

PRÁCTICA

RELACIONES DE CONFIANZA ENTRE DOMINIOS DE DISTINTOS BOSQUES Y DELEGACIÓN DE CONTROL.

1.- OBJETIVOS.

- Establecer relaciones de confianza entre dominios.
- Delegar el control a otros dominios.

2.- CONTENIDOS TEÓRICOS.

Unidad 3 Administración de Usuarios en Windows Server 2019
Práctica guiada con contenidos teóricos

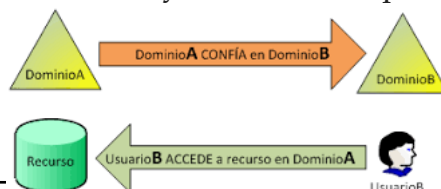
3.- MATERIAL NECESARIO.

- Ordenador conectado a Internet, procesador de textos.
- Máquina virtual con Windows Server 2019 instalado.
- Máquina virtual con Windows 10 instalado.

4.- RELACIONES DE CONFIANZA. ¿QUÉ SON?

Una **relación de confianza** es una relación establecida entre dos dominios de forma que permite a los usuarios de un dominio ser reconocidos por los Controladores de Dominio de otro dominio. Estas relaciones permiten a los usuarios acceder a los recursos de otro dominio, y a los **administradores** definir los permisos y derechos de usuario para los usuarios del otro dominio. Permite establecer comunicación entre varios controladores de dominio, con el fin de poder administrar desde un solo punto de la red a todos los usuarios y recursos que tengas.

Relación de confianza de bosques: deberemos crear este tipo de relaciones si necesitamos permitir que los recursos se compartan entre los bosques de Active Directory. Son siempre transitivas y la dirección puede ser unidireccional o bidireccional.



5.- REALIZACIÓN DE LA PRÁCTICA

CREACIÓN DE RELACIÓN DE CONFIANZA BIDIRECCIONAL ENTRE DOS DOMINIOS DE BOSQUES DIFERENTES

Esta práctica se hace de dos en dos. Escribe a continuación los servidores y dominios que van a intervenir junto con sus direcciones IP.

Habrás que hacer una captura de pantalla por cada paso.

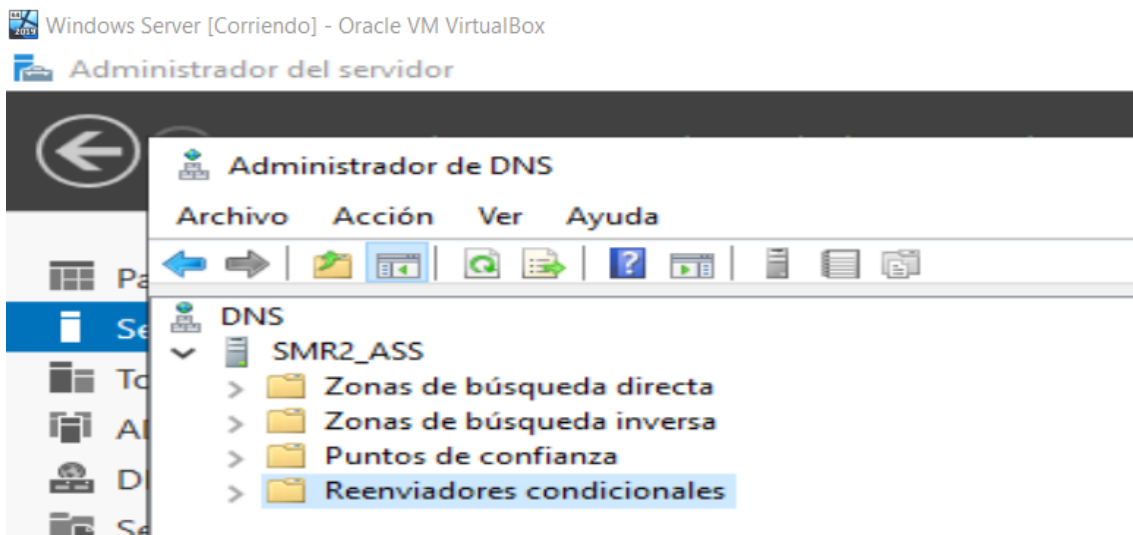
CONFIGURACIÓN DEL DNS.

Lógicamente, antes de establecer una relación de confianza entre los bosques, necesitamos que se vean, y para ello, deberemos configurar correctamente los servidores DNS.

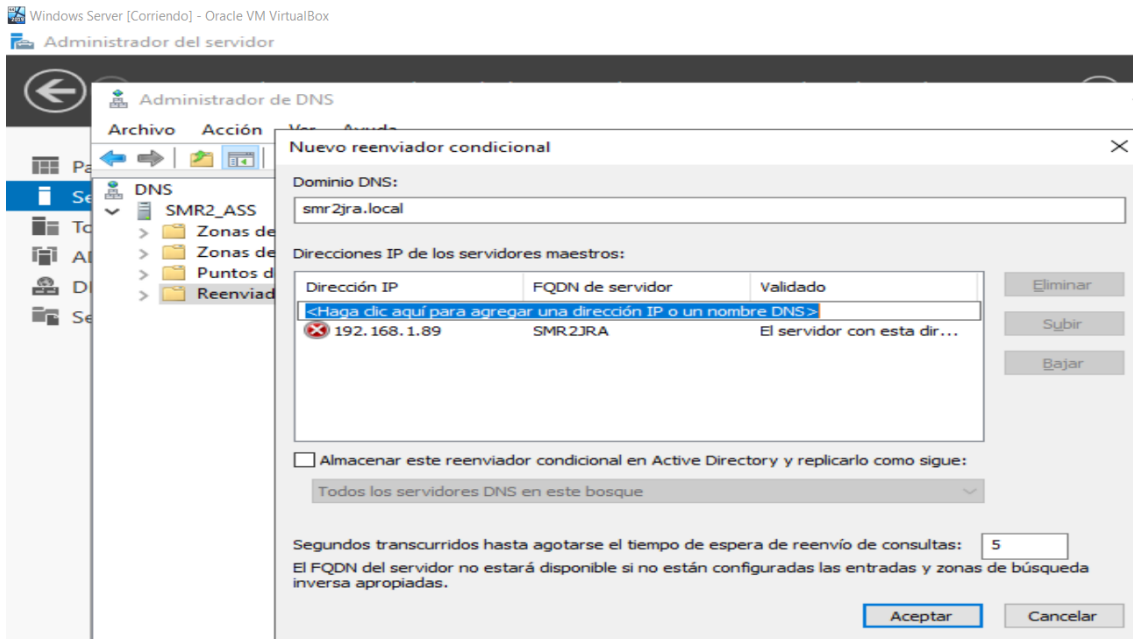
Sobre los DC Primarios :

1. Comenzamos en *Inicio>Herramientas administrativas>DNS*.

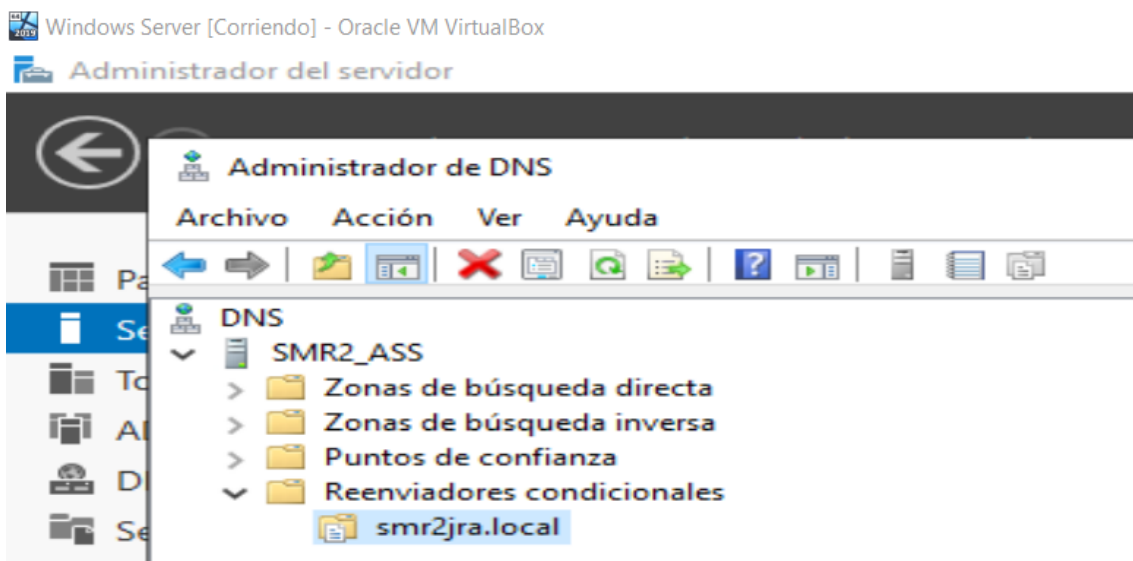
Cuando se abra la ventana Administrador de DNS, buscamos en el panel de la izquierda la entrada con el título *Reenviadores condicionales* y hacemos clic sobre ella con el botón derecho del ratón.



- Elegir la opción *Nuevo reenviador condicional...* En el cuadro de texto *Dominio DNS* escribir el nombre del dominio con el que se va a establecer la relación de confianza. En la lista de direcciones ip indicar la ip del DC Primario de dicho dominio (no pasa nada si no la comprobación no es satisfactoria).



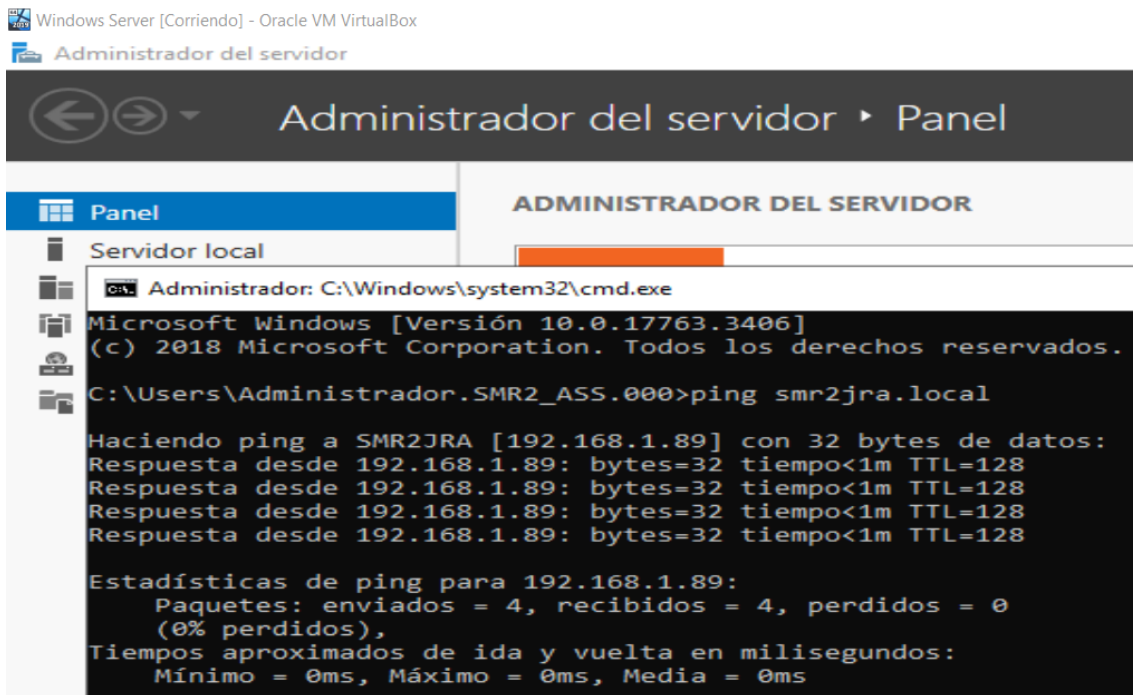
- En la ventana principal, comprobamos que ahora aparece la referencia al dominio con el que crearemos la relación de confianza. Una vez hecha la comprobación, podemos cerrar la ventana.



4. A continuación, debemos **repetir los mismos pasos con el controlador del segundo dominio** de forma que haga referencia al primero.

(Lo a hecho Jesus)

Comprobación: Ping desde *tu servidor hacia el de tu compañero* (ping smr2rag.local pericopalotes.local).



Windows Server [Corriendo] - Oracle VM VirtualBox

Administrador del servidor

Administrador del servidor ▸ Panel

Panel

ADMINISTRADOR DEL SERVIDOR

Servidor local

C:\Windows\system32\cmd.exe

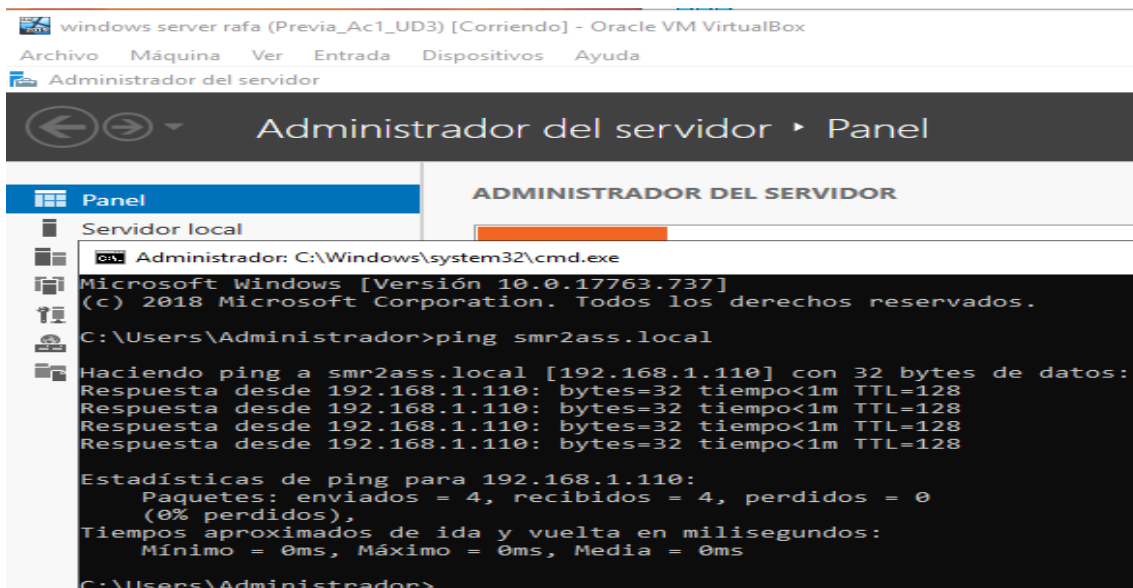
```
Microsoft Windows [Versión 10.0.17763.3406]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador.SMR2_ASS.000>ping smr2jra.local

Haciendo ping a SMR2JRA [192.168.1.89] con 32 bytes de datos:
Respuesta desde 192.168.1.89: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.89: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.89: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.89: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.89:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Ping desde *el servidor de tu compañero al tuyo* (ping pericopalotes.local smr2rag.local)



windows server rafa (Prevía_Ac1_UD3) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Administrador del servidor

Administrador del servidor ▸ Panel

Panel

ADMINISTRADOR DEL SERVIDOR

Servidor local

C:\Windows\system32\cmd.exe

```
Microsoft Windows [Versión 10.0.17763.737]
(c) 2018 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>ping smr2ass.local

Haciendo ping a smr2ass.local [192.168.1.110] con 32 bytes de datos:
Respuesta desde 192.168.1.110: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.110: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.110: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.110: bytes=32 tiempo<1m TTL=128

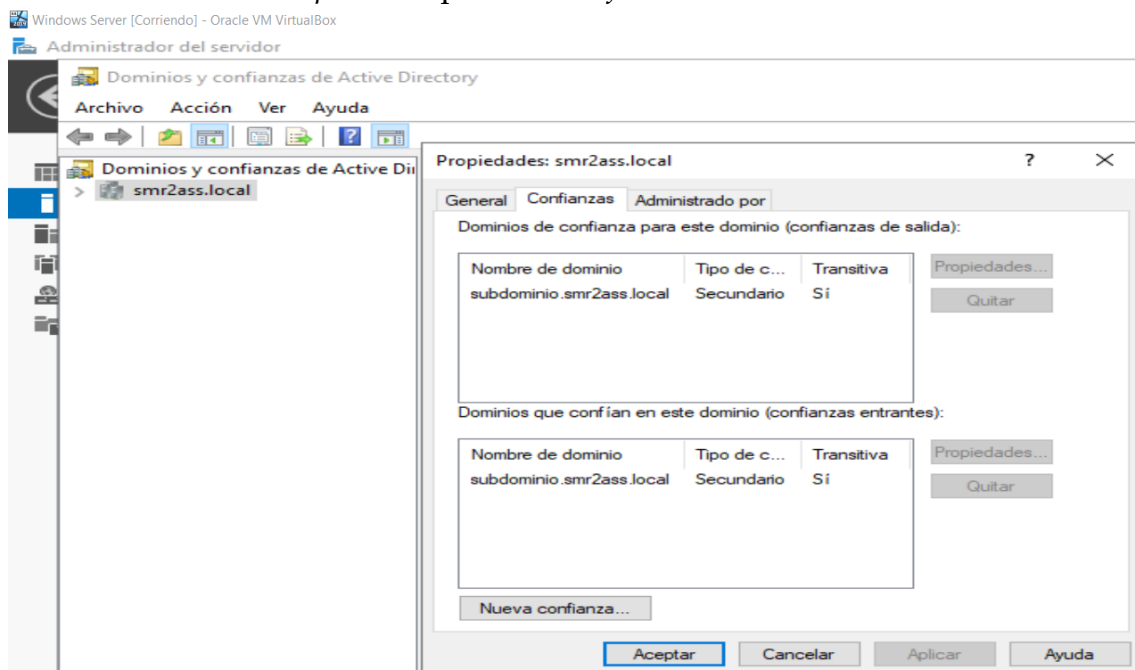
Estadísticas de ping para 192.168.1.110:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>
```

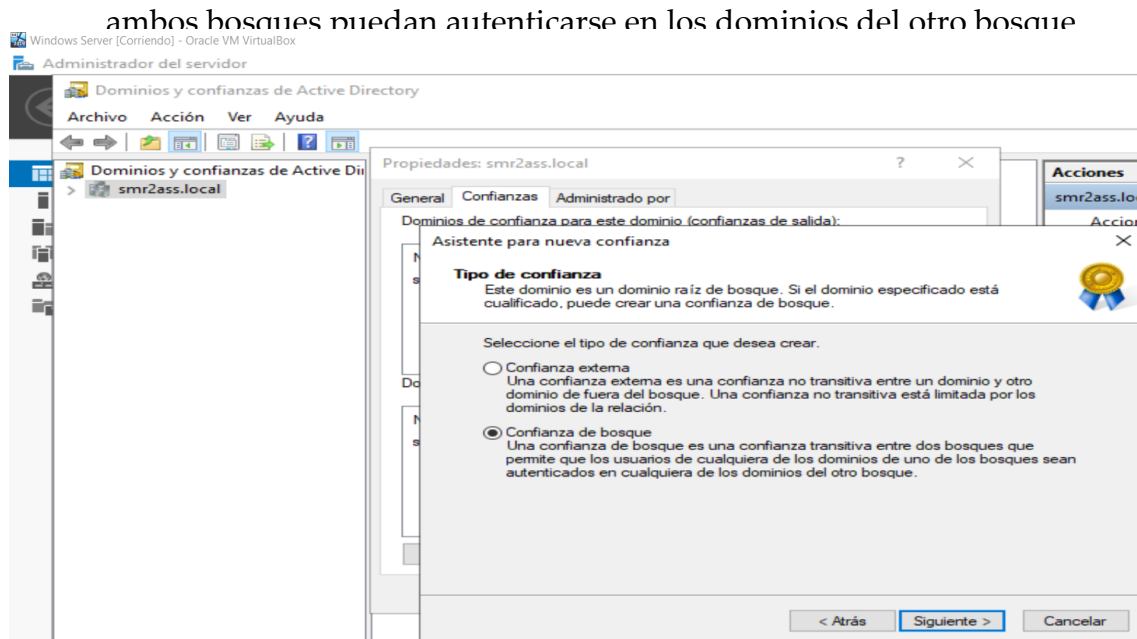
ESTABLECER LA RELACIÓN DE CONFIANZA

Desde el CD Principal de cualquiera de los 2 bosques abrimos *Dominios y confianzas de Active Directory* y realizaremos las siguientes operaciones:

1. En el panel izquierdo, hacemos clic con el botón derecho del ratón sobre el dominio, *Propiedades*, pestaña *Confía*

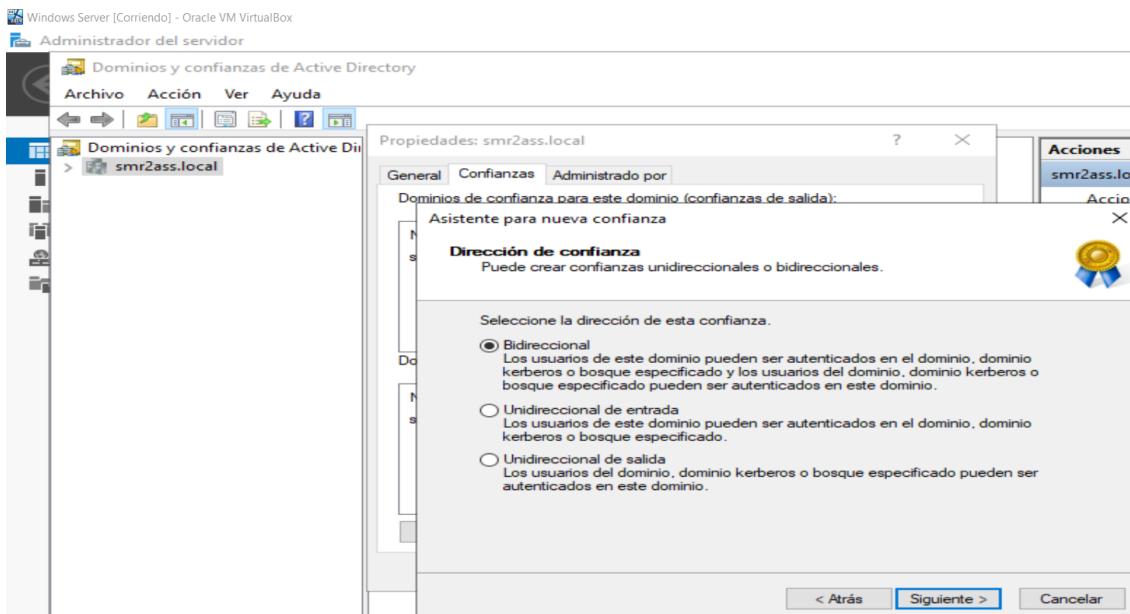


2. Clic en *Nueva confianza...* Seguir el asistente y en la pantalla donde pide el nombre de dominio con el que se quiere establecer la relación de confianza escribir su nombre DNS (smr2rag.local). A continuación, debemos establecer el tipo de confianza, que será una **Confianza de bosque** que permite que los usuarios de cualquiera de los dominios en



- **Bidireccional:** Con esta opción, cualquier usuario que pertenezca a cualquier dominio del bosque podrá autenticarse en el bosque *segundodominio.local* y cualquier usuario que pertenezca a un dominio del bosque *segundodominio.local* podrá autenticarse en el bosque *primerdominio.local*.
- **Unidireccional de entrada:** Si elegimos esta opción, cualquier usuario que pertenezca a cualquier dominio del bosque *primerdominio.local* podrá autenticarse en el bosque *segundodominio.local*, pero los usuarios que pertenezca a un dominio del bosque *segundodominio.local* no podrán autenticarse en el bosque *primerdominio.local*.
- **Unidireccional de salida:** Eligiendo esta opción, cualquier usuario que pertenezca a cualquier dominio del bosque *segundodominio.local* podrá autenticarse en el bosque *primerdominio.local*, pero los usuarios que pertenezca a un dominio del bosque *primerdominio.local* no podrán autenticarse en el bosque *segundodominio.local*.

En nuestro caso, nos decantamos por la primera opción.

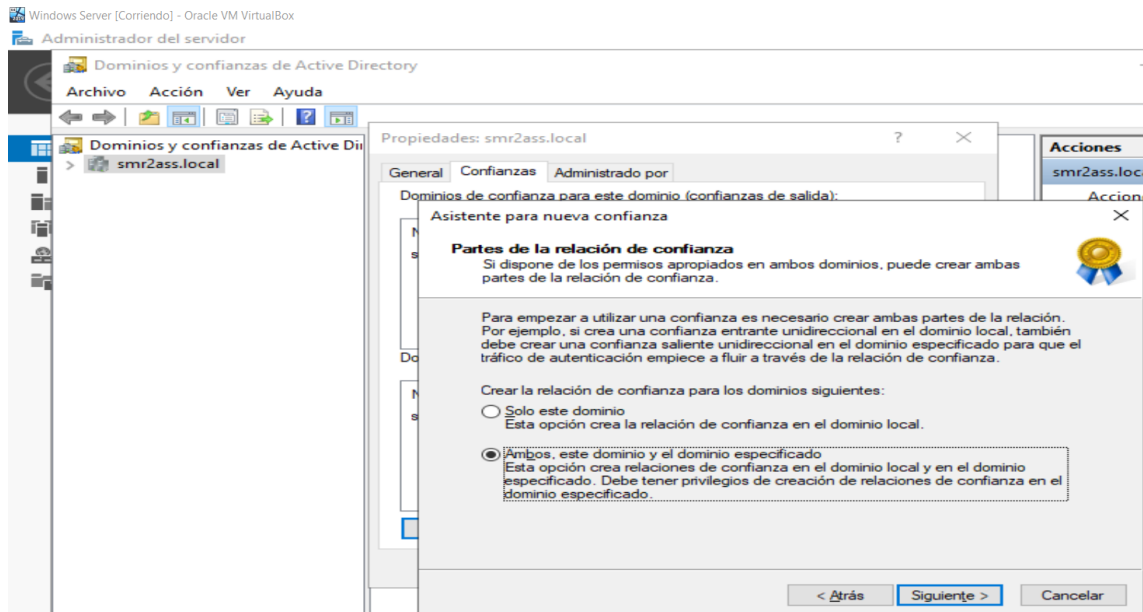


Llegados a este punto, debemos pensar que una **relación bidireccional** no es más que dos relaciones unidireccionales:

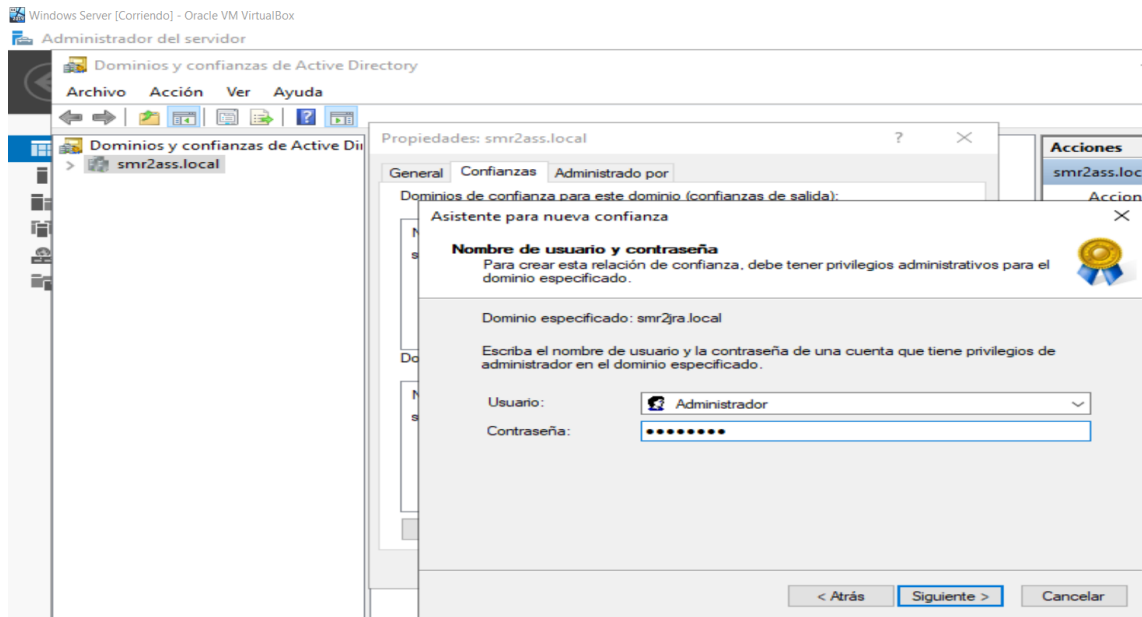
Una relación unidireccional donde *primerdominio.local* confía en *segundodominio.local*. Y otra donde *segundodominio.local* confía en *primerdominio.local*.

Parece lógico pensar que la primera debería establecerse desde *primerdominio.local*, con las credenciales de administración necesarias para este dominio, y que la segunda debería establecerse desde *segundodominio.local* con las credenciales adecuadas en el mismo.

No obstante, si disponemos del nombre de usuario y la contraseña adecuados en *segundodominio.local*, podemos realizar la segunda parte de la operación sin movernos de *primerdominio.local*. Para lograrlo, sólo debemos elegir, en la siguiente pantalla, la opción *Ambos*, este dominio y el dominio especificado.



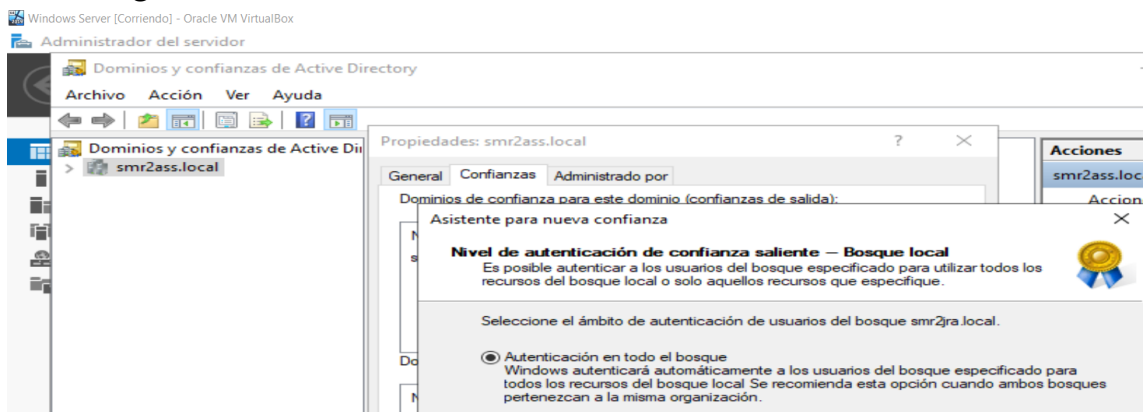
Después de esto, el asistente nos solicita las credenciales que permiten administrar *segundodominio.local*. Las escribimos y hacemos clic sobre el botón **Siguiente**.



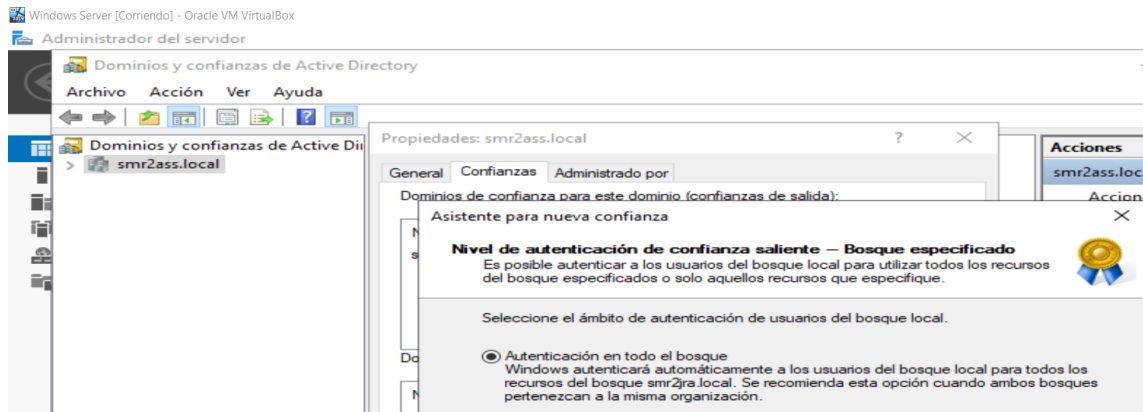
En los dos pasos siguientes debemos decidir si, una vez autenticado un determinado cliente, éste tendrá acceso a todos los recursos del bosque o si, por el contrario, deberemos conceder acceso, de forma individual a los recursos que queramos que estén disponibles.

La segunda opción es más conservadora en cuestiones de seguridad. Sin embargo, la primera es mucho más cómoda. En este ejemplo, nosotros nos decantaremos por la solución cómoda ;)

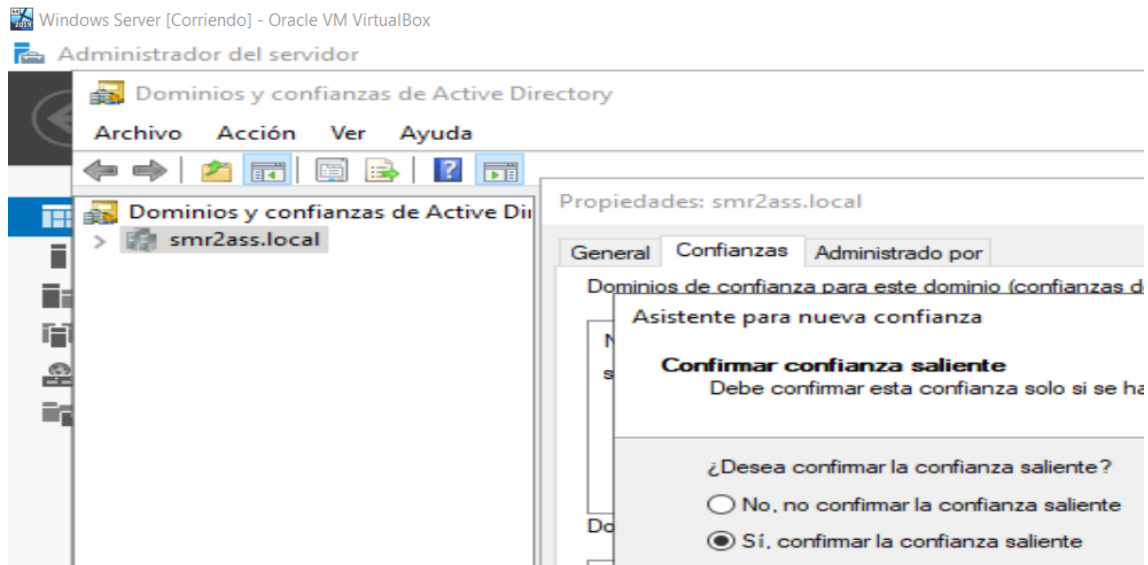
Por lo tanto, elegimos la opción *Autenticación en todo el bosque* para la confianza saliente del bosque local (es decir, para los usuarios que se identifiquen desde el bosque externo). Y hacemos clic sobre el botón **Siguiente**.



Después, volvemos a elegir la opción *Autenticación en todo el bosque* para la confianza saliente del dominio *segundodominio.local* (es decir, para los usuarios que se identifiquen desde el bosque local).

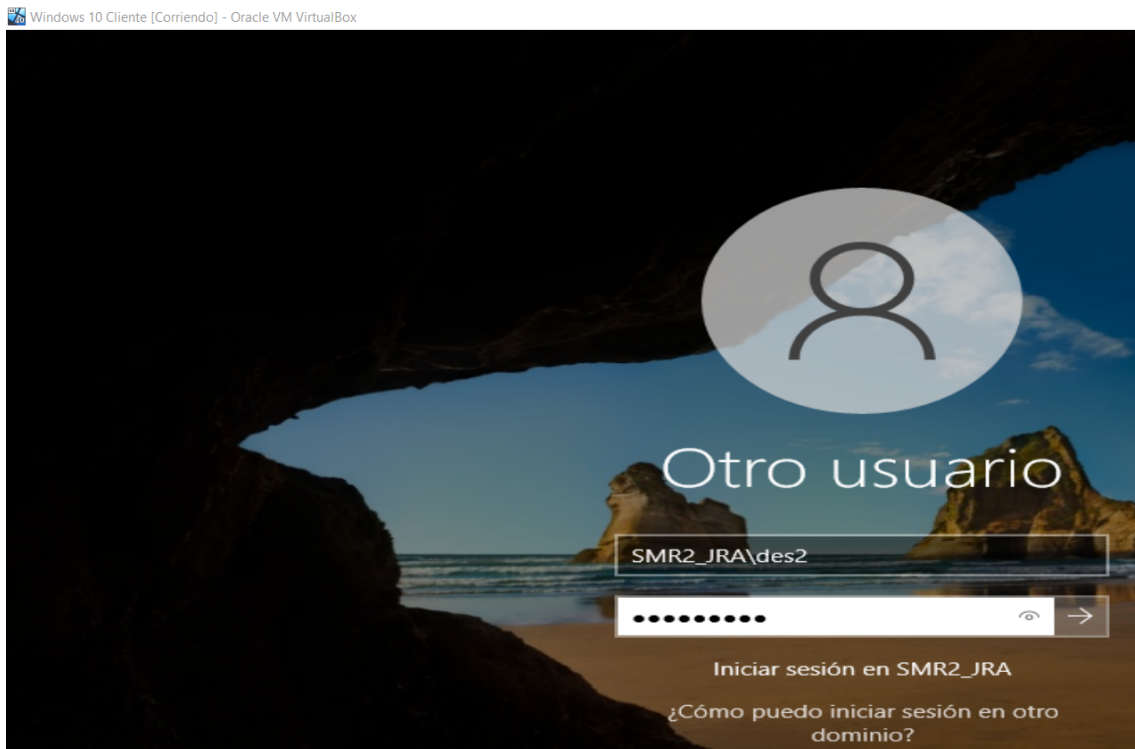


El asistente irá avanzando hasta que aparezca la ventana en la que debemos confirmar las confianzas para que se hagan efectivas. Comenzamos por la confianza saliente...



Elegimos la opción *Sí, confirmar la confianza saliente*. Después, confirmamos la confianza entrante...Elegimos la opción *Sí, confirmar la confianza entrante*. Al finalizar el asistente y de vuelta en la ventana de propiedades, podemos apreciar que aparece la nueva confianza

Comprobación: Desde un equipo de tu dominio inicia sesión con un usuario en el dominio de tu compañero, indicando su dominio en el identificador.



ADMINISTRAR UN CONTROLADOR DE DOMINIO WINDOWS SERVER 2019 DESDE OTRO CON EL QUE SE TIENE ESTABLECIDA UNA RELACIÓN DE CONFIANZA DE BOSQUE BIDIRECCIONAL.

Una vez establecidas las relaciones de confianza cuando estemos realizando cualquier operación podremos cambiar de dominio desde el que estemos trabajando. De esta forma podremos crear UO, usuarios, equipos, etc... en nuestro dominio y en el otro en el que confiamos.

1. Para administrar un controlador de dominio desde otro ejecutaremos la herramienta *Usuarios y equipos de Active Directory* o en *Dominios y confianza de Active Directory* -> *Administrar*
2. Nos situaremos en nuestro dominio y elegiremos la *opción cambiar dominio* donde pondremos el dominio en el que confiamos.
3. Nos aparecerá la ventana de usuarios y equipos del otro dominio. **Las contraseñas del usuario Administrador de los dos dominios debe de ser la misma.**

¿Podemos crear UO, usuarios, grupos...?

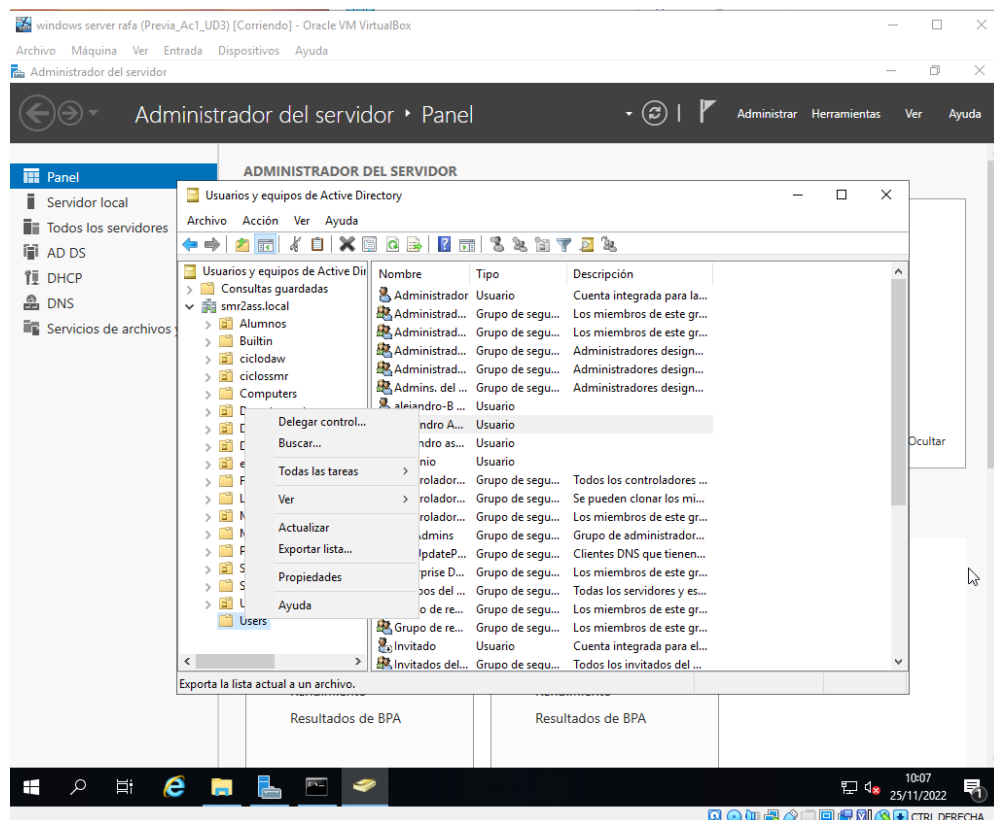
NO, aun no.

DELEGACIÓN DE CONTROL DE UN DOMINIO.

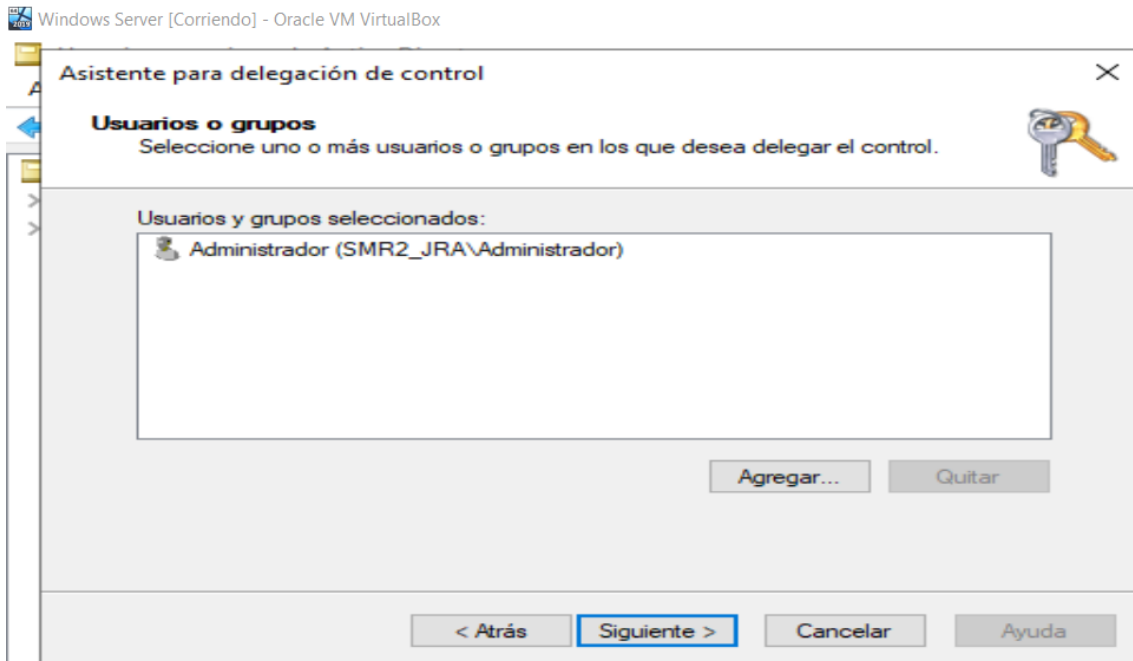
Aún no podemos crear nuevas UO, usuarios, grupos etc. porque no hemos delegado el control.

Si queremos que nuestro dominio pueda ser administrado por otro en el que confiamos tendremos que **delegar el control**.

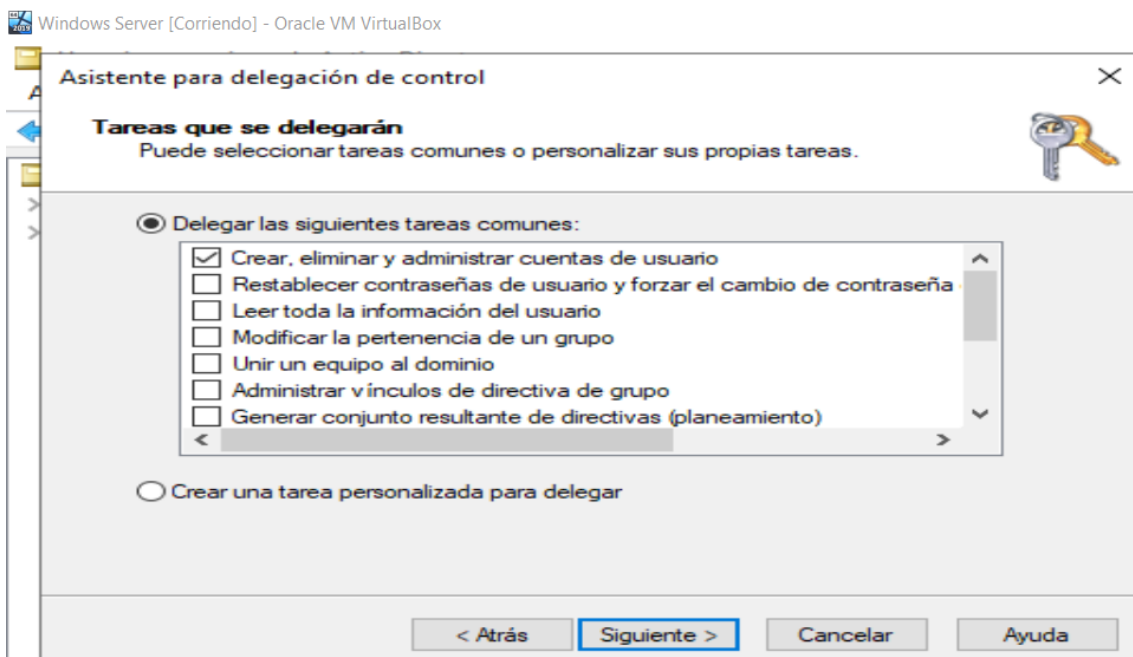
1. Captura una pantalla cambiándote al dominio en el que confías de forma que se vea que no se pueden crear UO, usuarios, etc.



2. Delegar el control; para ello nos vamos a *Usuarios y equipos de Active Directory* y en el dominio principal le damos a *delegar control*, elegimos los usuarios a los que se les va a poder dar permisos para administrar el segundo dominio. (nota ten cuidado a la hora de hacer la delegación porque puedes confundirte de dominio).



3. Elige un usuario en quien delegarás el control y dale los permisos que crees oportunos. Prueba ahora a crear usuarios.



Ahora, si nos deja crear usuario (el solo puede crear usuarios).

