PRACTICAS 2012 -- 2016

CREAR un SUBDOMINIO teniendo apagado el DC1 P@ssw0rd.

192.168.0.2

adicional

192.168.0.1

DC1xxx

DC2

valle.local Windows 2012 DC1 windows 2016-DC2

DC3xxx

2012-DC3

asir.valle.local 192.168.0.3

* Vamos a crear el subdominio asir.valle.local con un Windows 2012. Lo importante es que la función de Maestro de Nombres de dominio este en el controlador de dominio que tenemos encendido y trabajando...

1. Credenciales valle\administrador, mejor administrador@valle.local
2. Tenemos todas las funciones de Maestro de operaciones en DC1 y este equipo esta apagado solo tenemos encendido el 2012-DC2.
3. Vamos a crear el subdominio asir.valle.local Clonamos una maquina con 2012 ó otro windows.
   1. Red interna
   2. Cambiar el nombre del equipo DC3xxx12 donde xxx son las tres letras del nombre del alumno.
   3. Ponerle una IP fija 192.168.0.3 y en el DNS preferido la ip del controlador de dominio principal 192.168.0.1 y secundario 192.168.0.2

Lo que hace esto es que cuando se intenta poner en contacto con el DNS preferido, pero al ver que no funciona no está en marcha se pone en contacto con el secundario.

* 1. Desactivar el Firewall en las dos máquinas.
  2. Mirar si hay conexión física entre estas dos máquinas con ping ip, y en los dos sentidos, si todo está correcto continuamos, si nos da algún problema paramos y resolvemos los problemas. Siempre tiene que responder el ping.

1. Agregamos el Rol Servicio de dominio del Active Directory.
2. Tenemos que tener el CD de Windows.
3. Ejecutamos adprep /forestprep y adprep /domainprep lo ejecutamos en el controlador de dominio que tenga la función de Nombre de dominio, al que nos vamos a unir, pero como los dos son 2012 no es necesario.
4. Nos vamos al subdominio
   1. Ejecutamos el dcpromo dando a la banderita amarilla.
   2. Bosque existente
   3. Crear un dominio nuevo en un bosque existente
   4. Nombre de dominio valle.local
   5. Nombre de subdominio asir
   6. Establecer credenciales: valle\administrador ó administrador@valle.local

* Ahora nos da un error y nos dice que el error es porque el C.D que es el Maestro de Nomenclatura de Nombres de dominio esta sin conexión. Por lo tanto, no podemos unir ningún subdominio. Aceptamos y cancelamos el asistente.
* Ahora apagamos el 2016-DC2 y arrancamos el 2012-DC1
* Tenemos que tener el CD de Windows 2012.
* Ejecutamos adprep /forestprep y adprep /domainprep lo ejecutamos en el controlador de dominio que tenga la función de Nombre de dominio, al que nos vamos a unir, pero como los dos son 2012 no es necesario.
* Nos vamos al subdominio
  + Ejecutamos el dcpromo dando a la banderita amarilla.
  + Bosque existente
  + Crear un dominio nuevo en un bosque existente
  + Nombre de dominio valle.local
  + Nombre de subdominio asir
  + Establecer credenciales: valle\administrador ó [administrador@valle.local](mailto:administrador@valle.local) del windows DC1.
* En teoría tiene que ir bien.

YA TENEMOS CREADO EL SUBDOMINIO ---- asir.valle.local

Reiniciar las maquinas todas.

¿Qué tenemos que ver al crear el subdominio?

1. Arrancamos el controlador principal y el adicional de valle.local, para que el adicional que lo hemos tenido apagado se entere que se ha creado un subdominio y se actualice el DNS y los Sites.
2. Tenemos que ver la configuración IP del DC3xxx.

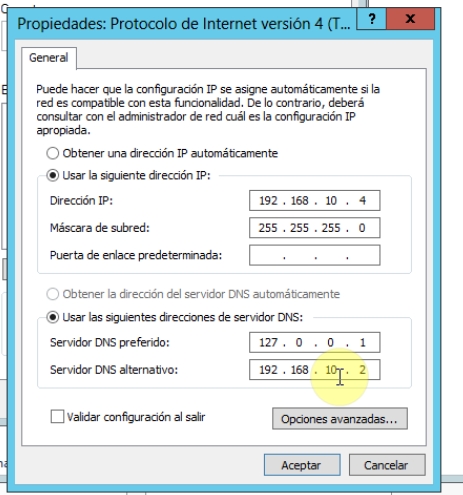
Al crear el subdominio nosotros le pusimos:

DNS preferido:192.168.0.1 y

DNS secundario: 192.168.0.2

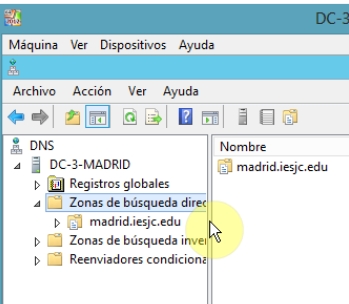
Pues Windows 2012 después de crear el subdominio automáticamente pone: c DNS preferido el mismo, 127.0.0.1 y como

DNS secundario 192.168.0.1

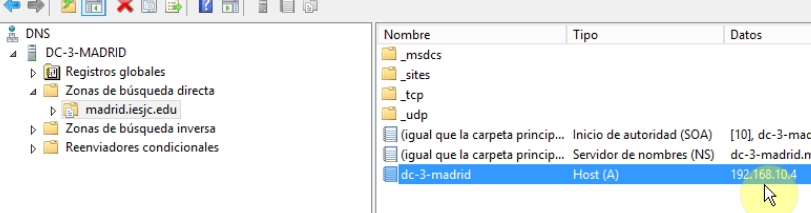


Esto está bien porque el subdominio ya tiene un DNS, Windows 2008 no lo hacía bien y teníamos que modificarlo después.

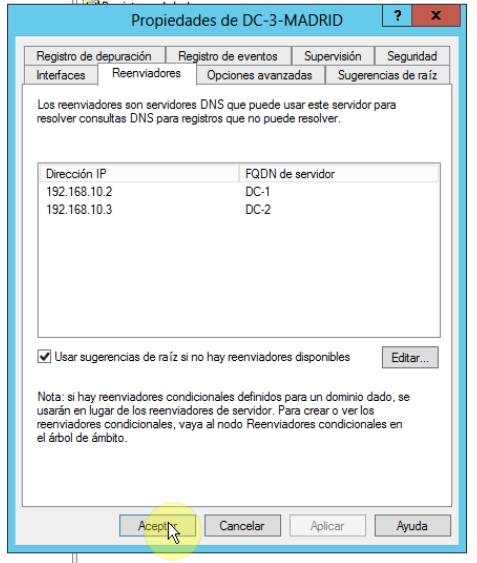
1. Nos vamos a ver el DNS del DC-3xxx12 y vemos que tenemos las zonas de búsqueda directa.



Zonas de búsqueda directa y debajo tengo asir.valle.local y que tenemos en el un host DC3 con la IP 192.168.0.4



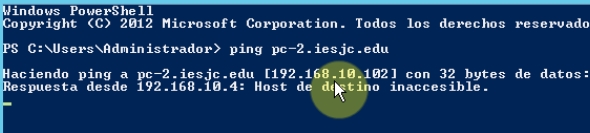
Si ahora nos vamos a las propiedades del servidor en Reenviadores, nos ha configurado 2 reenviadores, que dice mira tienes un posible servidor DNS en la 192.168.0.1 y en la 192.168.0.2.



Nos lo ha configurado correctamente.

Por lo tanto, cuando ahora hacemos un ping a un ordenador cliente enganchado con el DC1 es decir con el dominio valle.local. Ejemplo PC-2

Ping Cliente.valle.local.

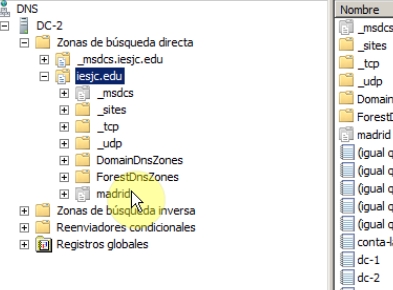
Este ping interroga al DNS 127.0.0.1 y este DNS, dice yo administro una zona que es asir.valle.local pero no valle.local que puede hacer, pues entonces se lo manda a los reenviadores, que son los que administran valle.local, y estos conocen a PC-2.valle.local y entonces le responden con la ip.

No hace ping porque está apagada, pero si resuelve la dirección ip.

Las maquinas que tengan como administrador DNS DC3, podrán resolver cualquier host que este en asir.valle.local como valle.local. Esto es muy importante a la hora de poder validarnos con un usuario de otro subdominio en

una máquina que pertenece a otro subdominio.

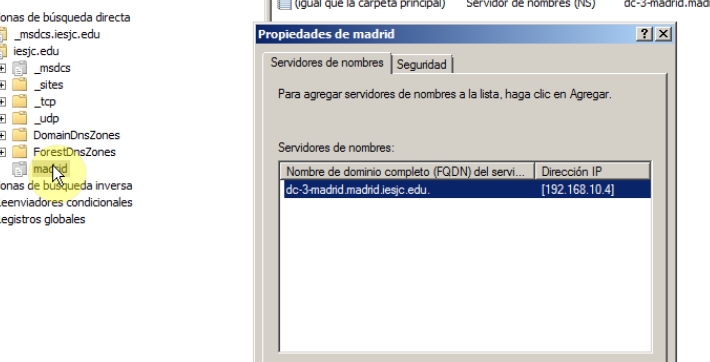
1. Ahora nos vamos al DC-2 o Dc1 al DNS.



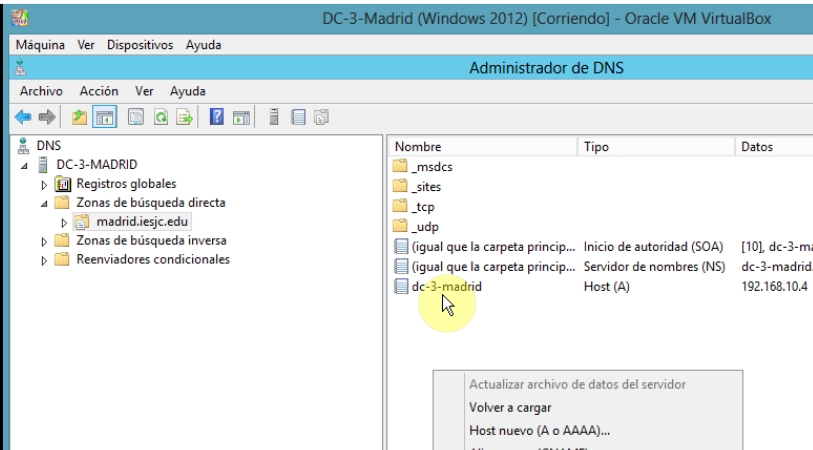
valle.local

Debajo de valle.local existe una delegación de zona que es asir (creada cuando se ejecuta el dcpromo)

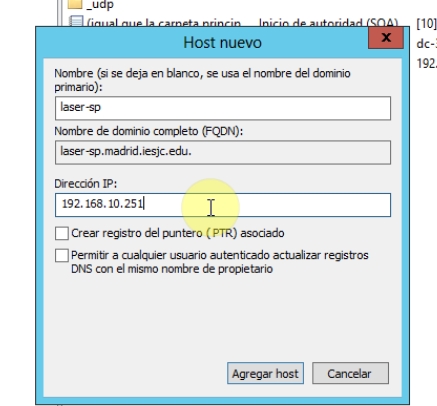
asir---- que tiene una delegación de zona, lo único que tiene es un nombre y dice que, para cualquier consulta de cosas de esta zona, la consulta se le pase al ordenador DC3xxx que es la IP—192.168.0.3.



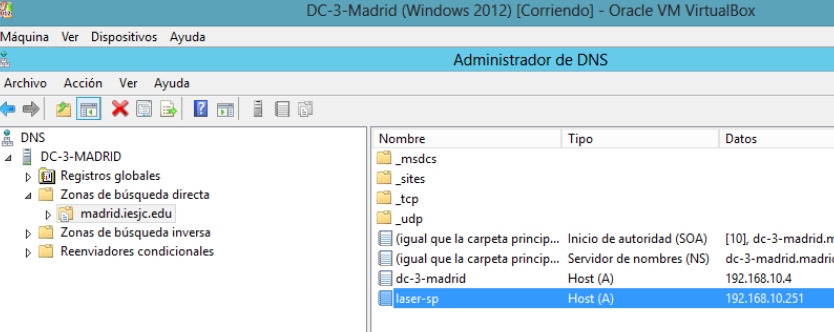
De tal manera que si nosotros ahora creáramos un host en DC3 dentro de asir.valle.local. Me voy a DC3 y en el administrador de DNS, creo un host.



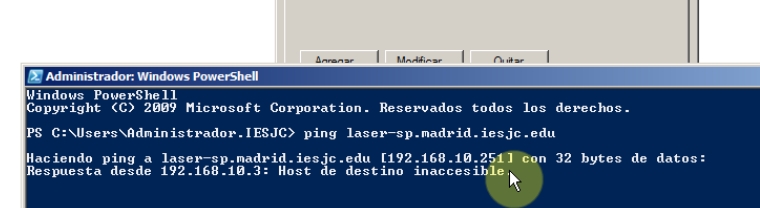
Ejemplo Laser-sp en asir.valle.local con una dirección ip xxx.



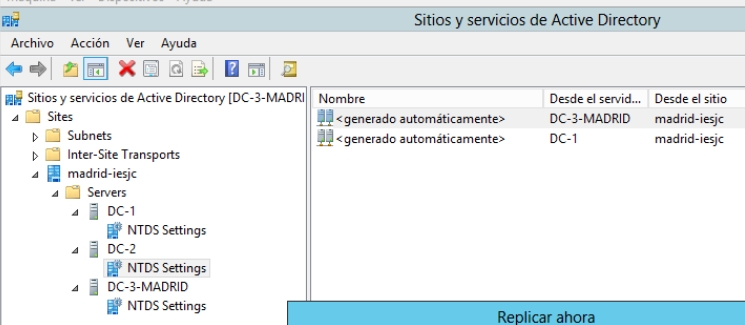
Se ha creado con éxito. Ya tenemos un láser-sp dentro de Dc3.



Si ahora desde DC2, le decimos que queremos hacer un ping a un host llamado laser-sp.asir.valle.local, él lo que dice es: valle.local es mi zona si, y dentro de esa zona que necesitamos un dominio que es asir, lo tengo sí, pero es una delegación yo no mantengo los host de las direcciones ip de esta zona sino que los mantiene el servidor DC-3 y entonces le pregunta al DNS del servidor DC-3 y este nos responde con la dirección.



1. Ahora nos vamos a Sitios y Servicios del Active Directorio del DC1.

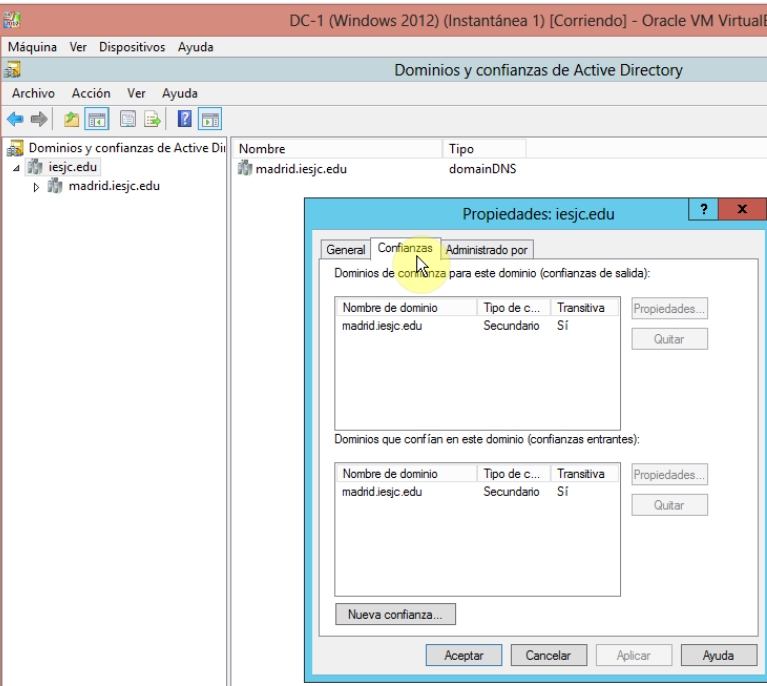


Cada servidor tiene que replicar con los otros dos servidores.

En el DC1 no tiene reenviadores solo tiene delegaciones de zona.

1. Se ha creado una confianza entre los dominios valle.local y asir esa confianza nos va a permitir que los equipos del dominio valle.local confíen en los usuarios de asir y viceversa.

Nos vamos a Dominios y confianzas del Active Directory del DC1



Tenemos las confianzas de salida de tipo secundario y transitivas.

asir.valle.local secundario y transitiva.

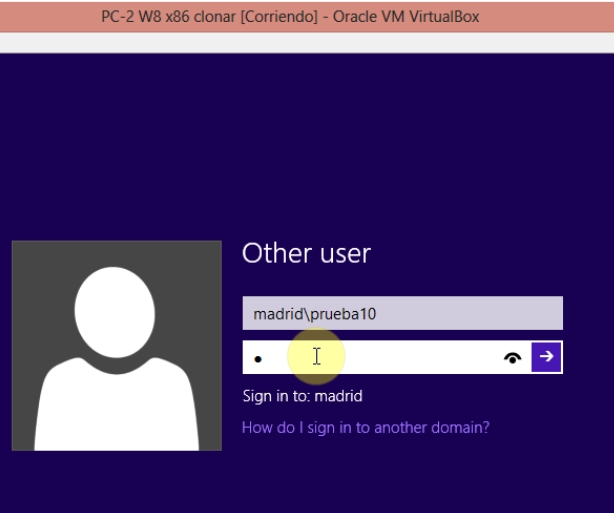
Pues si valle.local confía en asir, asir también confía en valle.local

También tenemos las confianzas entrantes. Estas confianzas se crean automáticamente.

1. Ahora nos vamos a Usuarios y equipos de DC3.

Creamos un usuario en DC3 sino lo tenemos creado.

Ahora nos vamos a un equipo cliente que está conectado al dominio Dc1 y con un usuario creado en el subdominio asir.valle.local nos validamos. Ejemplo asir1.



Nos validamos con un usuario del subdominio asir\nombre de usuario asir\asir11

Me estoy intentando validar con un usuario de un dominio al cual no pertenece esta máquina. Lo que ocurre es que este equipo le manda la solicitud de validación a su controlador de dominio valle.local y este dominio dirá: si este dominio asir es un subdominio en el cual confió y le dará la validación.

Esto permite que un usuario de un dominio pueda utilizar recursos (ejemplo un equipo) de otro dominio mediante las confianzas entre dominios.

Como hemos visto que las confianzas son transitivas, esto implica que desde cualquier equipo del dominio asir podría validarme con un usuario de valle.local y al revés.

La primera vez que nos validamos se crea el perfil.

Un administrador va a administrar a usuarios y a grupos frente a sus recursos, podrá administrar este recurso con sus usuarios y con usuarios de otros dominios en los cuales confía.

1. Tenemos dos dominios con dos administradores uno para cada dominio.

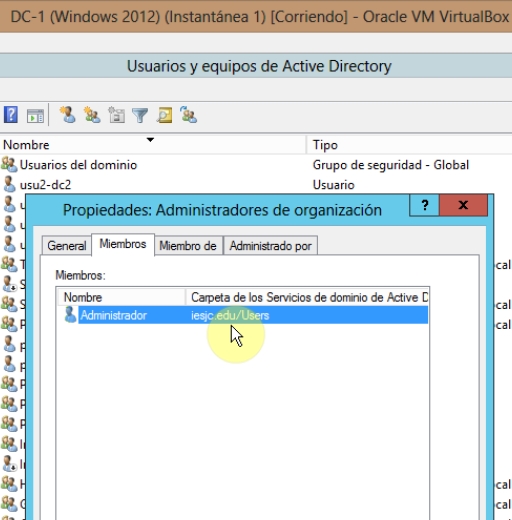
Ver el SID de cada administrador y ver que son distintos.

El Identificador de seguridad del administrador del dominio valle es distinto del identificador de seguridad del subdominio asir.

Nos vamos a usuarios y equipos del directorio activo del DC1 del valle.local.

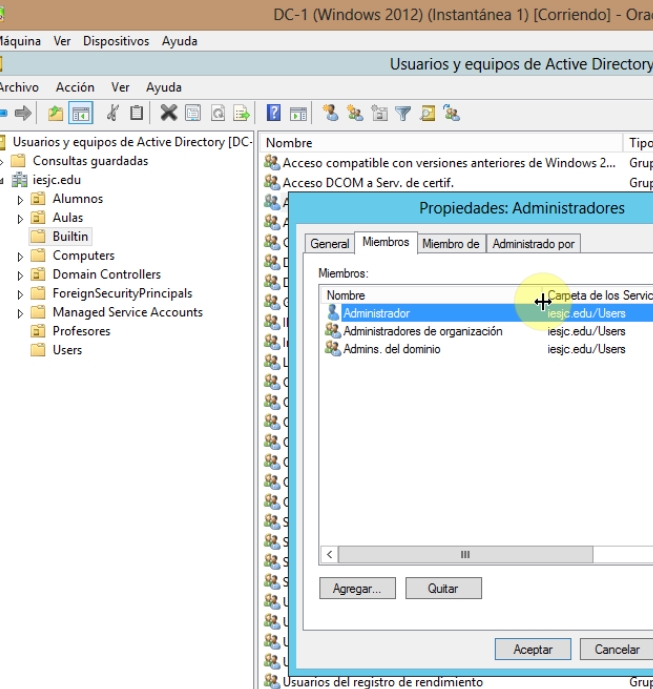
Quiero que veáis que existe un usuario administrador y un grupo especial que es Administrador de organización que son los que tienen permisos sobre cualquier controlador de dominio de nuestro dominio.

Administrador de organización miembros: Administrador de valle.local.



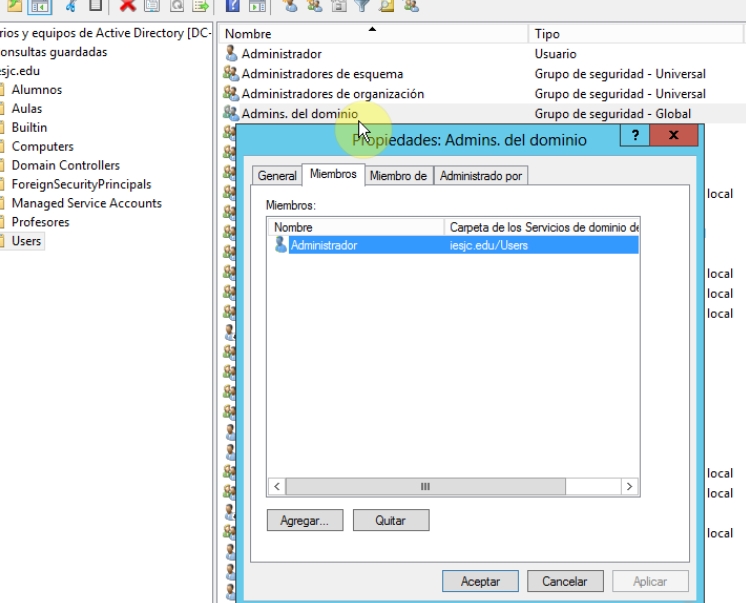
Para nosotros valle.local

Y si nos vamos a Builtin tendremos el grupo administradores y

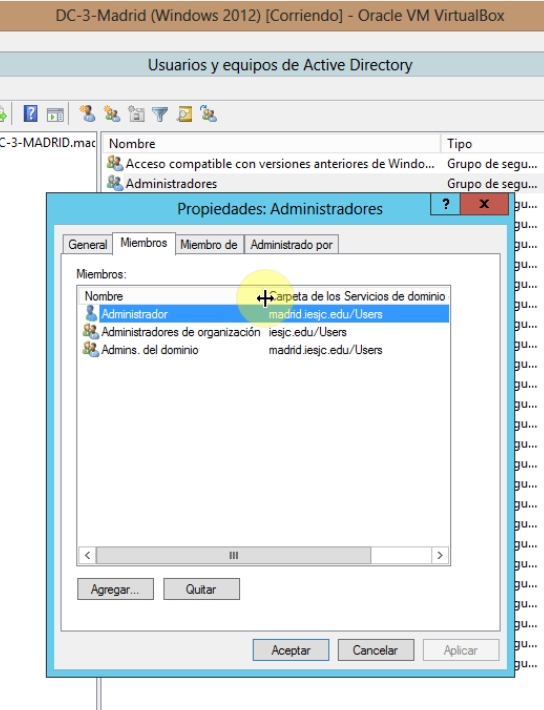


Quienes son los miembros del Grupo administradores: administrador de valle.local y el grupo administradores de organización y administrador del dominio valle.local.

Quien pertenece al grupo admis del dominio:

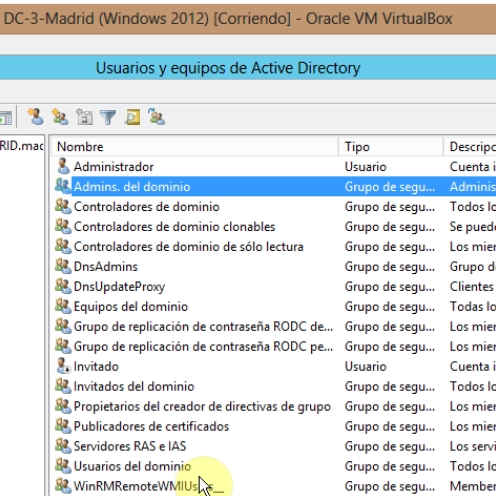


Por lo tanto, podríamos pensar que el administrador de organización y los administradores del dominio son los mismo pero no es así porque fijaros si nos vamos hasta DC3, otro dominio distinto y nos vamos al grupo administradores.



Miembros van a ser el administrador del subdominio asir y el grupo admins del subdominio asir pero también es miembro el grupo administradores de organización del valle.local. Aquí en administradores de organización está el administrador del otro dominio, del valle.local. Luego ese administrador también es administrador de este subdominio.

El grupo Administradores de Organización no existe en DC3 solo existe en el dominio raíz en el DC1.



1. **Vamos a ver qué ocurre si un administrador de DC-3** crea un usuario desde cmd en el contenedor Users , este contenedor no se referencia como OU sino como Cn=Users.

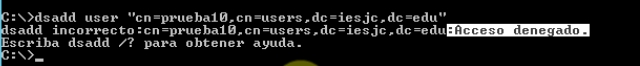
Dsadd user “cn=prueba10,cn=Users,dc=asir,dc=valle,dc=local”

Tiene que ser correcto.

Qué pasa si ahora queremos crear un usuario en el dominio valle.Local desde el DC3.

Dsadd user “cn=prueba10,cn=Users,dc=valle,dc=local” entonces nos dice incorrecto : Acceso denegado.

Esto es incorrecto porque un administrador de un subdominio, no puede crear objetos en el dominio superior o principal.



1. Que ocurre si nos trasladamos al dominio Raiz a valle.local y intentamos crear

Objetos del subdominio asir.

Nos vamos a DC1.

Dsadd users “cn=prueba10,cn=Users,dc=valle,dc=local” esto es correcto.

Y ahora creamos el usuario prueba11 en el subdominio asir.

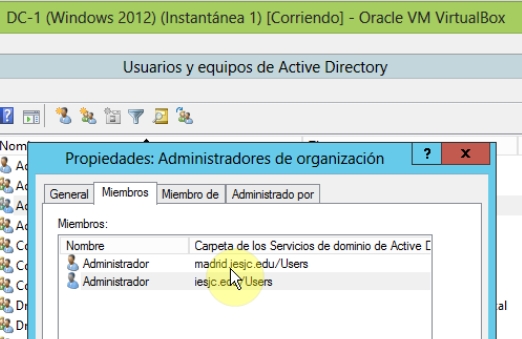
Dsadd users “cn=prueba11,cn=Users,dc=asir,dc=valle,dc=local”

Nos dice correcto.

Hemos podido crearlo porque el Administrador de valle.local es miembro del grupo Administradores de Organización, y en el grupo administradores del DC-3 esta como miembro el grupo Administradores de organización.

1. PROBAR. Como podríamos hacer para que el administrador de asir pudiera crear objetos en el valle.local.

Primero, agregar en administradores de organización y hacerle miembro al administrador del asir.valle.local.



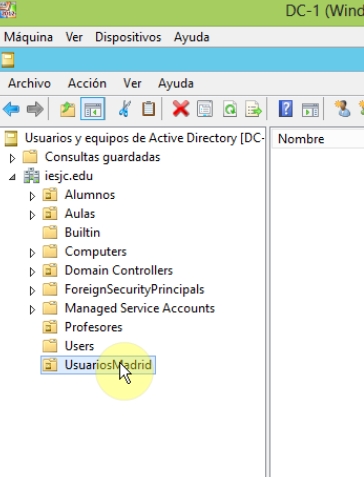
Esto funciona y terminamos de convertir al administrador de asir en un administrador de toda la organización, es decir sería administrador de todos los subdominios que tengamos.

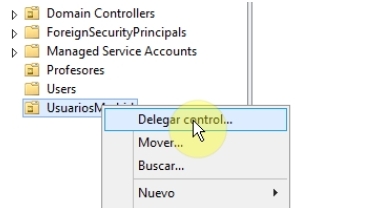
1. Cuando nos validamos en un subdominio con el administrador lo que ocurre es que al validarnos se crea un token de acceso y en ese token de acceso ponía que este usuario no pertenecía al grupo administradores de empresa, por lo tanto si yo ahora intento ejecutar otra vez el comando para crear el usuario en el dominio principal, hasta que no cierre sesión e inicie sesión otra vez la pertenencia a este grupo(administradores de empresa) no está en mi token de acceso, cuando yo intento ejecutar el comando para crear el usuario le mando mi token de acceso y no tengo suficientes privilegios para crear el usuario.

El grupo (Administradores de empresa) es un grupo de tipo universal y la pertenencia a los grupos universales se chequea mediante los catálogos globales y se gestiona en el dominio valle.local, entonces es posible que si están en sites distintos aunque cerremos sesión e iniciemos sesión no se actualicen y puede tardar más tiempo en que la pertenencia se viera reflejada.

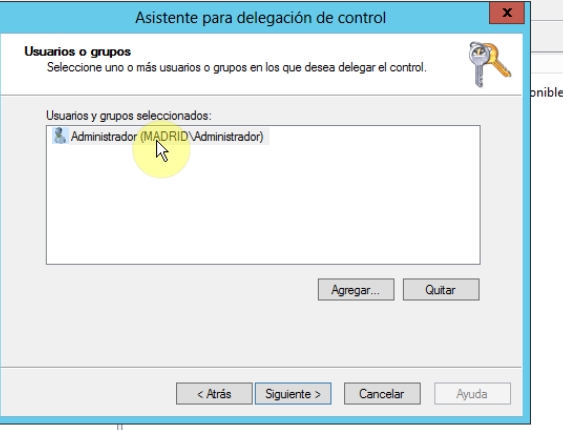
1. Existe otra forma de permitir que el administrador de asir.valle.local pueda crear objetos en valle.local. ¿Cómo? A través de las delegaciones.
2. Desde hace bastante existe los que se llama delegación.

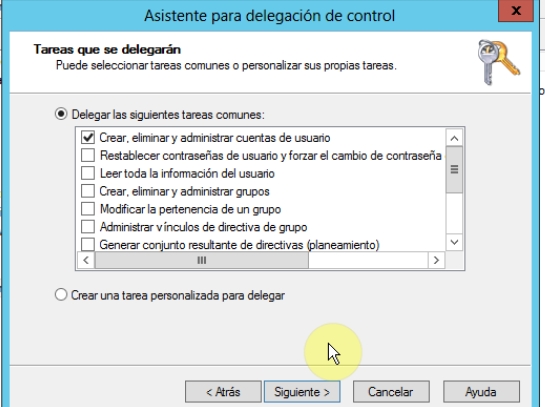
* Le voy a crear una unidad organizativa en DC1. Llamada UsuariosAsir. Y aquí vamos a delegar control.



Aquí en la unidad organizativa UsuariosAsir lo que voy a hacer es delegar control.

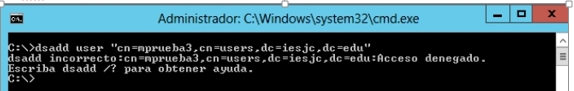
Nos sale un asistente y después le doy a agregar para seleccionar al administrador del dominio asir.valle.local a este usuario que tareas comunes le voy a delegar pues “crear eliminar tareas comunes”.



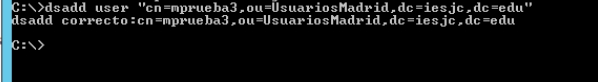


Siguiente, siguiente y finalizar.

Como hemos delegado en esta unidad organizativa la creación de usuarios, borrar y administrar Esto permite que el administrador de asir.valle.local pueda crear usuarios dentro de esta unidad organizativa pero no en otras unidades organizativas. Con lo cual el administrador de la empresa puede venir a esta unidad organizativa y ver que usuarios a creado el administrador de dominio asir.valle.local.

* Si ahora desde DC3 intentamos crear usuarios en el contenedor users no nos deja y nos da acceso denegado.

Pero, qué ocurre, si en vez de crear usuarios dentro de users, intento crear los usuarios dentro de la unidad organizativa UsuariosAsir pues que entonces si nos deja.



Antes de nada, hacer instantáneas de todos los C.D.

risa.local 192.168.0.1

192.168.0.2

adicional

DC2

DC1

subrisa.risa.local 192.168.0.3 subad.risa.local 192.168.0.4

Ahora vamos a instalar un subdominio con Windows 2016 teniendo apagado el DC1 y encendido el DC2 adicional que es el controlador de dominio secundario

La máquina 2016

Red interna. En la misma red que están el resto de controladores.

1. Cambiamos el nombre para que nos diga algo
2. Ponerle una IP fija 192.168.0.5 y en el DNS:

preferido la ip del controlador de dominio principal :192.168.0.2

Secundario la ip del controlador de dominio secundario :192.168.0.3

Lo que hace esto es que cuando se intenta poner en contacto con el DNS preferido, pero al ver que no está en marcha se pone en contacto con el secundario.

* 1. Desactivar el Firewall en las dos máquinas.
  2. Mirar si hay conexión física entre estas dos máquinas con ping ip, y en los dos sentidos, si todo esta correcto continuamos, si nos da algún problema paramos y resolvemos los problemas. Siempre tiene que responder el ping.

1. Agregar ROLES y CARACTERISTICAS.

Servicios y dominios de Active Directory

Agregar características Instalar.

Tenemos el DC2 en marcha funcionando y el DC1 apagado.

* Nos vamos a la Alerta amarilla que hay al lado del Administrador, para poder ejecutar el dcpromo en Windows 2012 se realiza automáticamente con esta alerta.
* Características valle\administrador ó administrador @valle.local —p@ssw0rd
* Ahora nos da un error y nos dice que el error es porque el C.D que es el Maestro de Nomenclatura de Nombres de dominio esta sin conexión. Por lo tanto, no podemos unir ningún subdominio. Aceptamos y cancelamos el asistente.
* Ahora ponemos en marcha el DC1 y transferimos la función de Nombre de dominio al DC2. ¿Cómo se hace?

La podemos transferir desde el DC2.

En sitios y servicios de Active directory replicamos manualmente todo.

Transferimos la función de Nombres de Dominio.

* Nos vamos al DC2
* Nos vamos a dominios y confianzas de Active directory. Maestro de operaciones, nos dice que es el DC1.

Entonces aquí le decimos que queremos cambiar de controlador de dominio de Active Directory. A cual, al DC2

WIN2008-----DC1

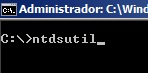
WIN2012----DC2. Seleccionamos el DC2 y damos a aceptar. Ahora después si le damos a Maestro de Operaciones nos dice que está en el DC1 y si queremos lo podemos cambiar al DC2. Se ha transferido con existo el Maestro de operaciones.

* Transferimos también el Maestro de esquemas porque si no nos da error. ¿Cómo lo hacemos? Si no nos funciona a través del menú lo hacemos a través de línea de comandos.

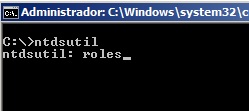
Son unos pasos muy sencillos a seguir y que nos facilitara cambiar nuestro maestro de esquema a un nuevo Domain Controller.

**Nota:** Tenemos que realizar los siguientes pasos des del servidor que queramos que sea maestro de esquema.

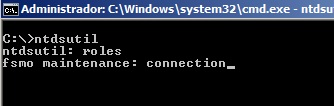
* Abrimos la ventana de comandos
* Escribimos: **ntdsutil**



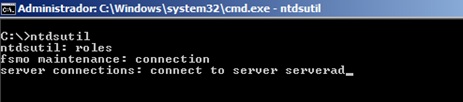
* En el símbolo del sistema de **ntdsutil**, escribimos: **roles**

[](http://www.infoskaind86.com/wp-content/uploads/2012/09/3.jpg)

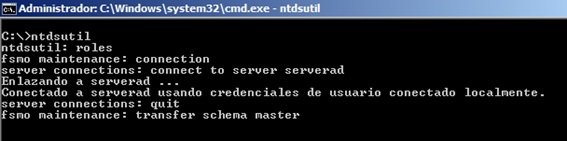
* En el símbolo del sistema de **fsmo maintenance**, escribimos: **connection**

**[](http://www.infoskaind86.com/wp-content/uploads/2012/09/4.jpg)**

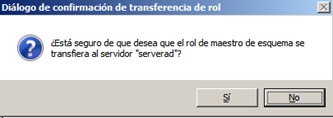
* En el símbolo del sistema de **server connections**, escribimos: **connect to server “controladorDeDominio”**

***[](http://www.infoskaind86.com/wp-content/uploads/2012/09/5.jpg)***

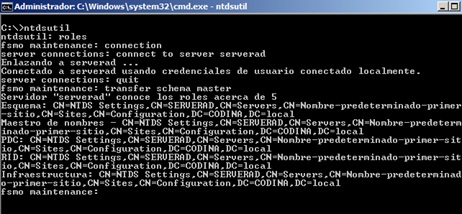
* En el símbolo del sistema de **fsmo maintenance**, escribimos: **transfer schema master**

**[](http://www.infoskaind86.com/wp-content/uploads/2012/09/7.jpg)**

* Confirmamos el mensaje que nos sale.

[](http://www.infoskaind86.com/wp-content/uploads/2012/09/8.jpg)

* Ahora ya estamos.

[](http://www.infoskaind86.com/wp-content/uploads/2012/09/9.jpg)

Después de estos sencillos pasos ya tendremos transferido el maestro de esquemas de un **Domain Controller**a otro.

Ya está transferido el maestro de esquemas también al DC-2.

* Ahora apagamos otra vez el DC1, o como tarda mucho en apagarse le quitamos la red—Dejamos sin conexión en la red.

Nos vamos a Abrir centro de redes y recursos compartidos

Cambiar configuración del adaptador

Botón derecho Desactivar—Ya no tenemos red.

* Ahora nos vamos otra vez al DC4 a la alerta para ejecutar otra vez el dcpromo

Elegimos promover el servidor a controlador de dominio.

Nivel funcional del dominio 2012

Opciones DNS

Siguiente…. Al terminar reinicia

* Comprobamos ciertas cosas.
* 1) Configuración Ip del DC44asir1

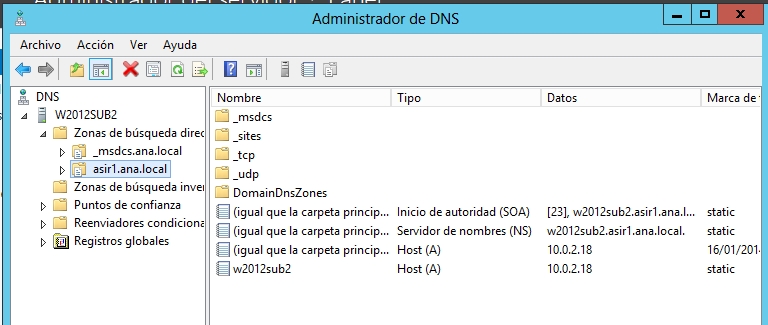
Abrir centro de redes y recursos ¿Qué hace? Lo hace bien

Servidor Dns preferido: 127.0.0.1

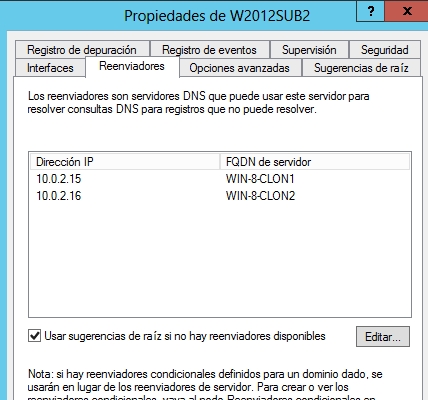
Servidor dns alternativo: 192.168.0.3

Nosotros le habíamos puesto preferido:2 y alternativo:3 y él lo modifica bien.

* Vamos a ver el DNS del DC4 windows 2012.



Si nos vamos a las propiedades del servidor, en reenviadores nos ha configurado dos reenviadores, tienen un posible servidor DNS con ip 192.168.0.2 y otro en la 192.168.0.3



Entonces cuando ahora hacemos ping a Ana1-PC.ana.local, que es un ordenador cliente conectado al dominio ana.local , el DNs tiene que resolver.

