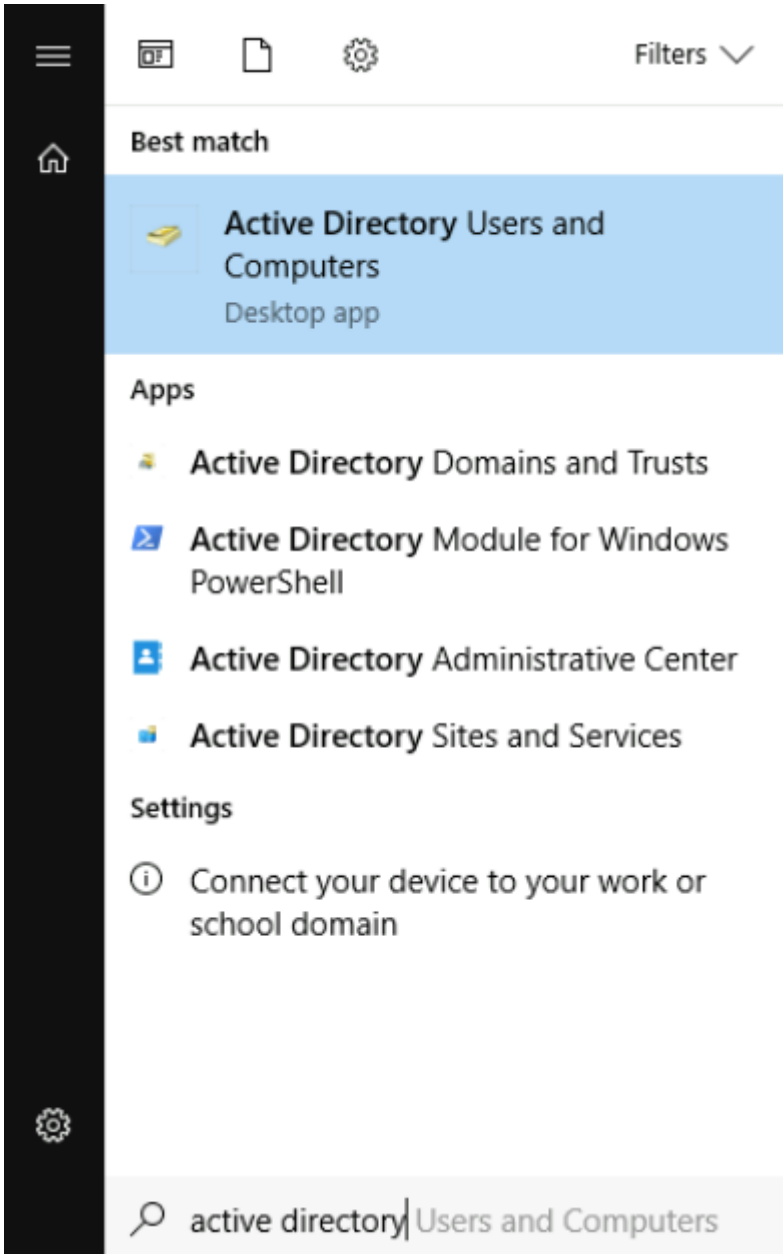
Security Groups

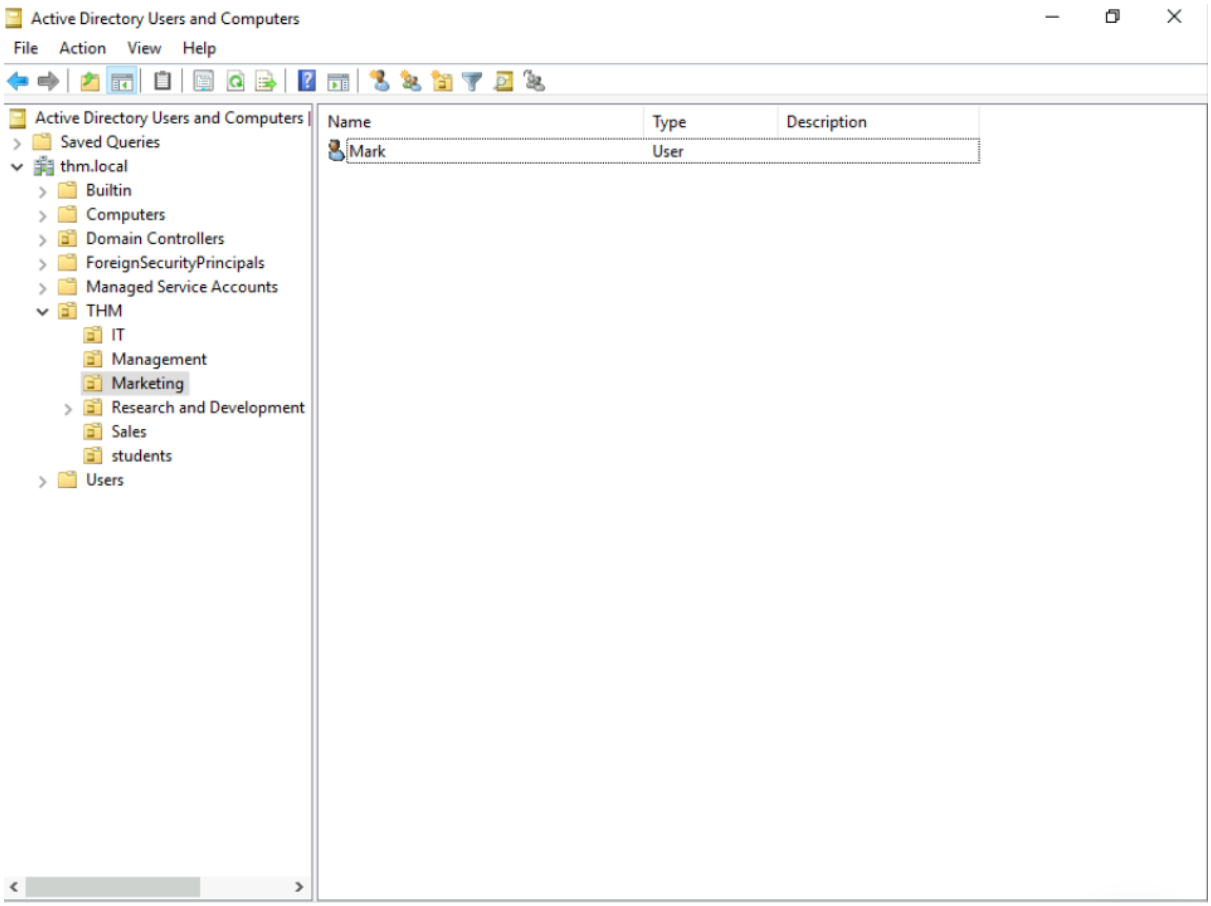
- They are also considered security principals.
- They can have both users and machines as members.
- They can include other groups as well.
- Some of the most important groups in a domain are:
  - **Domain Admins**: Users of this group have administrative privileges over the entire domain. By default, 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 in the domain.

Active Directory Users and Computers

- We need to login in DC and run “Active Directory Users and Computers” to configure user, groups or machines in AD.
- Objects in AD are organized in **Organizational Units** (OUs).
- OUs are mainly used to define set of users with similar policing requirements.
- For example- The people in the Sales department of an organization are likely to have a different set of policies applied than the people in IT.
- A user can only be a part of a single OU at a time.


Filters
Best match
Active Directory Users and Computers
Desktop app
Apps
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Administrative Center
Active Directory Sites and Services
Settings
Connect your device to your work or school domain
active directory Users and Computers

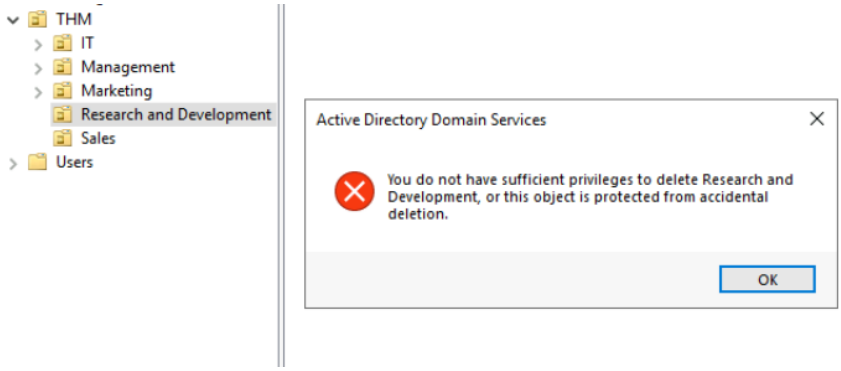


- Here THM is an OU with 6 child OU.
- On opening any OU, we can see the users they contain and perform simple tasks like creating, modifying or deleting them as needed.
- There are other default containers other than the THM OU:
  - **Bullitin:** Contains default groups available to any Windows host.
  - **Computers:** Any machine joining the network will be put here by default.
  - **Domain Controllers:** Default OU that contains the DCs in the network.
  - **Users:** Default users and groups that apply to a domain-wide context.
  - **Managed Service Accounts:** Holds accounts used by services in our Windows domain.

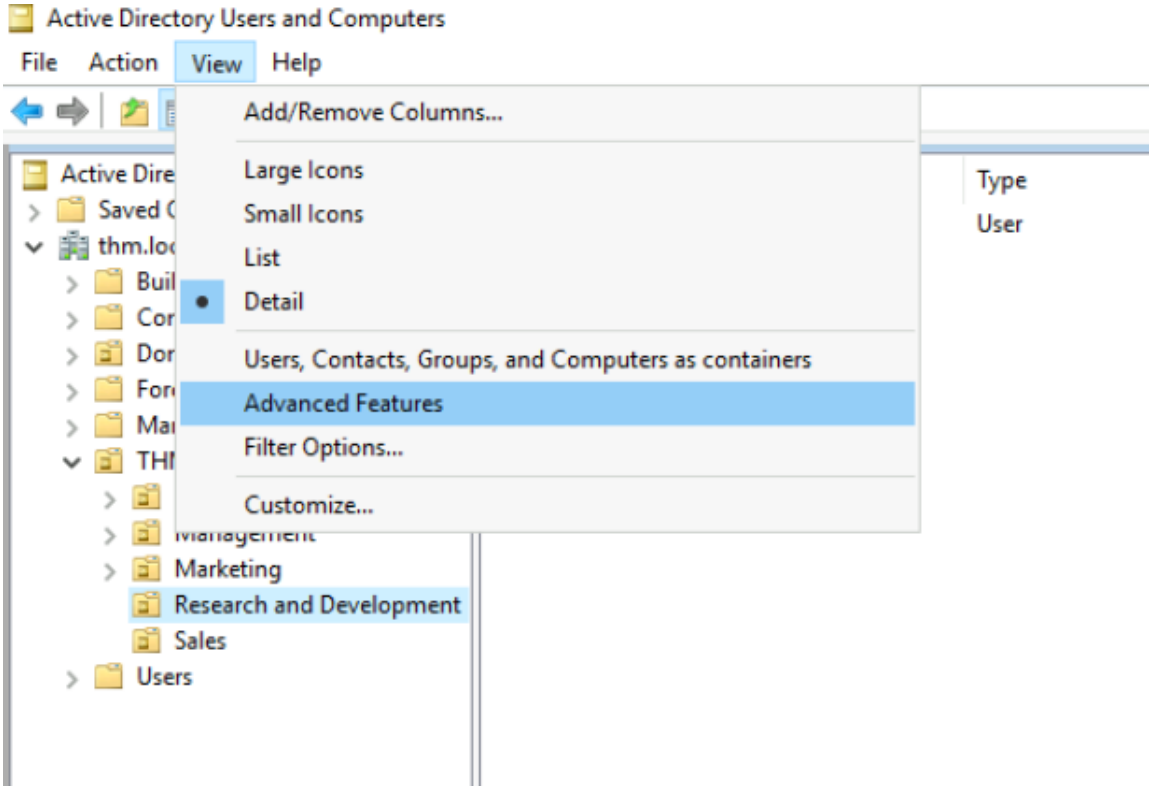
Managing Users in AD

Deleting extra OUs and users

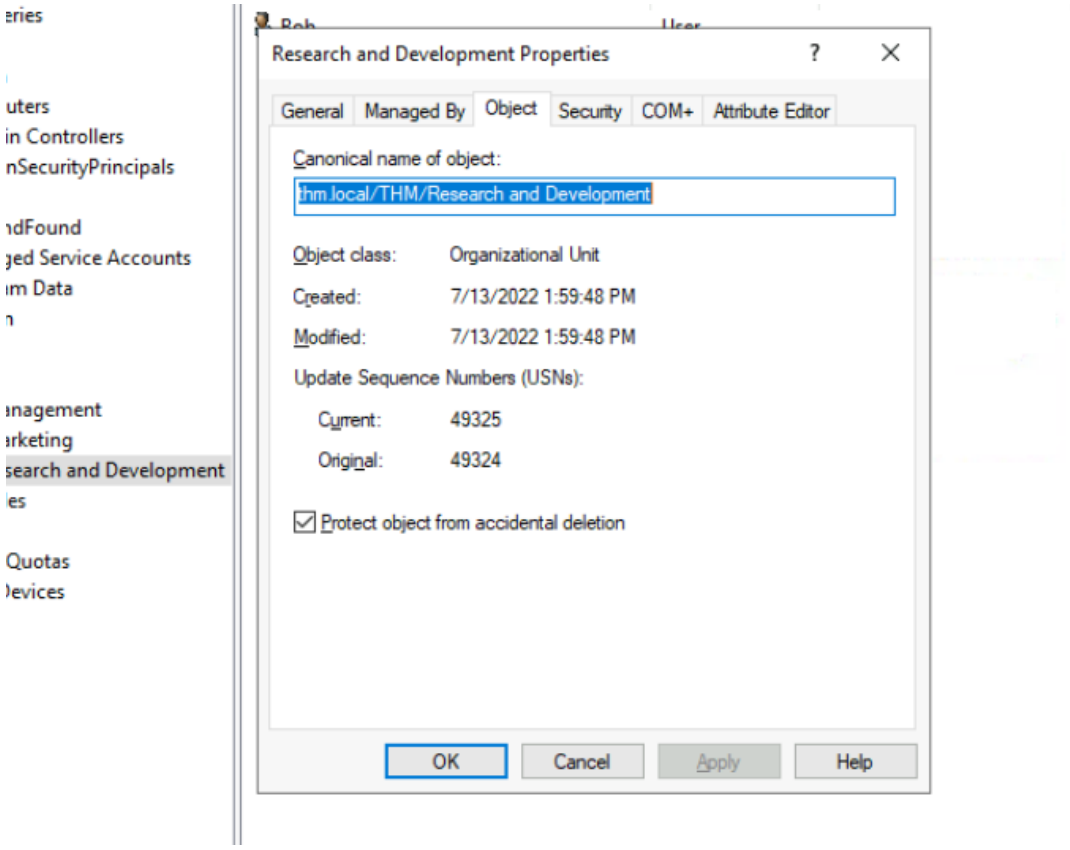
- By default OUs are protected against accidental deletion.
- On trying to delete the OU “Research and Development” we get:



- To delete the OU, we need to enable the *Advanced Features* in the view menu.



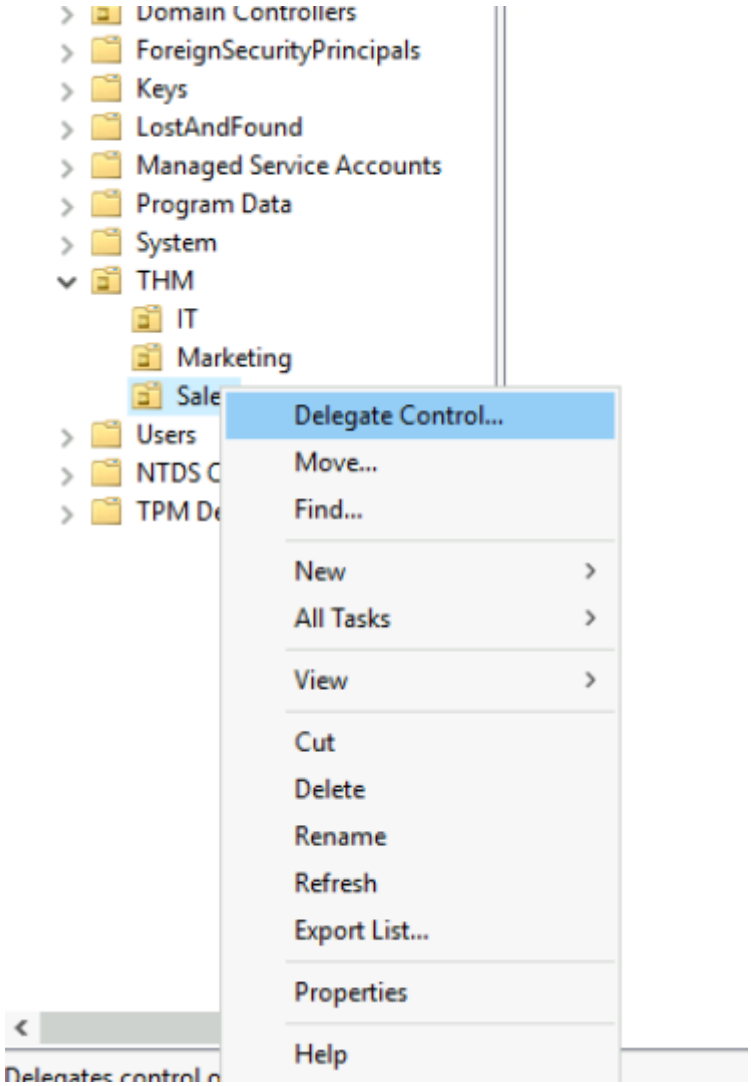
- On enabling the *Advanced Features* we can now right click on the OU we want to delete and go to the object tab in the properties option and uncheck the box “Protect object from accidental deletion”



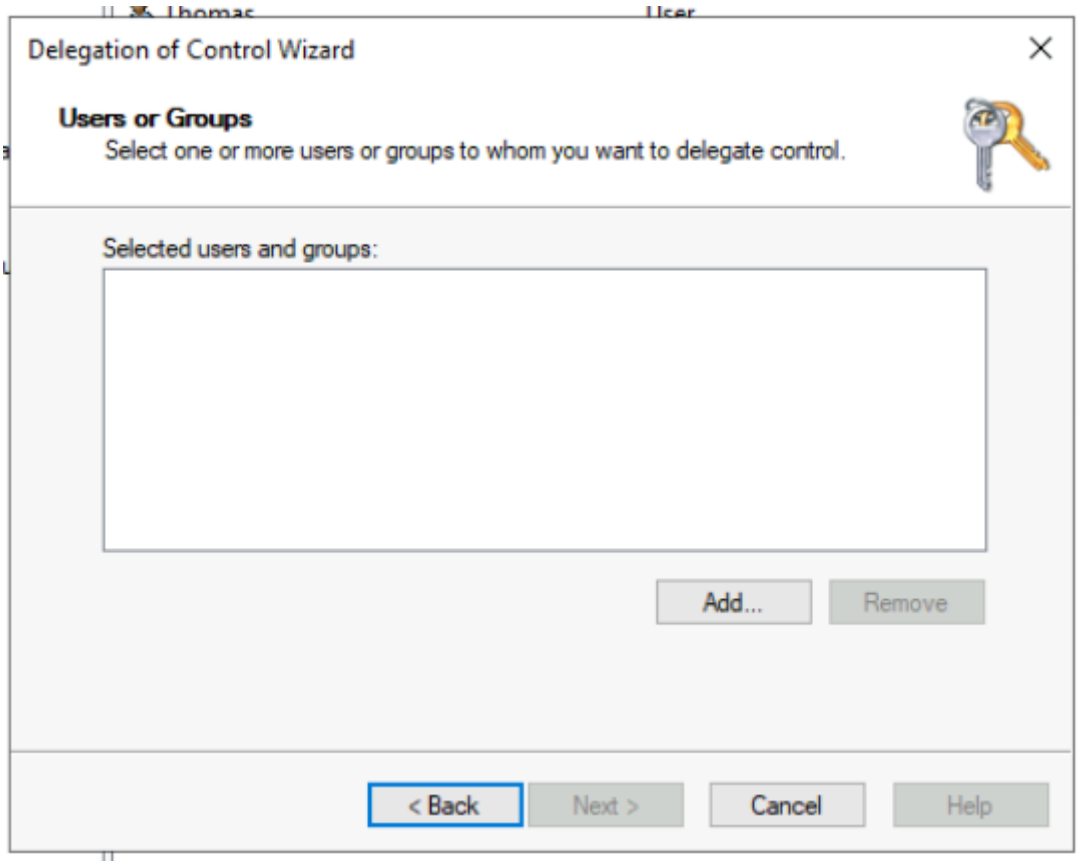
- After that we can successfully delete the OU.

Delegation

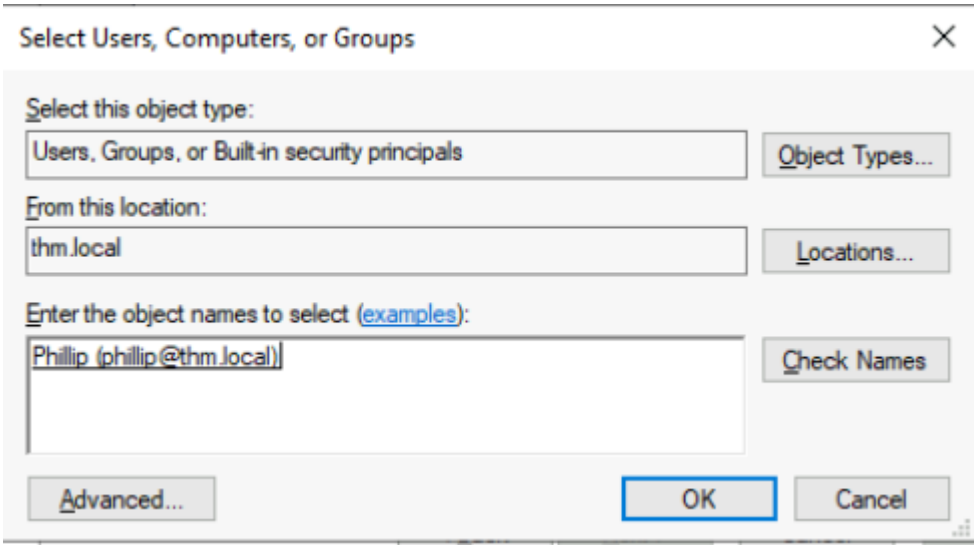
- One of the things we can do in AD is to give specific users some control over some OUs and this process is called delegation.
- It allows us to grant users specific privileges to perform advanced tasks on OUs without needing a Domain Administrator to step in.
- For example- Granting **IT support** the privileges to reset other low-privilege user's passwords.
- Here, we will try to delegate control over the Sales OU to Phillip (IT OU's users)
- Right click on the Sales OU and click on *Delegate Control*



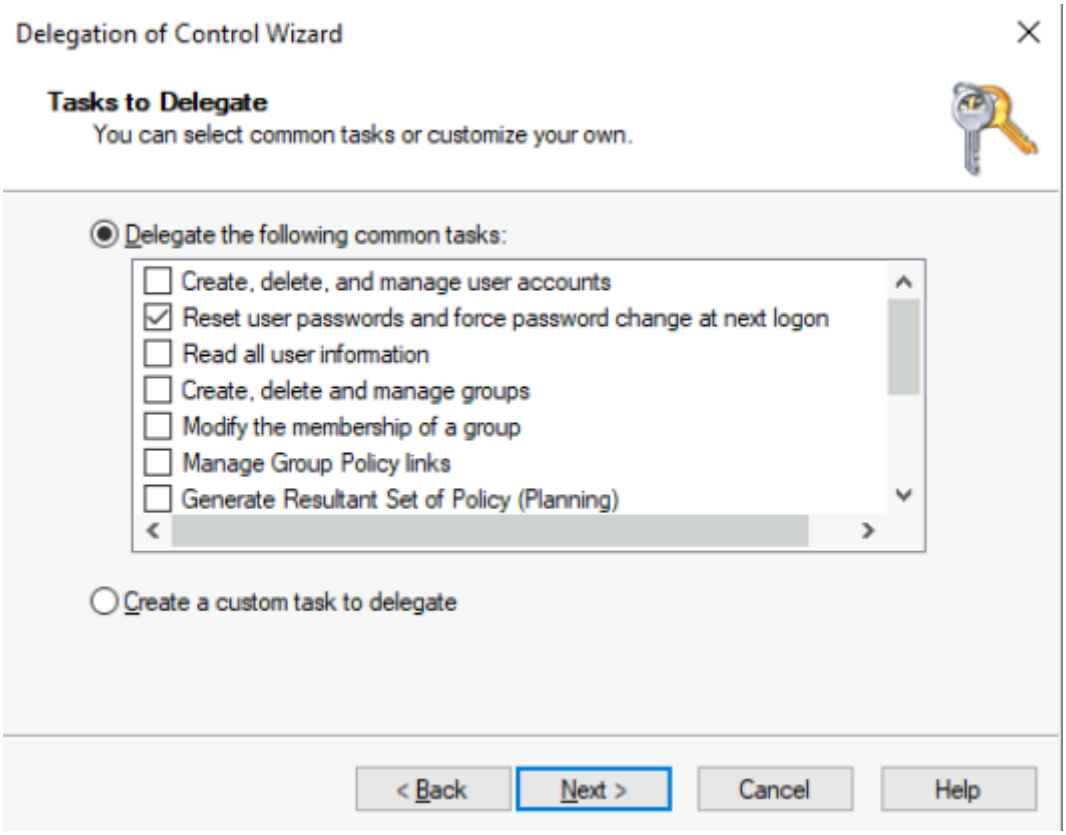
- Now it is asking for users to whom we want to delegate control.



- Here we click on “Add” button and enter the name “phillip” and then click on “Check Names”.



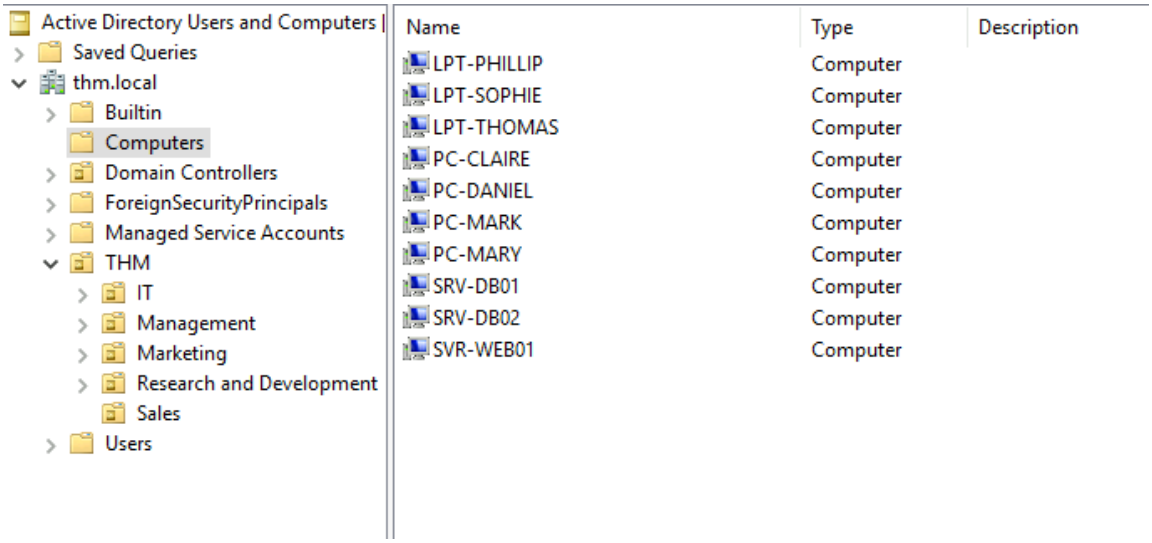
- Click OK, and on the next step, select the following option:



- Now, on clicking Next a couple of times, Phillip should be able to reset passwords for any user in the Sales Department.
- Now, we will try to reset “Sophie” password using Phillip’s power
- We would do that by logging into the system as Phillip and change the password of Sophie.
- After resetting Sophie’s password we would login as Sophie and get the flag.

Managing Computers in AD

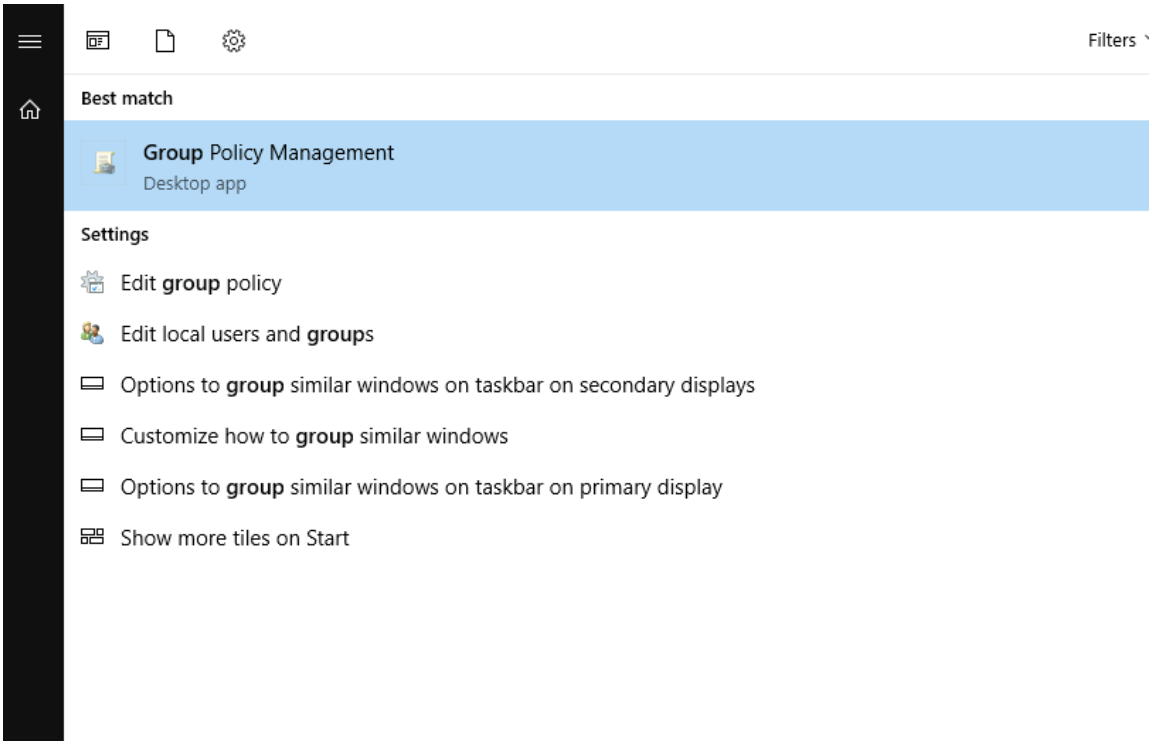
- By default, all the machines that join a domain (except for the DCs) are put in the container called "Computers”.



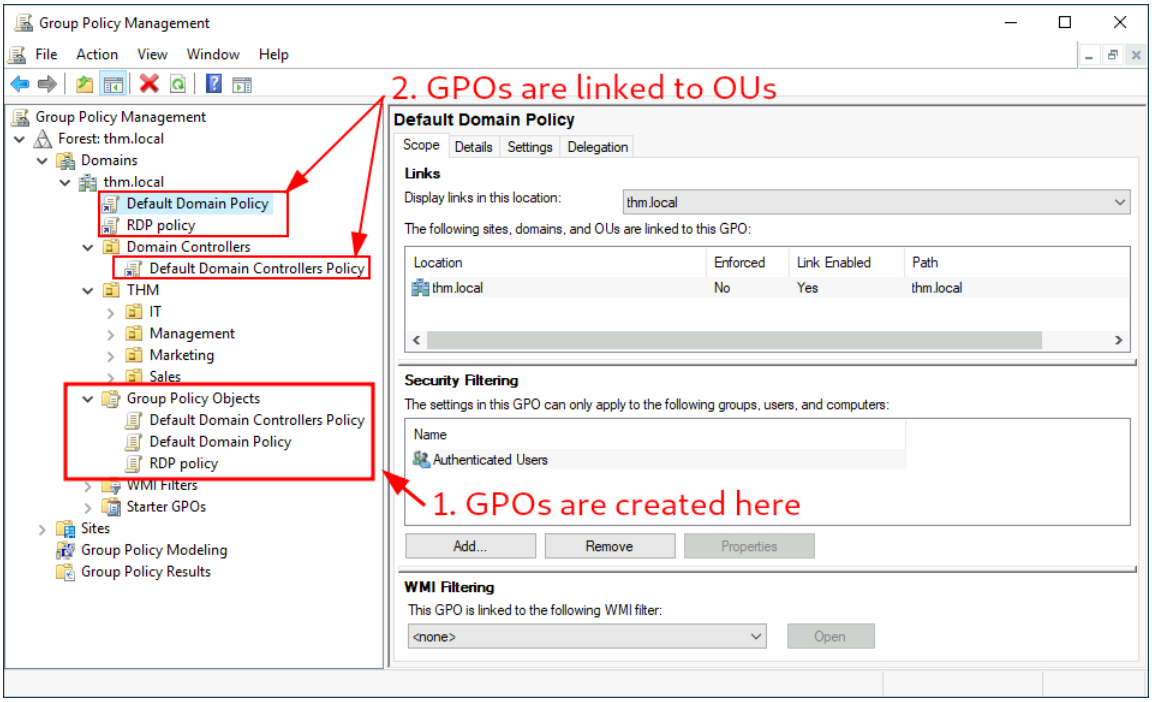
- We'd expect to see devices divided into at least the three following categories:
  - **Workstations:** They are one of the most common devices within an Active Directory domain.
  - **Servers:** Servers are the second most common device within an Active Directory domain. Servers are generally used to provide services to users or other servers.
  - **Domain Controllers:** They are the 3rd most common device within an Active Directory domain. They allow us to manage the AD Domain. These devices are often considered the most sensitive devices within the network as they contain hashed passwords for all the user accounts within the environment.

Group Policies

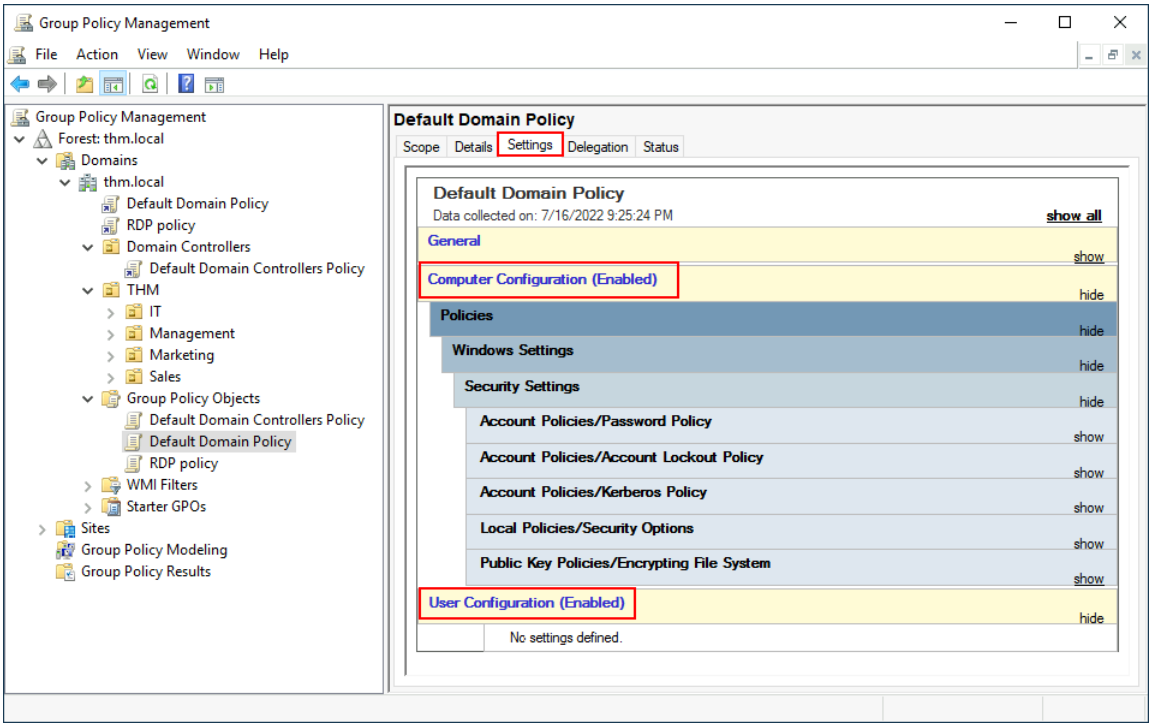
- Windows manages policies through **Group Policy Objects (GPOs).**
- GPOs are a collection of settings that can be applied to OUs.
- The main idea behind organizing the users and computers in different OUs is to deploy different policies for each OU individually.
- To configure GPOs, we can use the **Group Policy Management** tool in Windows.

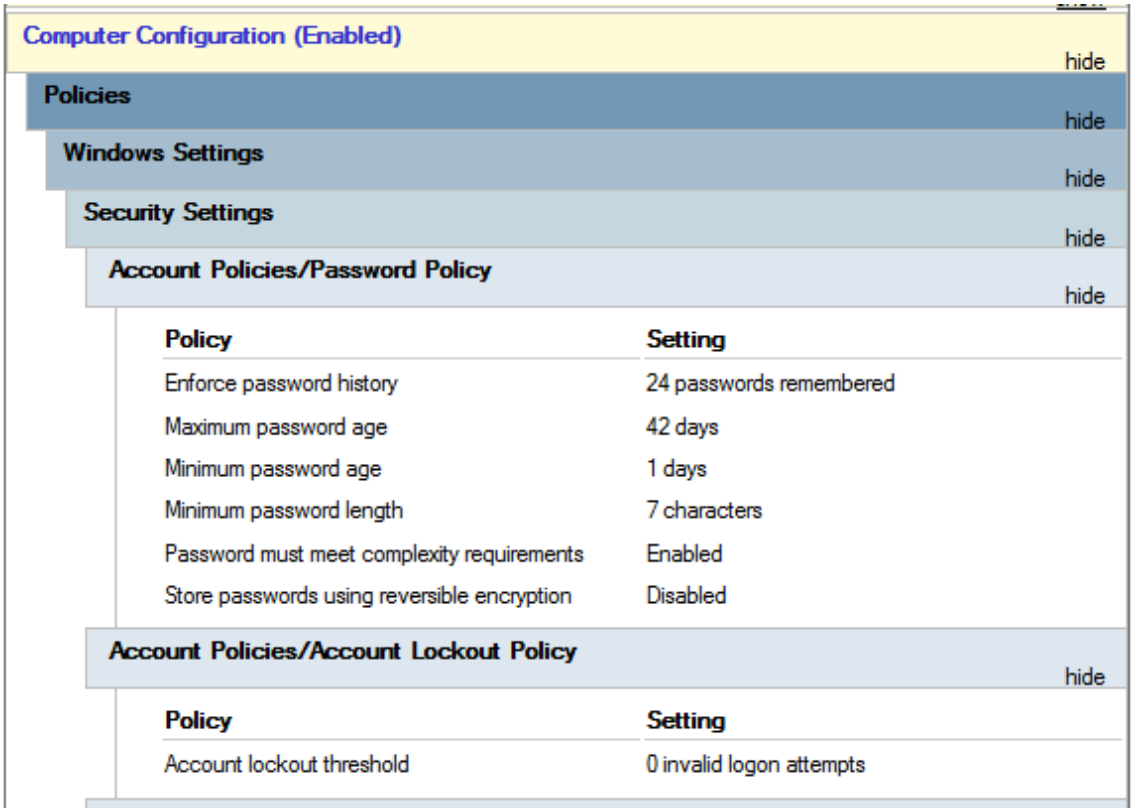


- We need to first create a GPO under Group Policy Objects and then link it to the GPO where we want the policies to apply.



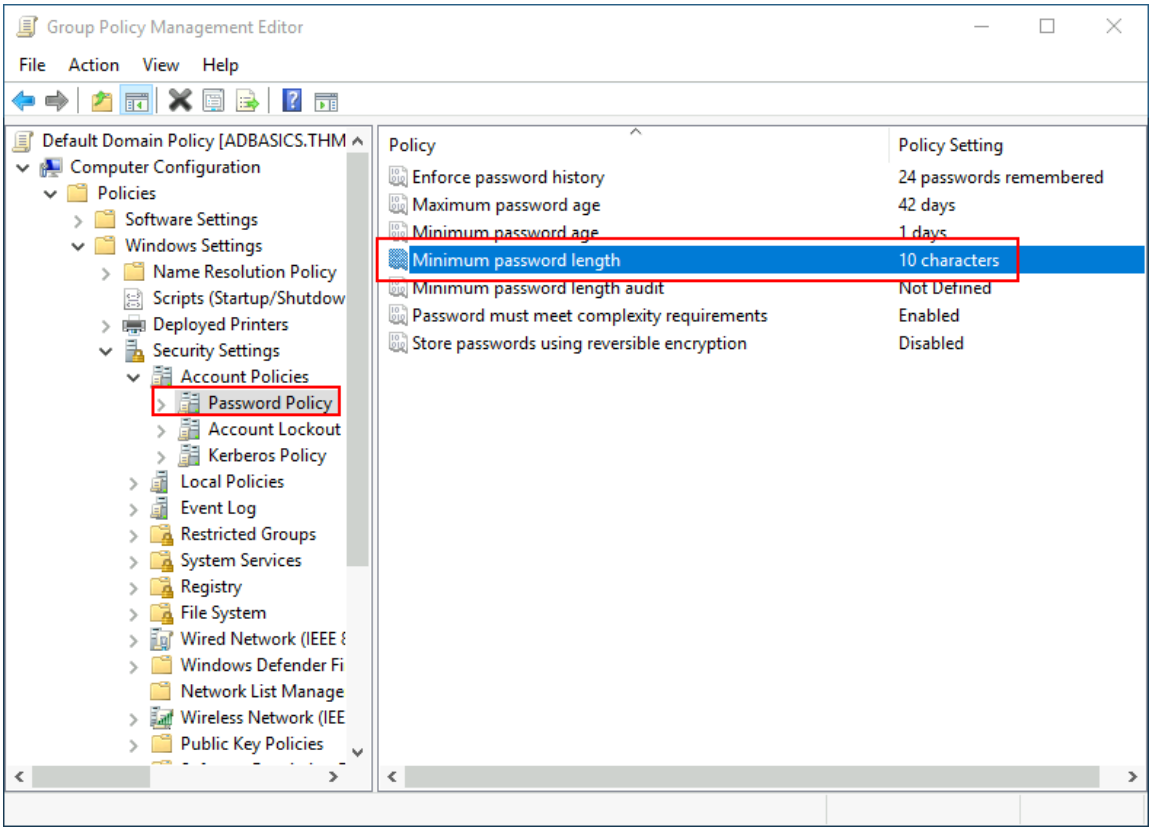
- Exploring the Default Domain Policy





- To change the minimum password length policy to require users to have at least 10 characters in their passwords, we need to go to -

  Computer Configurations→ Policies → Windows Setting → Security Settings → Account Policies → Password Policy



GPO Distribution

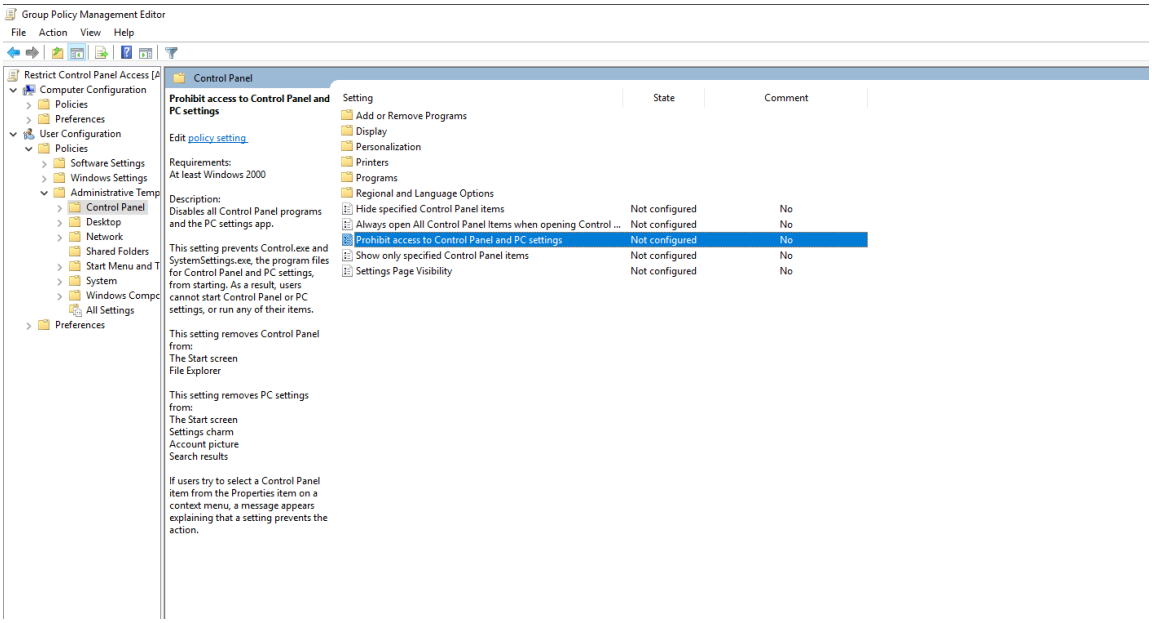
- GPOs are distributed to the network via a network share called `SYSVOL` which is stored in the DC.
- All users in a domain should should typically have access to this share over the network to sync their GPOs periodically.
- The SYSVOL share by default points to the `C:\Windows\SYSVOL\sysvol\` directory.
- It might take up to 2 hours for computers to catch up, if any change in GPOs are made.
- To force any particular computer to sync the GPO immediately, we can run the following command:

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

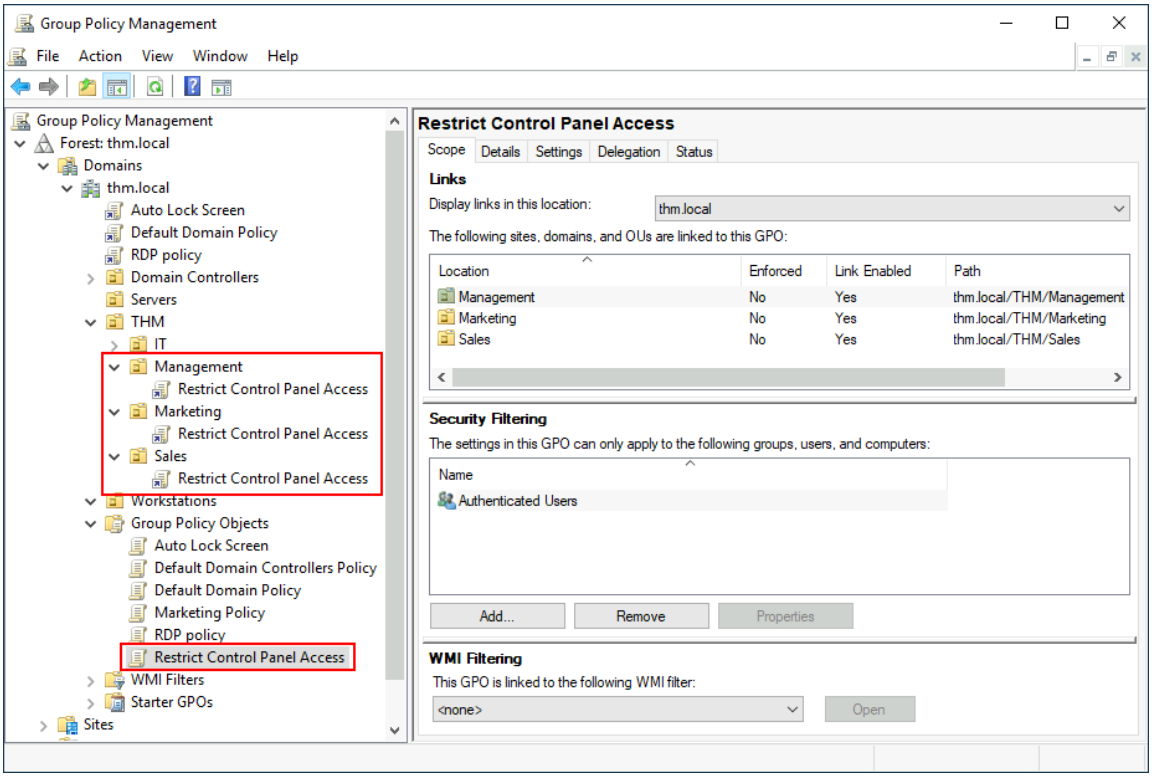
Creating GPOs

Creating a GPO called - **Restrict Control Panel Access**

- Create a GPO named - Restrict Control Panel Access.
- Right click on the GPO and open it for editing.
- Click on the *User Configuration* option as we want to apply this GPO to specific users.



- After that enable the “Prohibit Access to Control Panel and PC Settings”.
- Once the GPO is configured, we will need to link it to all of the OUs corresponding to users who shouldn't have access to the Control Panel of their PCs.
- Here, we will link the non-IT department i.e. **Marketing, Management** and **Sales** OUs by dragging the GPO to each one of them.



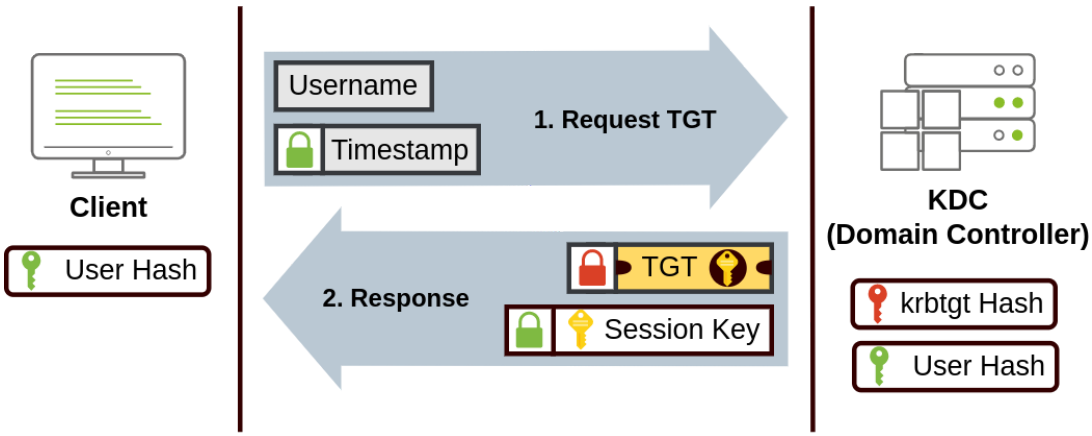
Authentication Methods

- All the credentials are stored in DCs while using Windows Domains.
- Two protocols can be used for network authentication in Windows domains:
  - **Kerberos:** Default protocol in any recent domain. Used by recent version of Windows.
  - **NetNTLM:** Legacy authentication protocol kept for compatibility purposes.
- Most networks have both protocols enabled.

Kerberos Authentication

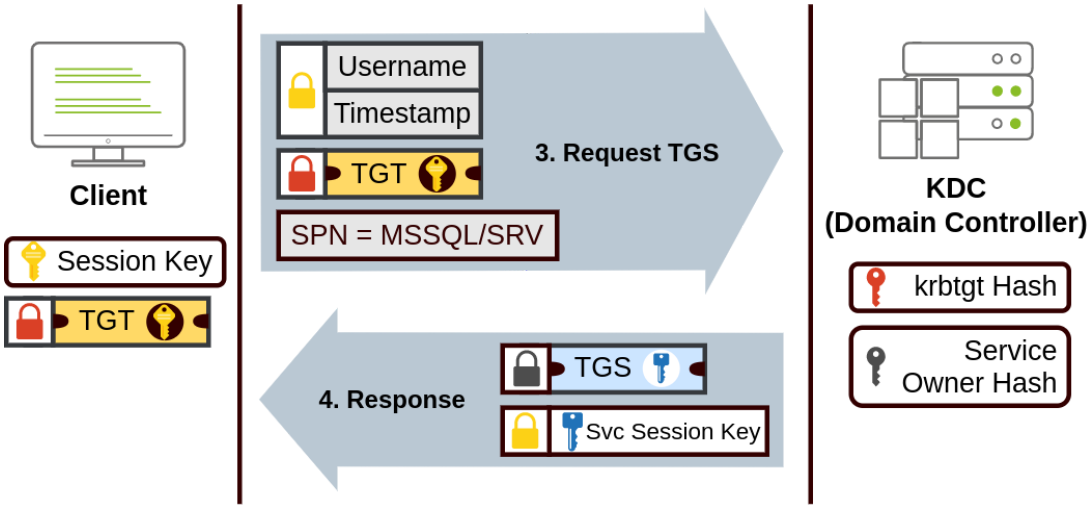
- Default authentication protocol for any recent version of windows.
- Users who log into a service using Kerberos are assigned tickets.
- Users with tickets can present them to a service to demonstrate they have already authenticated into the network.
- When Kerberos is used for authentication, the following process happens:

- User sends their username and a timestamp encrypted using a key derived from their password to the **Key Distribution Center (KDC).**
- KDC is a service usually installed on the Domain Controller in charge of creating Kerberos tickets on the network.
- The KDC creates and sends back a **Ticket Granting Ticket (TGT)**
- This allows users to request additional tickets to access specific services without passing their credentials every time they want to connect to a service.
- Along with the TGT, a **Session Key** is given to the user, which they need to generate the following requests.
- The TGT is encrypted using the **krbtgt** account's password hash, and therefore the user can't access its contents.
- The encrypted TGT includes a copy of the Session Key as a part of its contents.
- The KDC has no need to store the Session Key as it can recover a copy by decrypting the TGT if needed.

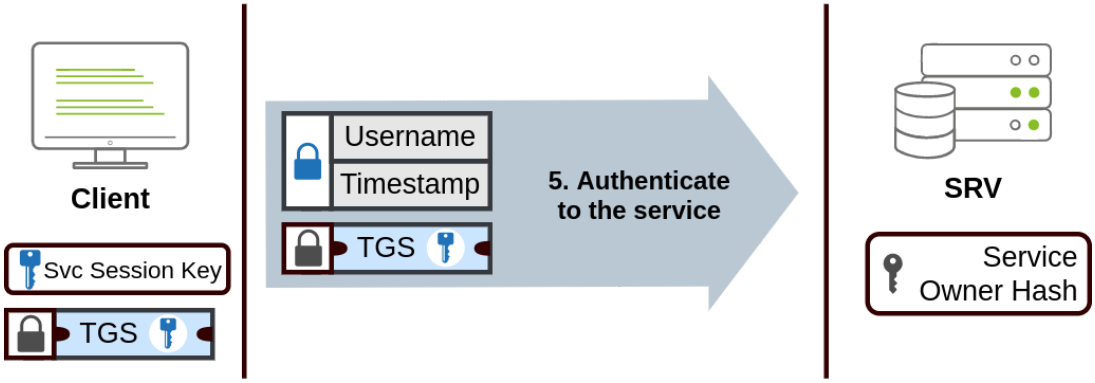


- When a user wants to connect to a service on the network like a share, website or database, they use their TGT to ask the KDC for a **Ticket Granting Service (TGS).**
- TGS are tickets that allow connection only to the specific service they were created for.
- To request a TGS, the user sends their username and a timestamp encrypted using the Session Key, along with the TGT and a **Service Principal Name (SPN).**

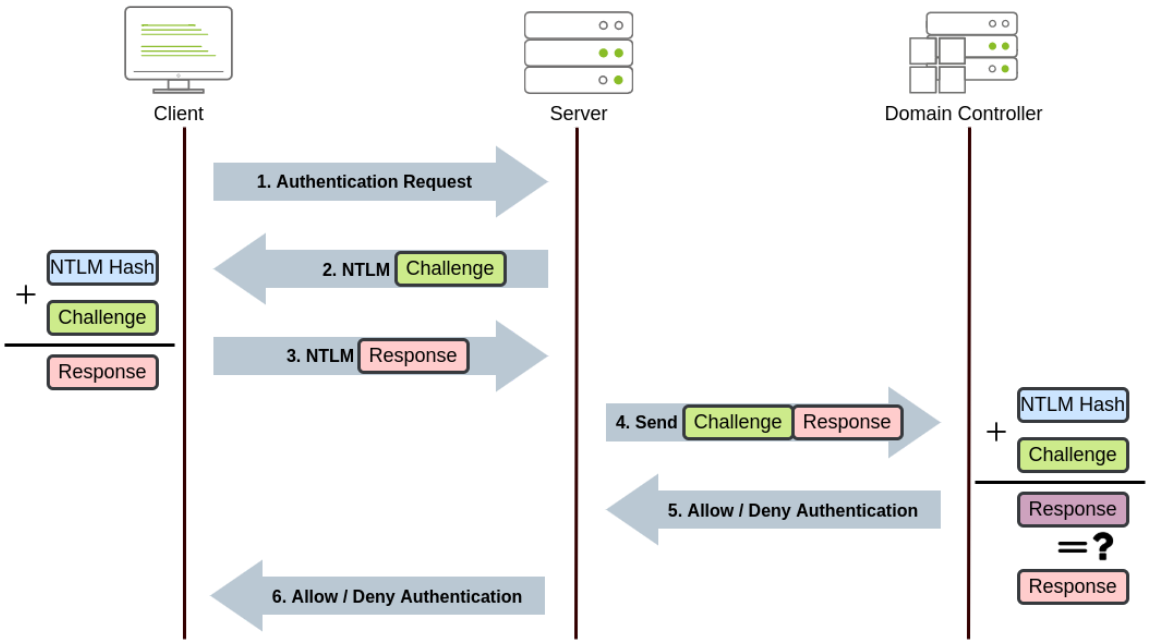
- SPN indicates the service and the server name we intend to access.
- The KDC will send us a TGS along with a **Service Session Key,** which we will need to authenticate to the service we want to access.
- The TGS is encrypted using a key derived from the **Service Owner** Hash.
- The Service Owner is the user or machine account that the service runs under.
- 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.



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



NetNTLM Authentication



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.

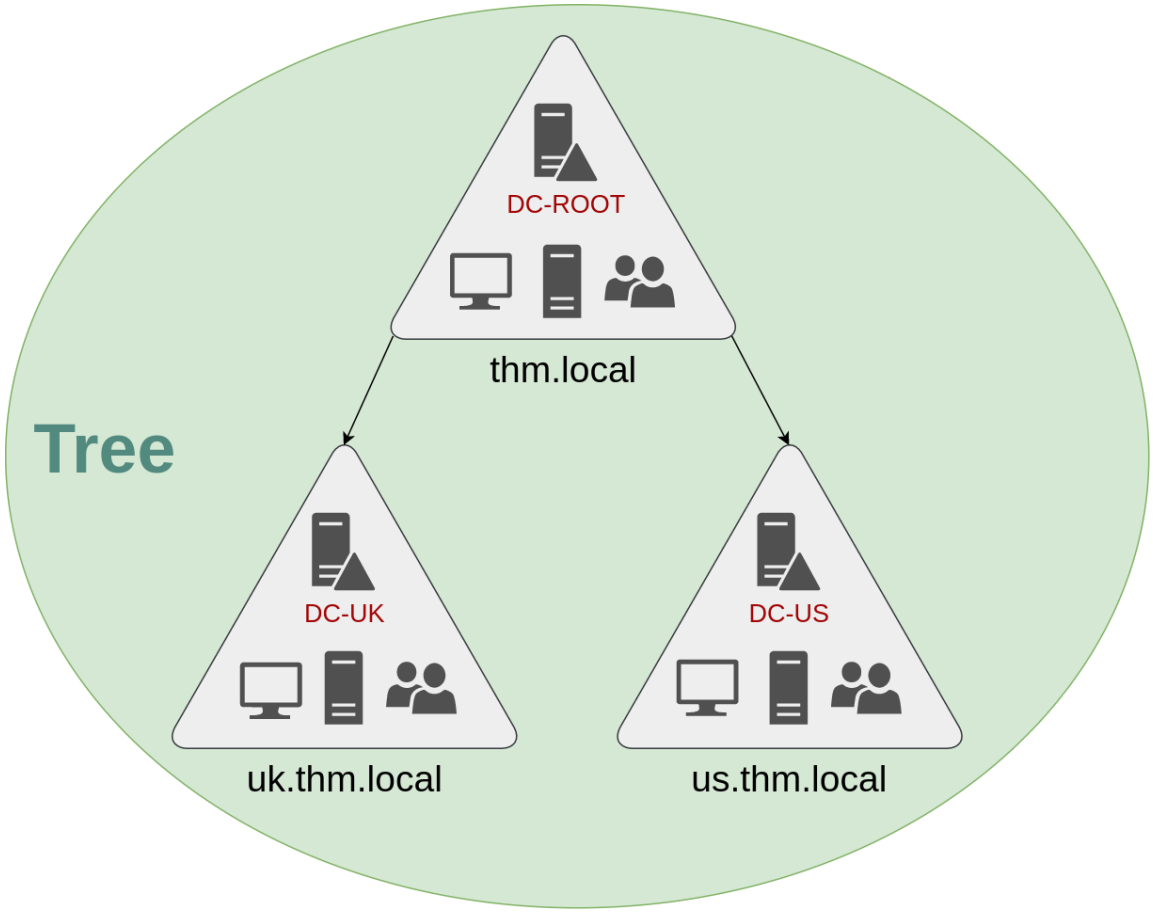
- The user's password (or hash) is never transmitted through the network for security.
- The described process in the above image applies when using a domain account.
- If a local account is used, the server can verify the response to the challenge itself without requiring interaction with the domain controller since it has the password hash stored locally on its SAM.

Trees, Forests and Trusts

Trees

- Active Directory supports integrating multiple domains so that you can partition your network into units that can be managed independently.

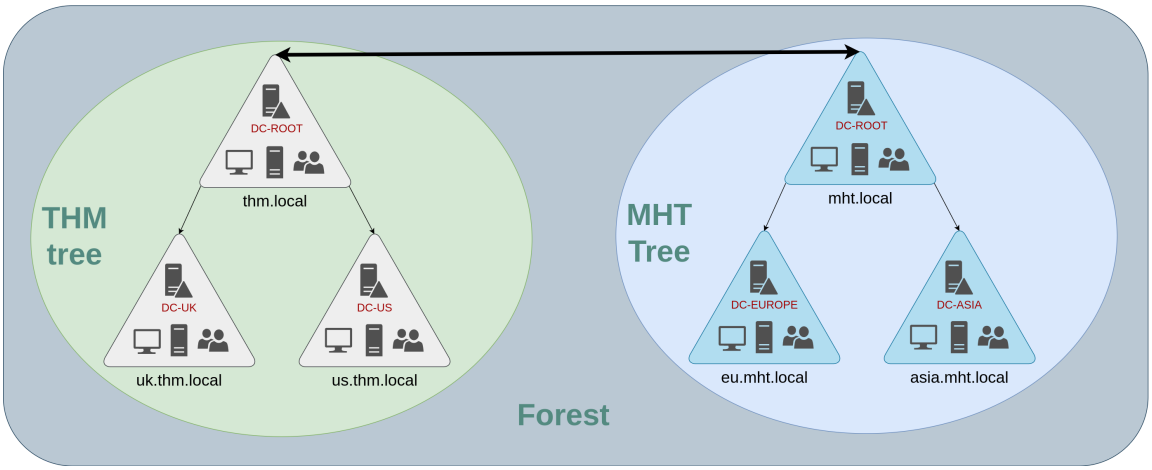
- If you have two domains that share the same namespace (`thm.local` in our example), those domains can be joined into a **Tree.**
- If our `thm.local` domain was split into two subdomains for UK and US branches, we could build a tree with a root domain of `thm.local` and two subdomains called `uk.thm.local` and `us.thm.local` each with its AD, computers and users.



- The Domain Administrators of each branch will have complete control over their respective DCs, but not other branches' DCs.
- Policies can also be configured independently for each domain in the tree.
- A new security group **Enterprise Admins** group will grant a user administrative privileges over all of an enterprise's domains.
- Each domain would still have its Domain Admins with administrator privileges over their single domains.
- The Enterprise Admins can control everything in the enterprise.

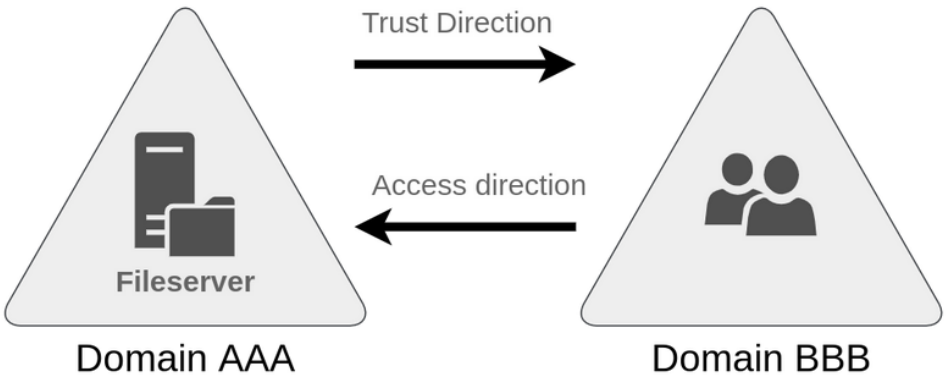
Forests

- The domains we manage, can also be configured in different namespaces.
- The union of several trees with different namespaces into the same network is known as a **forest.**



Trust Relationships

- Suppose a user at THM UK might need to access a shared file in one of MHT ASIA servers.
- For this to happen, domains arranged in trees and forests are joined together by **trust relationships**.
- Having a trust relationship between domains allows you to authorise a user from domain `THMUK` 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 authorized to access resources on AAA.



- **Two-way trust relationships** can also be made to allow both domains to mutually authorize users from the other.
- Having a trust relationship between domains doesn't automatically grant access to all resources on other domains.
- Once a trust relationship is established, we have the chance to authorize users across different domains.
- It’s up to us what is actually authorized or not.