3M2A

TEST, PROTECT, DEFEND

Active Directory Basics Room

Team members

Name	Phone	Email	LinkedIn
Mohamed Tamer	01098851920	mohamedtamer493@gmail.com	Mohamed Tamer
Mohamed Taha	01157504940	motahakhatttab98@gmail.com	Mohamed Khattab
Abdelrahman Nabil	01155642227	abdo12232000@gmail.com	Abdelrahman Nabil
Amr Abdelkhaleq	01065596524	amrkhaled78782@gmail.com	Amr Abdelkhalek
Mohamed Akram	01211075035	ma987236@gmail.com	Mohamed Akram

Task 1: Introduction

What Active Directory is

Active Directory (AD) is a directory service developed by Microsoft for managing and organizing resources in a networked environment, such as computers, users, and services. It is a key component of Windows Server operating systems and is commonly used in enterprise networks. Here's how it works:

Key Features of Active Directory:

1. **Centralized Management**: AD allows administrators to manage users, computers, and other resources in a centralized way, making it easier to enforce security policies and control access.
2. **Domain Services**: Active Directory Domain Services (AD DS) is the core service that stores information about network objects and makes it available to administrators and users. It organizes objects like users, groups, and computers into a hierarchical structure.
3. **Authentication and Authorization**: AD provides authentication (verifying users' identities) and authorization (controlling what users are allowed to access). It supports protocols like Kerberos for secure authentication.
4. **Group Policies**: AD allows administrators to use Group Policy to configure security settings and other policies across all computers and users in the domain. This helps standardize and enforce security measures.
5. **Organizational Units (OUs)**: These are containers within AD where you can group users, computers, and other resources. OUs help organize resources logically and apply policies at different levels.
6. **Active Directory Federation Services (ADFS)**: AD can also be extended with ADFS to provide Single Sign-On (SSO) capabilities, allowing users to access multiple applications with a single login.
7. **Replication**: AD uses replication to ensure that all domain controllers (servers that host AD services) within the network have the same information, providing redundancy and fault tolerance.

What an Active Directory Domain

An **Active Directory Domain** is a logical grouping of objects such as users, computers, printers, and other resources within a network that are managed and governed by **Active Directory Domain Services (AD DS)**. Domains are used to centralize administration and security across an organization's network.

Key Concepts of an Active Directory Domain:

1. **Centralized Management**: A domain allows administrators to manage all the resources and security policies from a single point, rather than managing each resource individually.
2. **Domain Controllers (DCs)**: A domain is controlled by servers called **Domain Controllers**. These DCs hold the Active Directory database, which stores all the information about objects in the domain, and are responsible for authentication and authorization within the domain.
3. **Authentication**: Users within a domain can access resources such as files, applications, and network printers based on their domain credentials. **Single Sign-On (SSO)** is a key benefit, as users need only one set of credentials to access multiple resources within the domain.
4. **Namespace**: Every domain has a unique namespace, typically in the format of a DNS name like example.com or corp.local. The domain name is used to identify and access the resources within that domain.
5. **Trust Relationships**: Domains can be linked together using **trust relationships**, allowing users in one domain to access resources in another domain, as long as appropriate permissions are set up.
6. **Security Boundaries**: A domain serves as a security boundary. All objects in the domain are subject to domain-wide security policies, and administrators have full control over access and permissions within their domain.
7. **Organizational Units (OUs)**: Inside a domain, objects like users and computers can be further organized into **Organizational Units (OUs)** for more granular management. OUs allow the application of different group policies and administrative delegation within the domain.

What components go into an Active Directory Domain

An **Active Directory Domain** is made up of several key components that work together to manage and organize network resources, security, and access control. Below are the core components that go into an Active Directory Domain:

1. Domain Controllers (DCs):

- **Domain Controllers** are servers that run Active Directory Domain Services (AD DS) and store the directory database. They handle **authentication**, **authorization**, and apply security policies across the domain.
- **Primary Domain Controller (PDC) Emulator**: A specialized DC that handles time synchronization, password changes, and serves as the authoritative source for managing certain legacy features in AD.
- **Global Catalog (GC)**: A DC that contains a partial, read-only replica of all objects in the forest, enabling faster searches across domains.

2. Active Directory Database (NTDS.DIT):

- This is the main database that stores all the information about users, computers, groups, and other objects in the domain. It is stored on Domain Controllers and replicates across all DCs in the domain.

3. Objects:

- Active Directory is object-oriented, meaning it stores various resources as **objects**. Each object has properties (attributes) and is classified into the following main types:
  - **User Objects**: Represent user accounts within the domain. These accounts are used to authenticate and authorize users.
  - **Computer Objects**: Represent workstations or servers that are part of the domain.
  - **Group Objects**: Collections of users, computers, or other groups. Groups are used to simplify permissions management.
  - **Printers and Other Resources**: Devices like printers, which are also treated as objects within the domain.

4. Organizational Units (OUs):

- OUs are **containers** used to group objects (such as users, computers, and groups) within a domain. They help in delegating administrative control and organizing resources logically.
- OUs enable the application of **Group Policy** settings at different levels within the domain, which allows for more granular management of policies.

5. Domain Name System (DNS):

- Active Directory relies on DNS for domain name resolution. Each domain must have a corresponding **DNS namespace** (e.g., example.com).
- **SRV Records**: Special DNS records used to locate services like Domain Controllers and Global Catalog servers.

6. Global Catalog (GC):

- A **Global Catalog** is a distributed data repository that contains a partial, read-only replica of all objects in the forest. It allows users and applications to search for objects across multiple domains within the same Active Directory forest.

7. Trust Relationships:

- Trusts are connections between two domains that allow for **resource sharing**. Trust relationships enable users from one domain to access resources in another domain.
    - **Two-way Trust**: Both domains trust each other.
    - **One-way Trust**: One domain trusts the other, but not vice versa.
    - **Transitive Trust**: Trust relationships that are automatically extended to other trusted domains.

8. Group Policy:

- **Group Policy Objects (GPOs)** are collections of settings that administrators can apply to users and computers across the domain. GPOs allow the configuration of security settings, software installations, and user environments in a consistent way across the network.

9. Security Principals:

- These are the **users**, **groups**, or **computer objects** that can be granted access to resources. Security principals are identified using **Security Identifiers (SIDs)**, which are unique IDs used in security permissions.

10. Sites:

- **Sites** represent the physical topology of the network. They are used to manage replication traffic and define the **network locations** of Domain Controllers. A site typically corresponds to a physical location, like a branch office.
- **Site Links** are used to define how replication occurs between Domain Controllers in different sites.

11. Replication:

- Active Directory uses **multi-master replication** to ensure that changes made on one Domain Controller are replicated to all other Domain Controllers within the domain or forest.
- Replication ensures consistency across DCs, so that all changes (like user account updates or policy changes) are propagated throughout the domain.

12. Forest and Trees:

- A **forest** is the top-level logical container in an Active Directory environment. It contains one or more domains that share a common schema and Global Catalog.
- A **tree** is a group of domains that share a contiguous namespace (e.g., corp.example.com and hr.corp.example.com).

13. LDAP (Lightweight Directory Access Protocol):

- Active Directory uses **LDAP** as the primary protocol to access and manage directory information. LDAP allows querying and modifying the AD database and is key to how applications interact with AD.

Forests and Domain Trust

Forests in Active Directory:

A **forest** is the highest-level logical container in an Active Directory environment. It serves as the **security and administrative boundary** that contains one or more domains, which share a common configuration, schema, and Global Catalog. Here's a breakdown:

Key Features of a Forest:

1. **Common Schema**: All domains in a forest share the same schema, which defines the object classes and their attributes within Active Directory (e.g., users, computers).
2. **Global Catalog (GC)**: Each forest has a Global Catalog that contains a partial replica of all objects in all domains within the forest, enabling users to search for objects across the entire forest.
3. **Transitive Trust**: Trust relationships between domains within a forest are **automatically transitive**, meaning a user in one domain can potentially access resources in another domain, provided they have the necessary permissions.
4. **Autonomy and Isolation**: Each forest is independent of other forests. While domains within a forest can have trust relationships, forests themselves do not inherently trust each other (though this can be configured via **forest trusts**).
5. **Schema Partition**: The forest contains a single **schema partition**, which is a master set of definitions for the types of objects and attributes in all domains of the forest.
6. **Forest Root Domain**: The first domain created in the forest is called the **forest root domain**. It is at the top of the hierarchy and often contains the administrative accounts used to manage the forest.

Forest Hierarchy:

- **Single-Domain Forest**: A forest can consist of a single domain (simpler to manage).
- **Multi-Domain Forest**: In larger organizations, multiple domains can exist within a single forest, but they share the same schema and Global Catalog.

Domain Trusts in Active Directory:

A **trust relationship** in Active Directory is a connection established between domains to allow users from one domain to access resources in another domain. Trusts can be set up within the same forest (between domains) or between separate forests.

Types of Trusts:

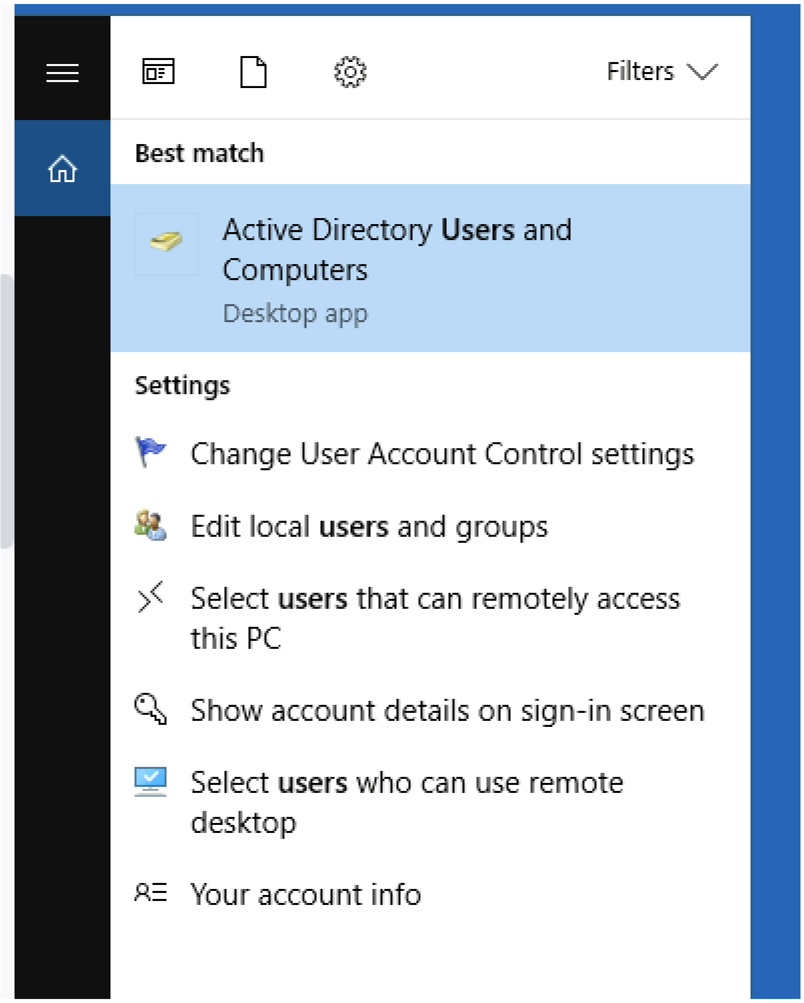
1. **Parent-Child Trust**:
   - Automatically established when a new child domain is created within a parent domain (e.g., corp.com and child.corp.com).
   - **Transitive**, meaning access can be extended beyond just the two domains in question (e.g., if corp.com trusts child.corp.com, child.corp.com can also trust other domains that corp.com trusts).
2. **Tree-Root Trust**:
   - Automatically created between the root domains of two domain trees within the same forest (e.g., corp.com and sales.com).
   - **Transitive** and enables trust between all domains in the two trees.
3. **External Trust**:
   - A **non-transitive** trust created between domains in different forests or between an Active Directory domain and a non-Active Directory domain (e.g., Windows NT domains).
   - Only the two domains explicitly involved in the trust have access to each other’s resources.
4. **Forest Trust**:
   - A **transitive trust** between the root domains of two different forests. It allows all domains in one forest to trust all domains in another forest.
   - This is useful for merging or collaborating between organizations with separate forests.
5. **Shortcut Trust**:
   - A **two-way trust** created between domains in the same forest to reduce authentication time. This is typically used in large forests with many domains where traversing through parent-child relationships would take too long.
6. **Realm Trust**:
   - A trust created between an Active Directory domain and a **Kerberos V5 realm** in a UNIX or other non-Windows environment.
7. **One-Way Trust**:
   - A trust where **only one domain trusts the other**, meaning that users in the trusted domain can access resources in the trusting domain, but not vice versa.
8. **Two-Way Trust**:
   - A mutual trust where **both domains trust each other**. Users in both domains can access resources across both domains (depending on permissions).

Task 2: Windows Domains

Question 1: In a Windows domain, credentials are stored in a centralized repository called.
Answer: Active Directory

Question 2: The server in charge of running the Active Directory services is called.
Answer: Domain Controller

Task 3: Active Directory



Filters

Best match

Active Directory Users and Computers
Desktop app

Settings

Change User Account Control settings

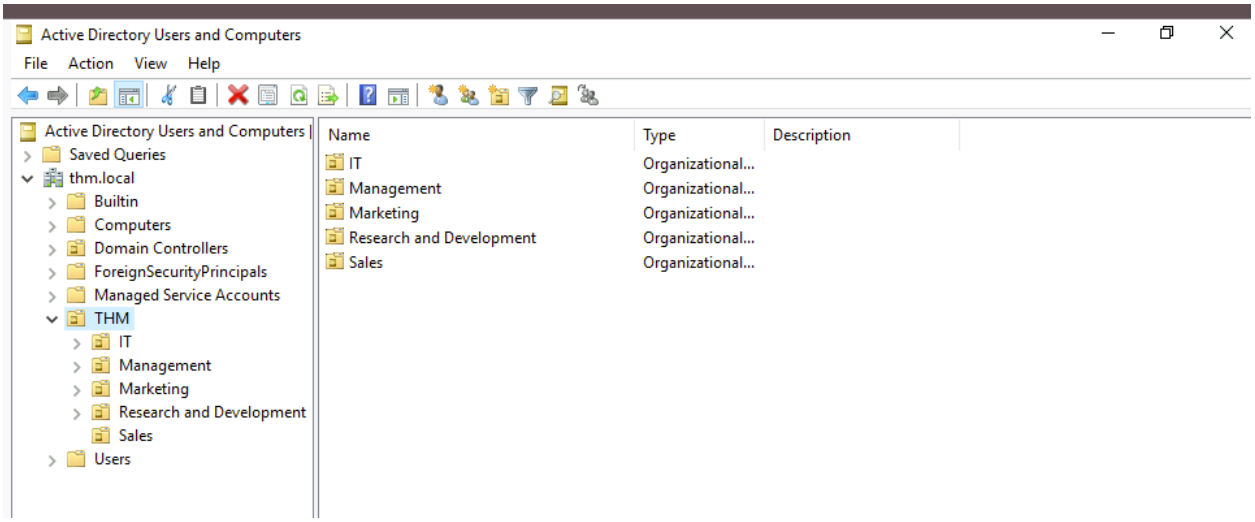
Edit local users and groups

Select users that can remotely access this PC

Show account details on sign-in screen

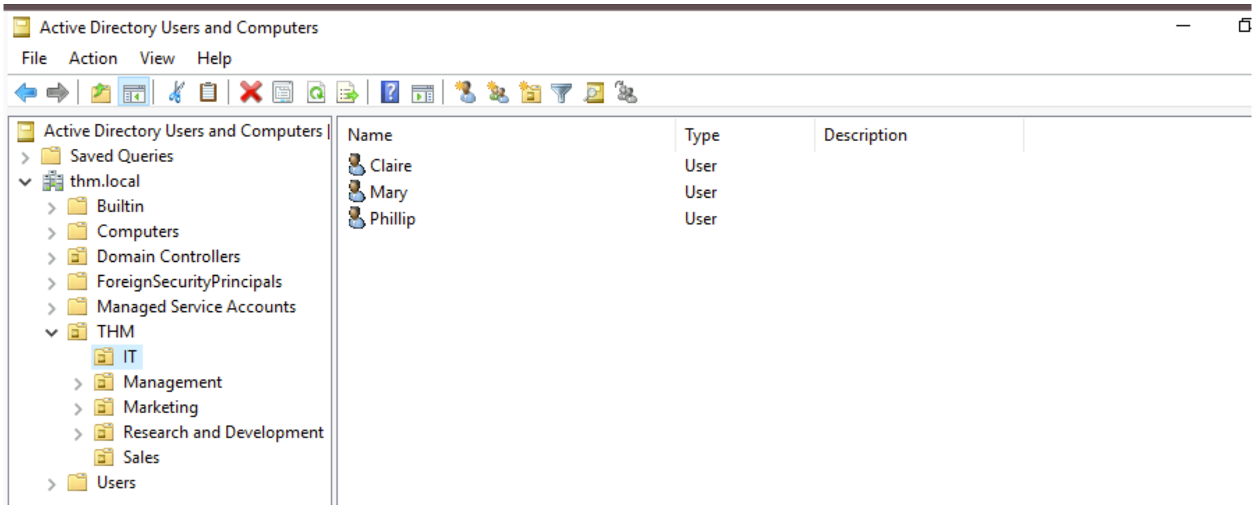
Select users who can use remote desktop

Your account info



- Active Directory Users and Computers
  - Saved Queries
  - thm.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - THM
      - IT
      - Management
      - Marketing
      - Research and Development
      - Sales
    - Users

Name	Type	Description
IT	Organizational...	
Management	Organizational...	
Marketing	Organizational...	
Research and Development	Organizational...	
Sales	Organizational...	



- Active Directory Users and Computers
  - Saved Queries
  - thm.local
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - THM
      - IT
      - Management
      - Marketing
      - Research and Development
      - Sales
    - Users

Name	Type	Description
Claire	User	
Mary	User	
Phillip	User	

Question 1: Which group normally administrates all computers and resources in a domain?
Answer: Domain Admins

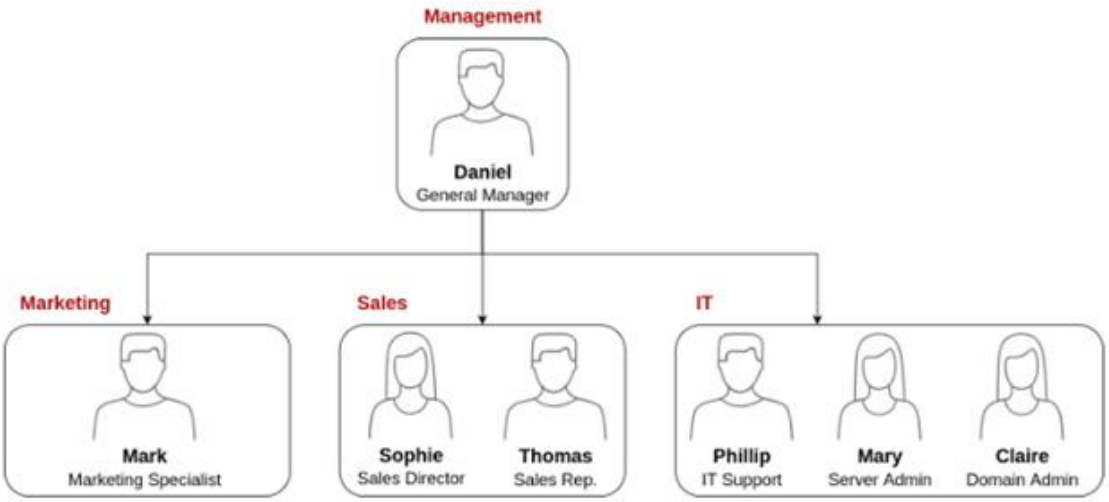
Question 2: What would be the name of the machine account associated with a machine named TOM-PC?
Answer: TOM-PC$

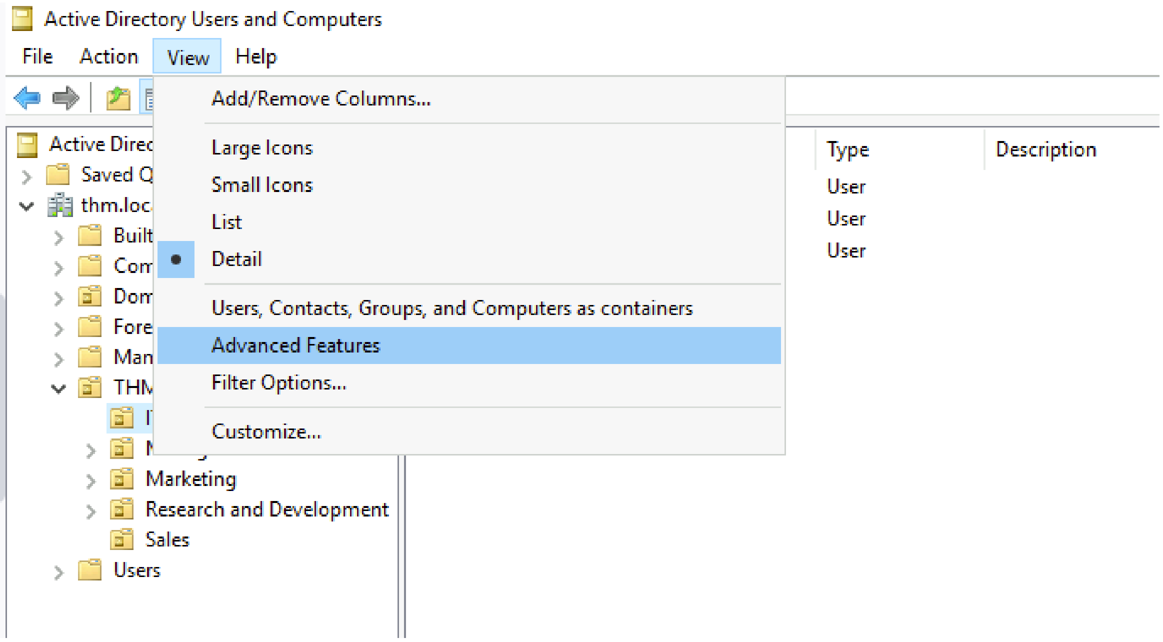
Question 3: Suppose our company creates a new department for Quality Assurance. What type of containers should we use to group all Quality Assurance users so that policies can be applied consistently to them?
Answer: Organizational Units

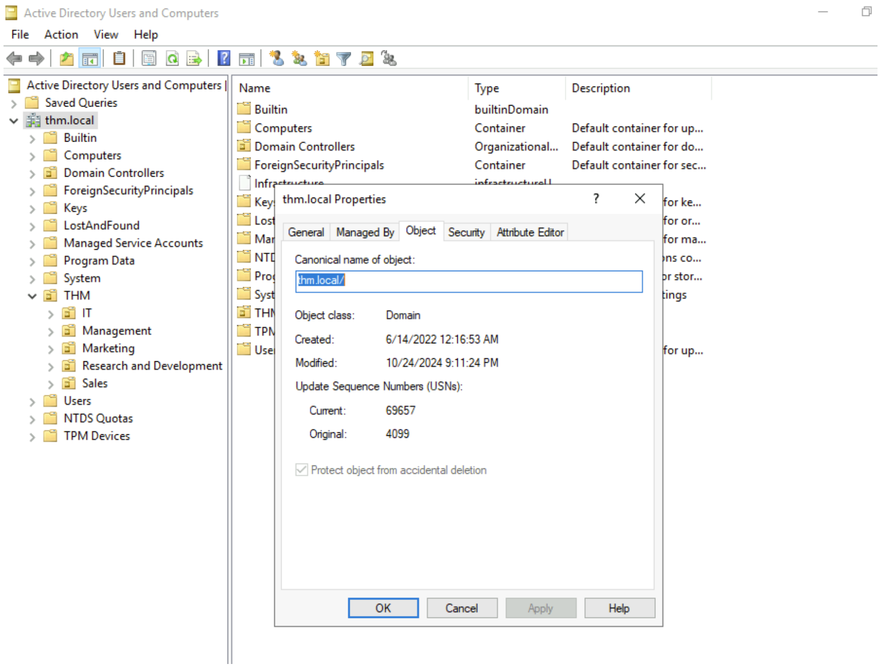
Task 4:

Question 1: What was the flag found on Sophie's desktop?
Login using sophie's username and new password to get the flag.

Answer: THM{thanks_for_contacting_support}





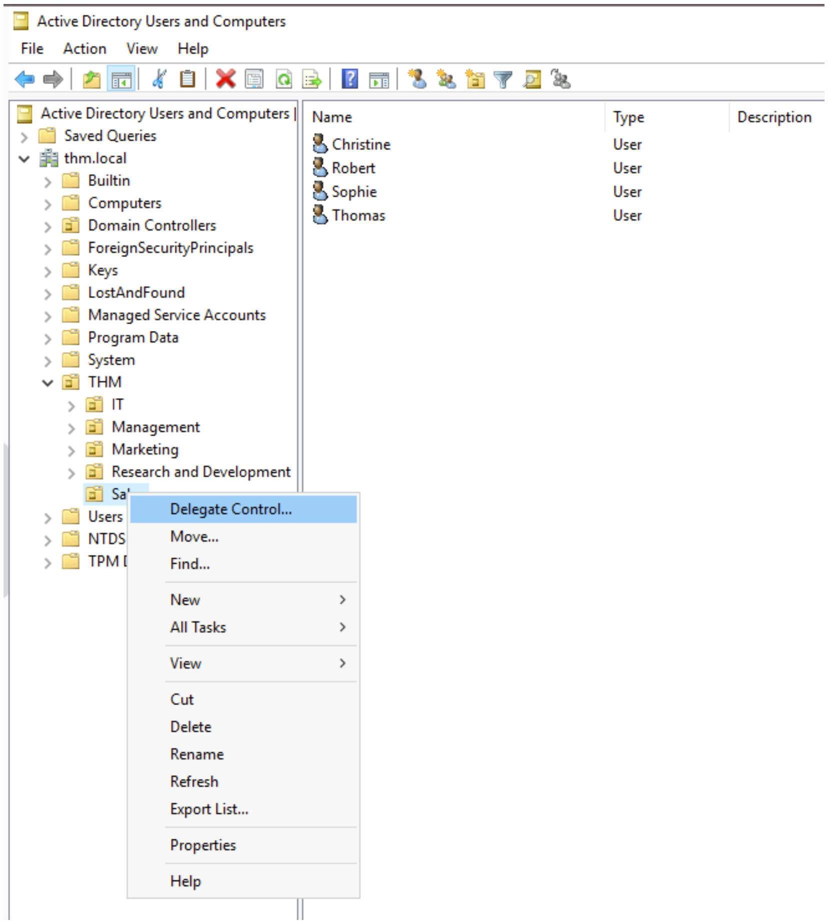


Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Controllers	Organizational...	Default container for do...
ForeignSecurityPrincipals	Container	Default container for sec...

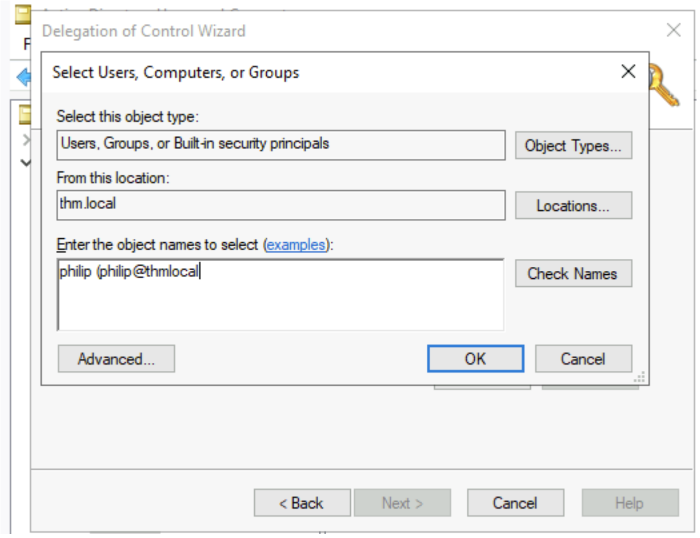
Canonical name of object:
thm.local/

Object class: Domain
Created: 6/14/2022 12:16:53 AM
Modified: 10/24/2024 9:11:24 PM
Update Sequence Numbers (USNs):
Current: 69657
Original: 4099

☑ Protect object from accidental deletion



Name	Type	Description
Christine	User	
Robert	User	
Sophie	User	
Thomas	User	



Delegation of Control Wizard
Select Users, Computers, or Groups

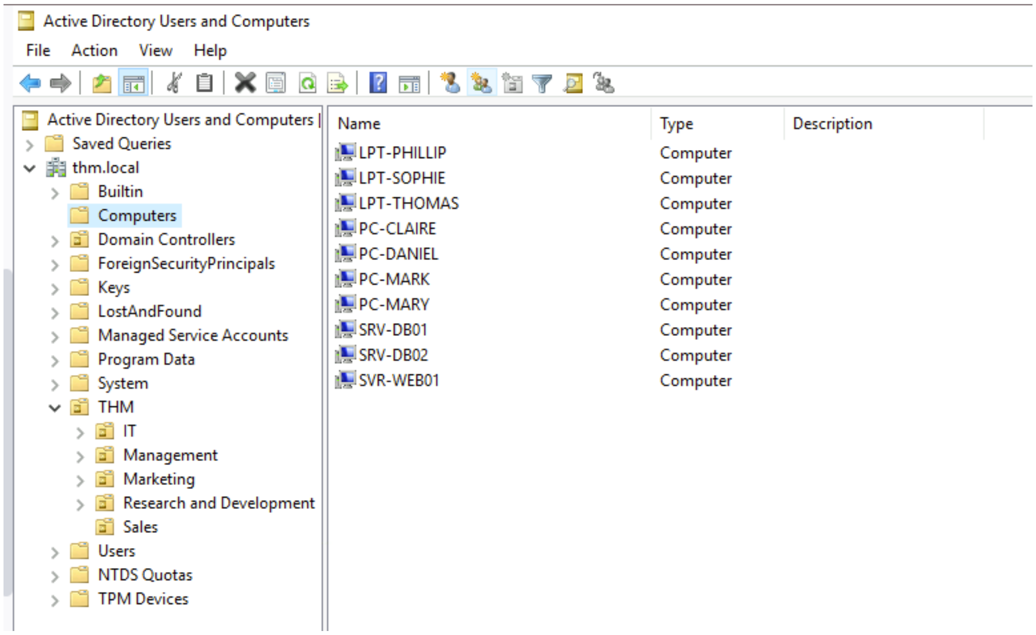
Select this object type:
Users, Groups, or Built-in security principals

From this location:
thm.local

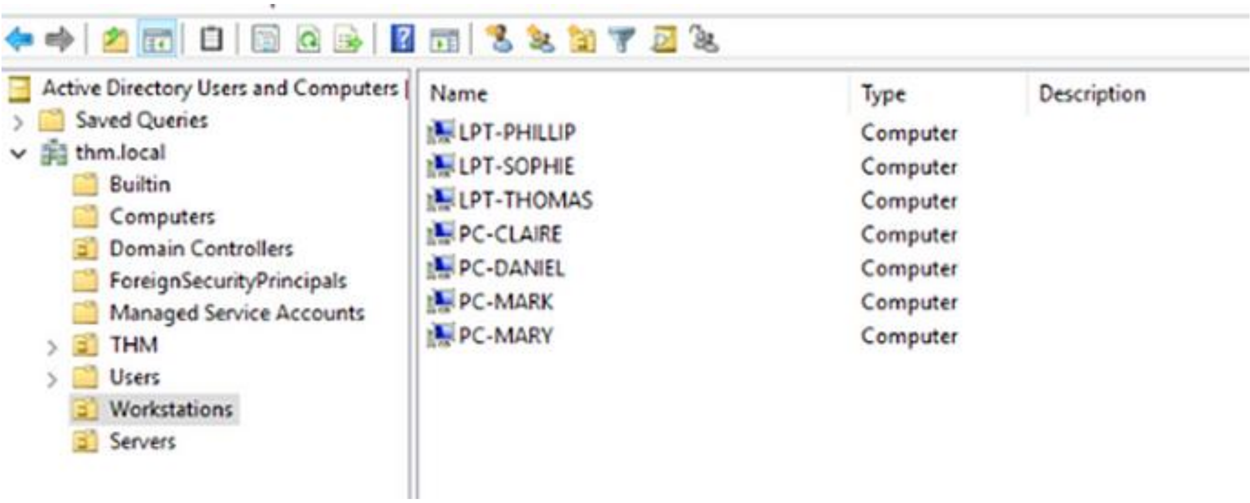
Enter the object names to select (examples):
philip (philip@thmlocal

Question 2: The process of granting privileges to a user over some OU or other AD Object is called.
Answer: Delegation

Task 5: Managing Computers in AD



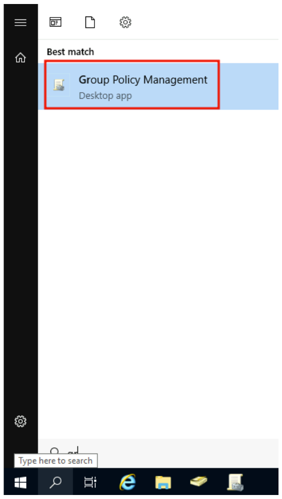
Name	Type	Description
LPT-PHILLIP	Computer	
LPT-SOPHIE	Computer	
LPT-THOMAS	Computer	
PC-CLAIRE	Computer	
PC-DANIEL	Computer	
PC-MARK	Computer	
PC-MARY	Computer	
SRV-DB01	Computer	
SRV-DB02	Computer	
SVR-WEB01	Computer	



Name	Type	Description
LPT-PHILLIP	Computer	
LPT-SOPHIE	Computer	
LPT-THOMAS	Computer	
PC-CLAIRE	Computer	
PC-DANIEL	Computer	
PC-MARK	Computer	
PC-MARY	Computer	

Question 1: After organizing the available computers, how many ended up in the Workstations OU?
Answer: 7
Question 2: Is it recommendable to create separate OUs for Servers and Workstations? (yay/nay)
Answer: yay

Task 6: Group Policies



Question 1: What is the name of the network share used to distribute GPOs to domain machines?
Answer: SYSVOL

Question 2: Can a GPO be used to apply settings to users and computers? (yay/nay)
Answer: yay

Task 7: Authentication Methods

Active Directory supports the following **authentication methods**:

1. **Kerberos**: The default protocol in AD, it uses a secure ticket-based system for authenticating users without sending passwords over the network. It ensures **mutual authentication** between client and server.
2. **NTLM (NT LAN Manager)**: A legacy protocol used when Kerberos isn't available. NTLM is less secure, relying on challenge-response mechanisms and is used mainly for backward compatibility.
3. **LDAP (Lightweight Directory Access Protocol)**: Used for querying and modifying Active Directory, LDAP supports simple authentication with username/password or Kerberos for secure binding.
4. **Smart Card Authentication**: Utilizes **multi-factor authentication** (MFA) where users provide a smart card and a PIN, enhancing security.
5. **Certificate-Based Authentication**: Uses digital certificates to authenticate users, often used for services like VPNs and wireless networks.

Each method balances security and compatibility based on the needs of the environment.

Question 1: Will a current version of Windows use NetNTLM as the preferred authentication protocol by default? (yay/nay)
Answer: nay

Question 2: When referring to Kerberos, what type of ticket allows us to request further tickets known as TGS?
Answer: Ticket Granting Ticket

Question 3: When using NetNTLM, is a user’s password transmitted over the network at any point? (yay/nay)
Answer: nay

Task 8: Trees, Forests and trusts

Question 1: What is a group of Windows domains that share the same namespace called?

Answer: Tree

Question 2: What should be configured between two domains for a user in Domain A to access a resource in Domain B?

Answer: a trust relationship