PRACTICAS Añadir controlador de dominio adicional

192.168.10.1

192.168.10.2

adicional

vallexxx.local W 2016 CD116 WCD222

1. Creamos un clon de Windows 2022 con las gest-aditions instaladas.
2. Para que veáis que podemos integrar controladores de dominio distintos uno con 2016 y otro con 2022 siempre que el nivel funcional del bosque y del dominio nos lo permitan.
3. Arrancamos y le llamamos 2022- CD222

-Configuración 1. Red🡪 red interna

2. Cambiar nombre del equipo, más cómodo CD222

3. Dirección IP fija y en la misma subred que el Controlador de dominio principal.

4. Servidor DNS preferido ponemos la IP del controlador de dominio principal CD1.

5. Desactivar el Firewall en las dos máquinas.

6. primero miramos si hay conexión física entre estas dos máquinas. Con ping ip, en los dos sentidos y si todo esta correcto continuamos, si nos da algún problema paramos y resolvemos los problemas. Siempre tiene que responder el ping.

3. No es necesario que sea un miembro del dominio para convertirlo en un C.D pero si lo hacemos ya nos aseguramos que tenemos conectividad lógica con el dominio.

Administrador @valle.local

En dominio

Vallexxx.local 🡪 se unió correctamente al dominio

8. Tenemos que tener el controlador de dominio principal CD1 corriendo.

1. Arrancamos la máquina CD222

--Agregar Roles🡪 Instalar servicio de dominio del Active Directory

--Ejecutamos dcpromo, que a partir de 2012 en adelante es ejecutar la

Banderita.

1. Bosque Existente
2. Agregar un C.D a un dominio existente

Nombre de dominio= vallexxx.local

Establecer credenciales alternativas 🡪 con

administrador @vallexxx.local.

1. Seleccione un dominio para este controlador de dominio vallexxx.local
2. En que sitio vas a ubicar este controlador. El nombre del sitio (site) suele ser igual o parecido al edificio físico donde se encuentra o la zona física.

**ANTES DE CONTINUAR VAMOS A CAMBIAR EL NOMBRE DEL SITE QUE TENEMOS ACTUALMENTE EN DC1**

Nos vamos a CD1 y nos vamos a Herramientas🡪 sitios y servicios del Active Directory.

Ahora nosotros aquí tenemos un site que se crea por defecto, y cuyo nombre se le da al instalar el CD1 , y tenemos un solo site con un solo servidor CD1 y tiene un nombre predeterminado

Nombre🡪 Default-First-Site-Name y aquí le cambiamos el nombre a site Madrid-risa.

Nos posicionamos encima del site y botón derecho, y modificamos el nombre.

Ahora nos regresamos al CD2

1. Damos marcha atrás.
2. Después continuamos y veremos que ya nos aparece el nombre de site que nosotros hemos modificado antes.
3. Mejor poner otro servidor DNS (un 2 DNS en el mismo dominio) para que este Controlador de dominio también tenga su propio DNS.

Es mejor que tenga un segundo servidor DNS y van a replicar los datos entre los dos DNS cada 15 minutos, los cambios que tengan y de esa manera en cualquier momento podemos apagar un equipo y lo lógico es que los clientes tuvieran como serdiro DNS principal al CD1 y como servidor DNS secundario del CD2.

1. Catalogo Global—Si
2. Como replican los datos del dominio a este equipo, a través de la red, desde un C.D.

Replicar los datos a través de la red

1. Cogemos un servidor que este en la red en nuestro site.
2. Contraseña en modo restauración servicio directorio. Esto es para cuando se tiene problemas con los servicios de directorio si nos da error … Reiniciamos y al reiniciar F8 Modo seguro y modo restauración de los servicios de Directorio.
3. Reiniciamos la máquina CD222.
4. Cuando arranque CD2, miramos la configuración Ip de la máquina.

A pesar de que nosotros le hemos dicho que tenga un DNs propio, en la configuración de este CD2 nos aparece

Servidor DNS preferido la iP del CD1, pero hay que modificarlo aunque 2016 hay veces que lo hace automáticamente y dejarlo:

DNS preferido: 127.0.0.1 o su ip

DNS alternativo en blanco.

**Ahora nosotros tenemos un dominio con dos controladores de dominio** distintos y con 2 DNS. Esto lo podemos aprovechar a la hora de instalar los clientes... De tal forma que si en un momento dado uno no está disponible automáticamente los clientes puedan utilizar el otro, y así también podemos balancear la carga.

Si tenemos 2 C.D con DNS propio si estamos trabajando ejemplo en un instituto donde tenemos 12 clases, pues entonces repartimos un poco la carga, a la vez que nos aseguramos que los clientes tengan siempre conectividad física.

Los clientes correspondientes a 6 clases en su configuración IP tendrían puesto:

DNs preferido DC1

DNS secundario DC2

Los clientes de las otras 6 clases restantes en su configuración Ip tendrían lo contrario:

DNs preferido DC2

DNS secundario DC1

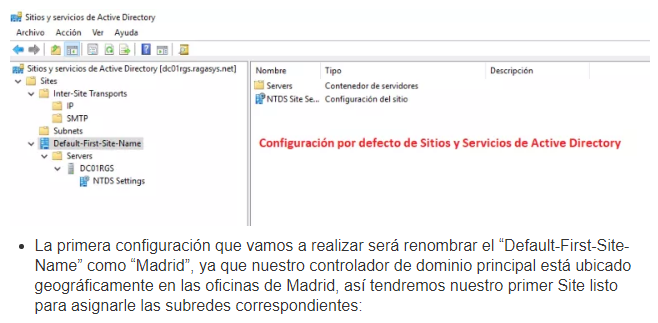
Normalmente un equipo siempre utiliza el DNS preferido, da igual que en un momento le hagamos una consulta que no sepa resolver, sino conoce la respuesta no va a ir a preguntarle al DNS secundario sino que va a ir a preguntar a los nodos superiores(o desinencias raíz) no al secundario. **El DNS secundario solo se utiliza si el primario no funciona por la causa que fuera.**

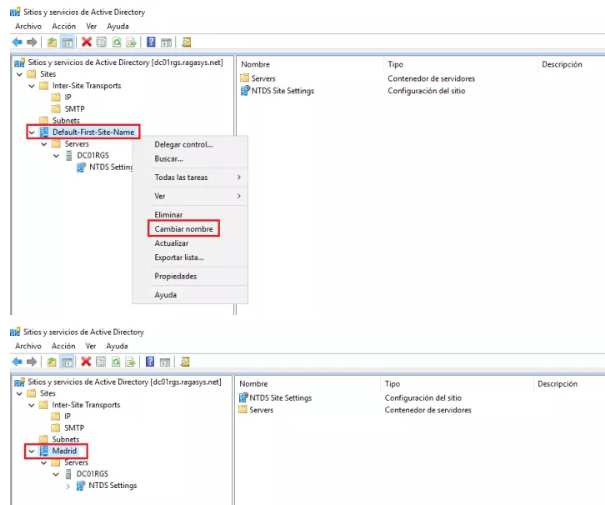
1. Ahora ya nos vamos al DC1 y nos vamos a usuarios y equipos del Active Directory. En la parte de Domains Controllers ya tiene que aparecer el DC2 como segundo controlador de dominio
2. Ahora vamos a ver el DNS del DC2 tienen que tener sus zonas y en el Dc1 también.

DC2 Aquí botón derecho propiedades en la pestaña Reenviadores, tengo como reenviador la IP del DC1, significa que este cuando no sepa resolver un registro porque no pertenezca al dominio valle,local, este le pasa el marrón al DC1 para que DC1 resuelva, si lo conoce lo resuelve y le da la respuesta, pero sino lo conoce como en su caso DC1 no tiene ningún reenviador, lo que hace es utilizar la sugerencia RAIZ, que son servidores DNs de Internet y le pasaría el marrón a ellos.

Ipconfig /flushdns---🡪 borra la cache de resolución DNS.

1. Mirar sitios y servicios del Active Directory.





1. Objetos NTDS Setting. Lo que ocurre en los controladores de dominio tenemos unos objetos donde se configura la replicación de datos = NTDs Setting del DC1

Este objeto lo que dice es que este controlador de dominio va a replicar los datos desde el servidor DC2, y en el DC2 tendremos su análogo, otro objeto similar que nos dice que la replicación de datos se hace des el DC1. De esta manera podemos configurar como se va a hacer la replicación de datos entre los distintos controladores de los distintos dominios y de los distintos sites para ir haciendo caminos que permitan que toda la información este en todos los sitios.

Normalmente en un site todos los controladores de dominio replican con todos los controladores de dominio replican con todos y además cada cierto tiempo definido.

* Ningún controlador de dominio es el maestro.
* Todos los C.D. son iguales y contienen una copia de la B.D., del directorio
* Los controladores de dominio replican los cambios entre ellos.
* Cualquier controlador de dominio puede procesar los cambios del directorio y replicarlos.
* Los controladores de dominio replican inmediatamente ciertas actualizaciones urgentes, por ejemplo la eliminación de una cuenta de usuario.
* Establecer varios controladores de dominio dentro de un dominio permite tolerancia a fallos
* Todos tienen asignada las mismas tareas salvo: Servidor de cabeza de puente, y la función del maestro de operaciones.

Botón derecho propiedades y cambiar programación aquí se le dice cada cuanto tiempo va a replicar y puede replicar hasta 4 veces en una hora, según necesidades.

También desde aquí podemos replicar ahora en el momento concreto que queramos.

NTDS site -🡪 Botón derecho y replicar ahora directamente en este momento.

Ipconfig /flushdns---🡪 borramos la cache de resolución DNS, y así si hacemos un ping, forzamos siempre a la búsqueda contra el servidor DNS.

1. CREAR OBJETOS EN EL DOMINIO

* Crear objetos en el DC1 mediante la herramienta gráfica.

Cada controlador de dominio tiene un rango de SID y utiliza su rango y de esa manera sus identificadores son únicos en el dominio.

¿Qué hacer para que el SID nos aparezca, en las propiedades del usuario?

Ver🡪Características avanzadas,

Para que nos muestre la ficha de Editor de atributos, en propiedades, aquí buscamos el objeto SID object sid.

Quien se encarga de gestionar los rangos de los SID,🡪 el maestro de RID

Cuando se agrega un nuevo controlador al dominio, se podrá en contacto con el RID para asignarle un nuevo rango, cada controlador de dominio tiene un rango de SID y así los identificadores son únicos en el dominio.