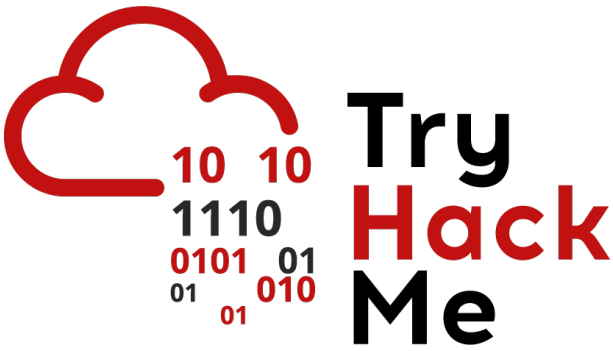
Writeup: Sala *Active Directory Basics*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción

En esta sala vamos a comprender el funcionamiento interno de **Active Directory (AD)**, una de las tecnologías más utilizadas para la administración de usuarios, equipos y políticas en redes corporativas Windows. Exploraremos los elementos fundamentales del entorno AD, desde su estructura jerárquica hasta sus métodos de autenticación y administración.

2. Sala

2.1. Tarea 1 – Introducción

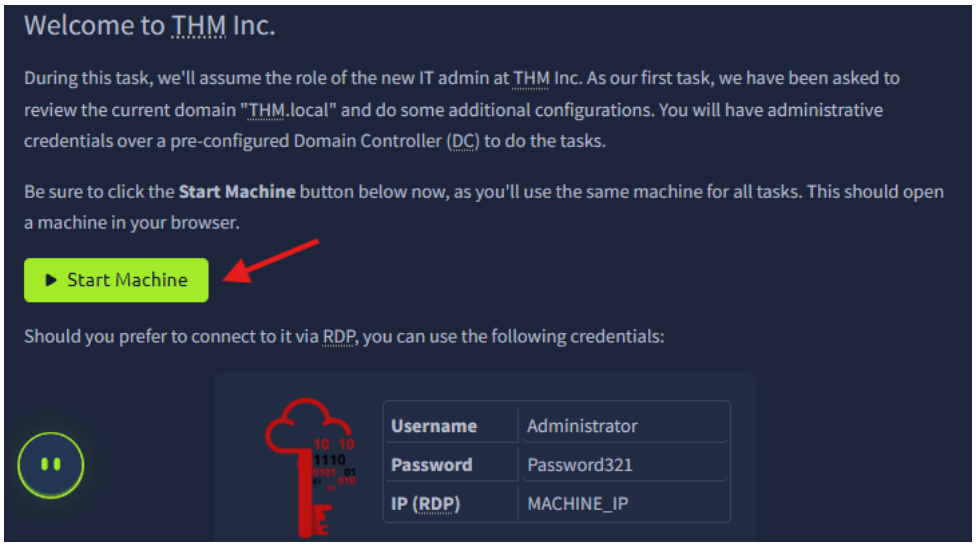
En esta primera tarea nos introduce el propósito de la sala, explicando que Active Directory (AD) es un sistema centralizado de gestión de usuarios, máquinas y permisos en entornos Windows.

Pregunta: Click and continue learning!
Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - Dominios de Windows

Aprenderemos los conceptos clave de dominio de Windows como qué es un dominio, el rol del Controlador de Dominio, y los beneficios de centralizar la administración de credenciales y políticas de seguridad en toda la red. Además, asumiremos el rol de un administrador TI proporcionandonos una máquina virtual la cual levantaremos para realizar las tareas posteriores o conectandonos mediante un RDP (Remote Desktop Protocol) con las credenciales correspondientes.

Para inicializar la máquina haremos clic en **Start Machine** que se encuentra en el lado inferior de la tarea.



Una vez inicializada la máquina, procederemos a responder las siguientes preguntas de la tarea.

Pregunta: In a Windows domain, credentials are stored in a centralised repository called...
Respuesta: **Active Directory**

Preguntas: The server in charge of running the Active Directory services is called...
Respuesta: **Domain Controller**

2.3. Tarea 3 - Directorio activo

En esta tarea conoceremos los objetos principales dentro de un AD (Active Directory) como usuarios, máquinas, grupos y unidades organizativas (OUs). También, se explica cómo funcionan las OUs como contenedores para aplicar políticas de forma diferencial

Después de entender un AD y sus objetos principales, responderemos las siguientes preguntas

Pregunta: Which group normally administrates all computers and resources in a domain?
Respuesta: **Domain Admins**

Pregunta: What would be the name of the machine account associated with a machine named TOM-PC?
Respuesta: **TOM-PC$**

Pregunta: Suppose our company creates a new department for Quality Assurance.

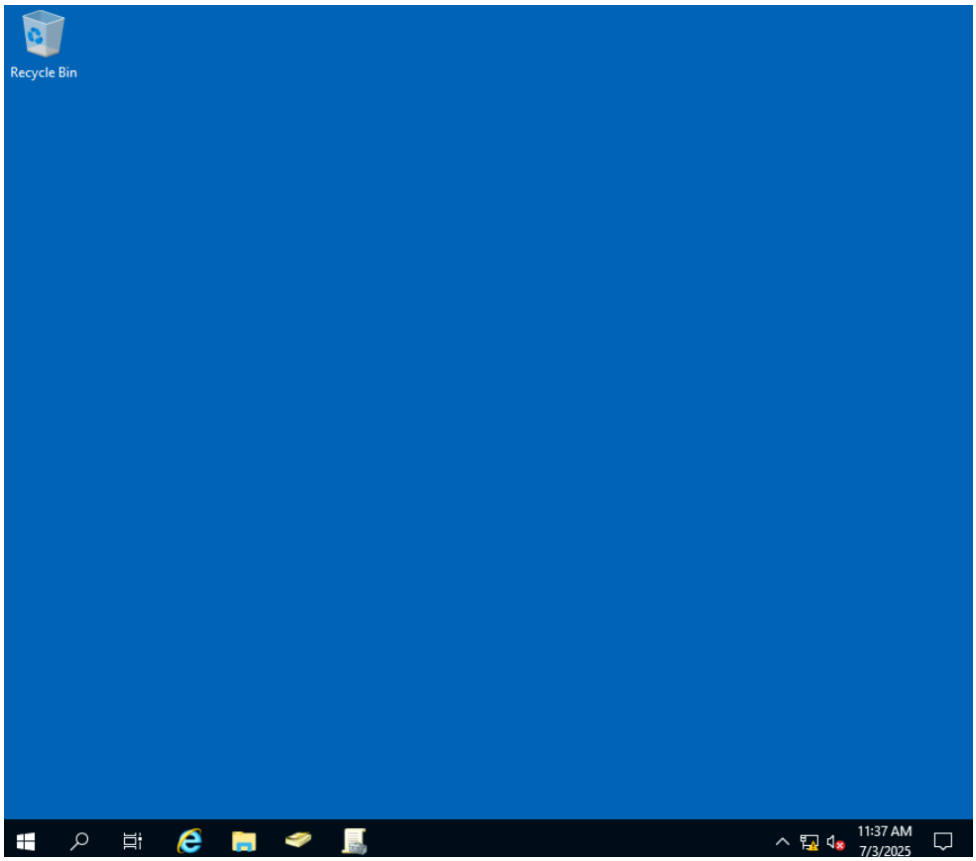
What type of containers should we use to group all Quality Assurance users so that policies can be applied consistently to them?

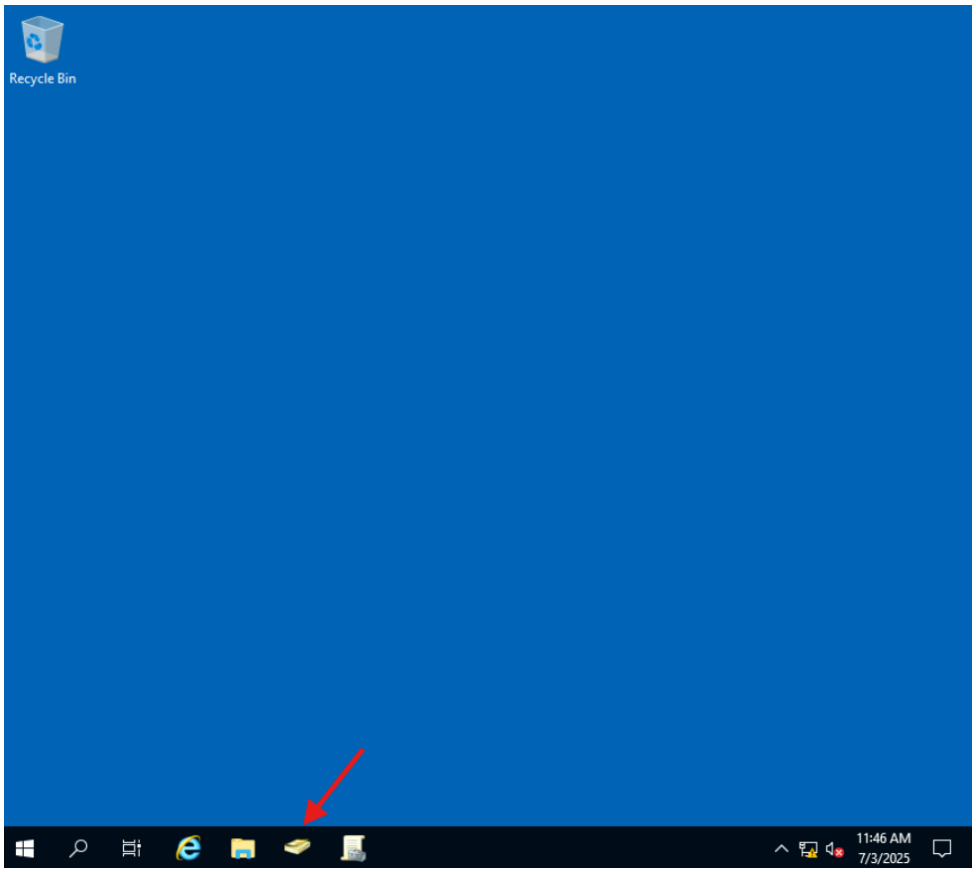
Respuesta: **Organizational Units**

2.4. Tarea 4 - Administrar usuarios en AD

Esta tarea nos enseña a gestionar usuarios y OUs, aprenderemos a eliminar OUs protegidas contra borrado accidental, crear o eliminar usuarios para alinear la estructura organizativa, e identificar buenas prácticas en administración de cuentas y contenedores.

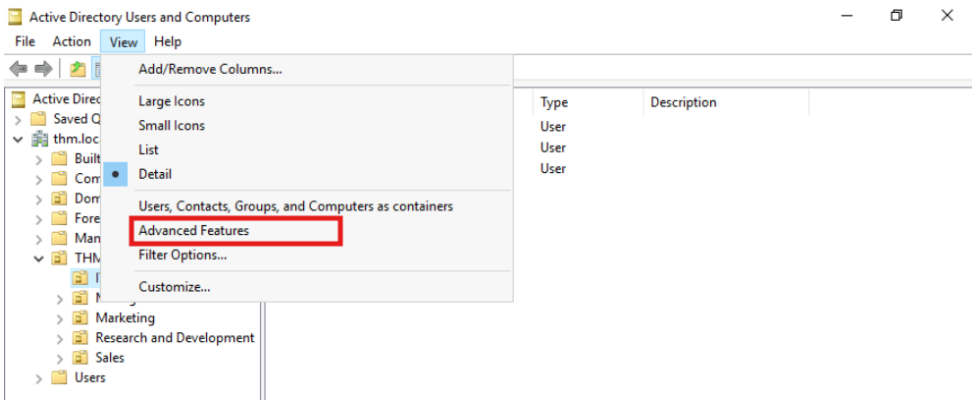
Para completar esta tarea debemos realizar una práctica logrando reforzar los conocimientos. Para ello, debemos ir a la máquina y abrir la aplicación **Active Directory Users and Computers** (la encontraremos en la barra de tareas).



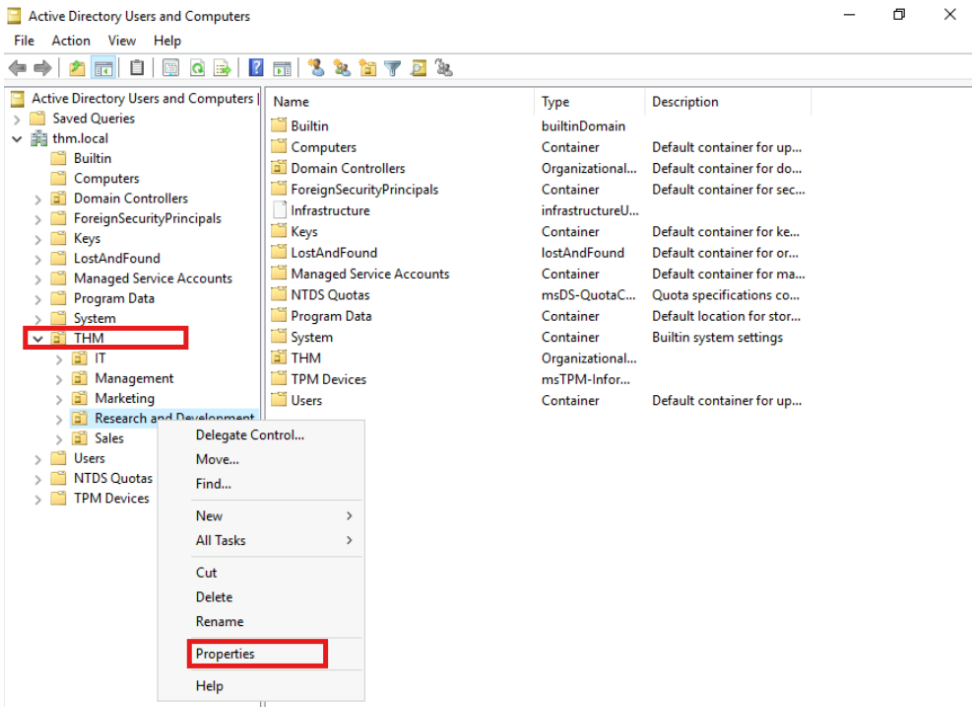


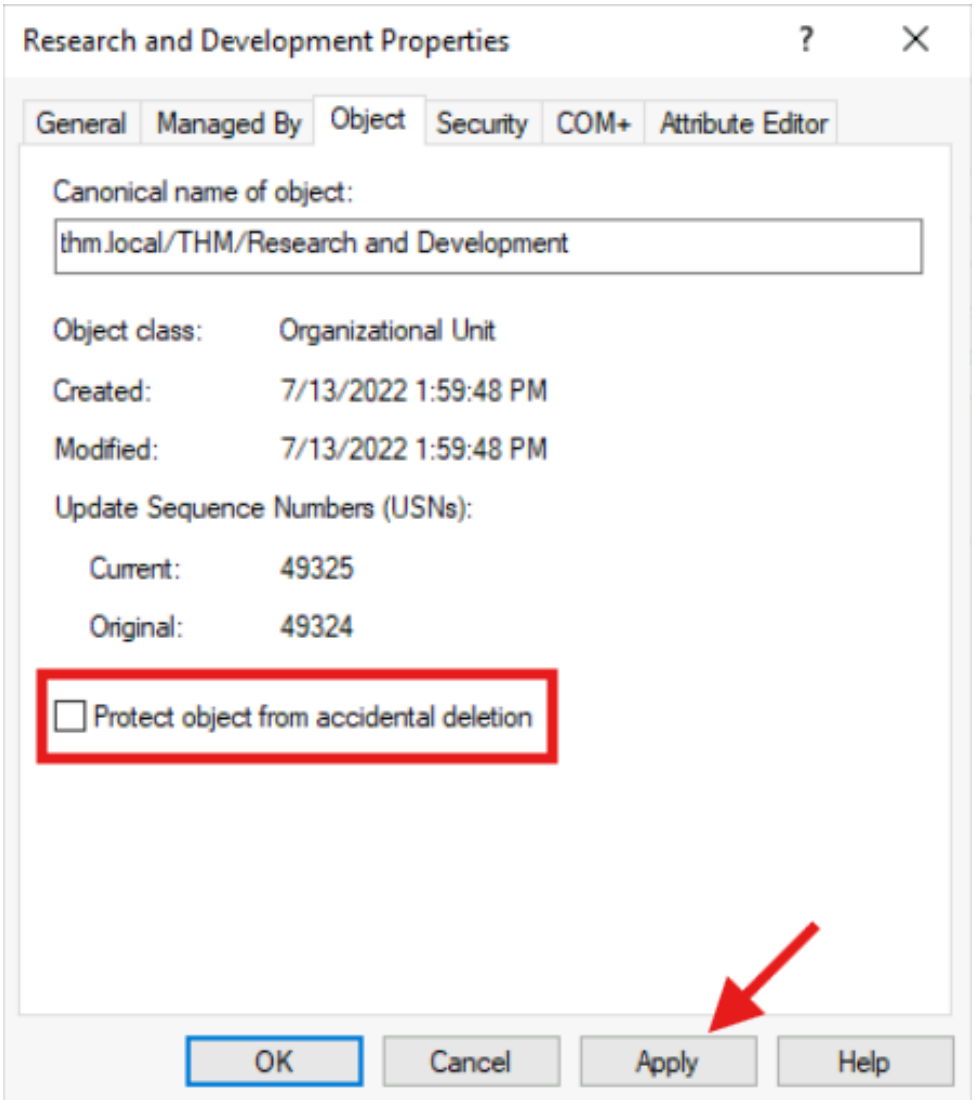
Una vez en la aplicación, debemos eliminar OUs y usuarios extras que se encuentran registrados. Para ello, nos dirigimos a la carpeta de **THM** y debemos eliminar la OUs llamada **Research and Development**. Al intentar eliminarla nos salta un error de que no tenemos privilegios suficientes (esto se debe por que de forma predeterminada, las unidades organizativas (OU) están protegidas contra borrados accidentales).

Para resolver este error, vamos a ir al lado superior de la aplicación y en la pestaña **View** haremos clic en la opción **Advanced Features**

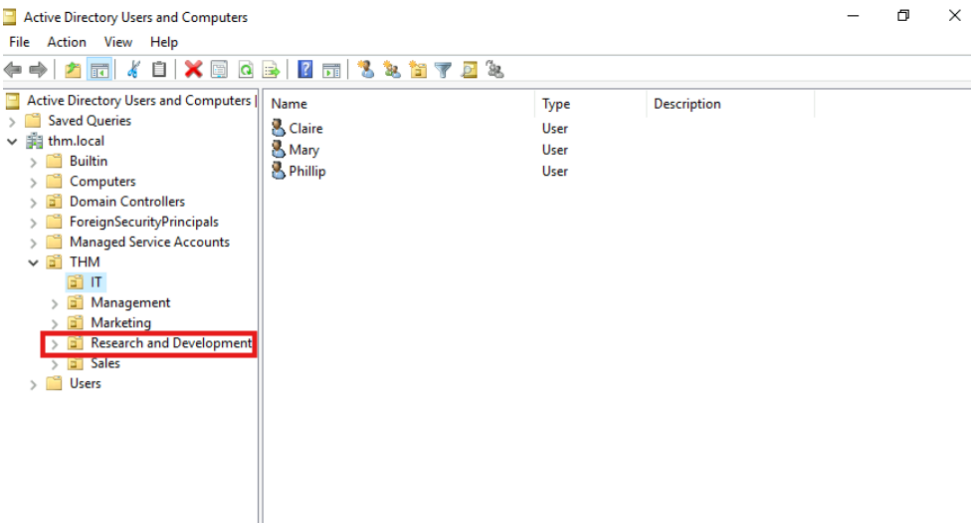


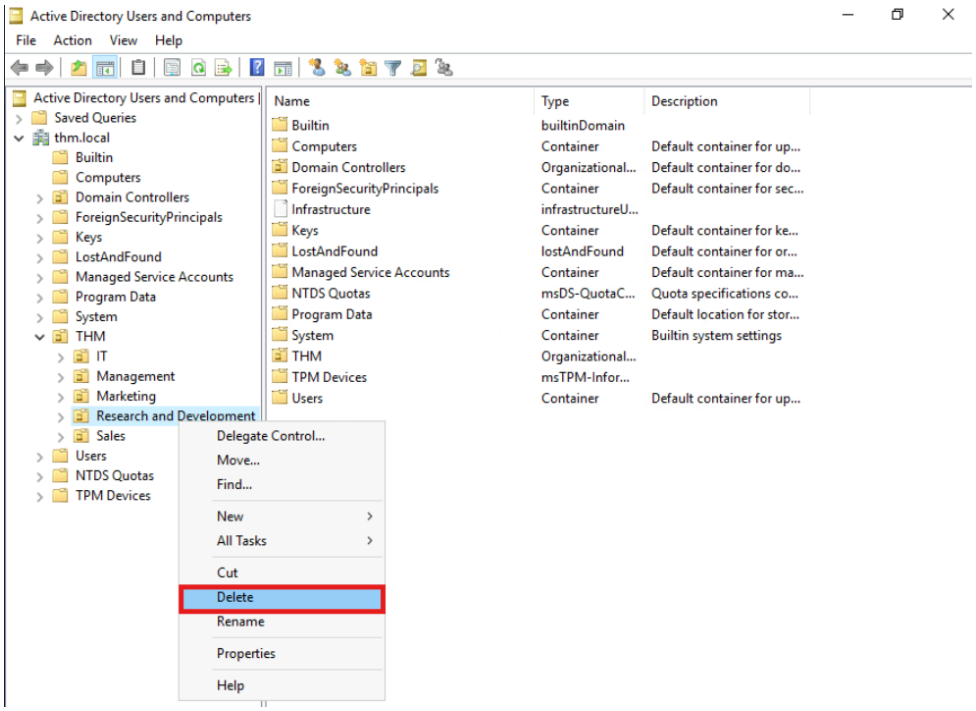
Posterior a eso, se nos mostrará algunos contenedores adicionales y se nos permitirá desactivar la protección contra borrado accidental, entonces, procederemos en hacer clic derecho en la carpeta de **Research and Development** y clic en **Properties** para abrir la pestaña de propiedades. Una vez en las propiedades iremos a la opción de **Object** y abajo del todo vamos a desactivar la protección contra borrado accidental.



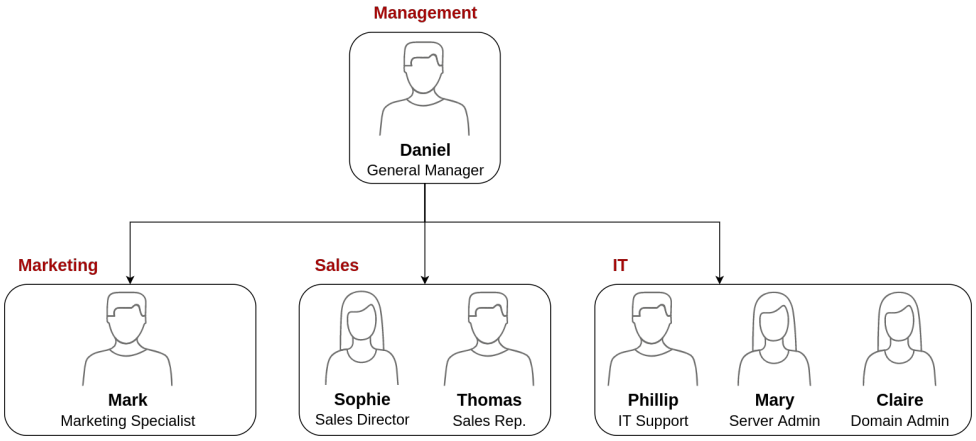


Ahora podemos eliminar la organización extra, para ello haremos clic derecho en ella y hacemos clic en la opción de **Delete** para eliminarla.

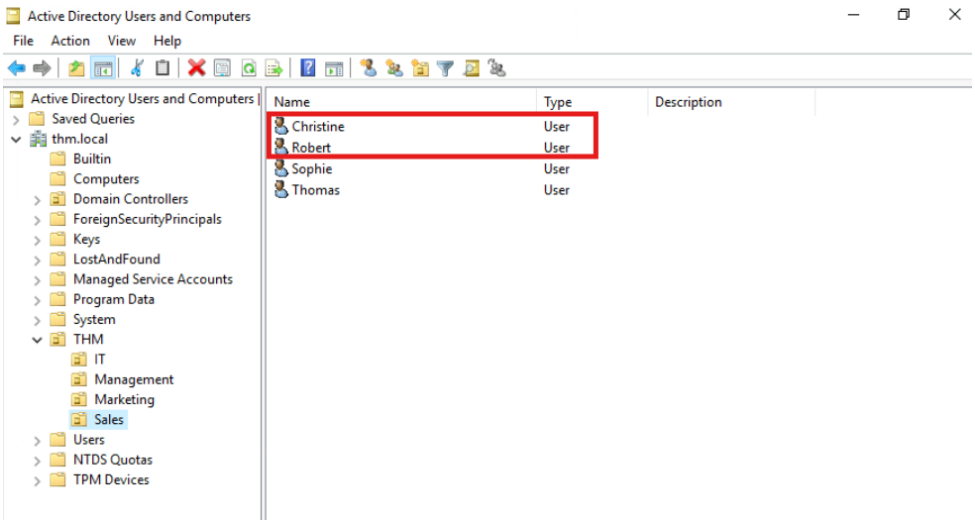




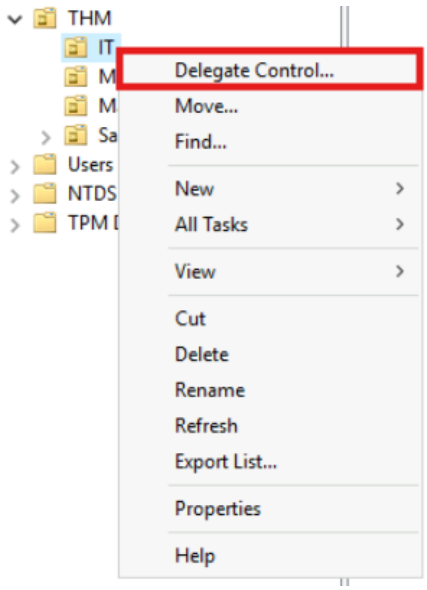
Bien, ahora debemos eliminar los usuarios extras. Para ello nos guiaremos del organigrama que nos proporciona la tarea.



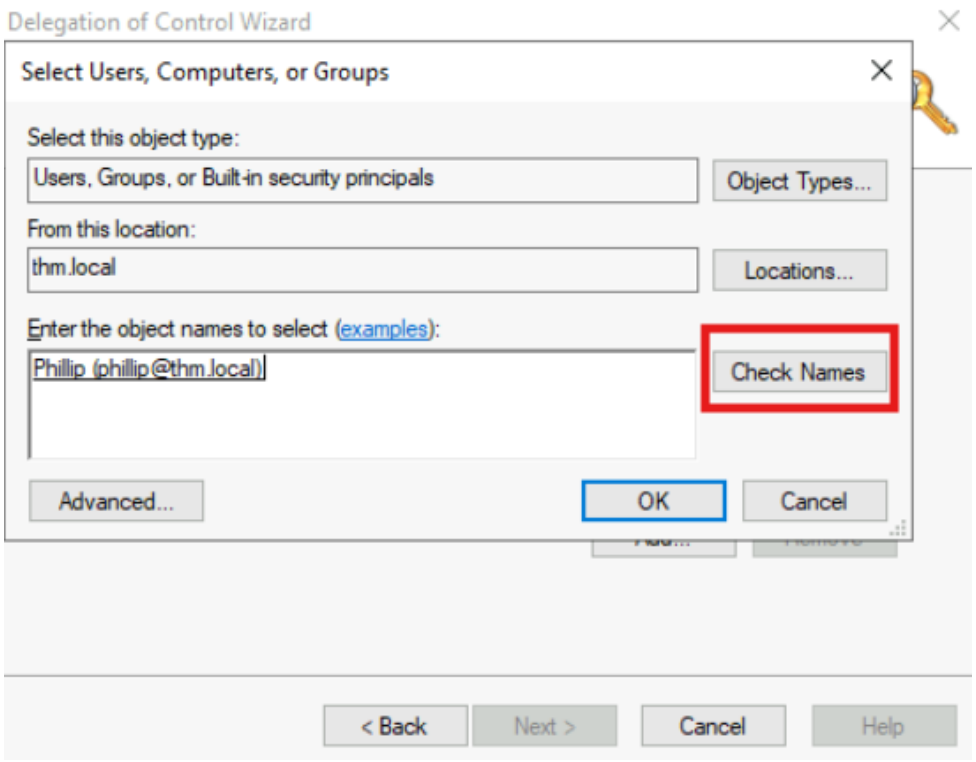
Una vez analizado el organigrama, nos posicionaremos en **THM** y revisaremos cada departamento. Notaremos que en **Sales** se encuentran los usuarios **Christine** y **Robert**, estos usuarios no corresponden con el organigrama, por ende, haremos clic derecho en cada uno y haremos clic en la opción de **Delete** para eliminarlos.



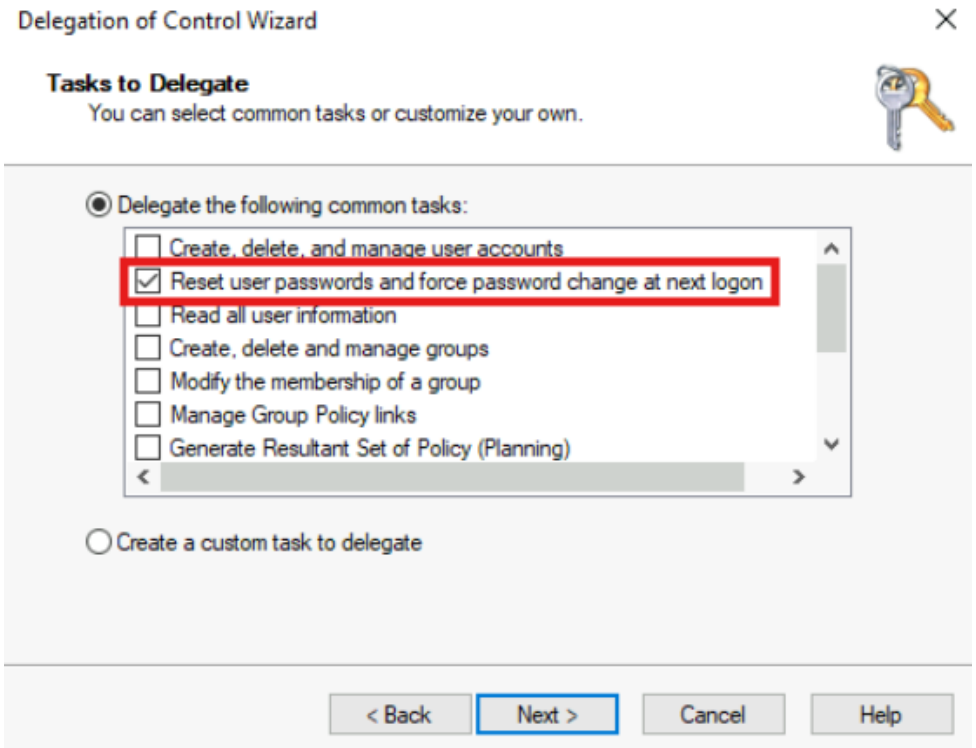
Una vez eliminado los usuarios, procederemos con lo siguiente que es realizar una delegación que nos permite otorgar privilegios específicos a los usuarios para realizar tareas avanzadas en las OU sin necesidad de la intervención de un administrador de dominio. Para ello, vamos a hacer clic derecho en **IT** y hacemos clic en la opción **Delegate Control**

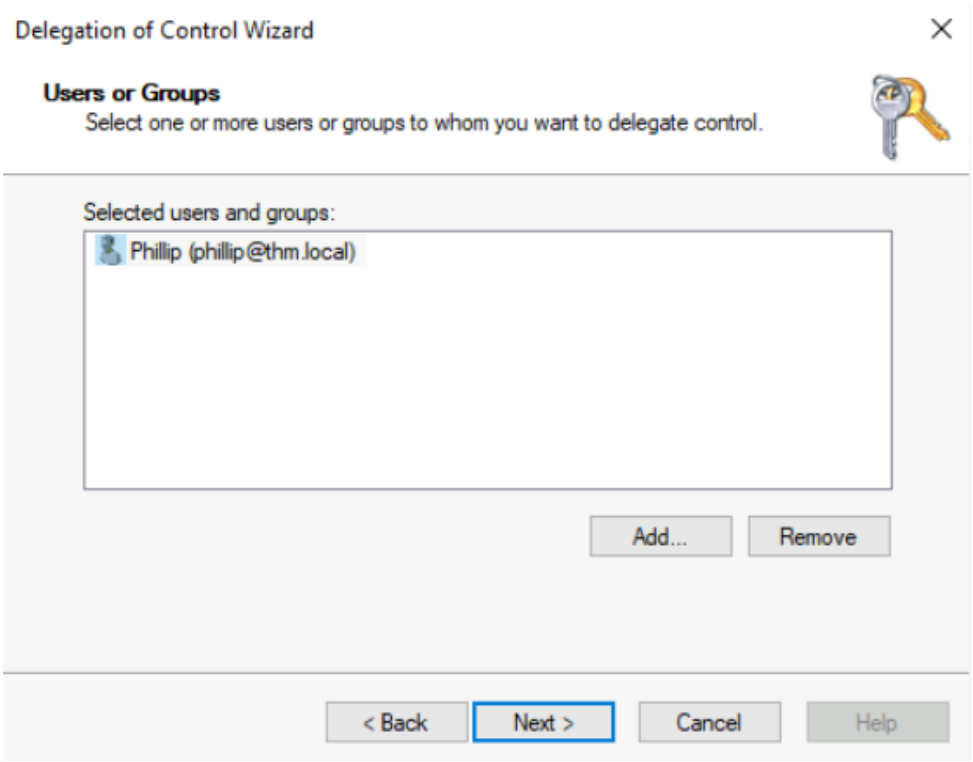


Se nos abrirá la pestaña para delegar permisos a usuarios. Haremos clic en **Add** para agregar un usuario y en el apartado de ingresar el nombre del objeto escribiremos **Phillip** y posterior a eso, haremos clic en **Check Names**, se nos auto completara el nombre del objeto una vez encontrado.

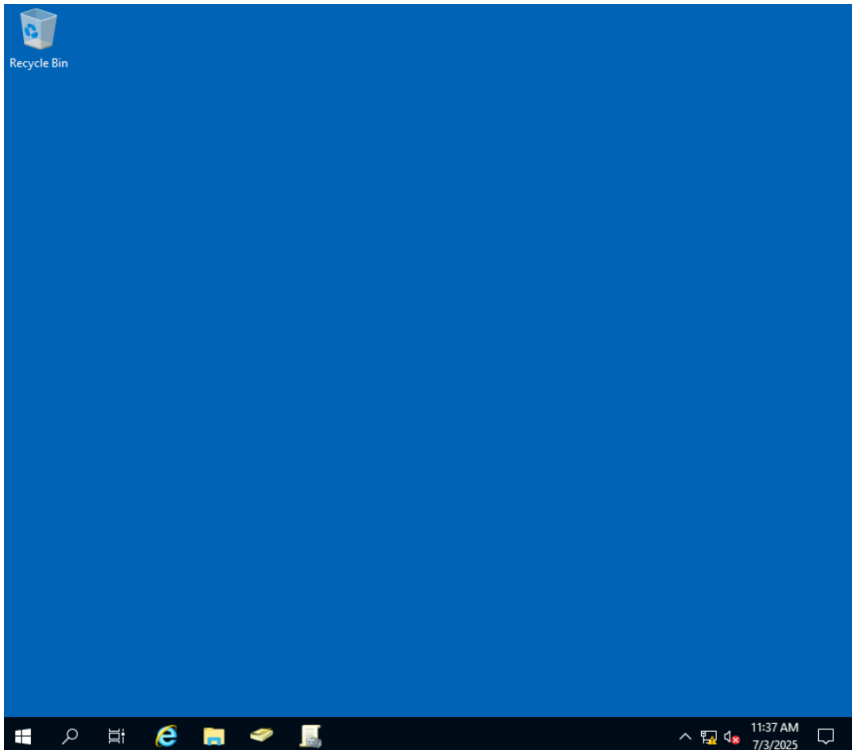


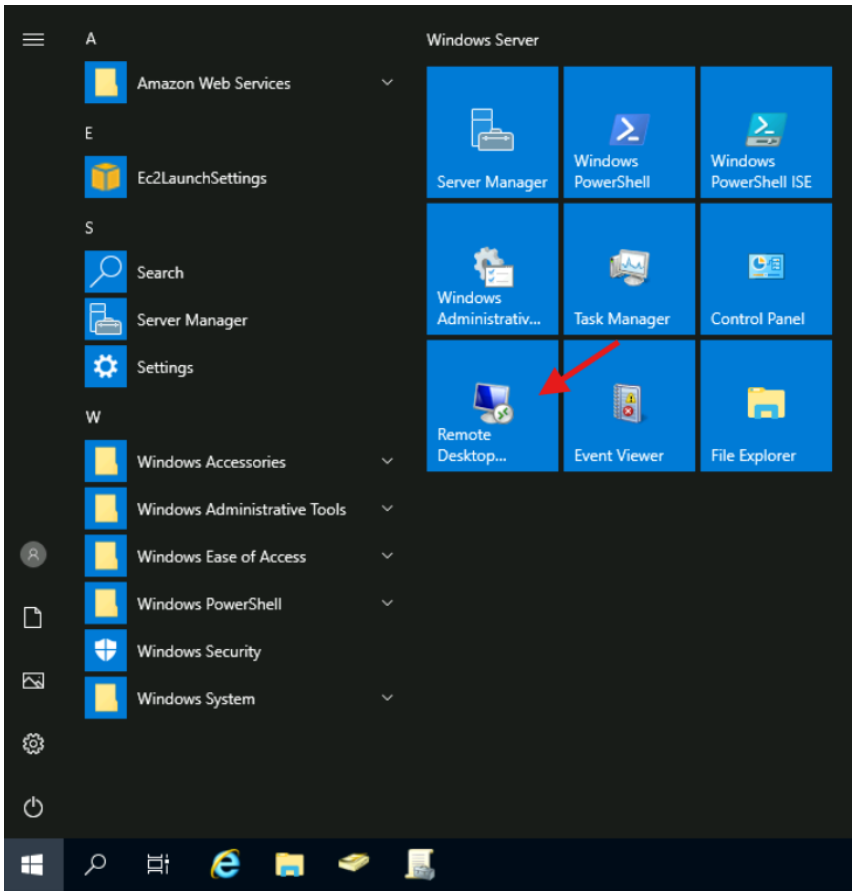
Hacemos clic en **OK** y se nos desplegara las diversas tareas que podemos delegar al usuario, procederemos en habilitarle la tarea de restablecer la contraseña del usuario y forzar el cambio de contraseña en el siguiente inicio de sesión

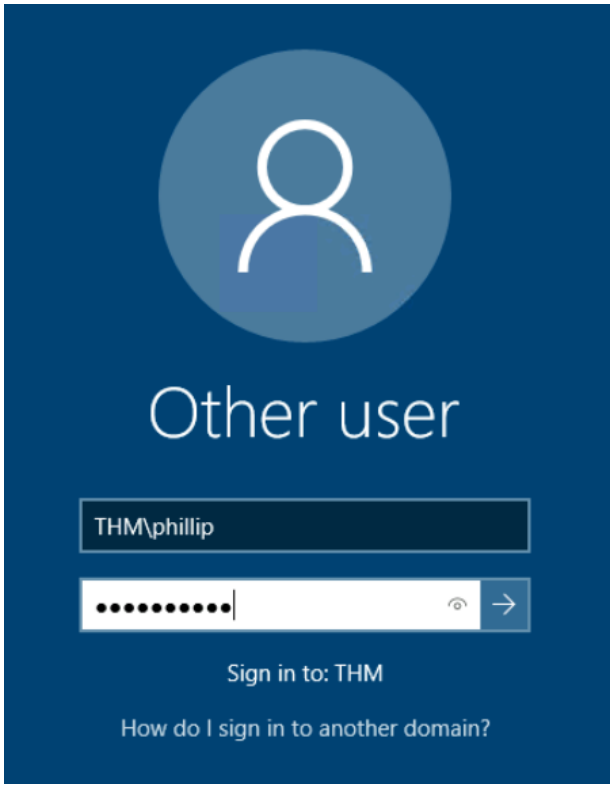




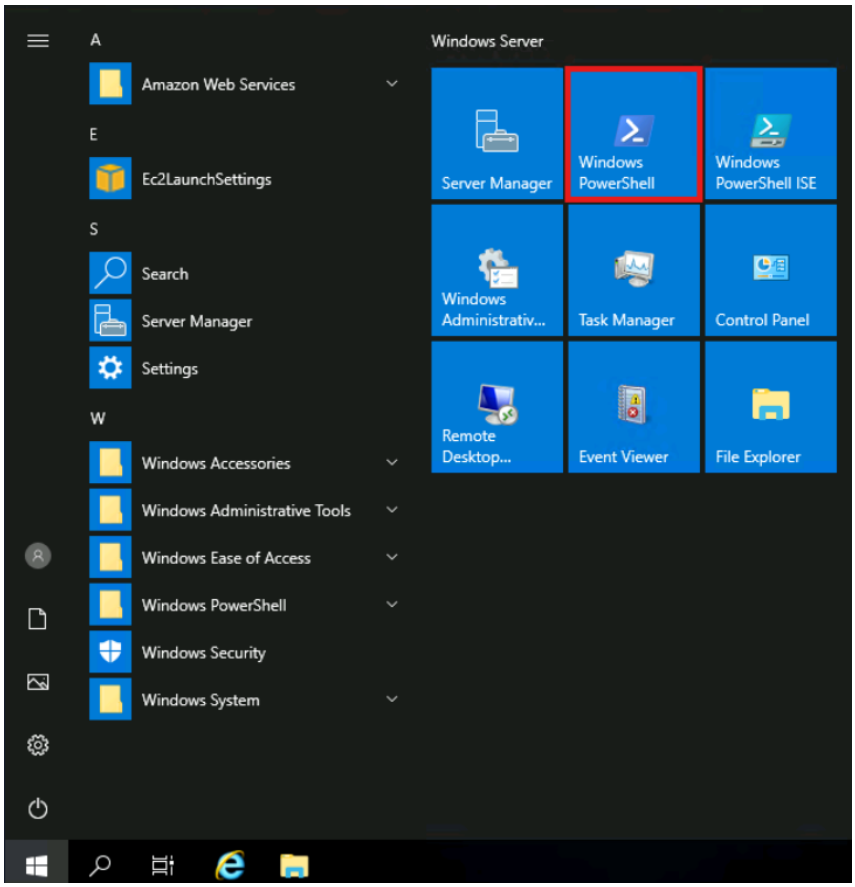
Ahora que logramos delegar permisos a un usuario, vamos a utilizarlos para restablecer la contraseña del usuario **Sophie**. Para ello, ingresaremos a través de RDP al escritorio de Phillip con las credenciales que nos proporciona la tarea.







Una vez dentro, vamos a utilizar **Windows PowerShell** para establecer una nueva contraseña al usuario de **Sophie**.



En la terminal debemos ejecutar el siguiente comando para establecer una contraseña nueva:

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

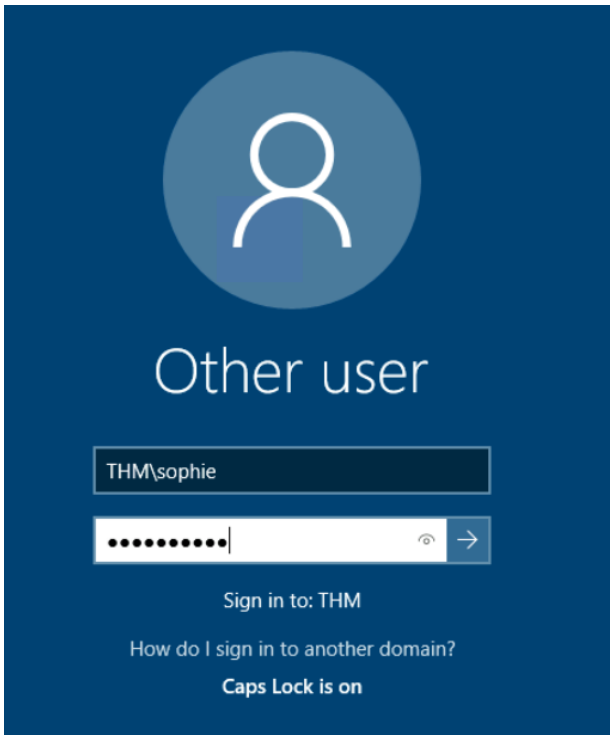
```
PS C:\Users\phillip> Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecureString -Prompt 'New Password'
-Verbose
New Password: **********
VERBOSE: Performing the operation "Set-ADAccountPassword" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
PS C:\Users\phillip>
```

Hemos logrado establecerle una nueva contraseña, pero, como no queremos que Sophie siga usando una contraseña que conocemos, también podemos forzar el restablecimiento de la contraseña en el próximo inicio de sesión con el siguiente comando:

- **Set-ADUser -ChangePasswordAtLogon $true -Identity sophie -Verbose**

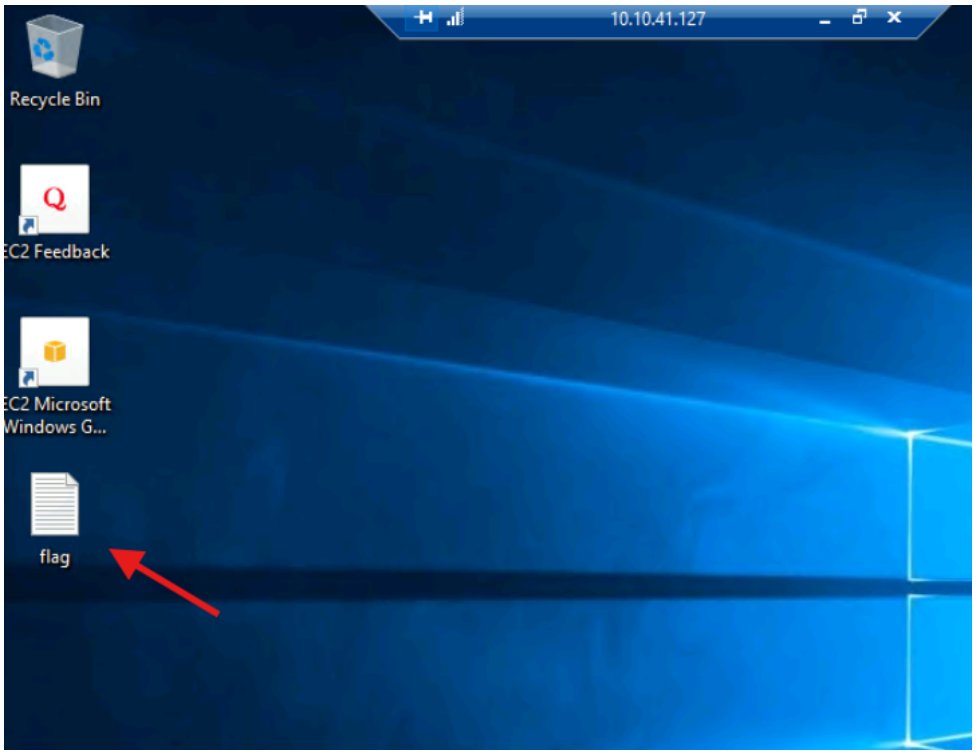
```
PS C:\Users\phillip> Set-ADUser -ChangePasswordAtLogon $true -Identity sophie -Verbose
VERBOSE: Performing the operation "Set" on target "CN=Sophie,OU=Sales,OU=THM,DC=thm,DC=local".
PS C:\Users\phillip>
```

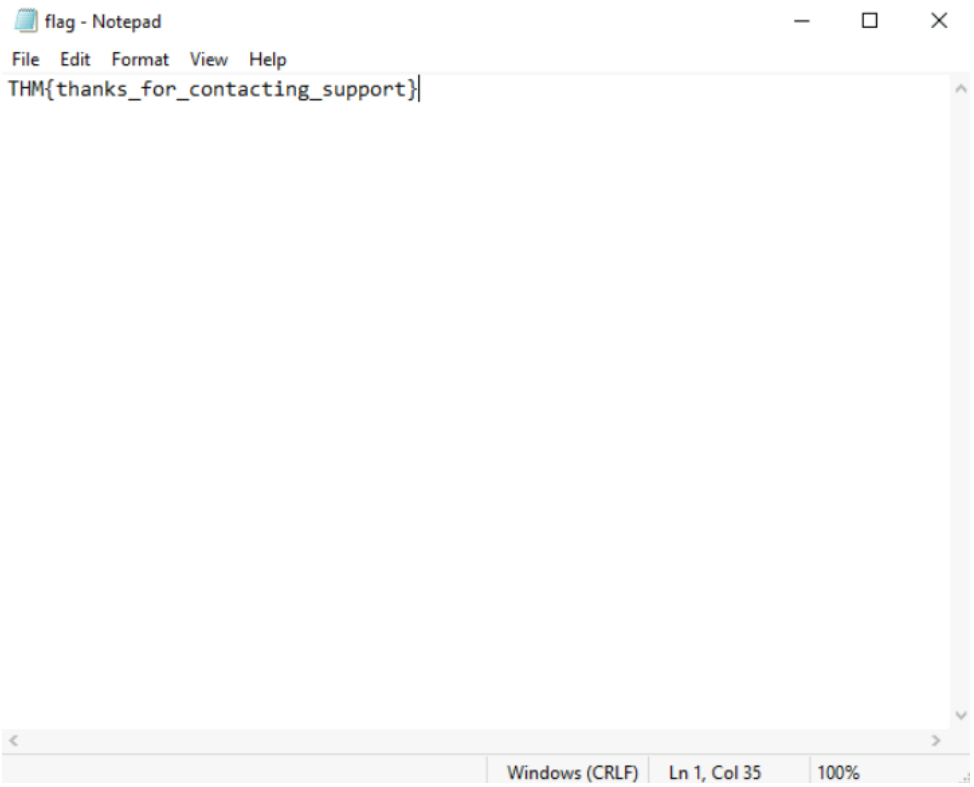
Ahora debemos concectarnos mediante RDP e iniciar sesión en la cuenta de Sophie con su nueva contraseña.



Pregunta: What was the flag found on Sophie's desktop?

En el escritorio de **Sophie** encontraremos un documento de texto llamado flag, accedemos a él para obtener la respuesta.





Respuesta: THM{thanks_for_contacting_support}

Pregunta: The process of granting privileges to a user over some OU or other AD Object is called...

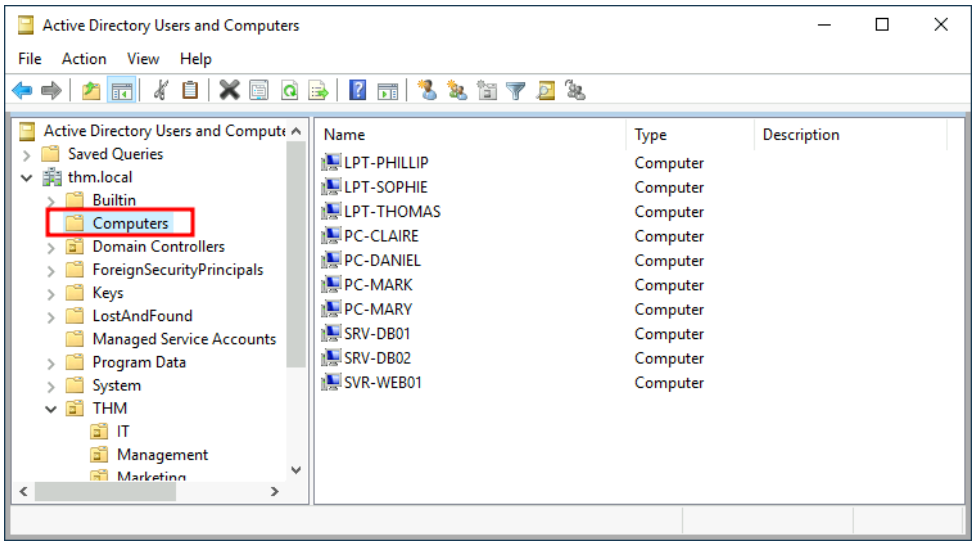
Respuesta: delegation

2.5. Tarea 5 - Administración de computadoras en AD

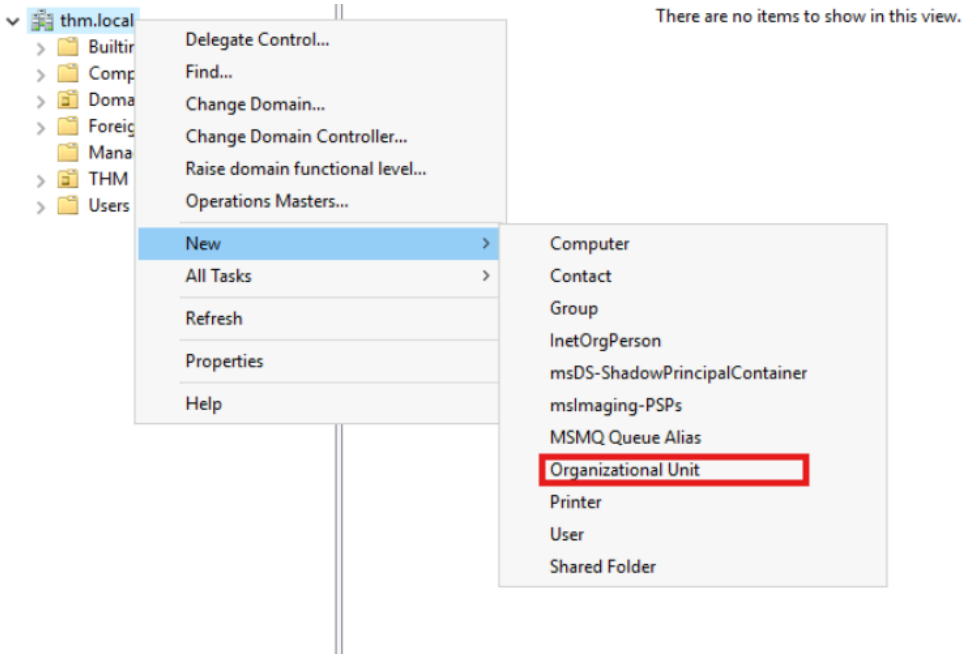
Esta tarea se centra en la organización de las máquinas del dominio, se separan en OUs para workstations y servidores para facilitar la aplicación de políticas específicas según sus roles. Además, se destaca la importancia de segregar dispositivos por su función administrativa.

Al igual que la anterior tarea, vamos a poner en práctica los conocimientos adquiridos. Para ello, iremos a nuestra máquina y nuevamente abriremos la aplicación **Active Directory Users and Computers**.

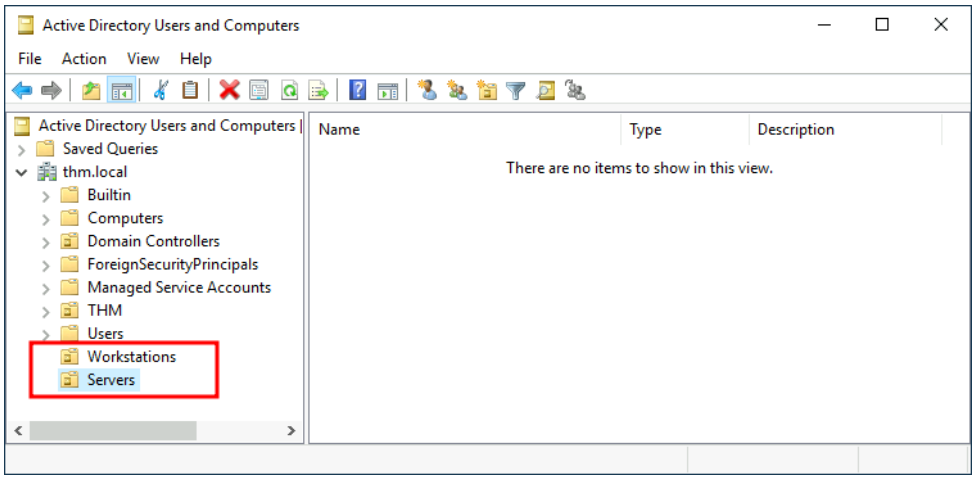
Una vez dentro, iremos a **THM** y haremos clic en **Computers**, por defecto, todas las máquinas que se unen a un dominio) se guardarán en el contenedor Computers. Si revisamos nuestro controlador de dominio, veremos que algunos dispositivos ya están ahí



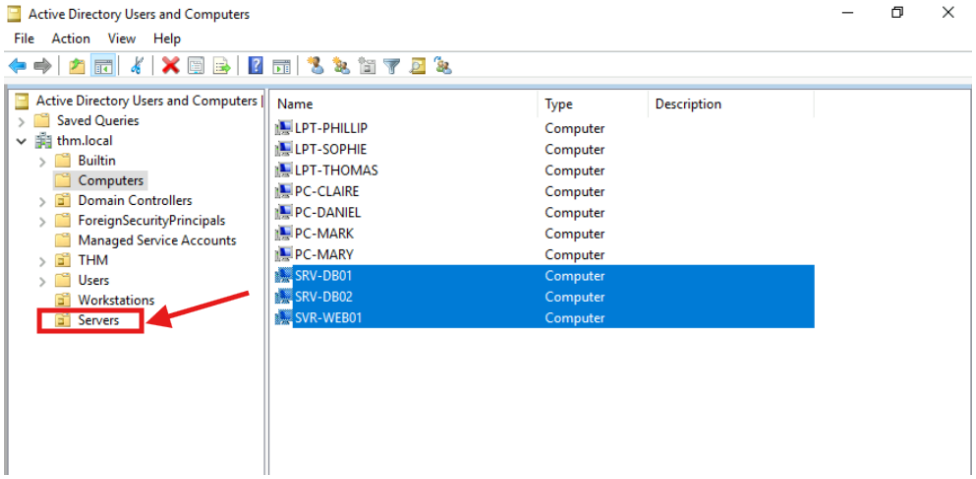
Ya que estamos organizando nuestro AD, crearemos dos unidades organizativas independientes: **Workstations** y **Servers**. Las crearemos directamente en el contenedorthm.local del dominio.

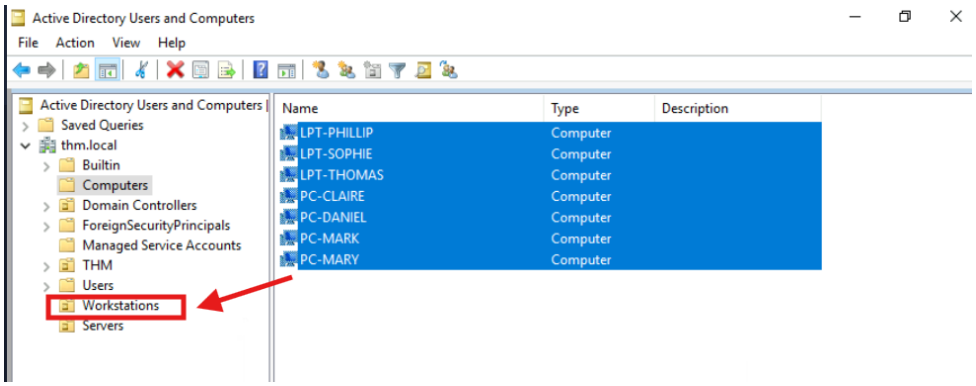


Al final, debería tener la siguiente estructura de unidad organizativa:



Ahora, debemos mover las computadoras personales y portátiles a la unidad organizativa **Workstations** y los servidores a la unidad organizativa **Servers** desde el contenedor **Computers**.





De esta manera logramos completar la práctica, procederemos a responder las siguientes preguntas.

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

Respuesta: 7

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

Respuesta: yay

2.6. Tarea 6 - Políticas de grupo

Nos explica qué son los **GPOs (Group Policy Objects)**, cómo se crean y vinculan a OUs, y las diferencias entre configuraciones para usuarios y máquinas. Además, proporciona ejemplos como políticas de longitud de contraseña, bloqueo de Panel de Control o bloqueo automático de pantalla, y menciona la ruta de replicación vía SYSVOL.

Una vez que comprendemos las políticas de grupo, vamos a responder las siguientes preguntas.

Pregunta: What is the name of the network share used to distribute GPOs to domain machines?

Respuesta: sysvol

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

Respuesta: yay

2.7. Tarea 7 - Métodos de autenticación

Vamos a introducirnos en los protocolos de autenticación en AD como:

- **Kerberos (ticketing moderno)**
- **NetNTLM (mecanismo heredado por desafío-respuesta)**

explicando sus flujos básicos y contrastando ambos

Ahora que entendemos los métodos de autenticación, responderemos las siguientes preguntas.

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

Respuesta: nay

Pregunta: When referring to Kerberos, what type of ticket allows us to request further tickets known as TGS?

Respuesta: Ticket Granting Ticket

Pregunta: When using NetNTLM, is a user's password transmitted over the network at any point? (yay/nay)

Respuesta: **nay**

2.8. Tarea 8 - Arboles, Bosques y Confianza

Conoceremos los conceptos de escalabilidad en AD:

- **Árboles (conjunto de dominios con namespace compartido)**
- **Bosques (colecciones de árboles con namespace distintos)**
- **relaciones de confianza entre dominios para permitir acceso de usuarios de un dominio en otro**

Una vez comprendemos estos conceptos de escalabilidad, procederemos a responder las siguientes preguntas.

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

Respuesta: **Tree**

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

Respuesta: **A Trust Relationship**

2.9. Tarea 9 - Conclusión

Esta última tarea nos explica que esta sala solo debe servir como introducción a los conceptos básicos, ya que hay mucho más que explorar para implementar un entorno de Active Directory listo para producción.

Pregunta: Click and continue learning!

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

3. Conclusión sobre la Sala

Al finalizar la sala, hemos logrado comprender los conceptos clave de Active Directory, incluyendo su estructura organizacional, la gestión de usuarios y equipos, y el uso de políticas de grupo para controlar el entorno. También, aprendimos cómo funciona la autenticación dentro del dominio y cómo se estructuran múltiples dominios a través de árboles y bosques.