



ACT2.4 Añadir nuevo controlador de Dominio

Fecha de realización: 19 - 10 - 22

1.- OBJETIVOS.

Agregar un controlador de dominio adicional a tu dominio, con objeto de mejorar el rendimiento y la seguridad del mismo.

2.- CONTENIDOS TEÓRICOS.

Servicio de Directorio en Windows

3.- MATERIAL NECESARIO.

Máquina virtual con Windows Server 2019 Standard instalado.
Segunda Máquina virtual con Windows Server 2019 Standard instalado (No clonar. Realizar instalación de nuevo)

4.-Índice.

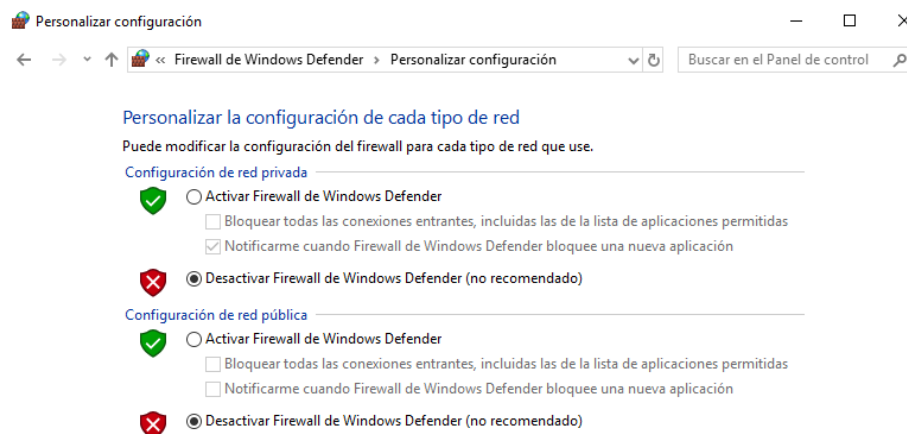
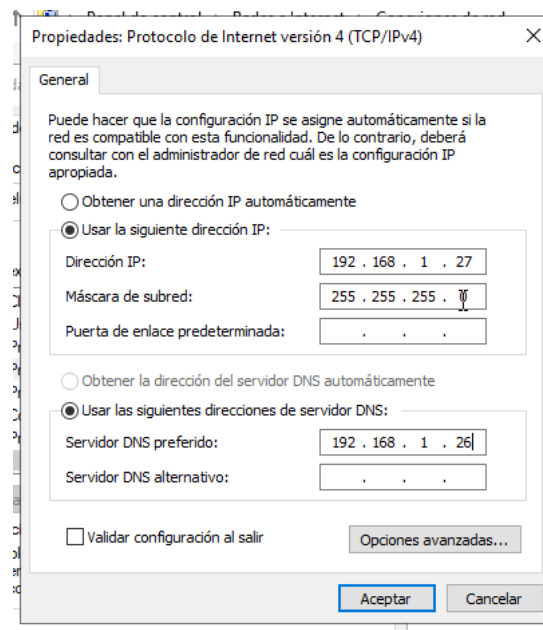
- 1. INSTALAR UNA NUEVA MÁQUINA VIRTUAL CON W2019 SERVER**
- 2. CONFIGURAR EL DNS DEL DC PRINCIPAL**
- 3. UNIR EL NUEVO EQUIPO COMO CLIENTE DEL DOMINIO**
- 4. AÑADIR EL ROL AD AL NUEVO EQUIPO**
- 5. AJUSTAR LA CONFIGURACIÓN DE RED**
- 6. COMPROBACIONES**



1. INSTALAR UNA NUEVA MÁQUINA VIRTUAL CON W2019 SERVER

1.1 Configura la red de manera adecuada para que las dos máquinas puedan comunicarse. ¡¡¡Importante!!! Su DNS será el DC principal (de momento, el único que hay en el dominio). Comprueba que ambas máquinas hacen ping.

A nuestro servidor que vamos a usar para replicar, lo llamaremos, segundo servidor. Vamos a configurar la interfaz de red y el firewall:





Ahora comprobaremos si se ha realizado bien, haciendo ping del servidor a la otra máquina:

```
C:\Users\Administrador>ping 192.168.1.26

Haciendo ping a 192.168.1.26 con 32 bytes de datos:
Respuesta desde 192.168.1.26: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.26: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.26: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.1.26: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 192.168.1.26:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Administrador.SMR2_FEC>ping 192.168.1.27

Haciendo ping a 192.168.1.27 con 32 bytes de datos:
Respuesta desde 192.168.1.27: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.27: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.27: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.1.27: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.1.27:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

Con estas imágenes podemos comprobar que tenemos una conexión entre los dos servidores, ahora vamos a proceder con las siguientes configuraciones.

2. CONFIGURAR EL DNS DEL DC PRINCIPAL

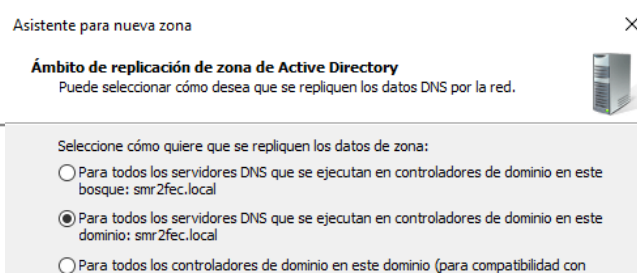
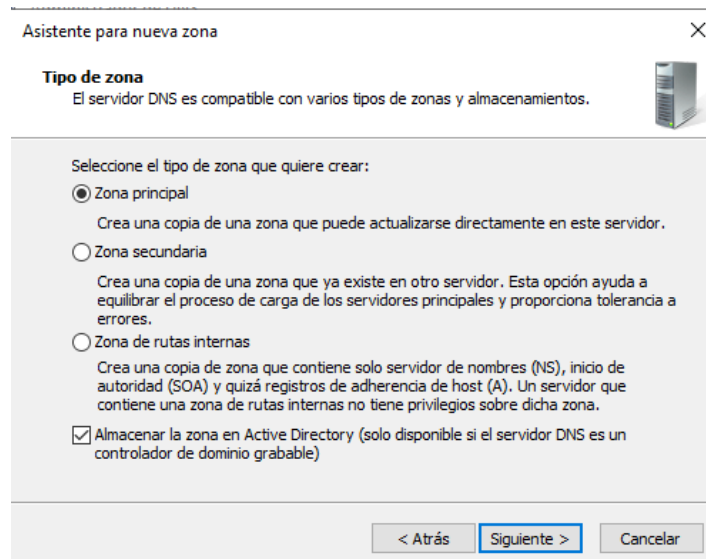
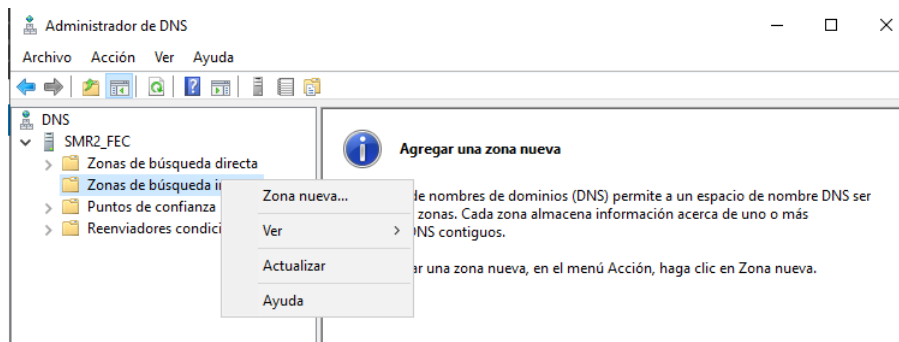


1.1 Se deberá configurar el servidor DNS para que sea capaz de atender las peticiones del rango de ips que forman nuestra red interna (192.168.1.1 – 192.168.1.255)

Ahora vamos a añadir unos pasos muy sencillos, nos dirigiremos a la siguiente ubicación:

“Administración del servidor” → “Herramientas” → “DNS”.

Cuando se haya abierto la ventana del Admin del DNS, seleccionaremos Zonas de búsqueda inversa y en el rango le podremos 192.168.1, eso hará que todas las peticiones de nuestra red, nuestro servidor las atenderá. Cuando la creamos, pondremos que esta nueva zona, sea principal y que se almacene en nuestro AD y próximamente, que se replique en todos los servidores DNS del dominio. A continuación, dejo capturas:





Asistente para nueva zona

Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Elija si desea crear una zona de búsqueda inversa para direcciones IPv4 o direcciones IPv6.

Asistente para nueva zona

Nombre de la zona de búsqueda inversa
Una zona de búsqueda inversa traduce direcciones IP en nombres DNS.

Para identificar la zona de búsqueda inversa, escriba el Id. de red o el nombre de zona.

☒ Id. de red:
192.168.1

El Id. de red es la parte de la dirección IP que pertenece a esta zona. Escriba el Id. de red en su orden normal (no en el inverso).

Si usa un cero en el Id. de red, aparecerá en el nombre de la zona. Por ejemplo, el Id. de red 10 crearía la zona 10.in-addr.arpa, y el Id. de red 10.0 crearía la zona 0.10.in-addr.arpa.

☐ Nombre de la zona de búsqueda inversa:
1.168.192.in-addr.arpa

Asistente para nueva zona

Actualización dinámica
Puede especificar si esta zona DNS aceptará actualizaciones seguras, no seguras o no dinámicas.

Las actualizaciones dinámicas permiten que los equipos cliente DNS se registren y actualicen dinámicamente sus registros de recursos con un servidor DNS cuando se produzcan cambios.

Seleccione el tipo de actualizaciones dinámicas que desea permitir:

☒ Permitir solo actualizaciones dinámicas seguras (recomendado para Active Directory)
Esta opción solo está disponible para las zonas que están integradas en Active Directory.

☐ Permitir todas las actualizaciones dinámicas (seguras y no seguras)
Se aceptan actualizaciones dinámicas de registros de recurso de todos los clientes.
 Esta opción representa un serio peligro para la seguridad porque permite aceptar actualizaciones desde orígenes que no son de confianza.

☐ No admitir actualizaciones dinámicas
Esta zona no acepta actualizaciones dinámicas de registros de recurso. Tiene que actualizar sus registros manualmente.

< Atrás **Siguiente >** Cancelar

DNS

- SMR2_FEC
 - Zonas de búsqueda directa
 - Zonas de búsqueda inversa
 - 1.168.192.in-addr.arpa**
 - Puntos de confianza
 - Reenviadores condicionales

3. UNIR EL NUEVO EQUIPO COMO CLIENTE DEL DOMINIO



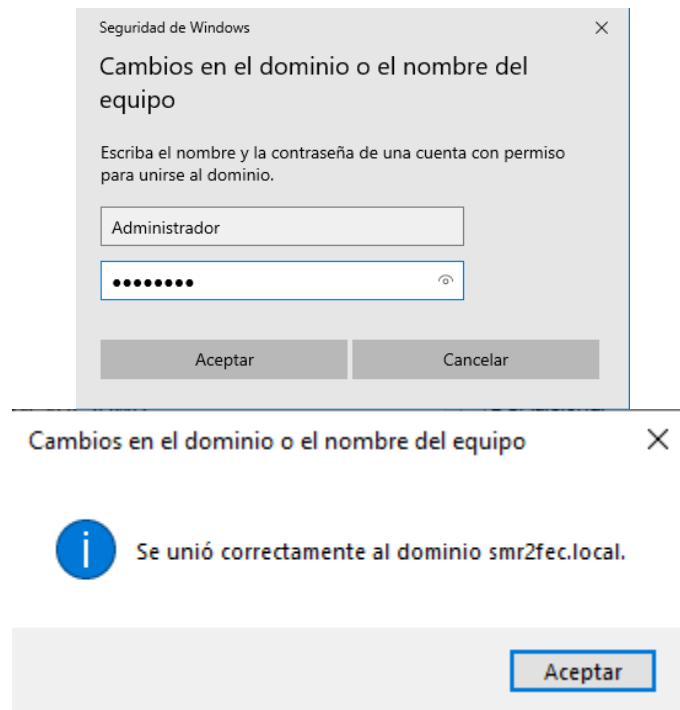
3.1 Para que la posterior promoción del nuevo DC funcione correctamente, es conveniente convertirlo en un nuevo equipo cliente del dominio. Para ello sigue los pasos que realizaste en la práctica anterior.

Para promocionarlo será muy sencillo, yo voy a hacer un resumen de los pasos más importantes, para más detalles, seguir la siguiente práctica:

<https://docs.google.com/document/d/1sD44Hm7CuFC2msu6yxFfwJbPGWk6QcgZ5xJoRhMzLY8/edit?usp=sharing>

La contraseña será DCadici0nal2#

3.2 El nombre que del que ya está configurado (en un caso smr2fec.local) se unirá al dominio





```
C:\Users\Administrador>ipconfig/all

Configuración IP de Windows

Nombre de host. . . . . : DCA adicional
Sufijo DNS principal . . . . : smr2fec.local
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: smr2fec.local
```

3.3 Asegúrate de que el equipo ha sido agregado al dominio correctamente. Para ello abre Herramientas → usuarios y equipos de AD → Computers

Nombre	Tipo
 DC-adicional	Usuario
 PC01	Equipo

4. AÑADIR EL ROL AD AL NUEVO EQUIPO



4.1 Promocionar el equipo al que hemos llamado DC-Adicional para que actúe como segundo controlador del dominio, en mi caso smr2rag.local. El proceso es similar al que realizaste con el primer DC

The screenshot shows the Windows Server 2012 R2 Server Manager interface. The 'Administrar' menu is open, showing options: 'Agregar roles y características', 'Quitar roles y funciones', 'Agregar servidores', 'Crear grupo de servidores', and 'Propiedades del Administrador del servidor'. Below this, the 'Asistente para agregar roles y características' wizard is running. The 'Selección de roles' pane shows the 'Roles de servidor' step selected. The main pane displays a warning: '¿Desea agregar las características requeridas para Servicios de dominio de Active Directory?'. It lists the required features: 'Administración de directivas de grupo', 'Herramientas de administración remota del servidor', 'Herramientas de administración de roles', 'Herramientas de AD DS y AD LDS', 'Módulo de Active Directory para Windows PowerShell', 'Herramientas de AD DS', 'Centro de administración de Active Directory', and 'Complementos y herramientas de línea de comandos de Active Directory'. The 'Incluir herramientas de administración (si es aplicable)' checkbox is checked. The 'Agregar características' button is highlighted. The bottom of the wizard shows navigation buttons: '< Anterior', 'Siguiente >', 'Instalar', and 'Cancelar'.

Ver progreso de la instalación

Iniciando instalación



Administración de directivas de grupo
Herramientas de administración remota del servidor



Podemos ver la bandera con el símbolo amarillo, promover el servidor:

anel

Configuración posterior a la implementación

Requiere configuración para Servicios de dominio de Active Directory en DCADICIONAL

[Promover este servidor a controlador de dominio](#)

Detalles de tarea

y.

Seleccionar la operación de implementación

☐ Agregar un controlador de dominio a un dominio existente

☒ Agregar un nuevo dominio a un bosque existente

☐ Agregar un nuevo bosque

Especificar la información de dominio para esta operación

Seleccionar tipo de dominio: Dominio secundario

Nombre de dominio principal: smr2fec.local [Seleccionar...](#)

Nuevo nombre de dominio: smr2fec-local

Proporcionar las credenciales para realizar esta operación

SMR2FEC\Administrador [Cambiar...](#)

El nuevo controlador de dominio tendrá el nombre de dominio de smr2fec-local, he cambiado el . por un guión para poder hacerlo diferente:



Seleccionar nivel funcional del nuevo dominio

Nivel funcional del dominio: Windows Server 2016

Especificar capacidades del controlador de dominio e información del sitio

☒ Servidor de Sistema de nombres de dominio (DNS)

☒ Catálogo global (GC)

☐ Controlador de dominio de solo lectura (RODC)

Nombre del sitio: Default-First-Site-Name

Escribir contraseña de modo de restauración de servicios de directorio (DSRM)

Contraseña: ••••••••

Confirmar contraseña: ••••••••

Especificar opciones de delegación DNS

☒ Crear delegación DNS

Credenciales para crear delegaciones

SMR2FEC\Administrador

Verifique el nombre NetBIOS asignado al dominio y cámbielo si es necesario

Nombre de dominio NetBIOS: SMR2FEC-LOCAL

Configuración de implem...

Opciones del controlador...

Opciones de DNS

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisi...

Especificar la ubicación de la base de datos de AD DS, archivos de registro y SYSVOL

Carpeta de la base de datos: F:\Datos\Base de datos

Carpeta de archivos de registro: F:\Datos\Archivos de registro

Carpeta SYSVOL: F:\Datos\SYSVOL

Con estos pasos, habremos instalado el controlador de dominio a la perfección:



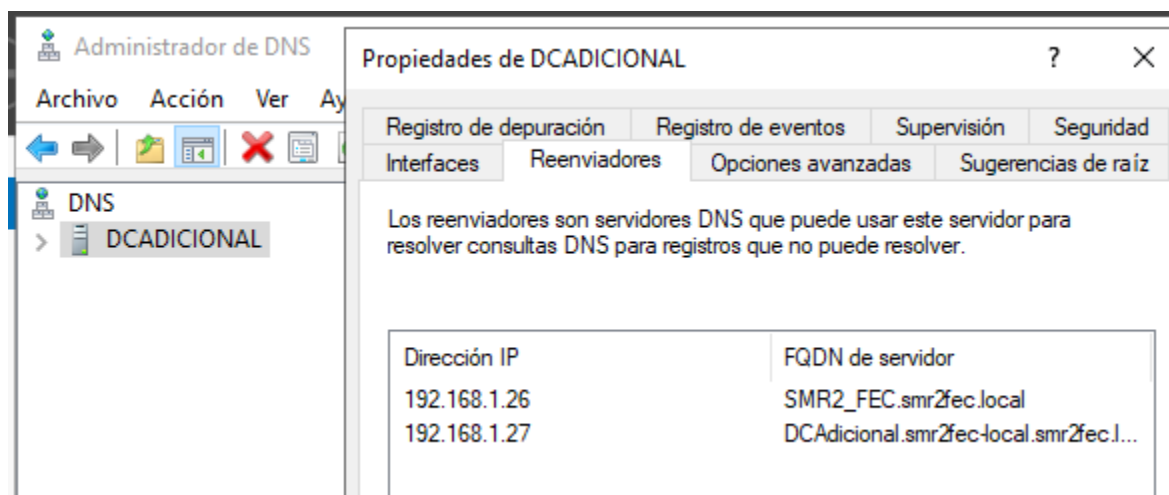
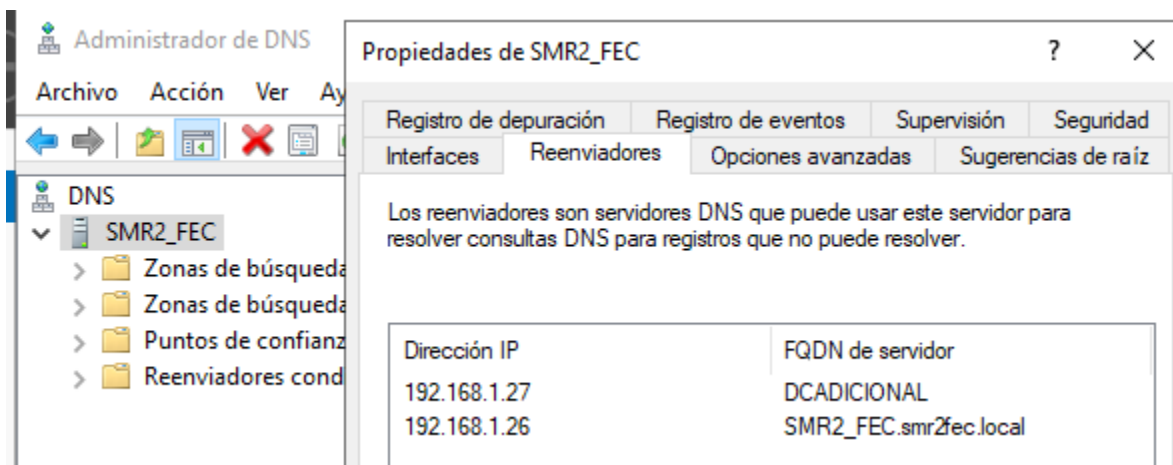
Instalación

Configuración de implem...

Progreso

5. AJUSTAR LA CONFIGURAR DE RED

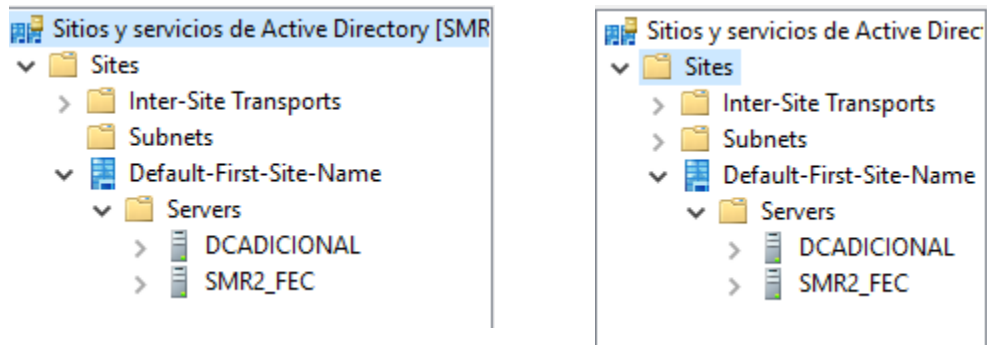
5.1 Cada servidor hará referencia como servidor DNS preferido al equipo contrario y como Servidor DNS alternativo, a él mismo.



6. COMPROBACIONES



6.1 Comprobaremos que la configuración DNS de los dos equipos está correctamente (Tienes que comprobarlo en los dos servidores). Comprueba que en Sitios y Servicios de Active Directory, dentro de Servers aparecen los nombres de los dos equipos.

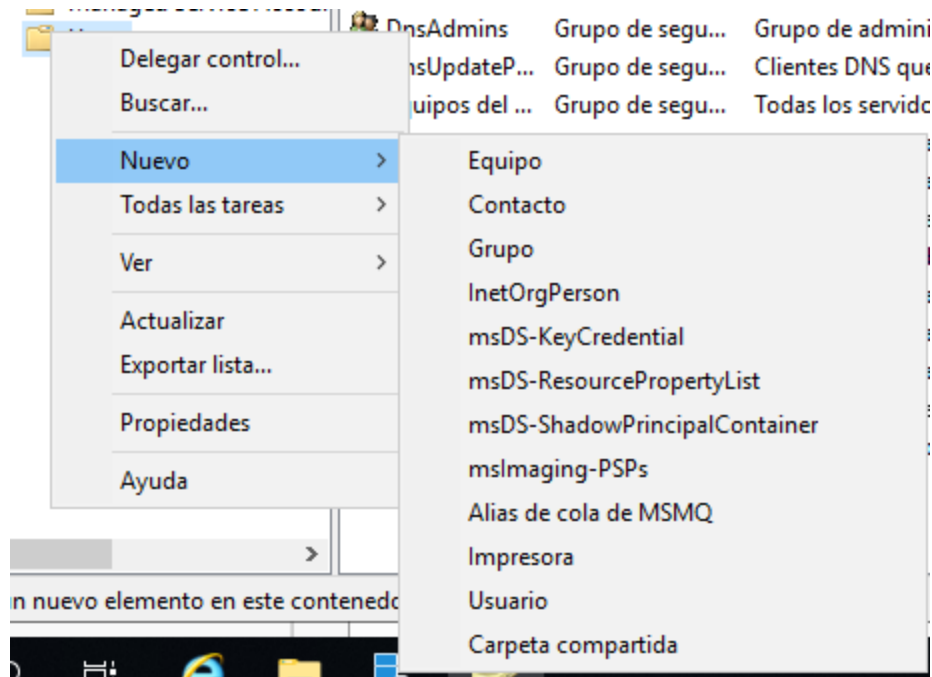


Están correctamente configurados, como podemos ver en las imágenes

DNS	Nombre	Tipo	Datos	Marca de
<ul style="list-style-type: none"> DCADICIONAL <ul style="list-style-type: none"> Zonas de búsqueda directa <ul style="list-style-type: none"> smr2fec-local.smr2fec.local Zonas de búsqueda inversa Reenviadores condicionales 	<ul style="list-style-type: none"> _msdcs _sites _tcp _udp (igual que la carpeta princip... (igual que la carpeta princip... (igual que la carpeta princip... dcadicional Serverprincipal 	<ul style="list-style-type: none"> Inicio de autoridad (SOA) Servidor de nombres (NS) Host (A) Host (A) Host (A) 	<ul style="list-style-type: none"> [16], dcadicional.smr2fec-... dcadicional.smr2fec-local-... 192.168.1.27 192.168.1.27 192.168.1.26 	<ul style="list-style-type: none"> static static 21/10/202 static

DNS	Nombre	Tipo	Datos
<ul style="list-style-type: none"> SMR2_FEC <ul style="list-style-type: none"> Zonas de búsqueda directa <ul style="list-style-type: none"> _msdcs.smr2fec.local smr2fec.local Zonas de búsqueda inversa Puntos de confianza Reenviadores condicionales 	<ul style="list-style-type: none"> _msdcs _sites _tcp _udp DomainDnsZones ForestDnsZones smr2fec-local (igual que la carpeta princip... (igual que la carpeta princip... (igual que la carpeta princip... (igual que la carpeta princip... DCAdicional PC01 smr2_fec 	<ul style="list-style-type: none"> Inicio de autoridad (SOA) Servidor de nombres (NS) Host (A) Host (A) Host (A) Host (A) Host (A) Host (A) 	<ul style="list-style-type: none"> [52], smr2_fec.smr2fec.lo smr2_fec.smr2fec.local. 192.168.1.26 192.168.1.125 192.168.1.27 192.168.1.29 192.168.1.26

creando un nuevo usuario en éste y viendo cómo se replica en el DC principal.



6.3 Apaga el DC principal y logueate con un usuario del dominio en el equipo cliente.

Nuevo objeto: Usuario

Crear en: smr2fec-local.smr2fec.local/Users

Nombre de pila: prueba Iniciales:

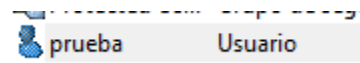
Apellidos:

Nombre completo: prueba

Nombre de inicio de sesión de usuario: prueba @smr2fec-local.smr2fec.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000): SMR2FEC-LOCAL\ prueba

< Atrás Siguiente > Cancelar

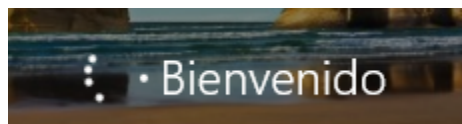
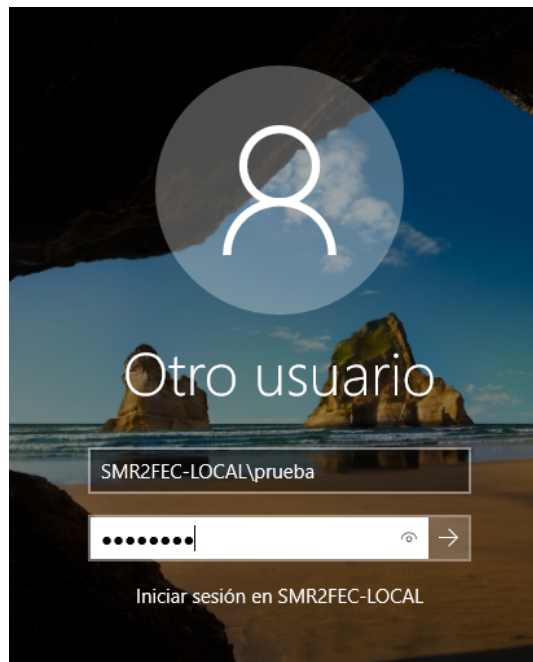


Contraseña Pru3ba1#

Ahora apagaremos el servidor y nos logueamos con este nuevo usuario:



Apagando el equipo



Aquí podemos comprobar que se nos ha creado a la perfección en el controlador de dominio adicional, a continuación, veremos como se ha replicado perfectamente

6.4 Replicar los DC

- Durante los próximos minutos los DC se replicarán. Esta tarea



también se puede realizar manualmente. Accede a Herramientas Sitios y servicios de AD.. Desplegar del panel de la izquierda Sites / Default..../ y verás los DC del dominio (si se han replicado aparecerán los dos, sino, solamente el principal).

Sitios y servicios de Active Directory [SMR]					
<div> <div> <div>Sites</div> <div>Inter-Site Transports</div> <div>Subnets</div> <div>Default-First-Site-Name</div> <div>Servers</div> <div>DCADICIONAL</div> <div>NTDS Settings</div> <div>SMR2_FEC</div> <div>NTDS Settings</div> </div> </div>					
Nombre	Desde el servid...	Desde el sitio	Tipo	Descripción	
<generado automátic...	SMR2_FEC	Default-First-Si...	Conexión		

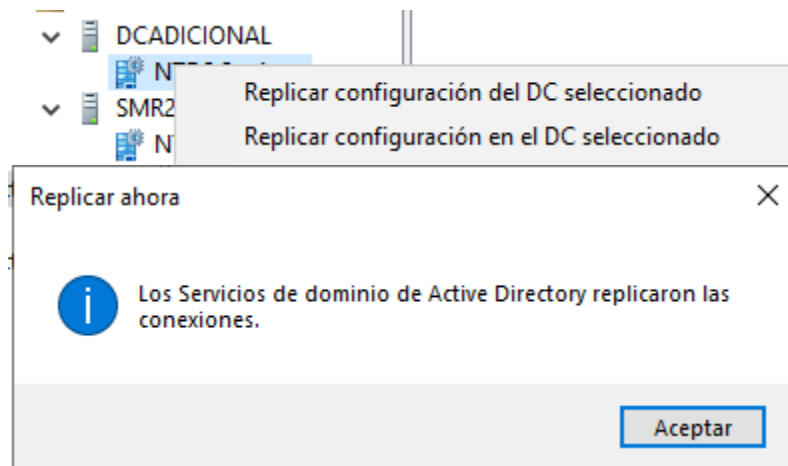
Sitios y servicios de Active Directory [SMR]				
<div> <div> <div>Sites</div> <div>Inter-Site Transports</div> <div>Subnets</div> <div>Default-First-Site-Name</div> <div>Servers</div> <div>DCADICIONAL</div> <div>NTDS Settings</div> <div>SMR2_FEC</div> <div>NTDS Settings</div> </div> </div>				
Nombre	Desde el servid...	Desde el sitio	Tipo	Descripción
<generado automátic...	DCADICIONAL	Default-First-Si...	Conexión	

Como podemos ver en las imágenes, los servidores se han replicado automáticamente a la perfección.

- Desplegando cada DC verás la configuración NTDS en el caso de que la réplica haya dado a realizarse. Si no es así, puedes forzar a que se realice de manera manual la creación de los objetos haciendo clic sobre cada entrada NTDS Settings con el botón



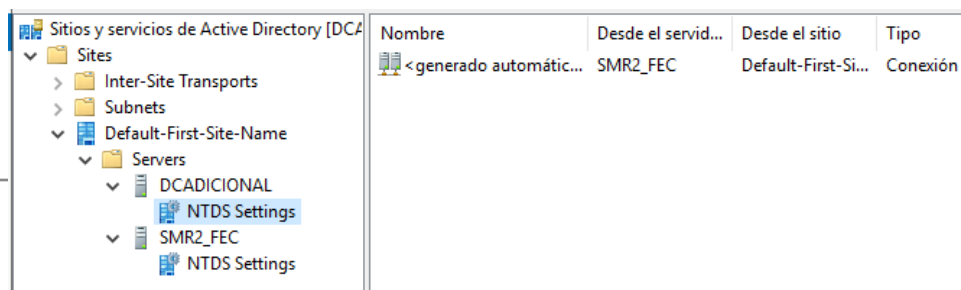
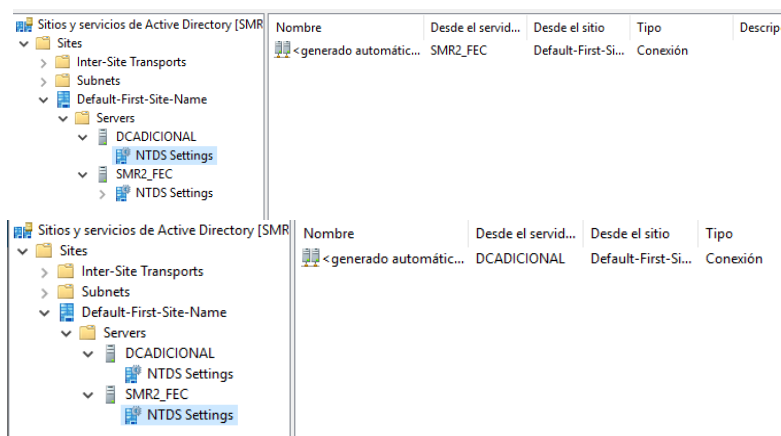
derecho del ratón y eligiendo, en el menú de contexto que aparece, la opción Todas las tareas.



Si queremos hacerlo manualmente, pulsamos clic derecho en el archivo NTDS y lo replicamos, y nos saldrá un mensaje como en la imagen.

- **Réplica manual.** Para comprobar que la réplica se ha realizado sin problemas puedes acceder a Usuarios y equipos de ambos controladores y deben tener lo mismo.

Servidor principal





Sitios y servicios de Active Directory [DCA]				
▼ Sites				
> Inter-Site Transports				
> Subnets				
▼ Default-First-Site-Name				
▼ Servers				
▼ DCADICIONAL				
NTDS Settings				
▼ SMR2_FEC				
NTDS Settings				

Nombre	Desde el servid...	Desde el sitio	Tipo
<generado automátic...	DCADICIONAL	Default-First-Si...	Conexión

Con esto daríamos por terminada nuestra práctica de hoy. Cómo hemos podido ver , ya tenemos un controlador de dominio funcionando a la perfección, y replicándose automáticamente.

Gracias por su tiempo!!!