**Cuestiones teórico/prácticas**

1.- **(c.e. a), c.e. e). c.e. i))**

Contesta a las siguientes cuestiones realizando una captura de pantalla que corroboren lo contestado.

* En tu escenario tienes un dominio y un subdominio. ¿Qué servicio/s has tenido que instalar en ambos dominios? ¿Cuál es la configuración de red de ambos servidores?
* ¿Qué contiene la UO **Domain Controllers en ambos servidores**?
* ¿Qué tipo de **relación de confianza** existe entre ambos dominios?
* ¿Cuál es el **nivel funcional de tu bosque**?
* Demuestra que un usuario del subdominio puede acceder a una carpeta compartida en el dominio.

2.- **(c.e. b))**

Vamos a investigar sobre los roles FSMO. Estos roles son necesarios para el correcto funcionamiento de un dominio de AD. Contesta a las siguientes cuestiones realizando una captura de pantalla que corroboren lo contestado

* Busca información sobre los 5 roles FSMO.

**Roles a nivel de bosque:**

**-Schema Master:** El DC que tenga este rol es el único autorizado para modificar el esquema de AD. Cualquier cambio en el esquema, no importa desde que DC se haga, siempre está conectado al DC con el FSMO rol de Schema Master.

**-Domain Naming Master:** Se encarga de autorizar el alta o baja de dominios en el bosque, así como mantener una lista actualizada de todos los dominios existentes. También tinene la función de añadir o eliminar particiones de aplicación en AD.

**FSMO roles a nivel de dominio:**

**-PDC Emulator (Emulador de PDC - Primary Domain Controller):** Este tiene las siguiéntes funciones:

- Recibe las actualizaciones de las contraseñas de usuarios y equipos.

- Crea y actualiza las políticas de grupo (cuando modificamos las políticas del dominio desde la Group Policy Managment Console), esta trata de conectarse siempre al DC con el FSMO rol de PDC).

- Sincroniza tiempos, sólo él puede sincronizar la hora con un servidor externo. Los demás DCs sincronizarán la hora con él.

- Debe estar siempre online y accesible.

Es recomendable que el PDC Emulator y el RID Master residan en el mismo DC.

**-RID Master:** En un dominio, cuando se crea un objeto (sea un usuario, un grupo o un equipo), se le asigna un SID (Security Identifier) que es único y que nunca es reutilizado incluso aunque el objeto sea eliminado.

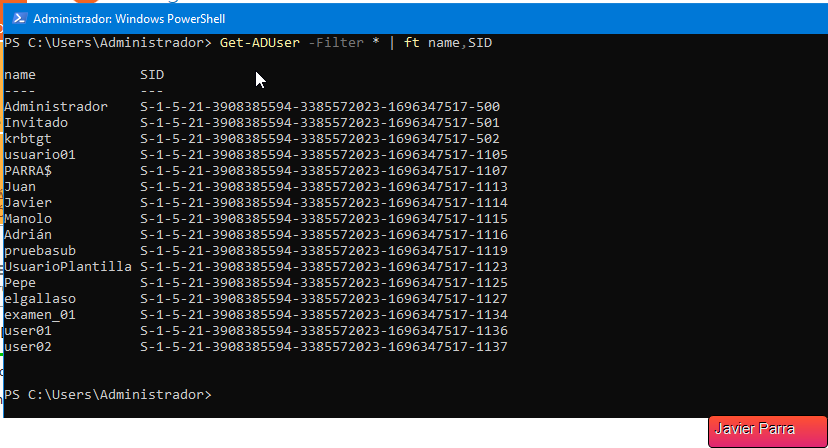
Un SID consta de tres partes:

- La primera parte es un identificador asignado por ISO que especifica:

**S-1:** Especifica que la cadena es un SID y la versión actual es 1.

**5:** Identifica a la autoridad (5 es para NT Authority, indica que es un SID específico de Windows)

**21:** Indica que lo que viene a continuación es un Domain ID



**- El Domain Identifier (Domain ID)** es un identificar del dominio, todas las cuentas de usuario, grupo y equipo de un mismo dominio comparten estos datos.

**- El Relative Identifier (RID)** es un número que se asigna de forma secuencial a partir del número 1000 a cada nuevo objeto que se crea en el dominio. Para los objetos creados por defecto en el sistema existen una serie de RIDs estándar: 500, para el administrador, 501 para el usuario invitado, 502 para el Kerberos Key Distribution Center...

**- Infraestructure Master:** En un entorno multidominio, es el responsable de actualizar las referencias de los objetos de un dominio en los objetos de otros dominios. Se encarga de traducir los GUIDs, los SIDs y los DNs de los objetos de otros dominios.

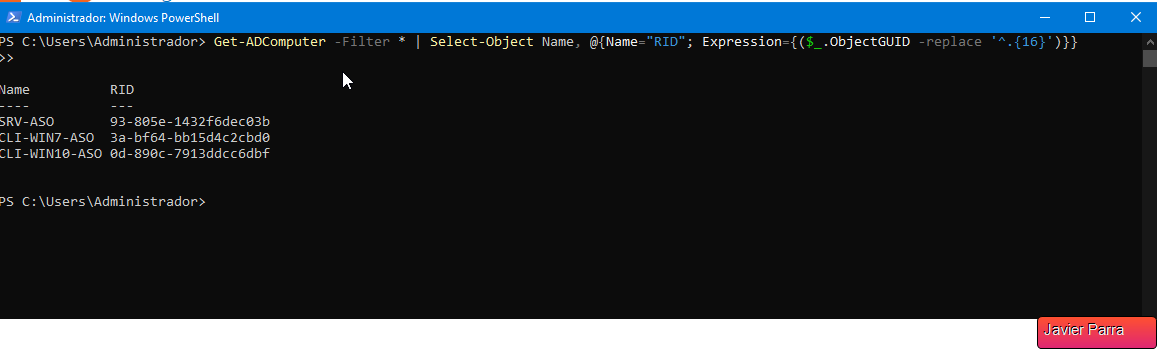
-Este rol sólo tienen trabajo cuando estamos en un entorino multidominio, y ninca debería estar ubicado en un DC que sea a su vez Global Catalog. Cuando un DC es Catálogo Global, este recibe actualizaciones periódicas de los objetos de todos los dominios mediante la replicación, de forma que la información sobre esos objetos siempre está actualizada.

- Si el maestro de infraestructuras y el GC se encuentran en el mismo DC, el maestro de infraestructuras no funcionará ya que nunca encontrará información actualizada, por lo que nunca se replicará los cambios a otros DCs del dominio.

- Si todos los DCs son Global Catalog, todos tendrán los datos más actuales y será irrelevante conocer el DC que disponga el rol de maestro de infraestructuras.

* ¿Cuáles son los RIDs de tus equipos clientes?

**> Get-ADComputer -Filter \* | Select-Object Name, @{Name="RID"; Expression={($\_.ObjectGUID -replace '^.{16}')}}**



* ¿Cuál puede ser el motivo de querer transferir un rol FSMO?

Puede ser por que queramos realizar un mantenimiento del servidor, por lo que es recomendable transferir el rol a otro servidor para evitar interrupciones en las operaciones de Active Directory.

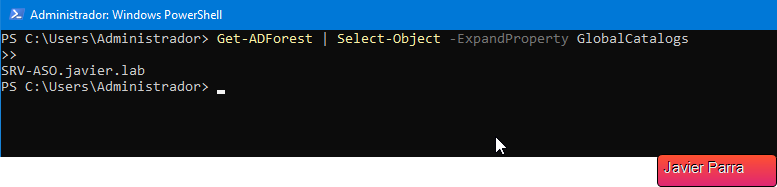
* ¿Qué significa Catálogo Global? Mis servidores, ¿son Catálogo Global?

**Un catálogo global GC es un almacén de información en un servidor de Active Directory que contiene una copia parcial de todos los objetos de directorio en el bosque de Active Directory. Estos objetos incluyen usuarios, grupos y recursos compartidos , entre otros.**

**El propósito principal de un catálogo global es facilitar búsquedas rápidas y eficientes en todo el bosque de Active Directory.**

**Usamos el siguiente comando PowerShell para saber si mi servidor está configurado como catálogo global:**

**> Get-ADForest | Select-Object -ExpandProperty GlobalCatalogs**



3**.- (c.e. c))**

* ¿Cuál es el propósito de instalar LDAP?
* Explica el proceso de instalación (paquetes, dependencias, …). LDAP ¿es un servicio?
* ¿Qué objetos has creado en LDAP? ¿Para qué?
* LDAP puede ser de gran utilidad junto a otros servicios, especialmente los relacionados con servidores de ficheros. En tu caso, ¿con qué servidor de ficheros lo has relacionado? ¿Cuál es la utilidad?

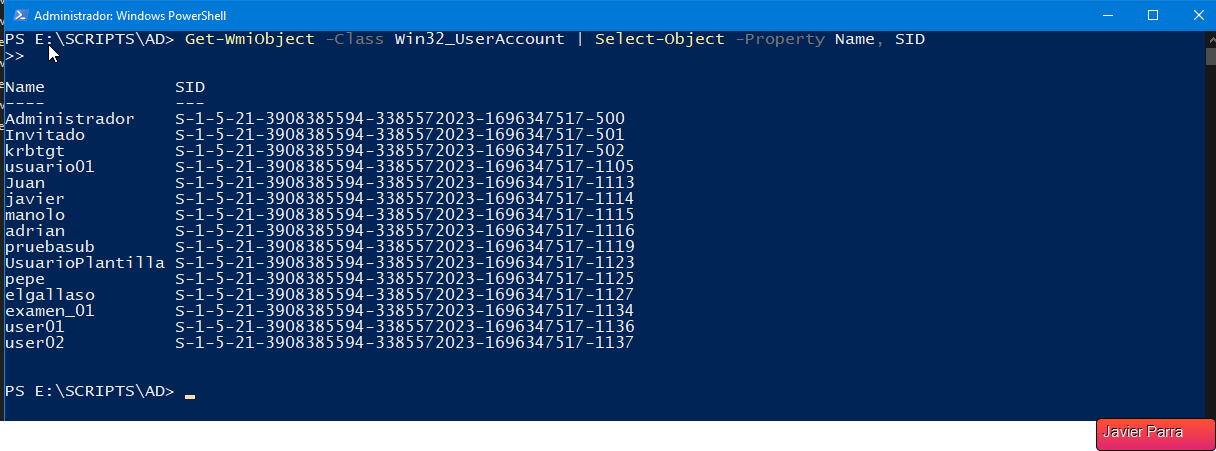
4.- **(c.e. d))**

* En el contexto de Active Directory, ¿qué es **WMI**? Diseña un ejemplo de aplicación.

Windows Management Instrumentation (WMI) es un marco de herramientas del sistema que se ha integrado en el sistema operativo Windows. Se puede acceder a WMI a través de las redes y permite a los usuarios consultar los sistemas remotos para obtener información sobre ellos. WMI es potente y flexible, y si se usa correctamente puede suministrar la información más importante sobre sus computadoras, servidores y equipos virtuales de Hyper-V.

Con el siguiente comando podemos recuperar las cuentas de usuario con su SID:

>Get-WmiObject -Class Win32\_UserAccount | Select-Object -Property Name, SID



5.- **(c.e. f))** En AD hay muchísimos objetos.

* Diseña un breve manual que ayude a los usuarios a realizar búsquedas de usuarios, grupos, equipos, etc.
* Diseña un breve manual que ayude a los usuarios a saber dónde buscar configuraciones a realizar en una GPO. Por ejemplo, quiero evitar que en los equipos clientes utilicen unidades extraíbles.

6.- (**c.e. g**))

* ¿Cómo puedes conseguir que los usuarios del dominio tengan a su disposición una carpeta cuyo nombre es su login?
* Un equipo del dominio, ¿**tiene contraseña**? En caso afirmativo, ¿cómo se le asigna? ¿Tiene fecha de caducidad?
* Modifica la política de seguridad de cuentas de usuario: esta se debe bloquear al tercer intento fallido y sólo el administrador la puede desbloquear. Los usuarios deben cambiar la contraseña a los 45 días. Deben recordar 3 contraseñas anteriores.