La Salle Institución	DEPARTAMENTO INFORMÁTICA	
	ADMINISTRACIÓN DE SISTEMAS OPERATIVOS	
	BOSQUE DE BONSAIS	

- Nombre y apellidos: Miguel Enrique Crespo Brito

1. OBJETIVO

- REALIZAR PRUEBAS DE COMPROBACIÓN Y EVIDENCIARLAS PARA

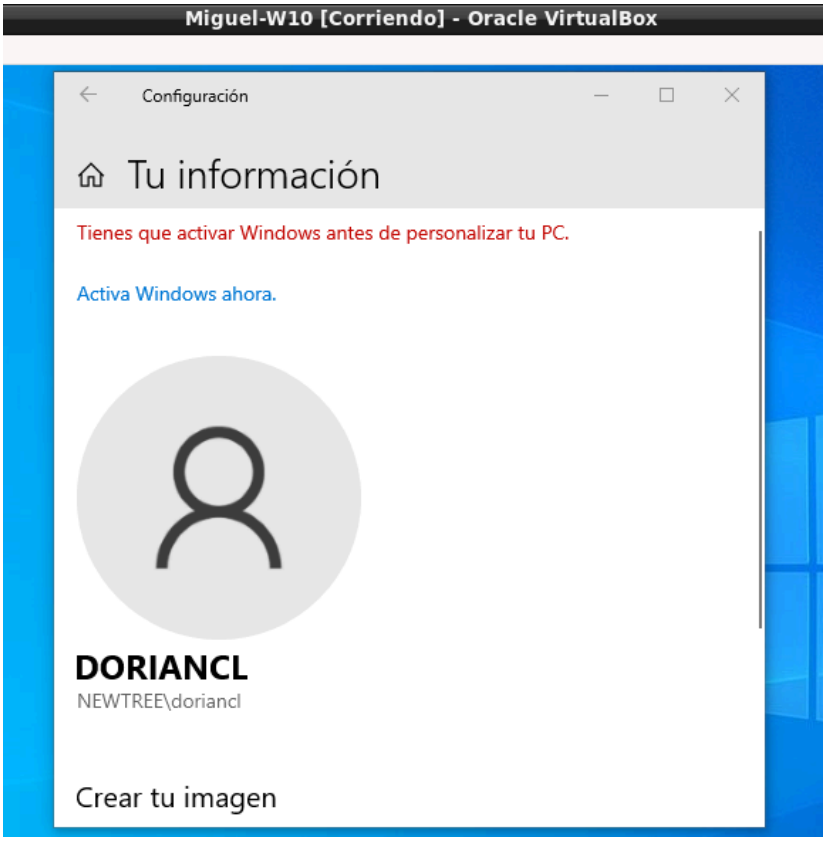
ALERTA: ESTA PRACTICA SE ESTA HACIENDO SIN DOS INTEGRANTES DEL GRUPO, NO HAN VENIDO A CLASES Y NO PODEMOS PERDER EL TIEMPO. SE HA HECHO LO QUE SE PUDO.

2. ADUC – ADMINISTRADOR DE EMPRESA.

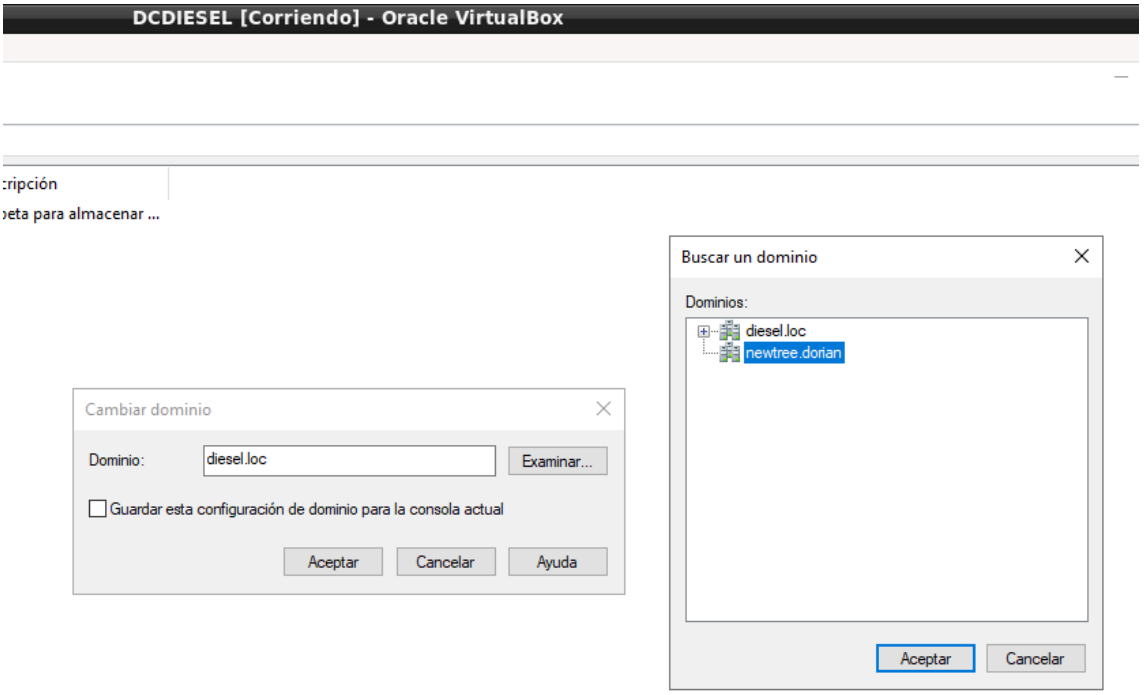
EVIDENCIAR

0.- Cualquier usuario puede iniciar sesión bajo cualquier dominio.

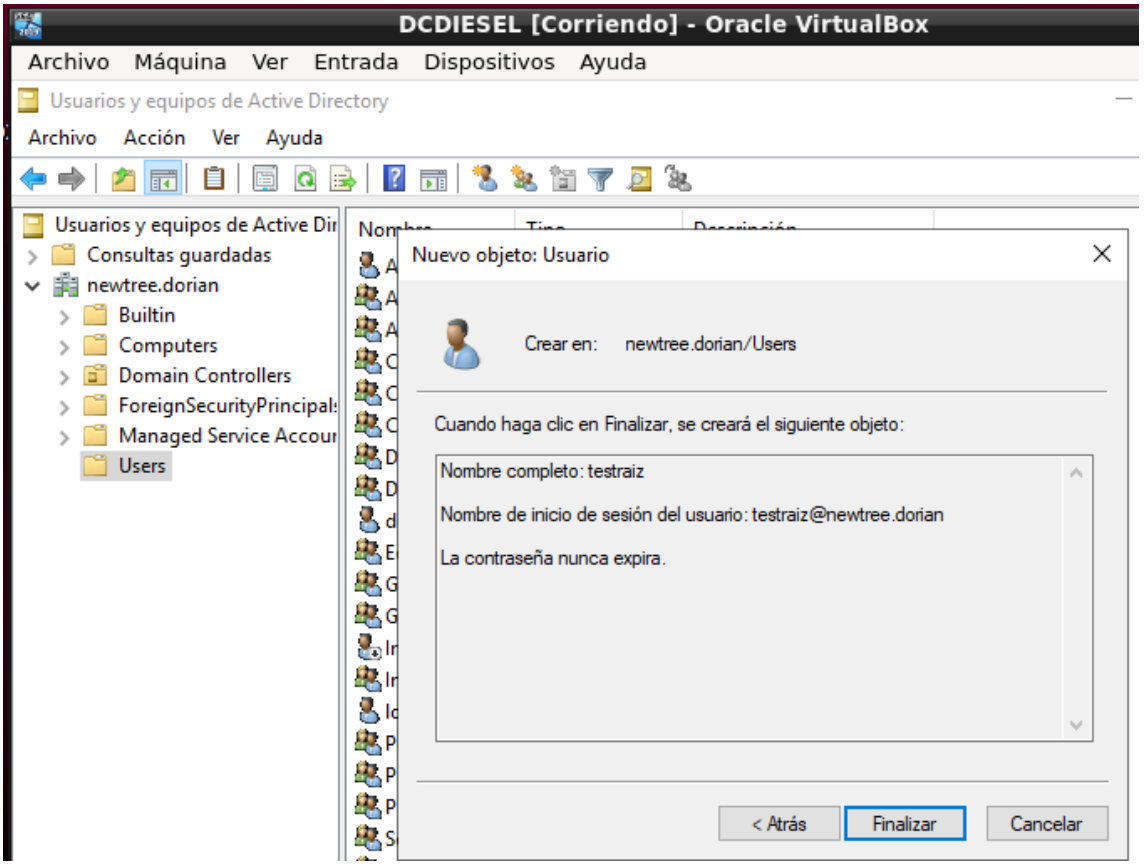
Puedo entrar con el cliente de dorian de su dominio.



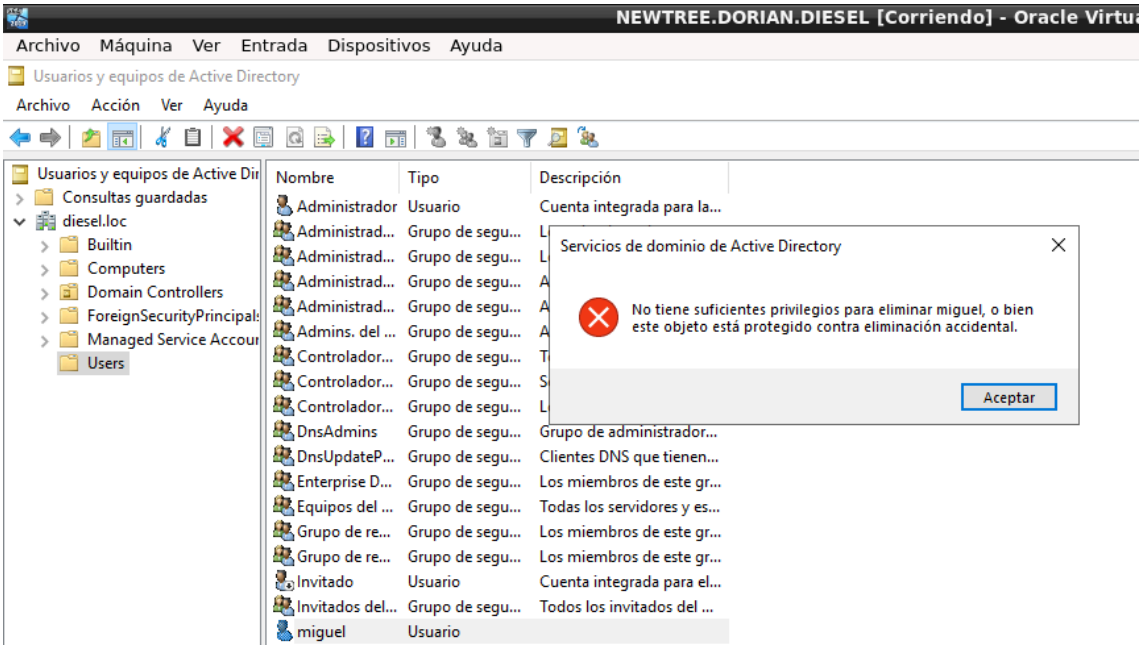
1.- En ADUC cualquier administrador de dominio puede acceder al directorio de otros dominios.



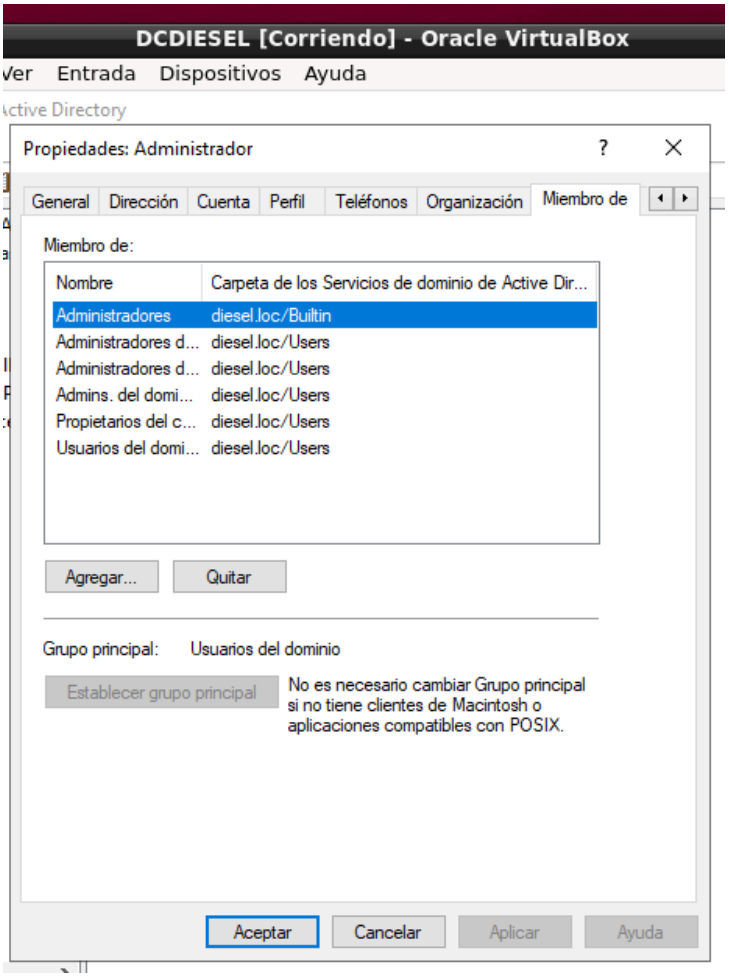
2.- El Administrador del dominio Raíz puede crear usuarios y realizar modificaciones en el Directorio de otros dominios.

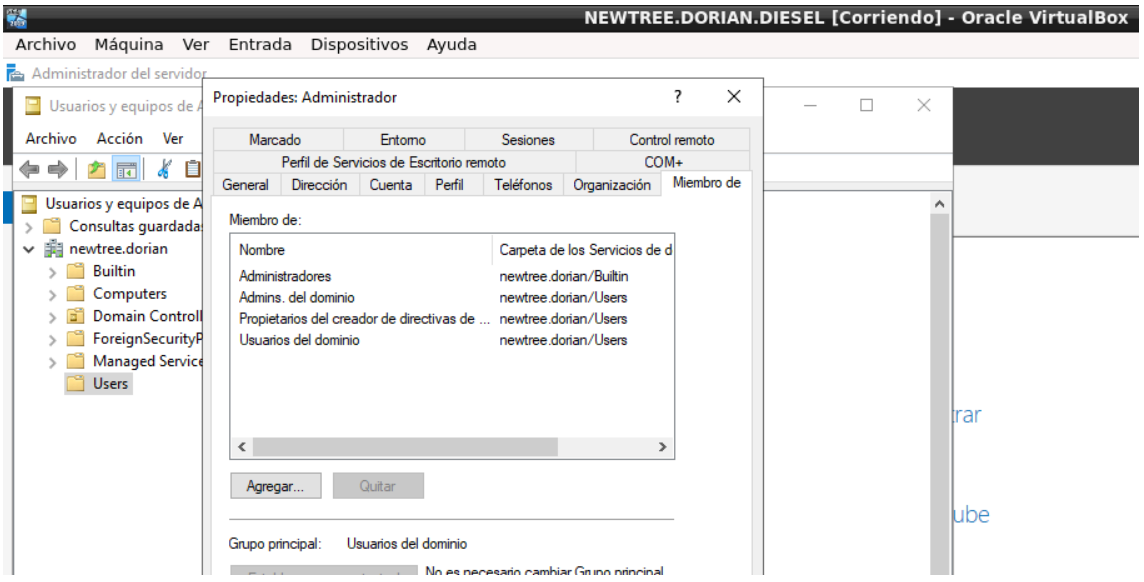


3.- Los administradores de los subdominios pueden consultar otros directorios, pero no pueden crear-modificar-eliminar usuarios fuera de su dominio.



4.- Realizar una comparación de las propiedades del Administrador en Pertenencia a grupos. Hay claras diferencias entre el administrador Raiz y los demás.

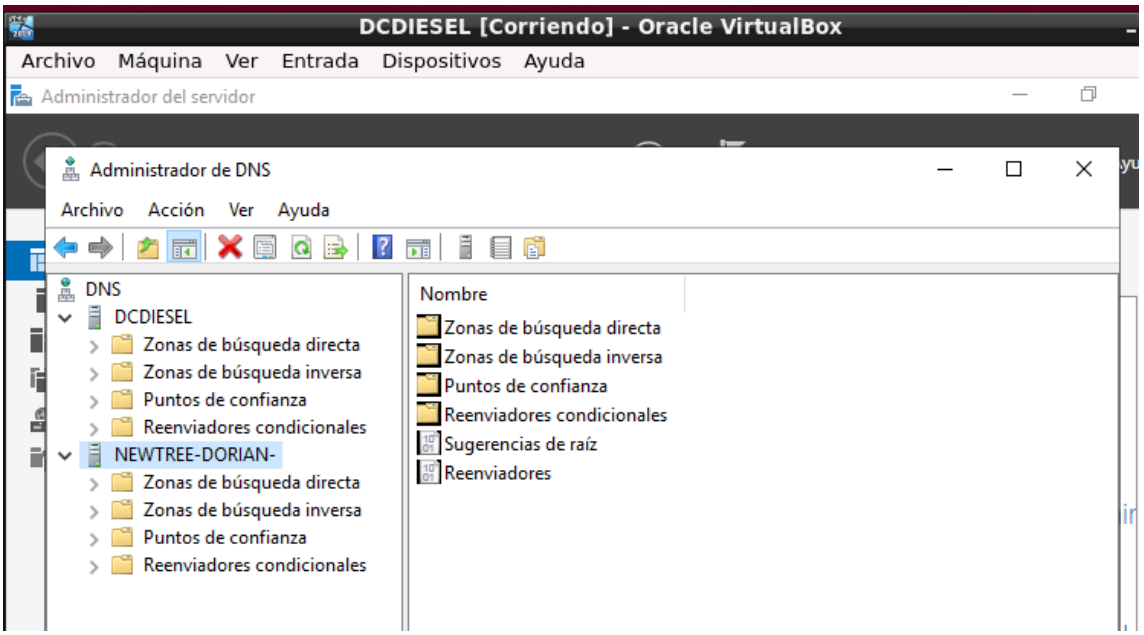


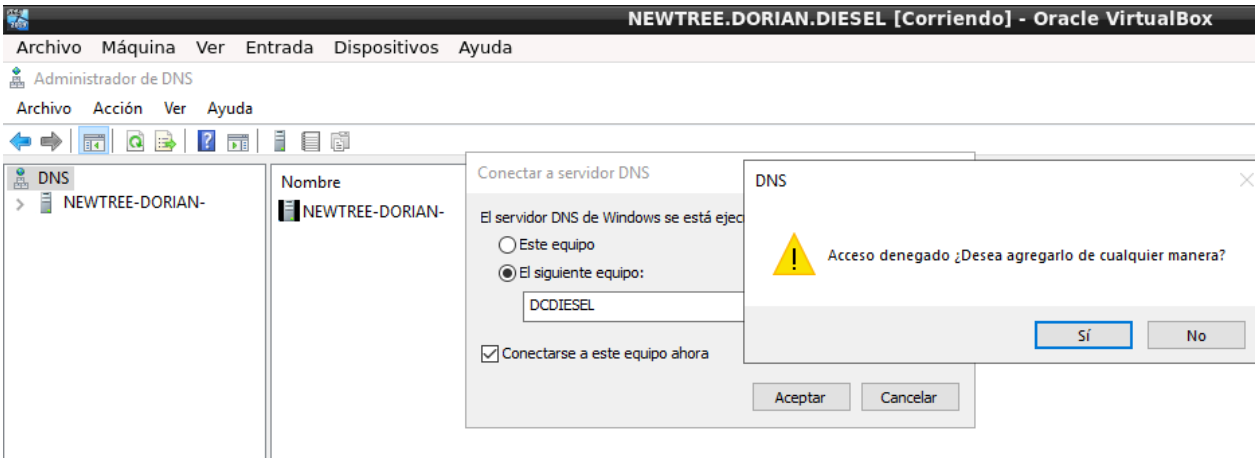


3. DNS

1.- Examinar las herramientas DNS de todos los dominios e intentar agregar además del DNS local, los demás. Solamente se acepta en el dominio raíz

EVIDENCIAS

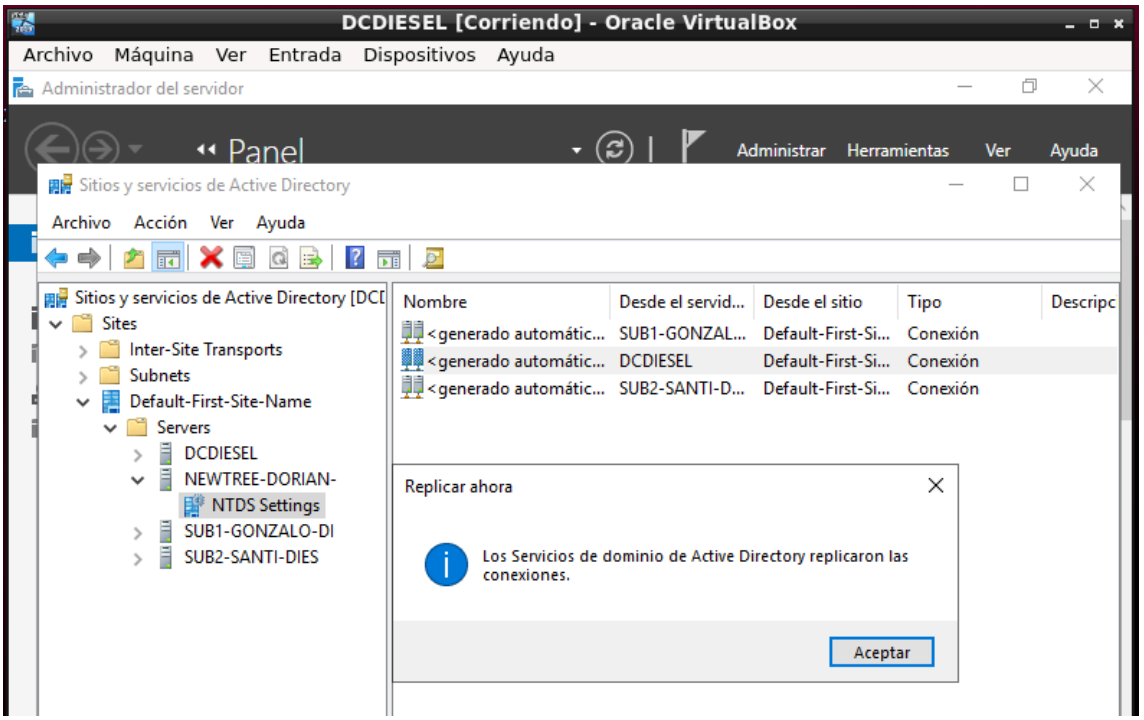




Es totalmente normal y es un comportamiento esperado en una jerarquía de Active Directory (AD) y DNS.

En los Controladores de Dominio (DC) de los subdominios, la herramienta DNS solamente muestra el servidor local porque el método preferido de resolución de nombres a través del bosque es la delegación y los reenviadores condicionales, no la adición manual de servidores.

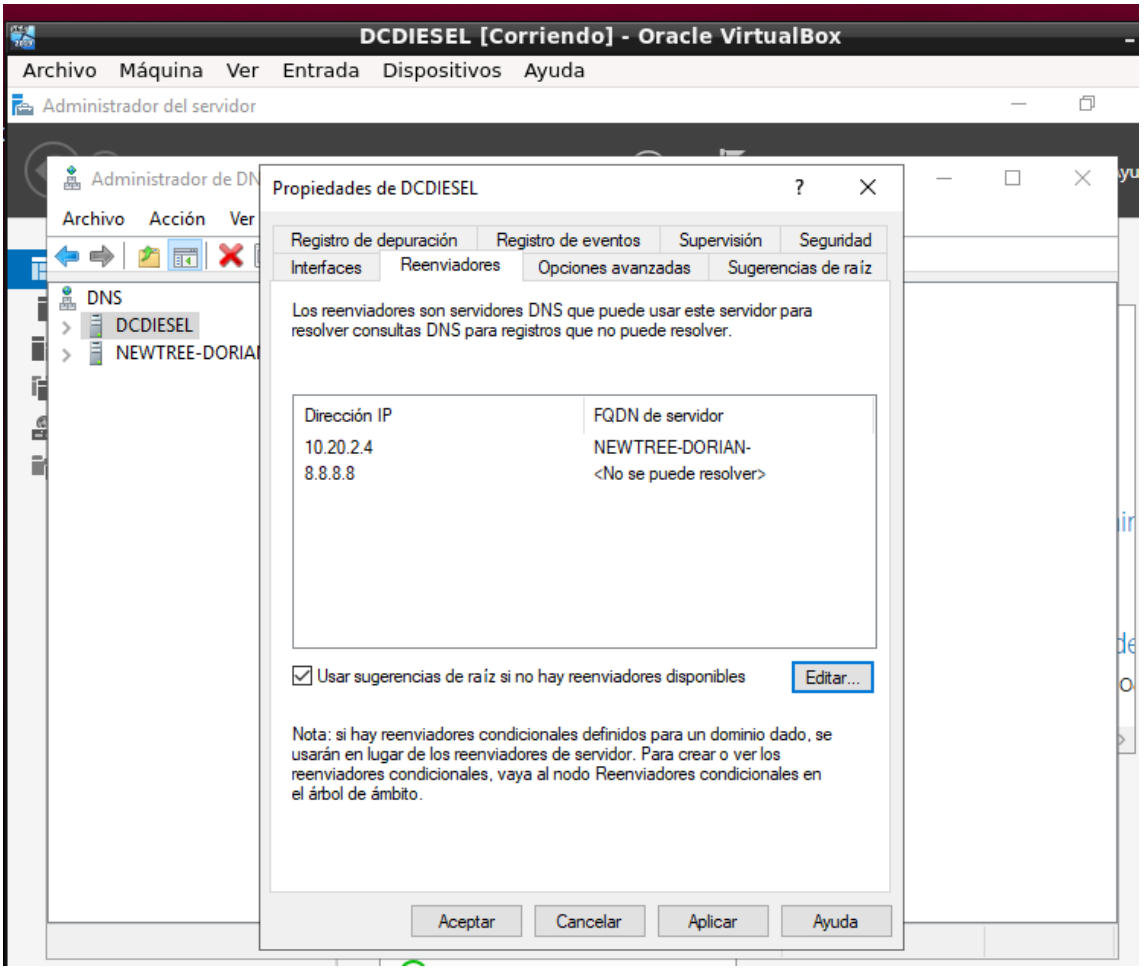
2.- Forzar la sincronización DNS. Hay varios métodos. Buscar cómo podemos replicar el servicio DNS desde la Herramienta Sitios y Servicios de Active Directory.



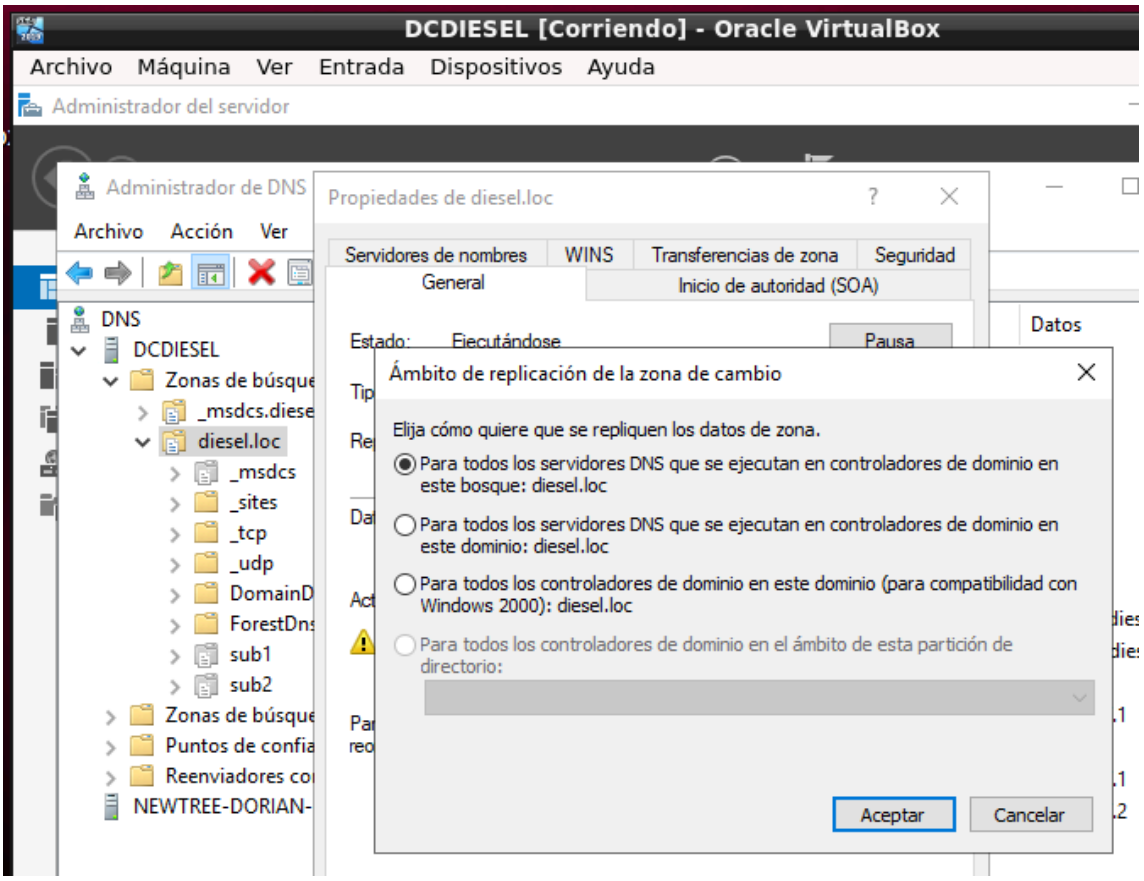
3.- Programar en el DNS RAIZ los reenviadores y la replicación hacia todo el bosque de la zona de búsqueda directa.

EVIDENCIAS

Reenviadores (Forwarders):



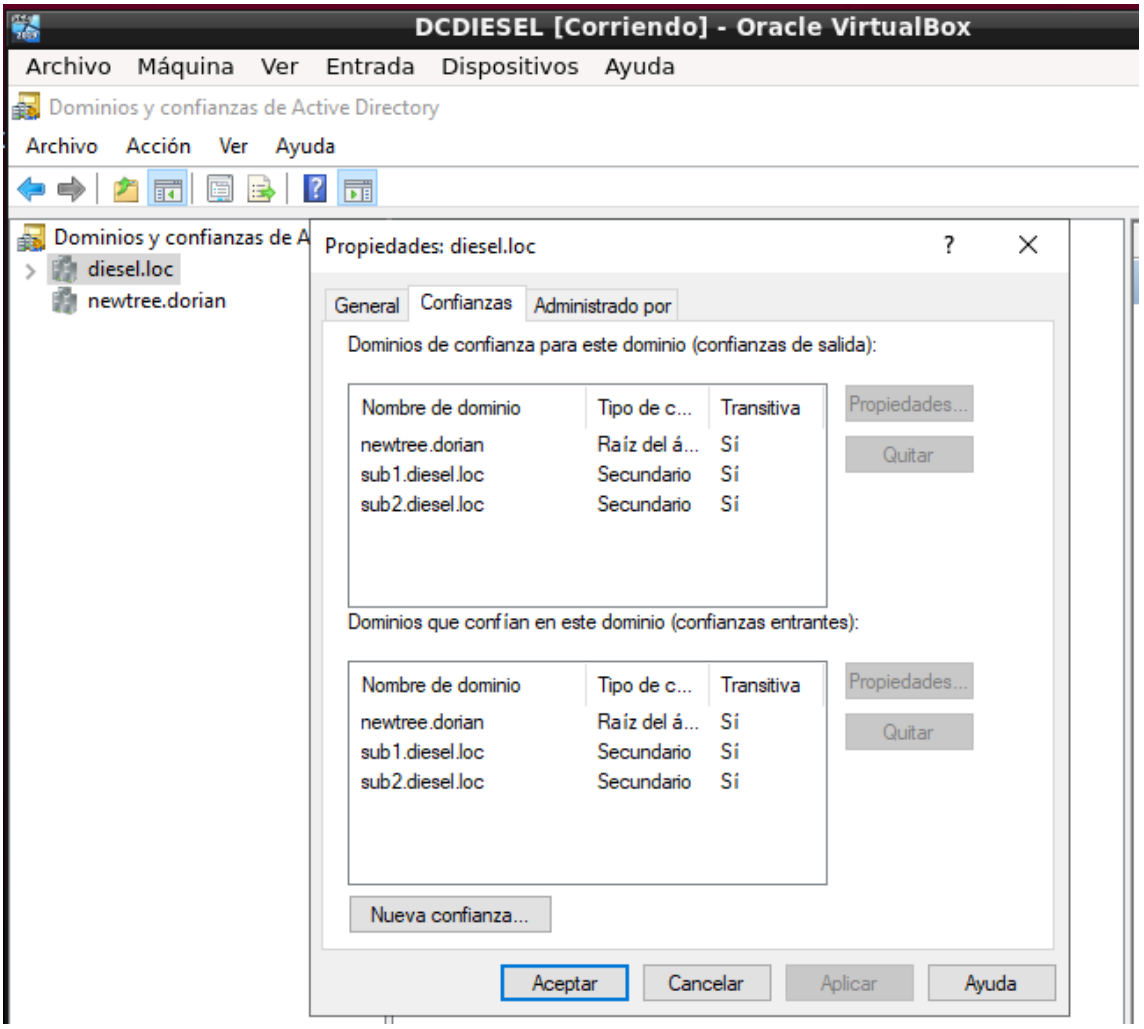
Replicación de Zona:



4. DOMINIOS Y CONFIANZAS DE ACTIVE DIRECTORY

En esta herramienta podemos acceder a las propiedades de cada dominio para comprobar las relaciones de confianza entre dominios.

EVIDENCIAS



5. FSMO – MAESTROS DE OPERACIONES

Aun teniendo un pequeño bosque, podemos comprobar si están los 5 roles FSMO adjudicados:

ROLES A NIVEL DE BOSQUE

1.- Schema Master (Maestro de esquema) Controla todas las actualizaciones y modificaciones al **ESQUEMA** de Active Directory.

2.- Domain Naming Master (Maestro de nombres de dominio) Responsable de **agregar o eliminar dominios en el bosque**.

ROLES A NIVEL DE DOMINIO

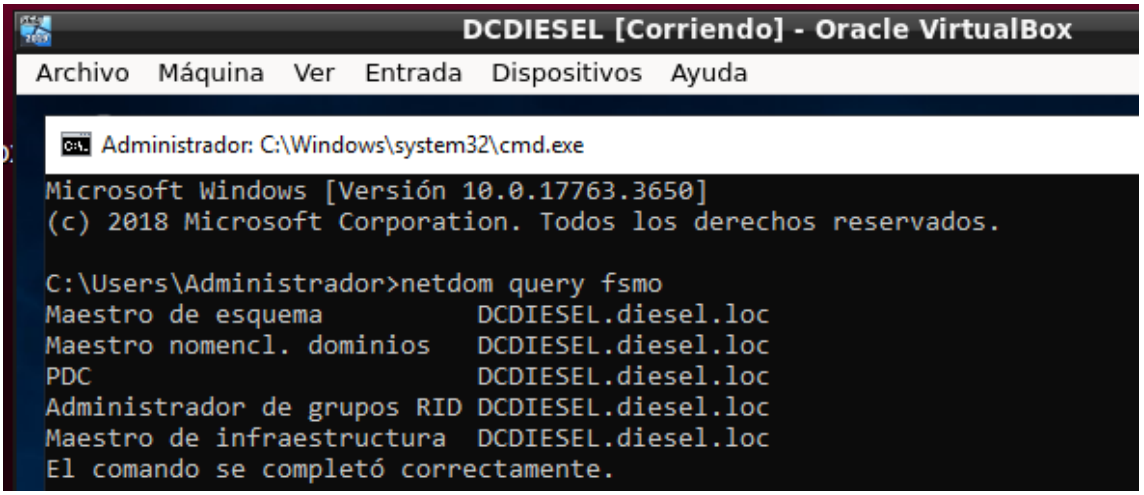
3.- RID Master (Maestro RID) Asigna bloques de identificadores únicos (**RIDs**) a los controladores de dominio para la creación de objetos.

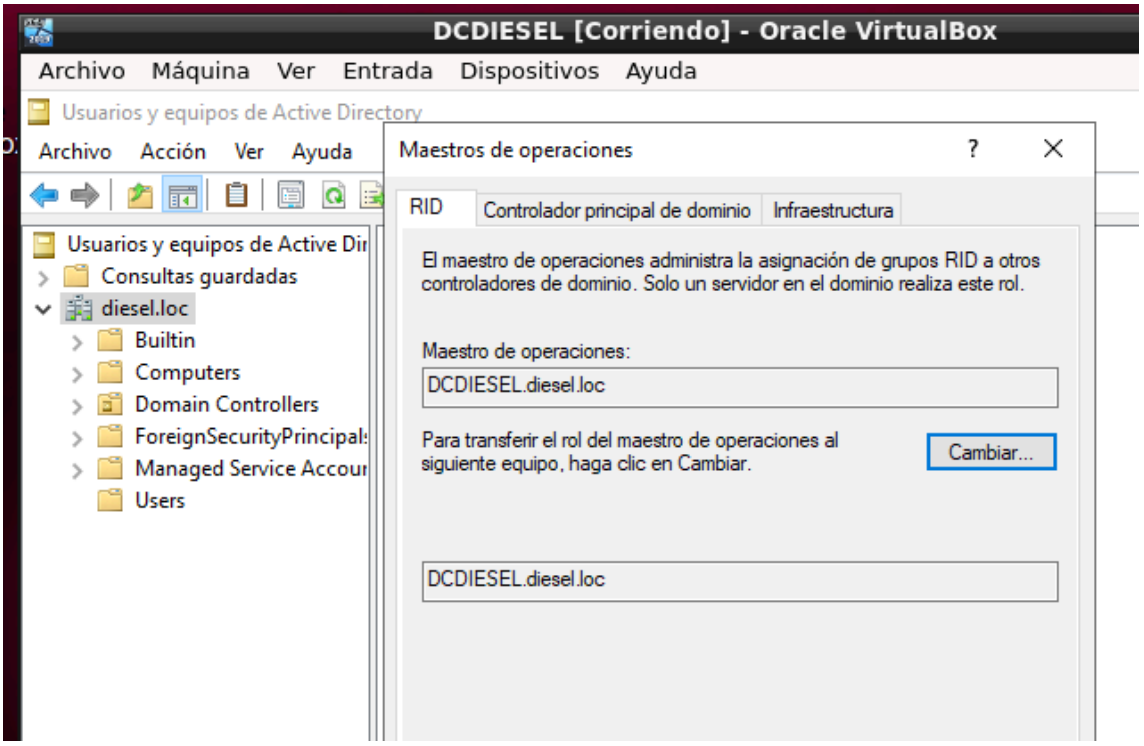
4.- PDC Emulator (Emulador PDC)

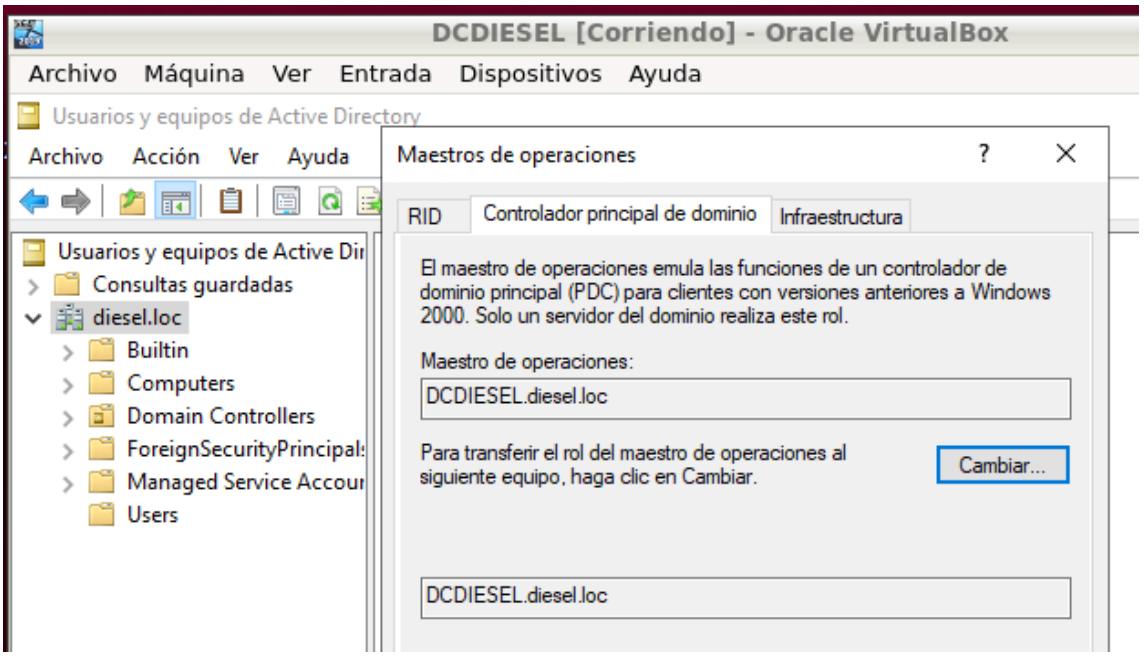
Emula un controlador de dominio primario para compatibilidad con **sistemas antiguos**. También gestiona la **sincronización de contraseñas** y la resolución de conflictos de autenticación.

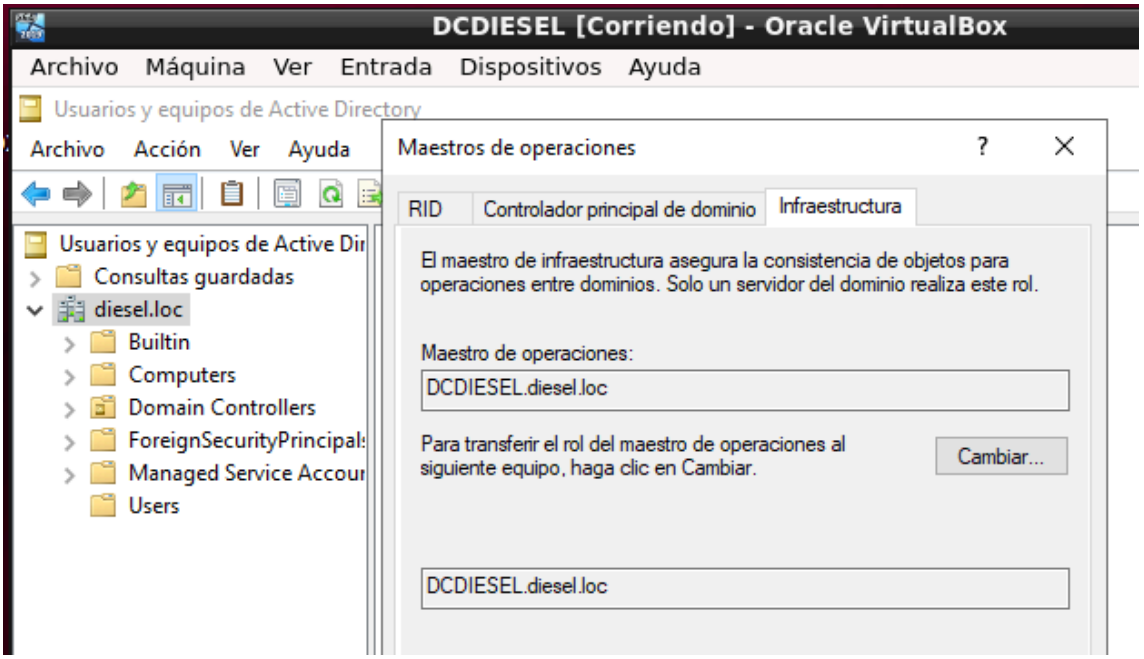
5.- Infrastructure Master (Maestro de infraestructura) Actualiza referencias de objetos entre dominios (por ejemplo, usuarios de otros dominios en **grupos locales**).

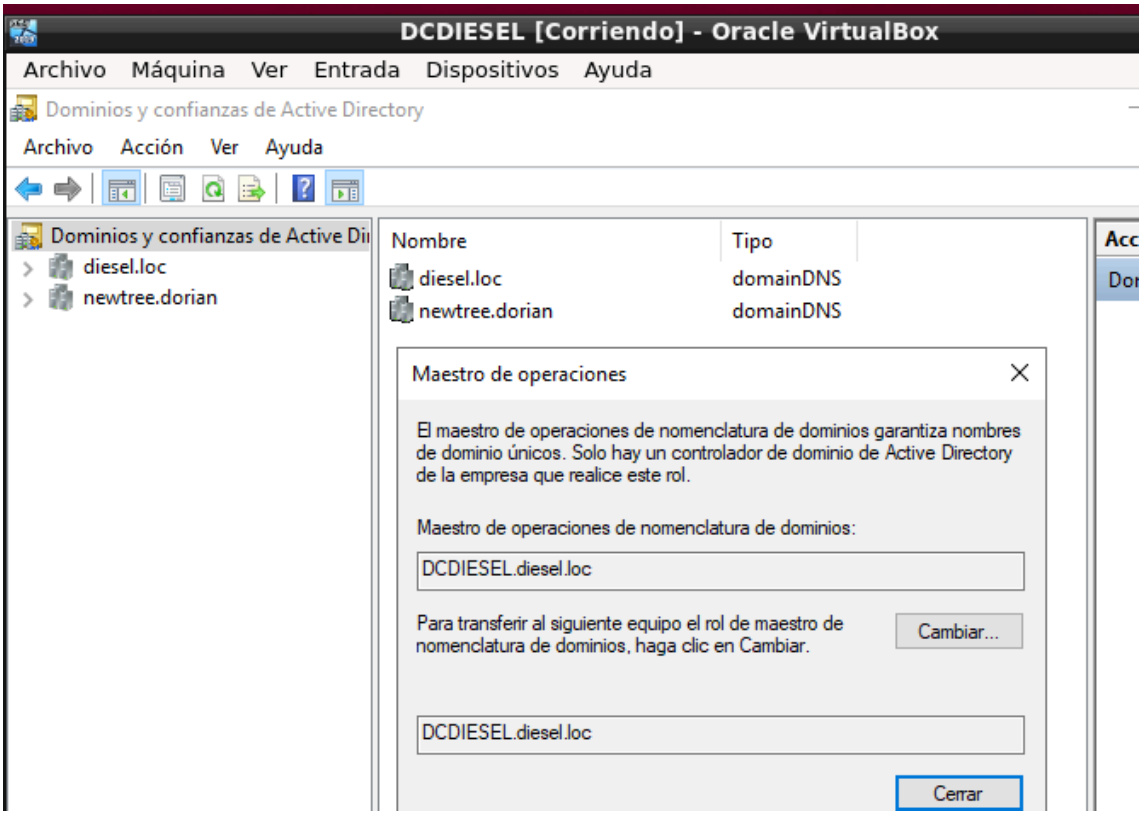
EVIDENCIAS: Buscar y mostrar de cada controlador qué roles de Maestros de Operaciones tienen. Desde **ADUC** y desde la consola **cmd**.




DCDIESEL [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Usuarios y equipos de Active Directory
Archivo Acción Ver Ayuda
Usuarios y equipos de Active Dir
Consultas guardadas
diesel.loc
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Maestros de operaciones
RID
Controlador principal de dominio
Infraestructura
El maestro de operaciones administra la asignación de grupos RID a otros controladores de dominio. Solo un servidor en el dominio realiza este rol.
Maestro de operaciones:
DCDIESEL.diesel.loc
Para transferir el rol del maestro de operaciones al siguiente equipo, haga clic en Cambiar.
Cambiar...
DCDIESEL.diesel.loc

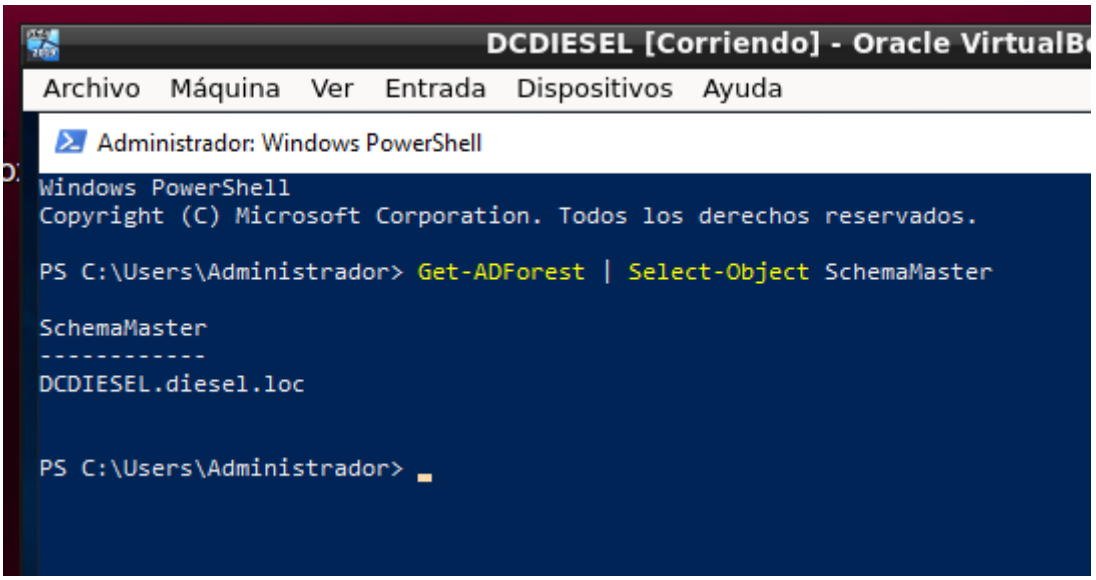

DCDIESEL [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Usuarios y equipos de Active Directory
Archivo Acción Ver Ayuda
Usuarios y equipos de Active Dir
Consultas guardadas
diesel.loc
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Maestros de operaciones
RID
Controlador principal de dominio
Infraestructura
El maestro de operaciones emula las funciones de un controlador de dominio principal (PDC) para clientes con versiones anteriores a Windows 2000. Solo un servidor del dominio realiza este rol.
Maestro de operaciones:
DCDIESEL.diesel.loc
Para transferir el rol del maestro de operaciones al siguiente equipo, haga clic en Cambiar.
Cambiar...
DCDIESEL.diesel.loc


DCDIESEL [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Usuarios y equipos de Active Directory
Archivo Acción Ver Ayuda
Usuarios y equipos de Active Dir
Consultas guardadas
diesel.loc
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal
Managed Service Accour
Users
Maestros de operaciones
RID
Controlador principal de dominio
Infraestructura
El maestro de infraestructura asegura la consistencia de objetos para operaciones entre dominios. Solo un servidor del dominio realiza este rol.
Maestro de operaciones:
DCDIESEL.diesel.loc
Para transferir el rol del maestro de operaciones al siguiente equipo, haga clic en Cambiar.
Cambiar...
DCDIESEL.diesel.loc


DCDIESEL [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Dominios y confianzas de Active Directory
Archivo Acción Ver Ayuda
Dominios y confianzas de Active Dir
diesel.loc
newtree.dorian
Nombre
Tipo
diesel.loc
domainDNS
newtree.dorian
domainDNS
Maestro de operaciones
El maestro de operaciones de nomenclatura de dominios garantiza nombres de dominio únicos. Solo hay un controlador de dominio de Active Directory de la empresa que realice este rol.
Maestro de operaciones de nomenclatura de dominios:
DCDIESEL.diesel.loc
Para transferir al siguiente equipo el rol de maestro de nomenclatura de dominios, haga clic en Cambiar.
Cambiar...
DCDIESEL.diesel.loc
Cerrar

5.1 SCHEMA MASTER (MAESTRO DE ESQUEMA)

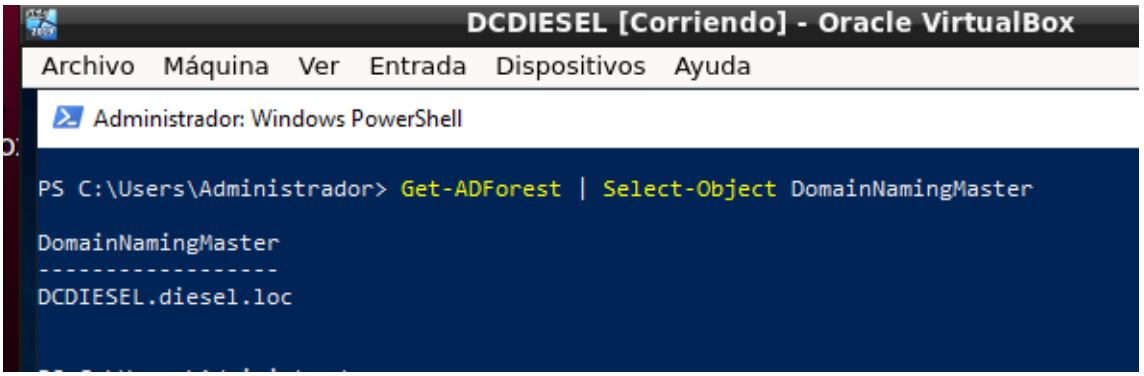
Cómo podemos saber quién es el maestro de Esquema en PowerShell. Procedimiento y evidencias.



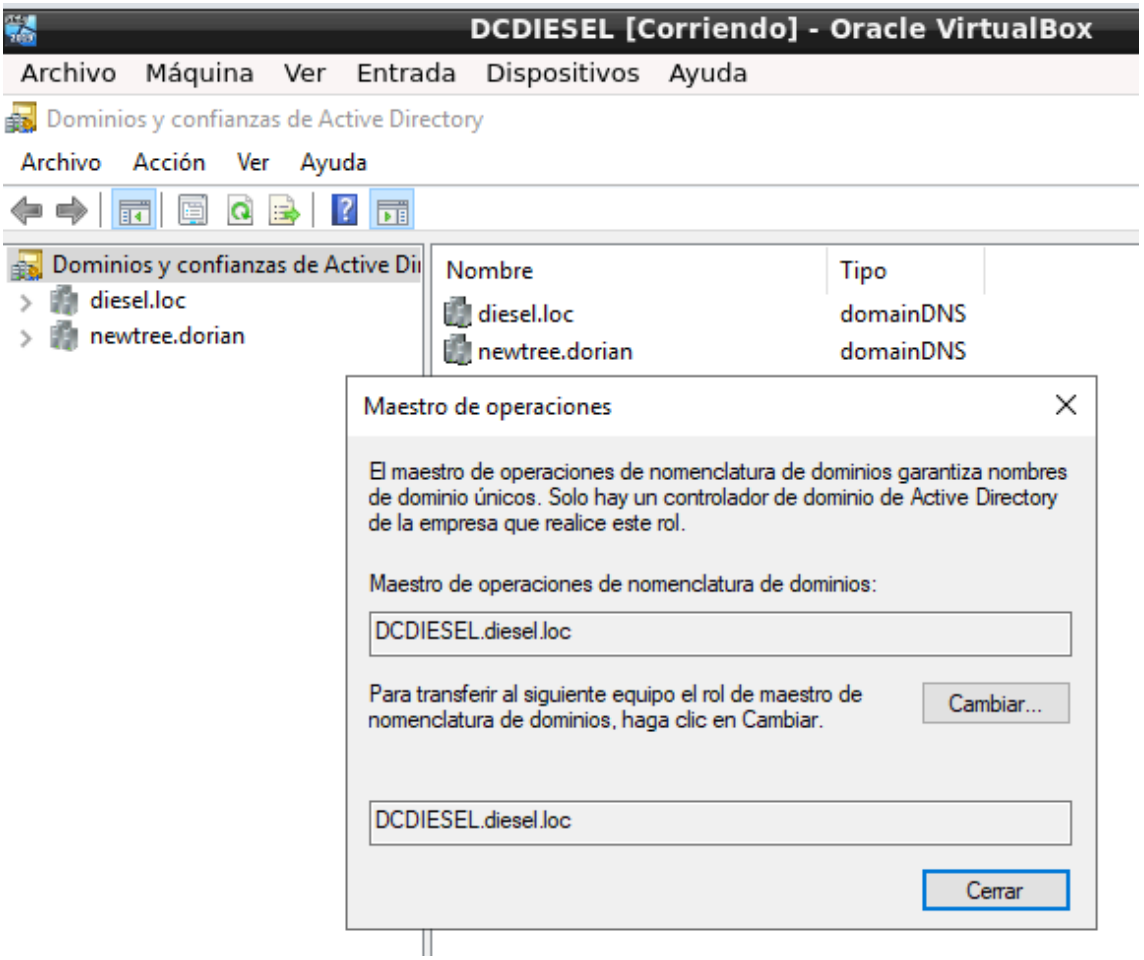
5.2 DOMAIN NAMING MASTER

Hay varios métodos para saber quién es el maestro de Nombres de Dominio. Procedimientos y evidencias. Desde PowerShell y Dominios y Confianzas.

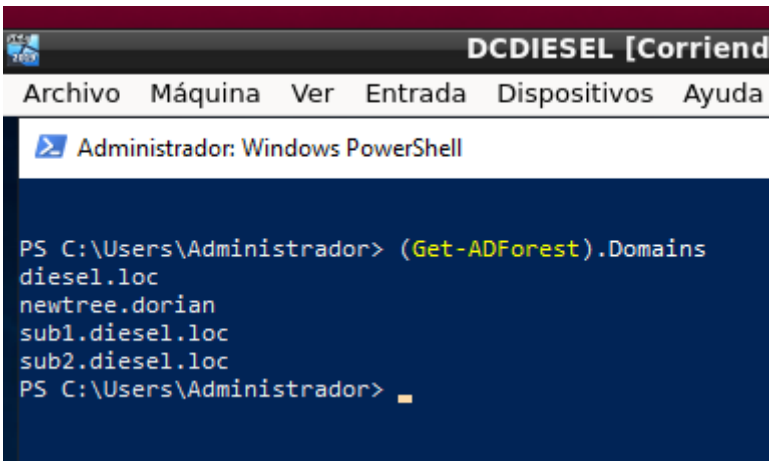
PS



En dominios y confianzas



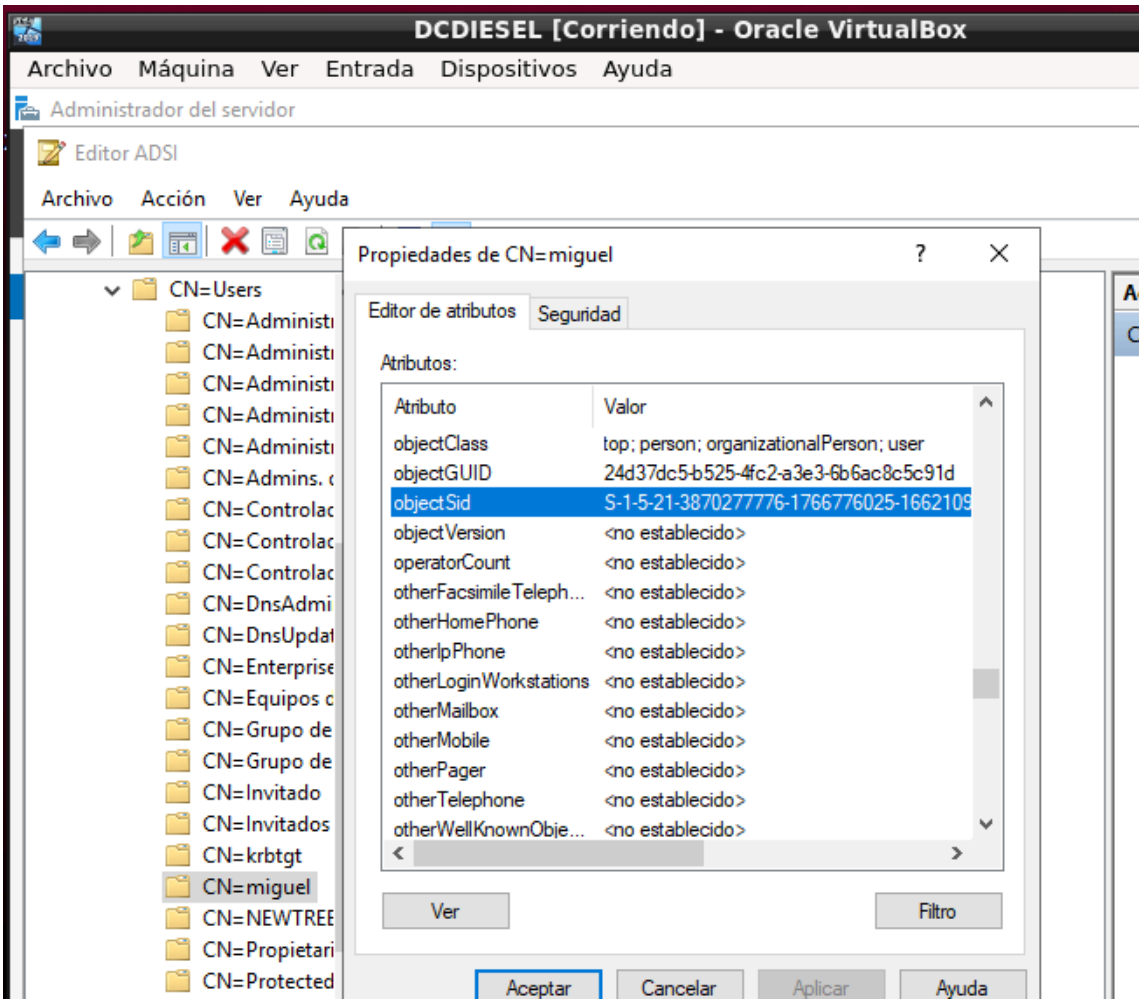
Hay un método para saber cuántos dominios existen en el bosque con PowerShell. Procedimiento y evidencia.



5.3 MAESTRO DE RDI

Para los tres dominios creados en el bosque buscar el SID del usuario creado en cada dominio.

Buscar el SID en el editor ADSI que en realidad estará compuesto por SID-RID (últimos 4 números o más). Ese valor es el RID empleado en cada dominio.



S-1-5-21-3870277776-1766776025-1662109121-1107

A través de **cmd** también se puede obtener datos del RDI actual – rango etc… Explorar esta opción y evidenciarla. Hacerlo en los tres controladores.

dcdiag /test:ridmanager /v

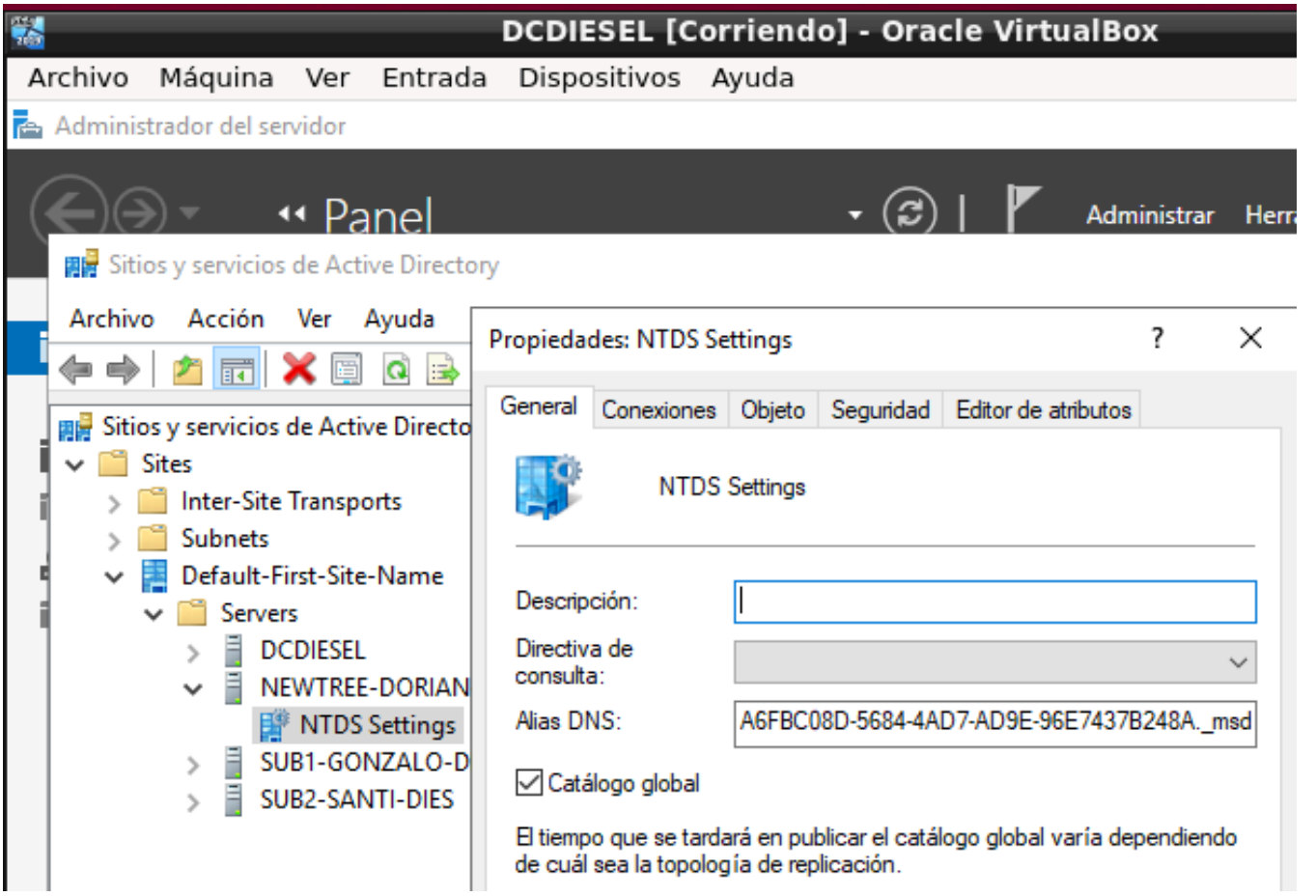
```
Realizando pruebas requeridas iniciales

   Probando servidor: Default-First-Site-Name\DCDIESEL
      Iniciando prueba: Connectivity
         * Active Directory LDAP Services Check
         Determining IP4 connectivity
         * Active Directory RPC Services Check
         ..... DCDIESEL superó la prueba Connectivity
```

```
      Iniciando prueba: RidManager
         * Available RID Pool for the Domain is 2100 to 1073741823
         * DCDIESEL.diesel.loc is the RID Master
         * DsBind with RID Master was successful
         * rIDAllocationPool is 1100 to 1599
         * rIDPreviousAllocationPool is 1100 to 1599
         * rIDNextRID: 1109
         ..... DCDIESEL superó la prueba RidManager
      Prueba omitida por solicitud del usuario: Services
```

6. CATALOGO GLOBAL

El catálogo es único, pero debe haber un servidor del catálogo global por dominio.

EVIDENCIA: Buscar cómo identificar-comprobar los Servidores del Catálogo Global del Bosque.



6.1 LPD.EXE

Desde esta herramienta podemos hacer consultas LDAP a la partición de dominio de la Base de Datos y también al Catálogo Global.

- Conexión a puerto 389 para conexiones estándar.
- Conexión al puerto 3268 para consultas al catálogo global.

Desde un controlador de dominio de un subdominio conectaros mediante la herramienta LPD, solicitar dos instancias, una para cada puerto y realizar una consulta sobre un usuario, equipo en ambas. La información proviene de distinta partición de la base de datos. Tiene que ser más extendida desde la partición de Dominio y más resumida, pero esencial desde el Catálogo Global.

7. GRUPO DE SEGURIDAD DE AMBITO LOCAL

Vamos a crear un recurso compartido,

RECORDATORIO:

Los grupos de seguridad pueden ser de ámbito global o de ámbito local.

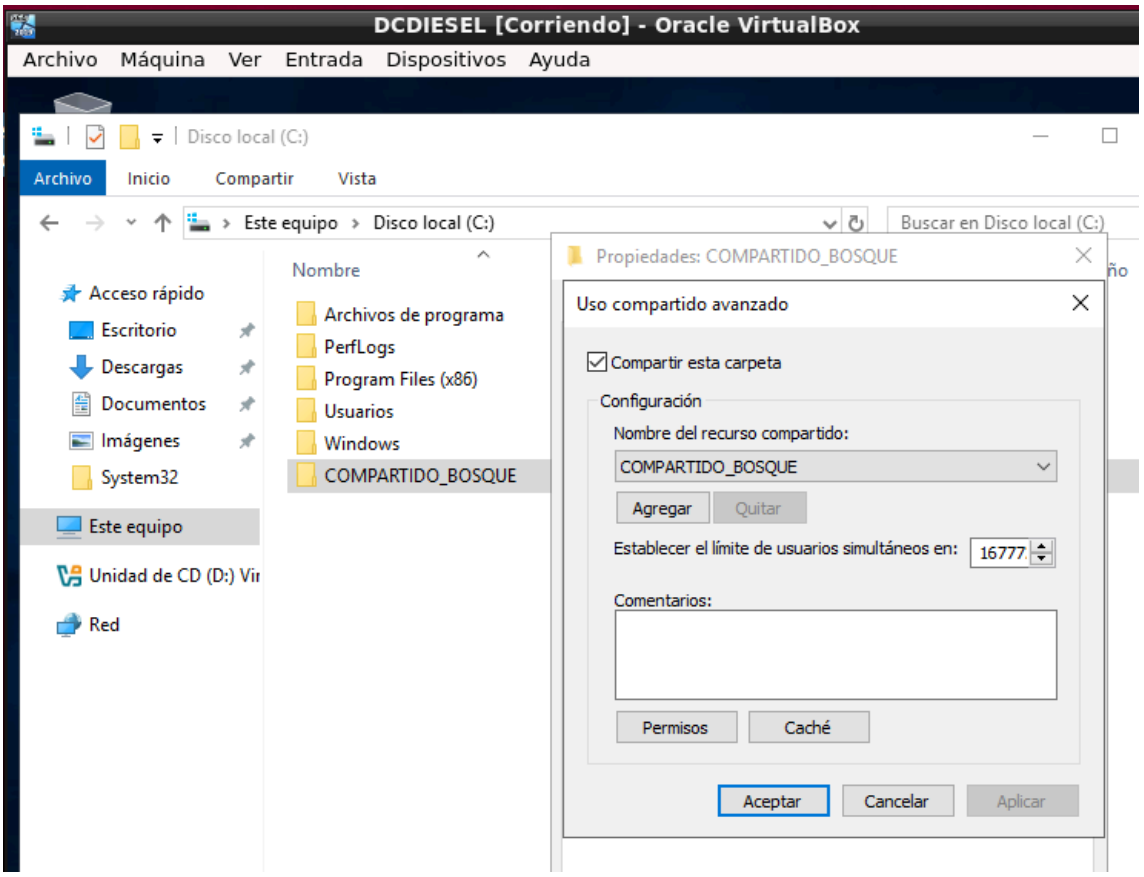
El grupo global lo forman usuarios de un solo dominio para otorgarles permisos de objetos de otros dominios.

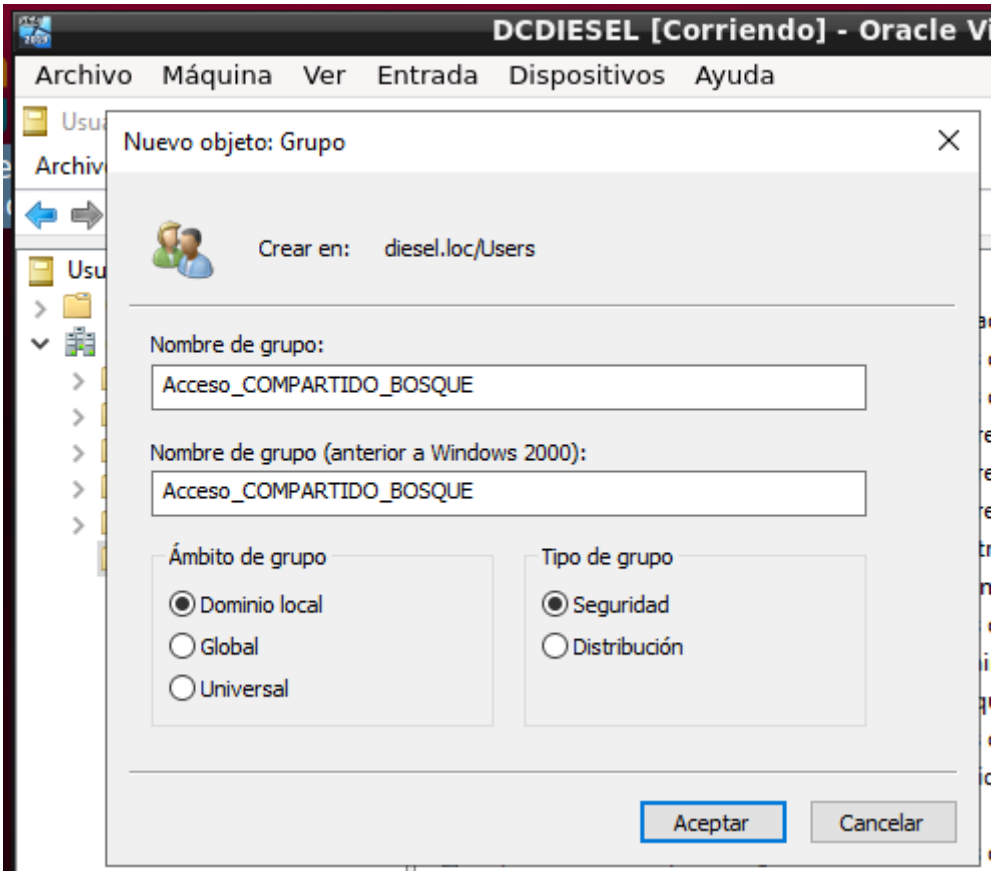
El ámbito local lo forman usuarios de varios dominios del bosque para acceder a un solo objeto de un dominio.

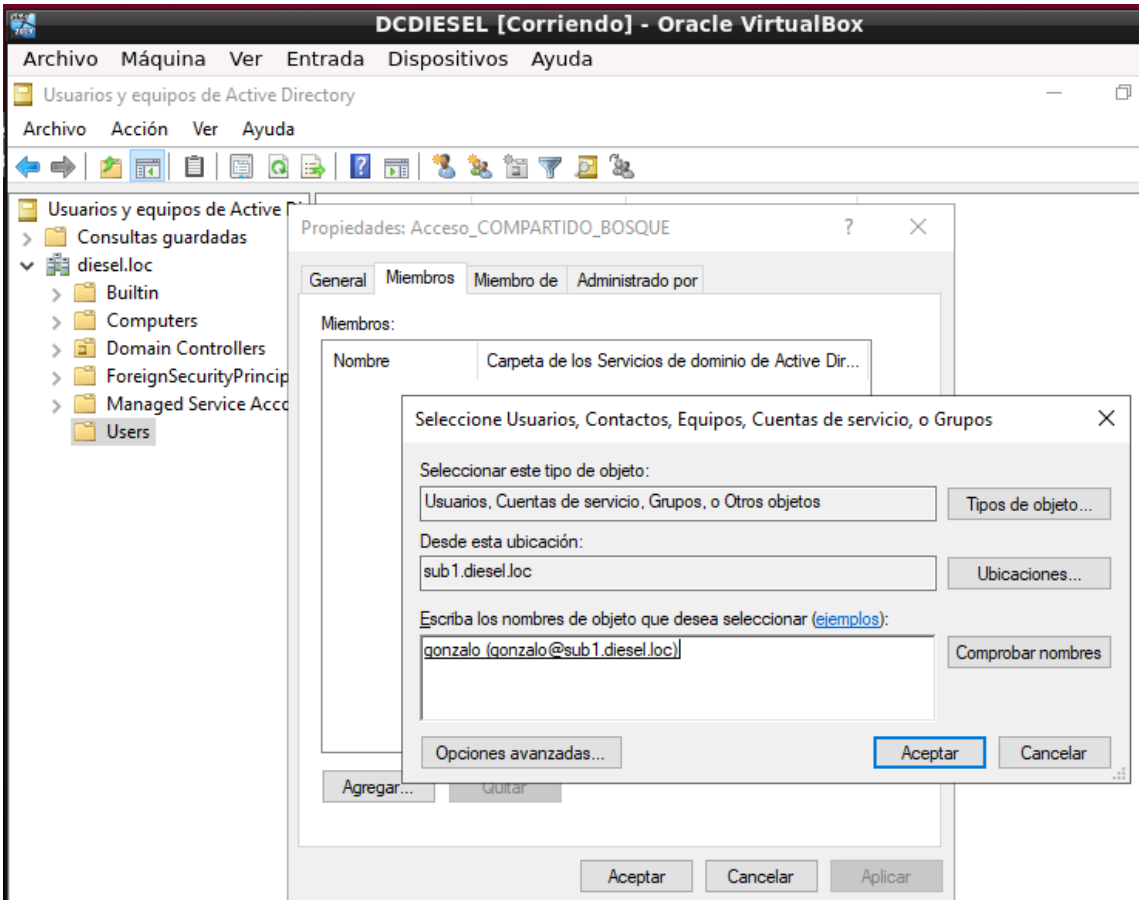
(VER DOCUMENTO TEORÍA DE GRUPOS – ÁMBITO LOCAL EN SALLENET)

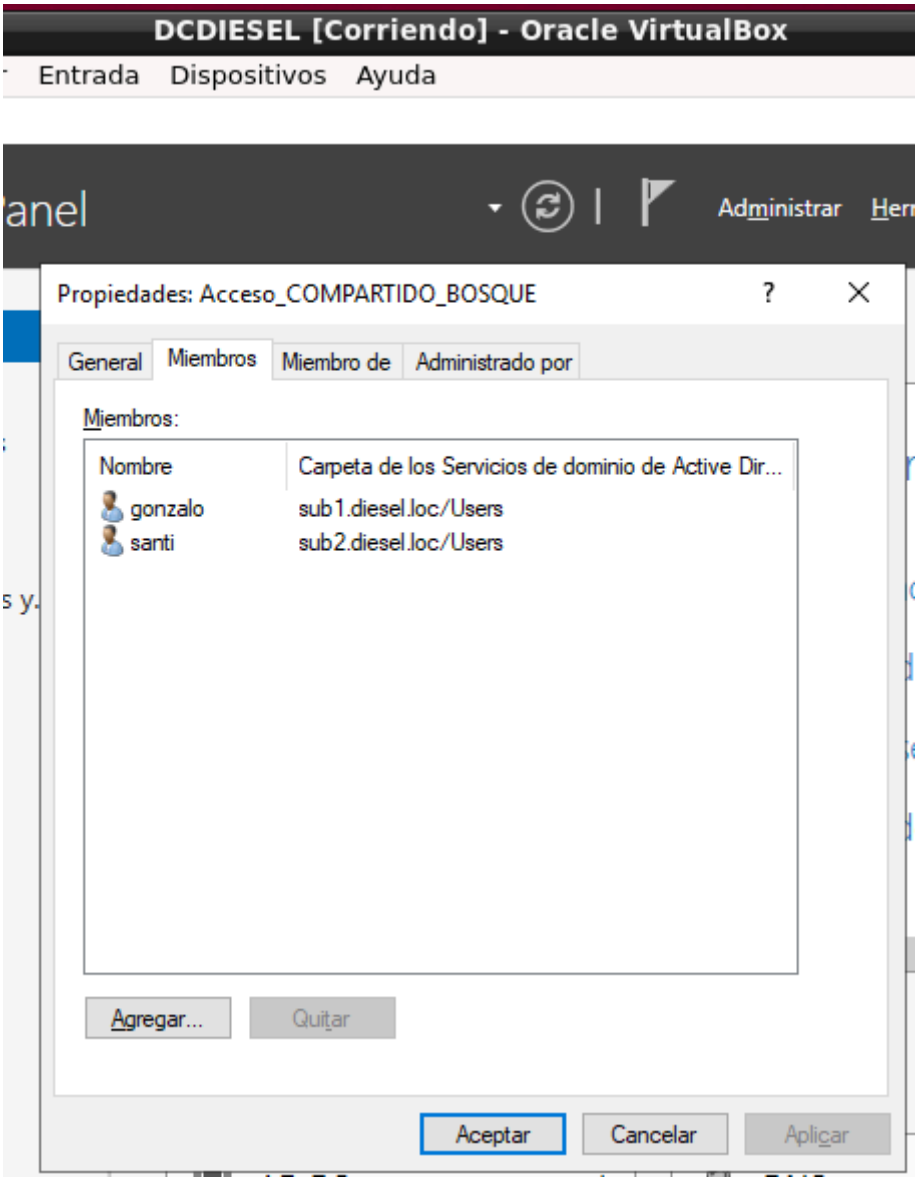
Crear un grupo local, usuarios de varios dominios, para otorgar permisos de un solo recurso.

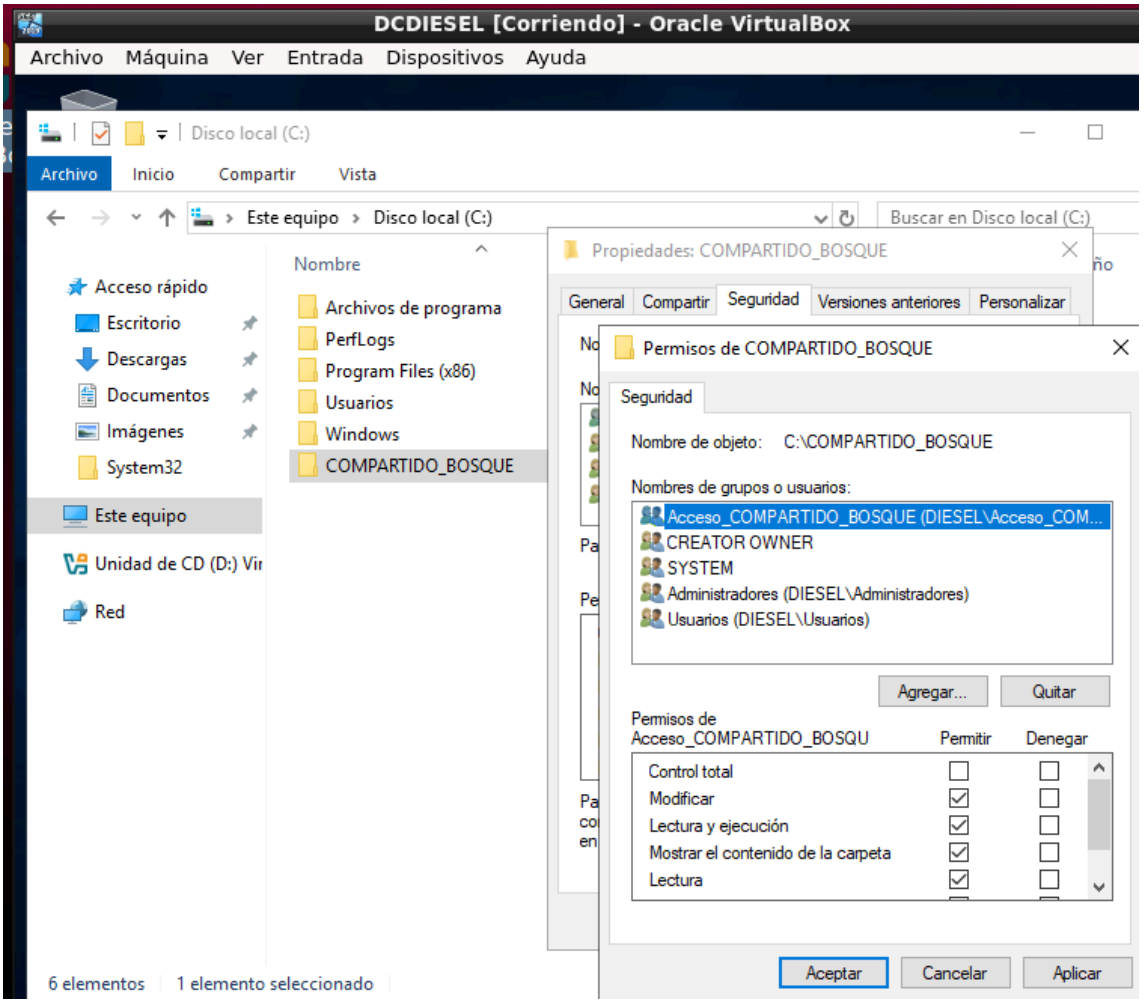
EVIDENCIAR el recurso, sus permisos, el grupo y sus usuarios.




DCDIESEL [Corriendo] - Oracle Vi
Archivo Máquina Ver Entrada Dispositivos Ayuda
Nuevo objeto: Grupo
Crear en: diesel.loc/Users
Nombre de grupo:
Acceso_COMPARTIDO_BOSQUE
Nombre de grupo (anterior a Windows 2000):
Acceso_COMPARTIDO_BOSQUE
Ámbito de grupo
Dominio local
Global
Universal
Tipo de grupo
Seguridad
Distribución
Aceptar
Cancelar


DCDIESEL [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Usuarios y equipos de Active Directory
Archivo Acción Ver Ayuda
Consultas guardadas
diesel.loc
Builtin
Computers
Domain Controllers
ForeignSecurityPrincip
Managed Service Acc
Users
Propiedades: Acceso_COMPARTIDO_BOSQUE
General Miembros Miembro de Administrado por
Miembros:
Nombre
Carpeta de los Servicios de dominio de Active Dir...
Seleccione Usuarios, Contactos, Equipos, Cuentas de servicio, o Grupos
Seleccionar este tipo de objeto:
Usuarios, Cuentas de servicio, Grupos, o Otros objetos
Tipos de objeto...
Desde esta ubicación:
sub1.diesel.loc
Ubicaciones...
Escriba los nombres de objeto que desea seleccionar (ejemplos):
gonzalo (gonzalo@sub1.diesel.loc)
Comprobar nombres
Opciones avanzadas...
Aceptar
Cancelar
Agregar...
Quitar
Aceptar
Cancelar
Aplicar


DCDIESEL [Corriendo] - Oracle VirtualBox
Entrada Dispositivos Ayuda
anel
Administrar
Propiedades: Acceso_COMPARTIDO_BOSQUE
General
Miembros
Miembro de
Administrado por
Miembros:
Nombre
Carpeta de los Servicios de dominio de Active Dir...
gonzalo
sub1.diesel.loc/Users
santi
sub2.diesel.loc/Users
Agregar...
Quitar
Aceptar
Cancelar
Aplicar


DCDIESEL [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Disco local (C:)
Archivo Inicio Compartir Vista
Este equipo › Disco local (C:)
Buscar en Disco local (C:)
Acceso rápido
Escritorio
Descargas
Documentos
Imágenes
System32
Este equipo
Unidad de CD (D:) Vir
Red
Nombre
Archivos de programa
PerfLogs
Program Files (x86)
Usuarios
Windows
COMPARTIDO_BOSQUE
6 elementos 1 elemento seleccionado
Propiedades: COMPARTIDO_BOSQUE
General Compartir Seguridad Versiones anteriores Personalizar
Permisos de COMPARTIDO_BOSQUE
Seguridad
Nombre de objeto: C:\COMPARTIDO_BOSQUE
Nombres de grupos o usuarios:
Acceso_COMPARTIDO_BOSQUE (DIESEL\Acceso_COM...
CREATOR OWNER
SYSTEM
Administradores (DIESEL\Administradores)
Usuarios (DIESEL\Usuarios)
Agregar... Quitar
Permisos de Acceso_COMPARTIDO_BOSQU Permitir Denegar
Control total
Modificar
Lectura y ejecución
Mostrar el contenido de la carpeta
Lectura
Aceptar Cancelar Aplicar

8. PARTICIÓN DE APLICACIONES.

Buscar info y posibles consultas o localizaciones sobre esta partición.

Son particiones de la base de datos de AD que se pueden replicar selectivamente.

Posibles prácticas de aprendizaje. Consultar IA.

Las zonas DNS integradas en AD se guardan en particiones de aplicaciones.

Acción: Ir al RAIZ-DC.

Paso 1: Abrir "Editor ADSI" (adsiedit.msc).

Paso 2: Hacer clic derecho en "Editor ADSI" ➡️ Conectar a....

Paso 3: En "Seleccionar un contexto de nomenclatura...", desplegar la lista.

Resultado: Ver las particiones:

- DC=DomainDnsZones,DC=diesel,...
- DC=ForestDnsZones,DC=diesel,...