

## ***Active Directory Basics***

### **Tarea 1: Introducción**

Active Directory de Microsoft es la columna vertebral del mundo corporativo. Simplifica la gestión de dispositivos y usuarios en un entorno corporativo. En esta sesión, profundizaremos en los componentes esenciales de Active Directory.

#### **Objetivos de la sala**

En esta sala aprenderemos sobre Active Directory y nos familiarizaremos con los siguientes temas

- ¿Qué es Active Directory?
- ¿Qué es un dominio de Active Directory?
- ¿Qué componentes forman parte de un dominio de Active Directory?
- Bosques y fideicomiso de dominios
- ¡Y mucho más!

#### **Requisitos previos de la habitación**

- Conocimiento general de Windows. Consulte el módulo Fundamentos de Windows para obtener más información.

P: ¡Haz clic y continúa aprendiendo!

R: No se necesita respuesta

### **Tarea 2: Dominios de Windows**

P1: En un dominio de Windows, las credenciales se almacenan en un repositorio centralizado llamado...

R1: Active Directory

P2: El servidor encargado de ejecutar los servicios de Active Directory se llama...

R2: Domain Controller

### **Tarea 3: Directorio activo**

P1: ¿Qué grupo normalmente administra todas las computadoras y recursos de un dominio?

R1: Domain Admins

P2: ¿Cuál sería el nombre de la cuenta de máquina asociada a una máquina llamada TOM-PC\$

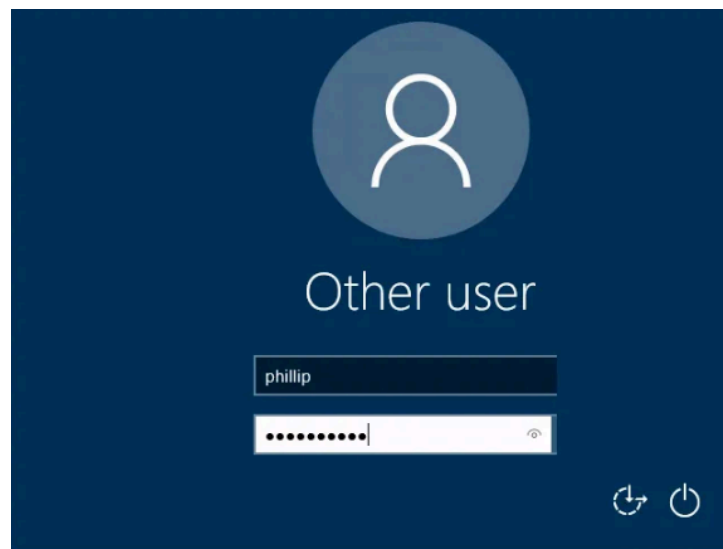
R2: TOM-PC\$

P3: Supongamos que nuestra empresa crea un nuevo departamento de Control de Calidad. ¿Qué tipo de contenedores deberíamos usar para agrupar a todos los usuarios de Control de Calidad y que las políticas se les apliquen de forma uniforme?

R3: Organizational Units

#### **Tarea 4: Administrar usuarios en AD**

P1: ¿Qué bandera era la que se encontró en el escritorio de Sophie?



```
Command Prompt - powershell
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

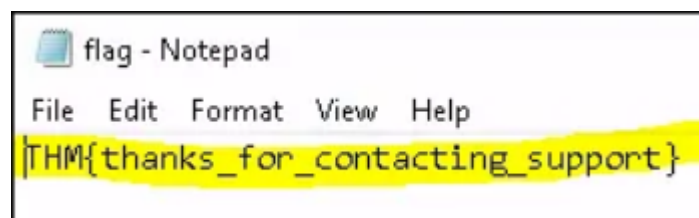
C:\Users\phillip>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\phillip> _
```

```
Command Prompt - powershell
Microsoft Windows [Version 10.0.17763.1821]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\phillip>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

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".
Set-ADAccountPassword : The password does not meet the length, complexity, or history requirement of the domain.
At line:1 char:1
+ Set-ADAccountPassword sophie -Reset -NewPassword (Read-Host -AsSecure ...
+ ~~~~~
+ CategoryInfo          : InvalidData: (sophie:ADAccount) [Set-ADAccountPassword], ADPasswordComplexityException
+ FullyQualifiedErrorId : ActiveDirectoryServer:1325,Microsoft.ActiveDirectory.Management.Commands.SetADAccountPassword
```



R1: THM{thanks\_for\_contacting\_support}

P2: El proceso de otorgar privilegios a un usuario sobre alguna OU u otro objeto de AD se denomina...

R2: Delegation

**Tarea 5:** Administración de computadoras en AD

P1: Después de organizar las computadoras disponibles, ¿cuántas terminaron en la unidad organizativa Estaciones de trabajo?

R1: 7

P2: ¿Es recomendable crear unidades organizativas independientes para servidores y estaciones de trabajo? (sí/no)

R2: Yay

**Tarea 6:** Políticas de grupo

P1: ¿Cuál es el nombre del recurso compartido de red utilizado para distribuir GPO a las máquinas del dominio?

R1: sysvol

P2: ¿Se puede usar una GPO para aplicar configuraciones a usuarios y computadoras? (sí/no)

R2: yay

**Tarea 7:** Métodos de autenticación

P1: ¿Una versión actual de Windows utilizará NetNTLM como protocolo de autenticación preferido de forma predeterminada? (sí/no)

R1: nay

P2: Al referirnos a Kerberos, ¿qué tipo de ticket nos permite solicitar tickets adicionales conocidos como TGS?

R2: Ticket Granting Ticket

P3: Al utilizar NetNTLM, ¿se transmite la contraseña de un usuario a través de la red en algún momento? (sí/no)

R3: nay

**Tarea 8:** Árboles, bosques y fideicomisos

P1: ¿Cómo se llama un grupo de dominios de Windows que comparten el mismo espacio de nombres?

R1: Tree

P2: ¿Qué se debe configurar entre dos dominios para que un usuario del dominio A pueda acceder a un recurso en el dominio B?

R2: A Trust Relationship

## Tarea 9: Conclusión

En esta sala, mostramos los componentes y conceptos básicos relacionados con Active Directory y los dominios de Windows. Tenga en cuenta 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.

Si le interesa aprender a proteger una instalación de Active Directory, no olvide consultar la Sala de Fortalecimiento de Active Directory . Si, por otro lado, desea saber cómo los atacantes pueden aprovechar las configuraciones erróneas comunes de AD y otras técnicas de hackeo de AD , el módulo "Compromiso de Active Directory" es la solución ideal.

P: ¡Haz clic y continúa aprendiendo!

R: No se necesita respuesta

---

 **LinkedIn:** <https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/>

 **GitHub:** <https://github.com/MaateoSuar>