Active Directory Basics

This room will introduce the basic concepts and functionality provided by Active Directory.

Task 2 Windows Domains

Question	Answer
In a Windows domain, credentials are stored in a centralised repository called...	Active Directory
The server in charge of running the Active Directory services is called...	Domain Controller

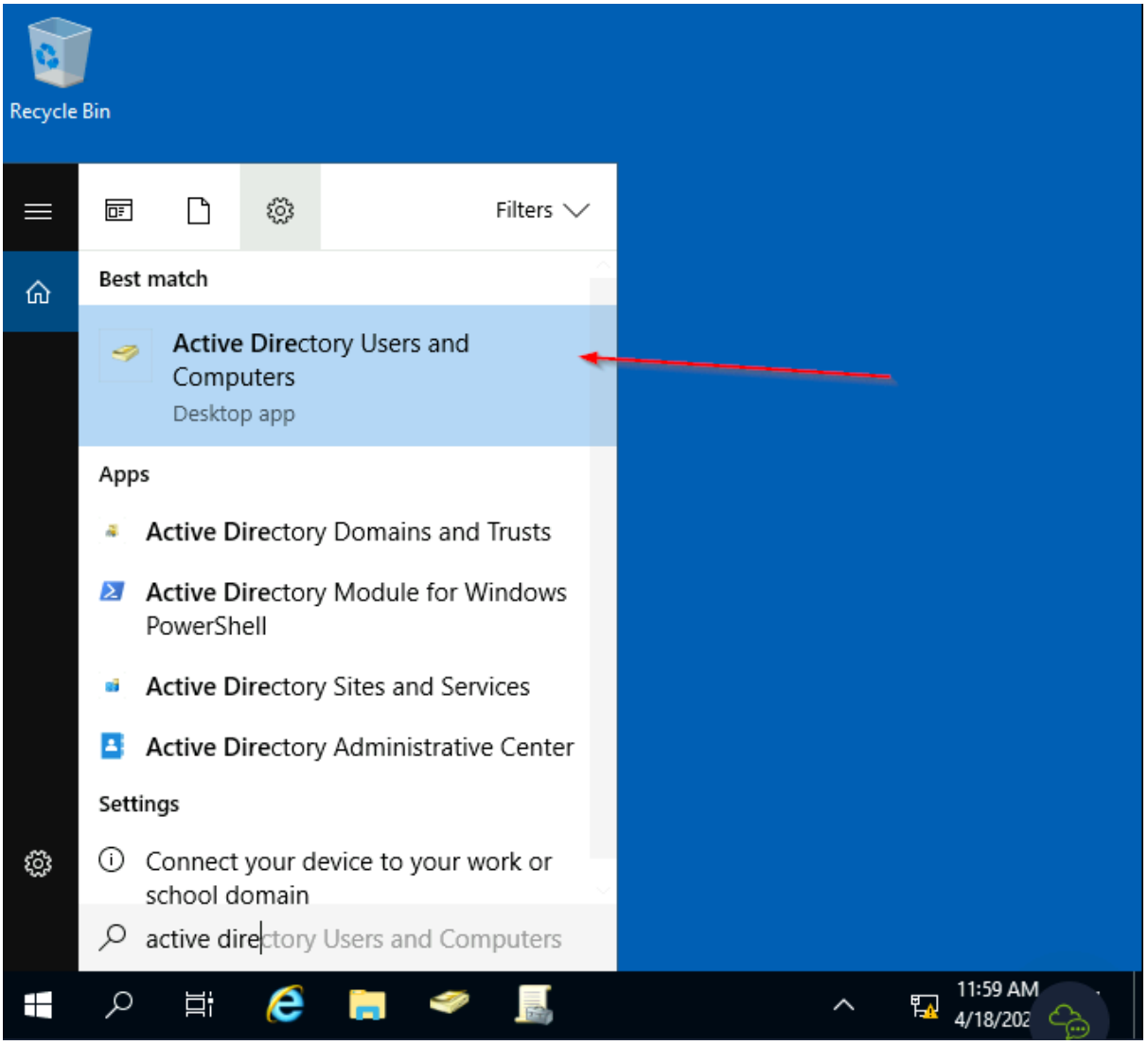
Task 3 Active Directory

Question	Answer
Which group normally administrates all computers and resources in a domain?	Domain Admins
What would be the name of the machine account associated with a machine named TOM-PC?	TOM-PC$
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?	Organizational Units

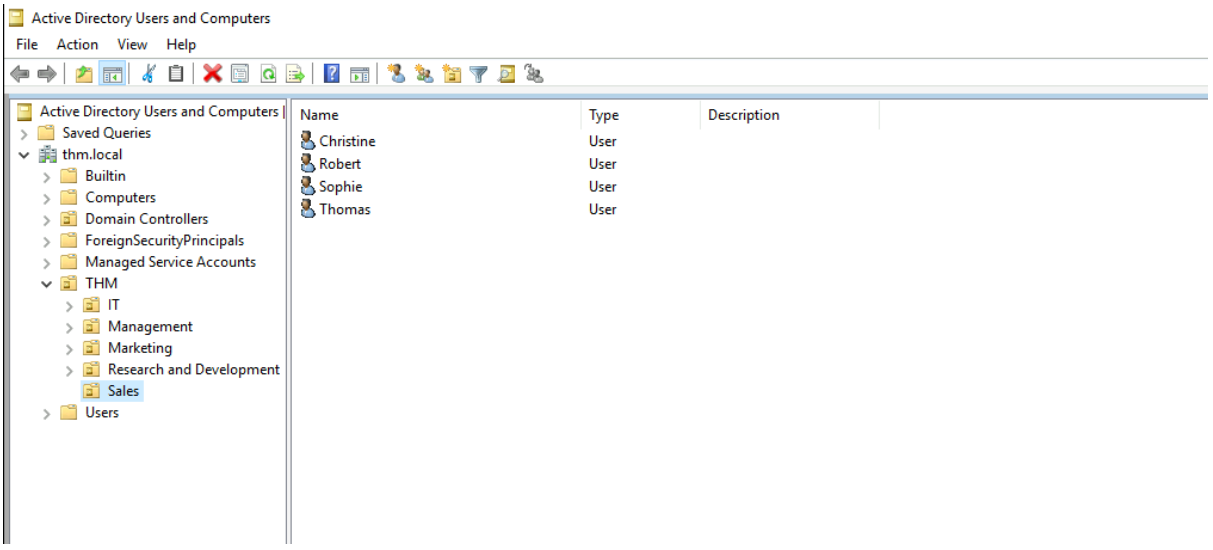
Task 4 Managing Users in AD

What was the flag found on Sophie's desktop?
Answer: **THM{thanks_for_contacting_support}**

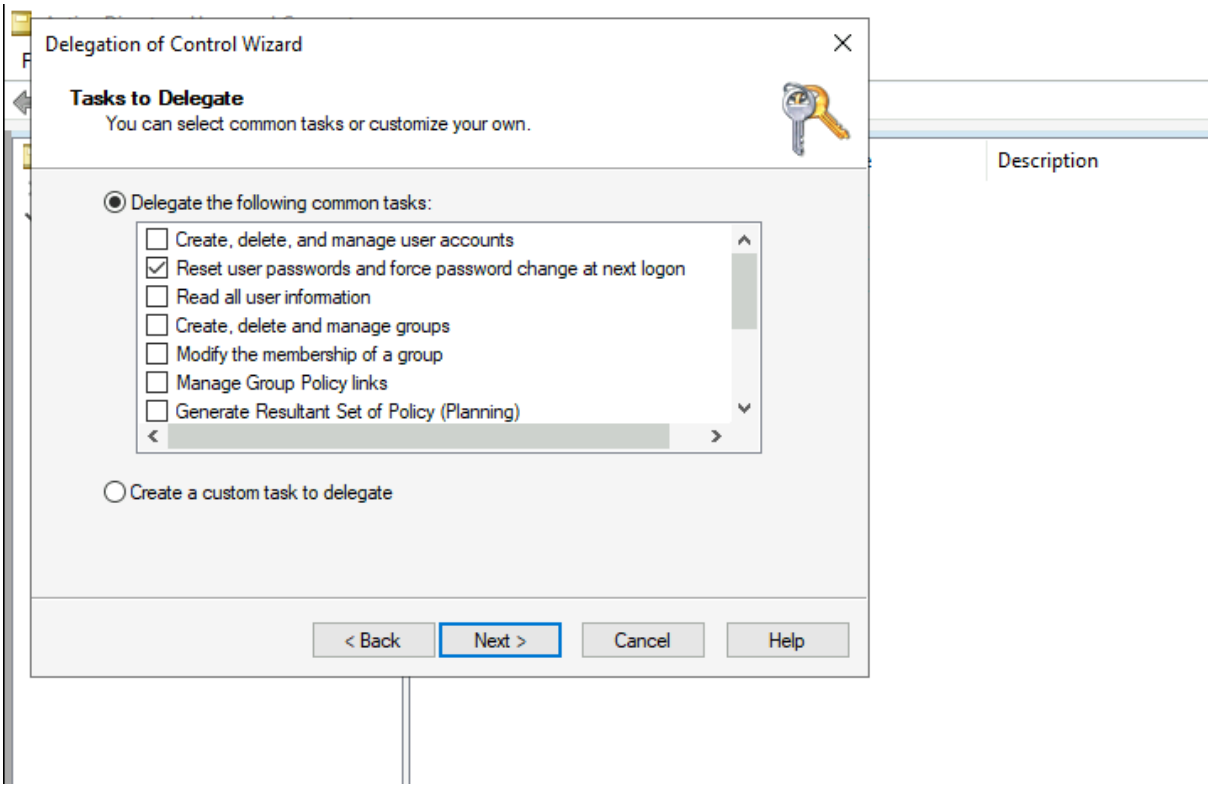
➔ I searched for “active directory” and clicked on “active directory users and computer”



➔ Here is the page it took me

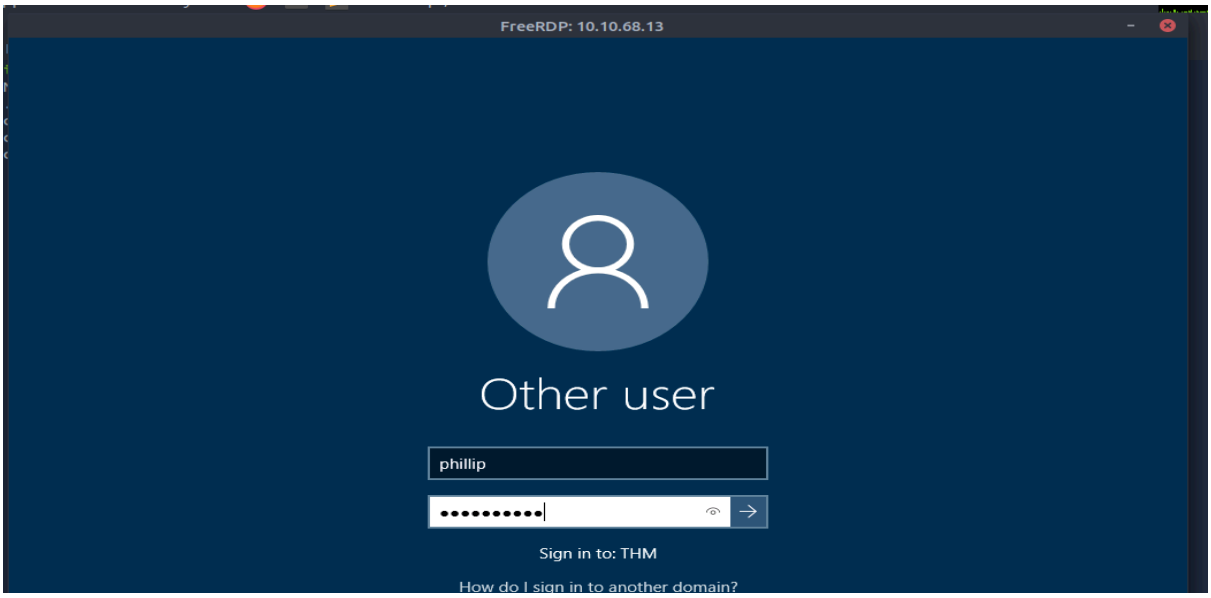


➔ I did delegation for Phillip
➔ I right clicked on sales, clicked on delegate control and followed the prompt
➔ When i got to the task to delegate,i made sure to pick that i want phillip to reset user password



➔ On my attack box,I used rdp(xfreerdp) to log into Phillip's account to try and reset Sophie's password where phillip username is phillip and password is Claire2008

Command: xfreerdp 10.10.68.13

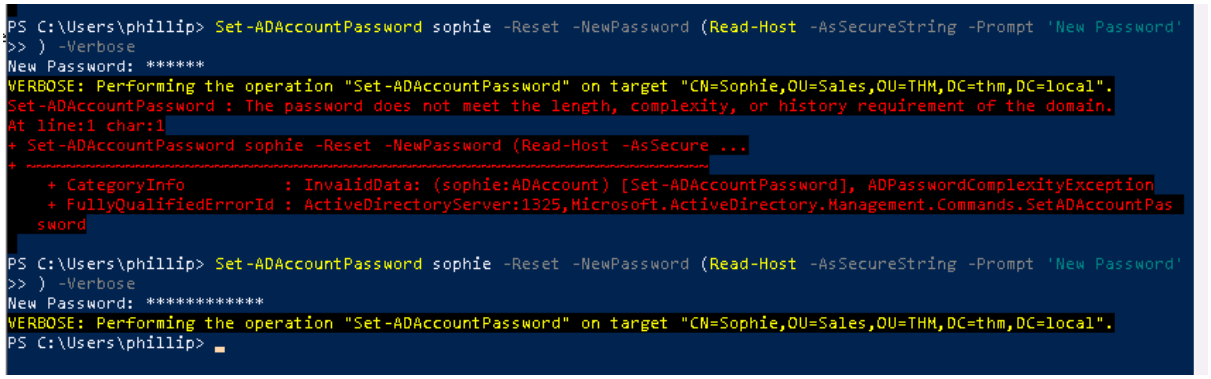


➔ Inside Phillip's account, i used the shortcut Windows logo key + S to open the search tab and clicked on powershell

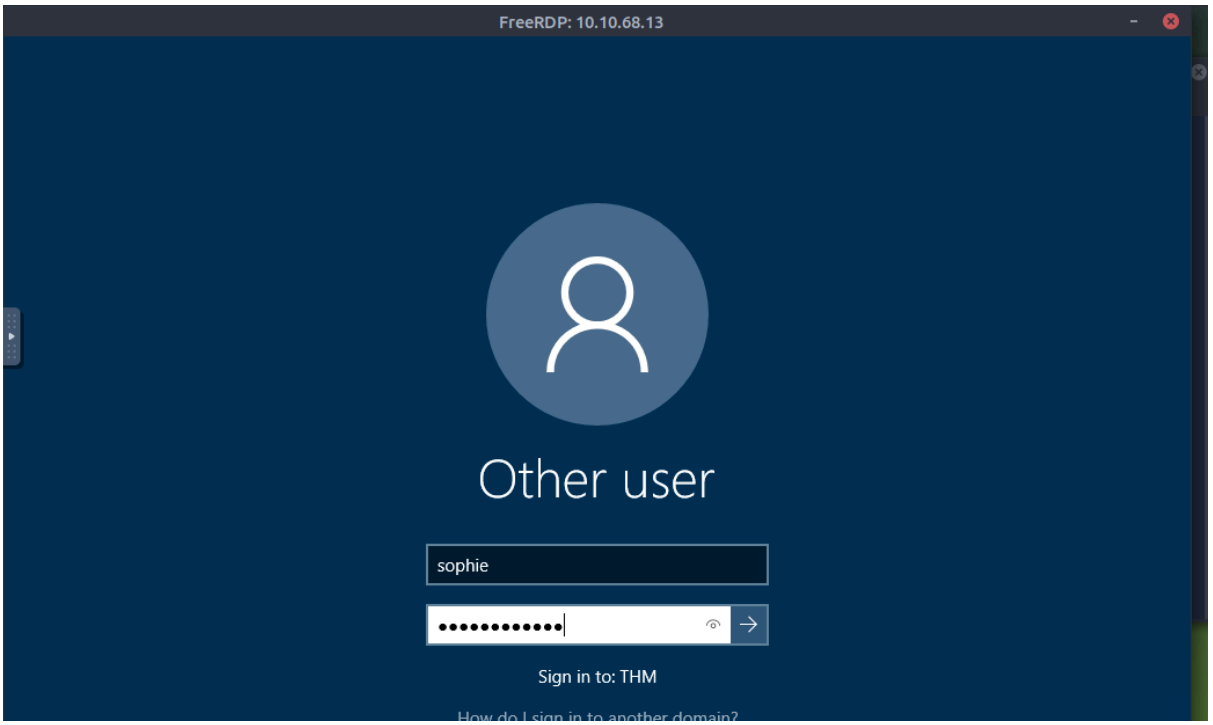
➔ Now i set Sophie password

Command: Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password') -Verbose

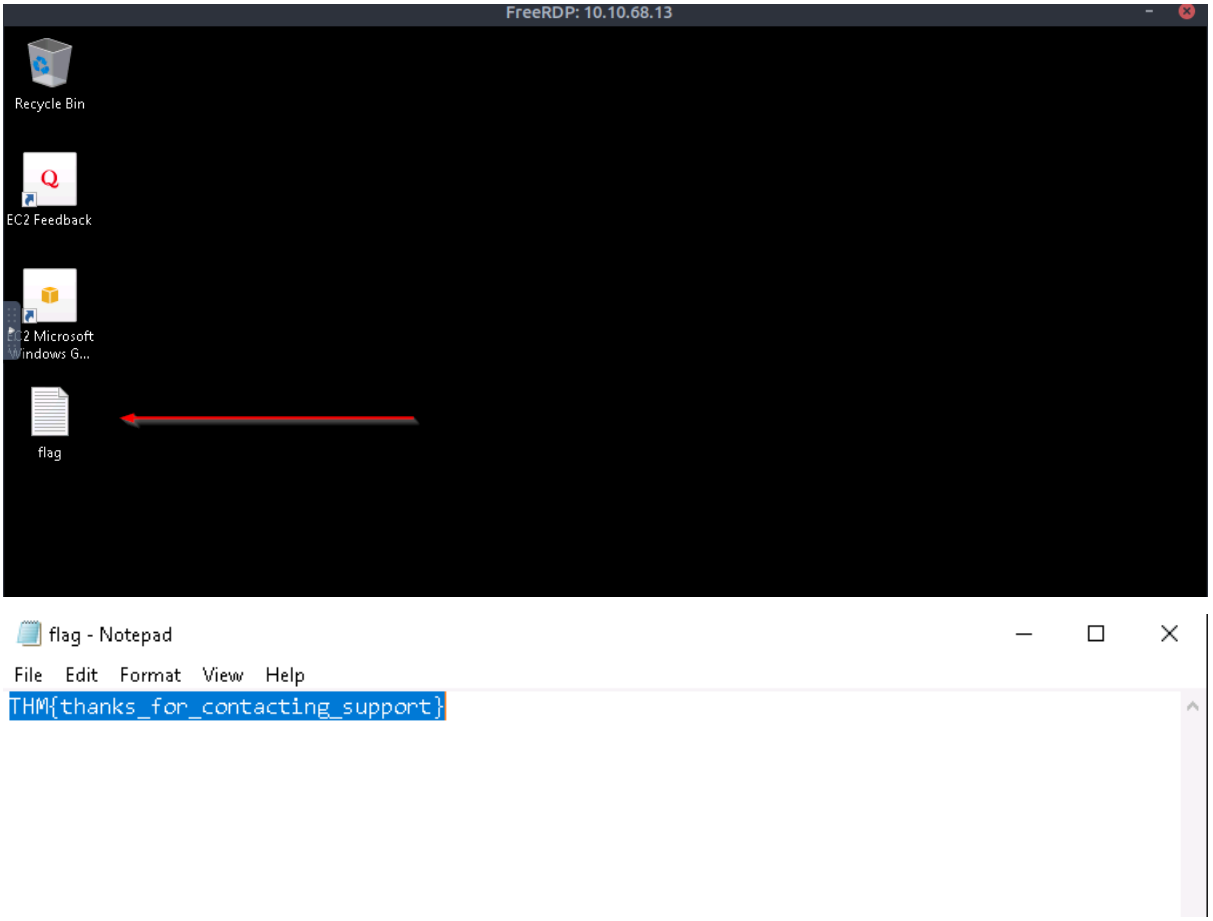
➔ Notice the password policy active?



➔ Here my password for sophie is Lovely@12345, i will rdp and login



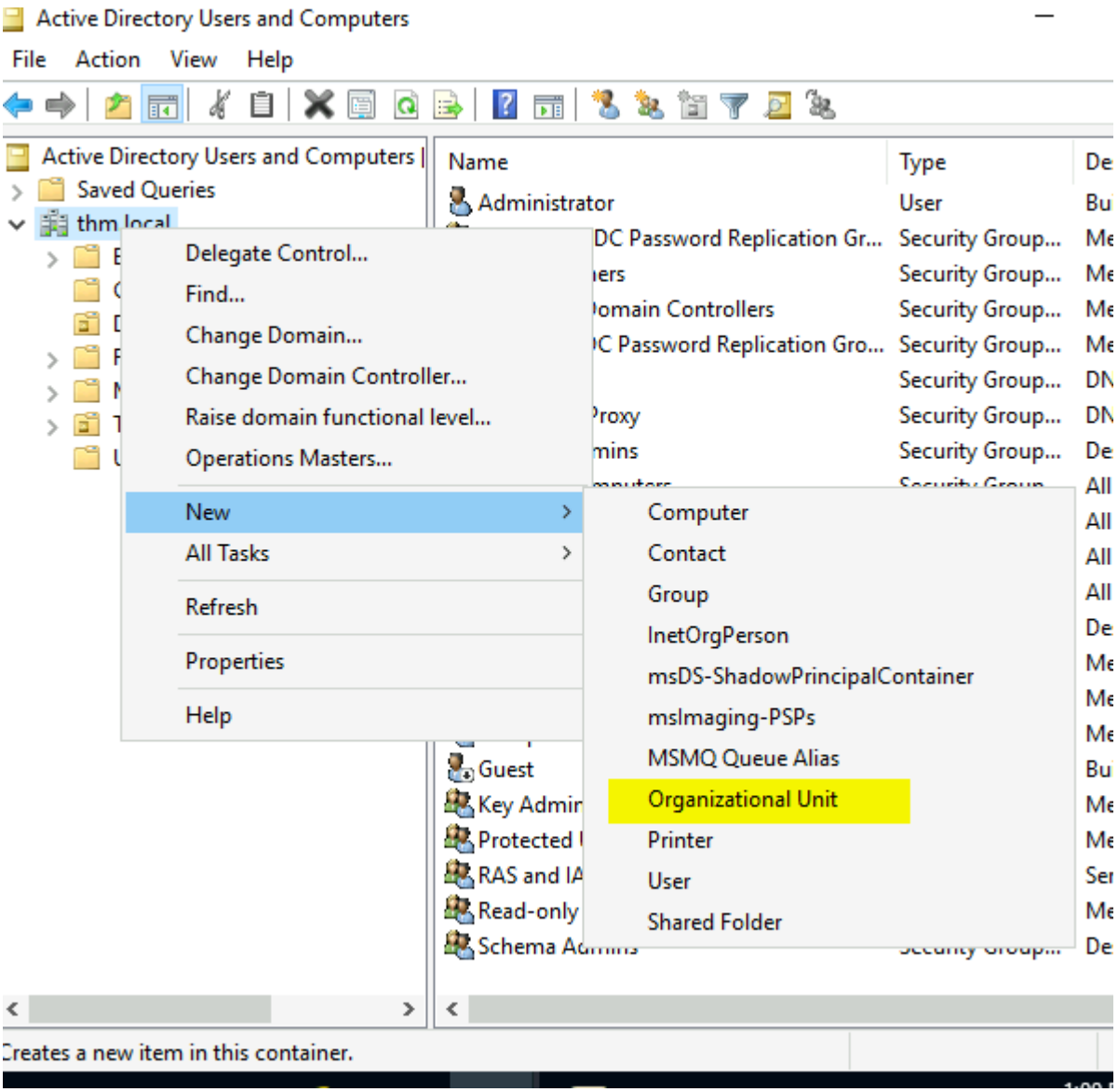
➔ Getting the flag

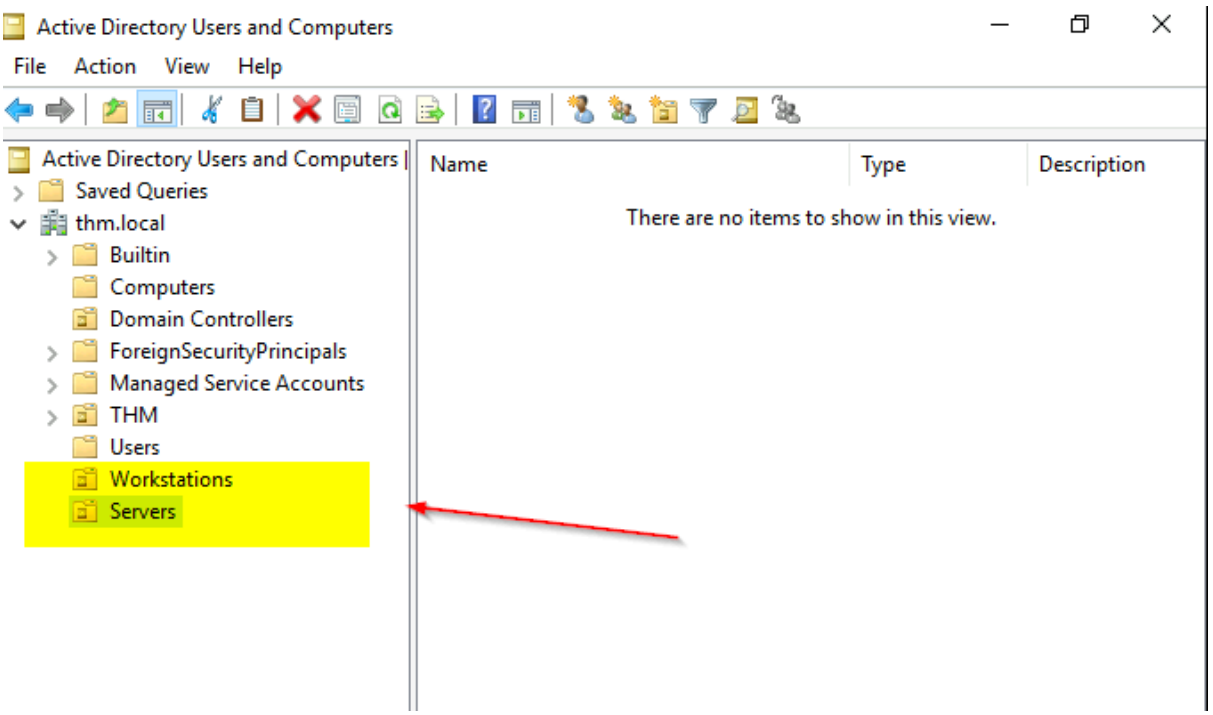


The process of granting privileges to a user over some OU or other AD Object is called…
Answer: **delegation**

Task 5 Managing Computers in AD

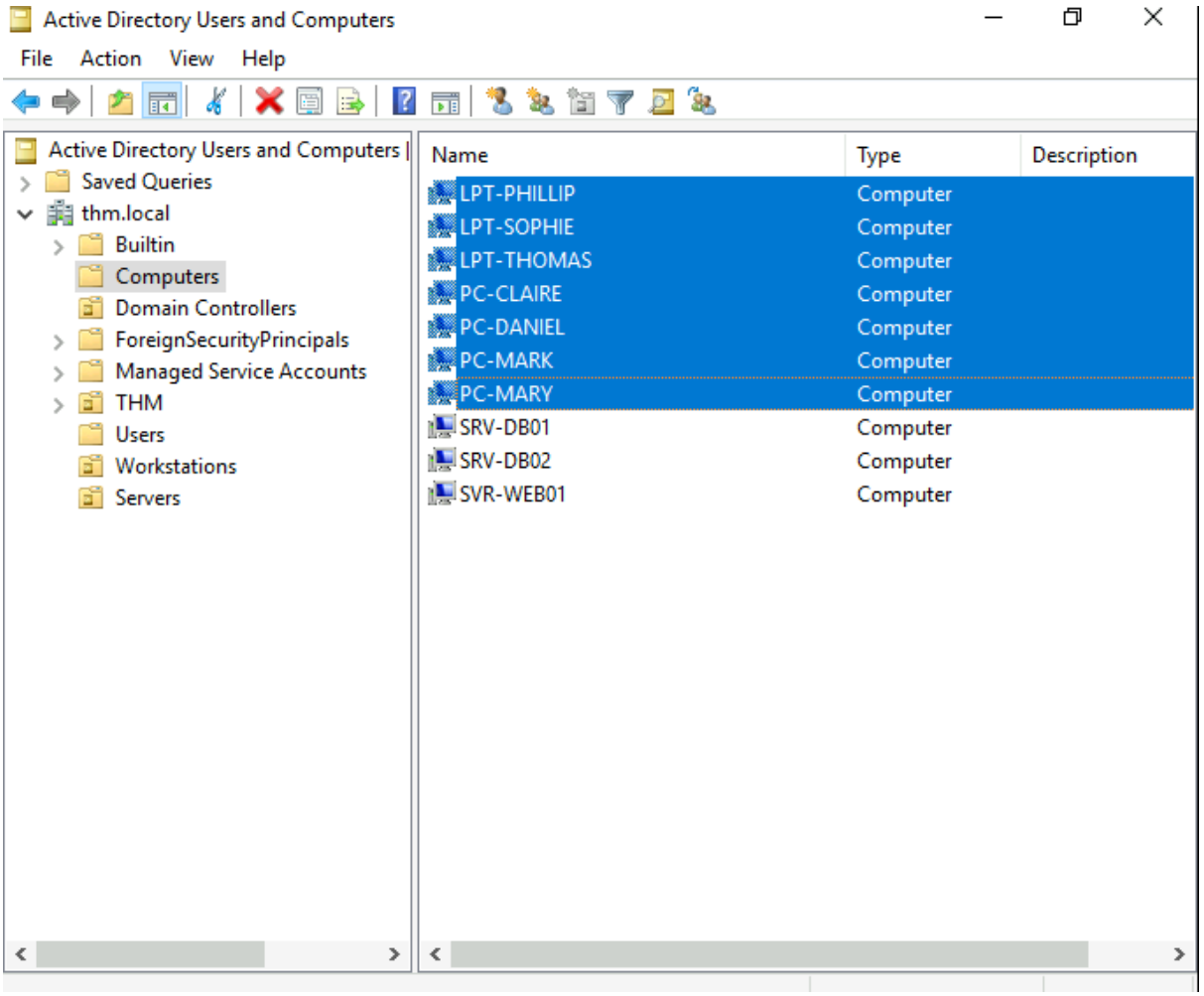
➔ I right clicked on thm.local and created new OUs, I named them workstations and servers


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers
Saved Queries
thm.local
Delegate Control...
Find...
Change Domain...
Change Domain Controller...
Raise domain functional level...
Operations Masters...
New
All Tasks
Refresh
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Organizational Unit
Printer
User
Shared Folder
Name
Type
Administrator
User
Guest
Read-only
Creates a new item in this container.



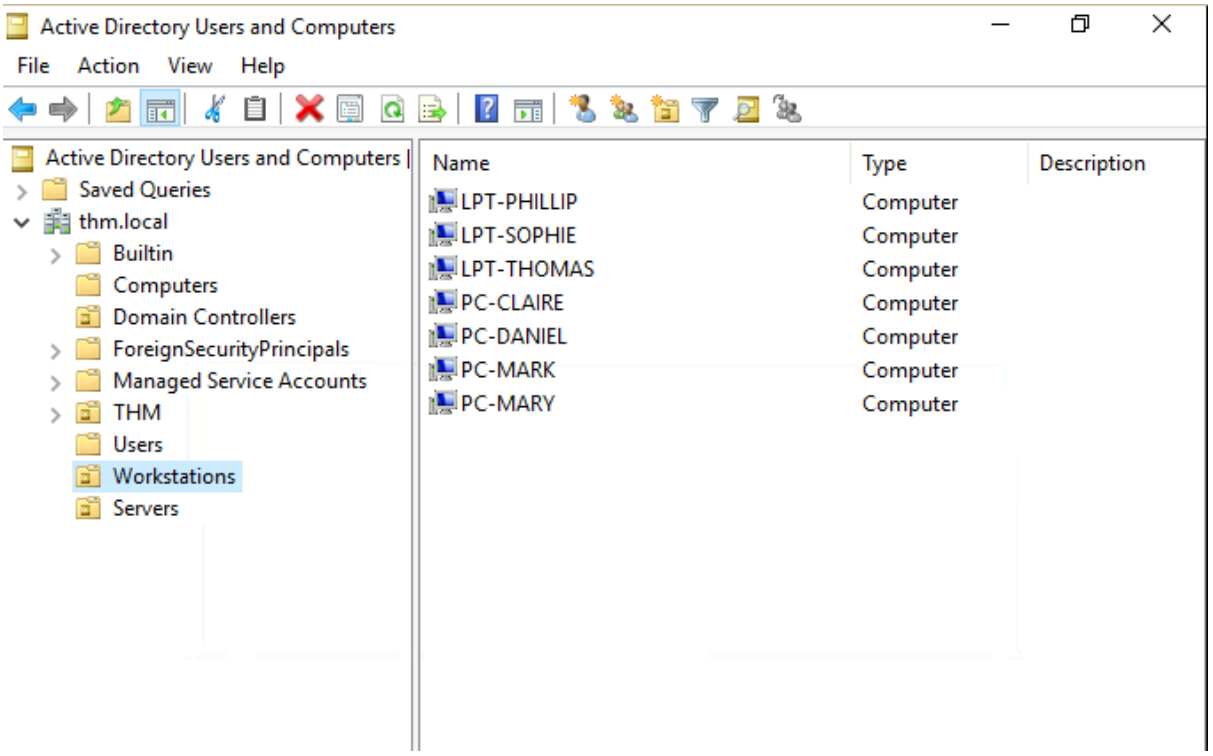
➔ Then I moved the personal computers and laptops to the Workstations OU and the servers to the Servers OU from the Computers container

➔ I pressed ctrl and click on them then dragged them to their respective OU



After organising the available computers, how many ended up in the Workstations OU?

Answer: 7



Is it recommendable to create separate OUs for Servers and Workstations? (yay/nay)
Answer: **yay**

Task 6 Group Policies

Question	Answer
What is the name of the network share used to distribute GPOs to domain machines?	SYSVOL
Can a GPO be used to apply settings to users and computers? (yay/nay)	yay

Task 7 Authentication Methods

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

When referring to Kerberos, what type of ticket allows us to request further tickets known as TGS?	Ticket Granting Ticket
When using NetNTLM, is a user's password transmitted over the network at any point? (yay/nay)	nay

Task 8 Trees, Forests and Trusts

Question	Answer
What is a group of Windows domains that share the same namespace called?	Tree
What should be configured between two domains for a user in Domain A to access a resource in Domain B?	2 trust relationship

END!!!