

**TABLA DE CONTENIDO**

<b>Windows Server.</b> .....	<b>5</b>
<b>Introducción a las técnicas de red.</b> .....	<b>5</b>
Servicios individuales.....	6
Grupos de trabajo. ....	7
Servicio de directorio. ....	9
LDAP.....	9
Active directory.....	10
<b>Rol de servidor. Dominio.</b> .....	<b>11</b>
<b>Active directory.....</b>	<b>13</b>
<b>Windows Server 2012 r2.</b> .....	<b>17</b>
Introducción.....	17
Instalación de Windows Server 2012 r2.....	18
<b>Instalación de active directory.....</b>	<b>22</b>
Promocionar controlador de dominio. ....	26
Creación de unidades organizativas, usuarios y grupos del dominio. ....	35
Unidades organizativas usando ADAC. ....	36
LDAP nombres distintivos. ....	37
Unidades organizativas usando PowerShell. ....	38
Cuentas de Usuario utilizando ADAC.....	39
Cuentas de usuario utilizando powershell. ....	40
Grupos. ....	42
Grupos de distribución.....	43
Grupos de seguridad. ....	43
Ámbito de los grupos.....	43
Integrantes de los grupos. ....	44
Tipos de grupos en Windows server.....	45
Anidamiento de grupos.....	46
Cuando utilizar cada tipo de grupo.....	46

Gestión de grupos utilizando ADAC .....	48
Gestión de grupos utilizando PowerShell.....	51
Delegación usando unidades organizativas. ....	53
Conexión de clientes al dominio. ....	57
Instalación de un controlador de dominio adicional. ....	62
Instalación de un nuevo dominio en un bosque existente. ....	65
Crear un nuevo bosque.....	66
<b>Instalación de active directory en Windows anteriores a 2012. ....</b>	<b>67</b>
Instalación de un controlador de dominio adicional en Windows 2003. ....	71
Creación de un dc para un dominio secundario en un árbol existente en Windows 2003. ....	72
Creación de un dc para un nuevo árbol en un bosque ya existente en Windows 2003.....	73
Degradación de controladores de dominios en Windows 2003.....	73
<b>Maestros de operaciones. ....</b>	<b>75</b>
Cambiar el maestro de operaciones para nombres de dominio.....	77
Cambiar el maestro de operaciones para maestro de esquema. ....	78
Cambiar el maestro de operaciones para emulador de pdc, maestro de rid y maestro de infraestructura.....	79
Catalogo global.....	80
<b>Servidores DNS y DHCP en Windows server.....</b>	<b>81</b>
<b>Servidor DNS. ....</b>	<b>81</b>
Descripción general de DNS en Microsoft Windows server. ....	82
Términos clave DNS. ....	82
Nombre de dominio.....	83
Dominios superiores.....	84
Registros de recursos de DNS. ....	84
Registros de recursos que admite Windows server. ....	85
Operación de solicitud de DNS. ....	87
Solicitud inversa.....	87
Clases de solicitudes de DNS. ....	88
Operación de actualización de DNS.....	88

Resolución de nombres: resolutor de DNS.....	88
Caché del resolutor de DNS. ....	88
Caché negativa.....	89
Delegación de zona.....	89
Cliente de actualización dinámica de DNS.....	90
<b>Instalación y configuración de un servidor DNS. ....</b>	<b>91</b>
Configuración del servicio DNS.....	91
Creación de una nueva zona. ....	92
Creación de subdominios y delegación de autoridad.....	93
Agregación de registros de recursos del host.....	94
Interoperación con otros servidores DNS. ....	94
Administración del servidor DNS. ....	95
Pestaña interfaces. ....	95
Pestaña Reenviadores .....	95
Pestaña Avanzadas .....	96
Pestaña sugerencias de raíz.....	96
Pestaña registros .....	97
Ficha inicio de autoridad (SOA) y ficha servidores de nombres .....	98
Ficha WINS .....	98
<b>Servidor DHCP. ....</b>	<b>100</b>
<b>Funcionamiento de dhcp.....</b>	<b>101</b>
Obtención de una concesión inicial.....	101
Renovación de una concesión.....	101
Cambios en subredes y servidores.....	102
Detección de servidores de dhcp no autorizados.....	103
Configurando un servidor dhcp.....	103
Creación de un nuevo ámbito. ....	104
Autorización del servidor dhcp y activación de los ámbitos. ....	107
Reservando direcciones.....	108

---

Uso de ipconfig para liberar, renovar o verificar una concesión. ....	109
<b>Cuentas de usuario y grupo en Windows server. ....</b>	<b>110</b>
<b>Tipos de cuentas.....</b>	<b>110</b>
Cuentas de usuario.....	110
Nombre principal de usuario (UPN). ....	110
Estrategias para nombrar cuentas. ....	110
Contraséñas. ....	111
<b>Perfiles de usuario en Windows server.....</b>	<b>113</b>
Perfiles de usuario locales. ....	113
Perfiles de usuario móviles.....	115
Posibles errores en un perfil móvil. ....	118
Perfiles de usuario obligatorios. ....	120
Perfiles de usuario súper obligatorios.....	125
Perfiles de usuario temporales. ....	125
Carpeta particular del usuario. ....	125
<b>Políticas de grupo (group policy). .....</b>	<b>127</b>
Conceptos .....	127
Políticas locales y objetos de políticas de grupo (GPO).....	128
Creación de una GPO. ....	129
Editar la GPO. ....	131
Aplicación de GPO.....	135
Principales políticas de una GPO. ....	137
Plantillas administrativas.....	138
<b>Directivas de auditoria. Visor de eventos. ....</b>	<b>139</b>

## Windows Server.

Ya hemos visto en temas anteriores como gestionar un sistema operativo cliente, vamos a estudiar ahora un sistema operativo servidor. En concreto vamos a tratar en este tema un sistema operativo servidor de la familia Windows, el Windows Server.

Windows Server es un sistema operativo de tipo servidor, preparado para gestionar una red de ordenadores mediante un sistema de dominios y un directorio activo que permite una administración centralizada. Antes de comenzar es interesante conocer algunos aspectos básicos sobre las técnicas de redes de ordenadores.

### Introducción a las técnicas de red.

Hemos visto en el tema sobre Windows cliente como estos clientes trabajan en una red entre iguales, usando los grupos de trabajo. Sin embargo este tipo de solución sólo es válida para redes simples.

En la actualidad hay un número creciente de redes que no son simples. Incorporan servidores múltiples (archivos, impresión, correo, web, etc.) y a menudo están distribuidos en diversas ubicaciones, y no es posible en este tipo de redes ir repitiendo cuentas de usuarios en distintos equipo y se hace necesario mayores posibilidades de Administración.

Asimismo, lo más frecuente en una red de este tipo es que los servidores almacenen muchos gigabytes de datos en distintos recursos. No es realista esperar que bajo estas circunstancias los usuarios sepan dónde están las cosas y sean capaces de manejarlas por ellos mismos recordando las direcciones IP o los nombres de cada máquina que comparte algo.

Es evidente además que en una red de este tipo necesitamos un sistema de control, ya que no todos los usuarios deben poder acceder a todos los recursos. Además, la administración de una red tan grande en un grupo de trabajo es realmente complicada.

Por ello, los diseñadores de redes han buscado la manera de simplificar el uso de este tipo de redes complejas y facilitar la ubicación de los recursos de cara a los usuarios. En este punto vamos a presentar varias técnicas que se usan para lograr esta simplificación, y vamos a profundizar en las especificaciones de Microsoft, basada en dominios y relaciones de confianza. Estos bloques de construcción permiten armar redes empresariales que resulten fáciles de manejar a los administradores y de utilizar para los usuarios.

Una LAN (Local Área Network, red de área local) puede ofrecer servicios de muy diversas maneras dependiendo del método empleado por la red. En esta sección haremos una revisión de las técnicas que han sido utilizadas para organizar los recursos en red:

- Servicios individuales.
- Grupos de trabajo.
- Servicios de directorio. (LDAP).

### Servicios individuales.

La gran mayoría de las primeras redes incorporaban un solo servidor, de manera que los usuarios tenían poca dificultad para ubicar archivos, impresoras u otros recursos compartidos. Todo estaba situado en el servidor central, y los equipos individuales no podían compartir absolutamente nada con el resto de la red.

NetWare ha sido el sistema operativo para redes dominantes en redes pequeñas. Estas redes incluyen sólo un servidor y 30 o menos estaciones de trabajo normalmente.

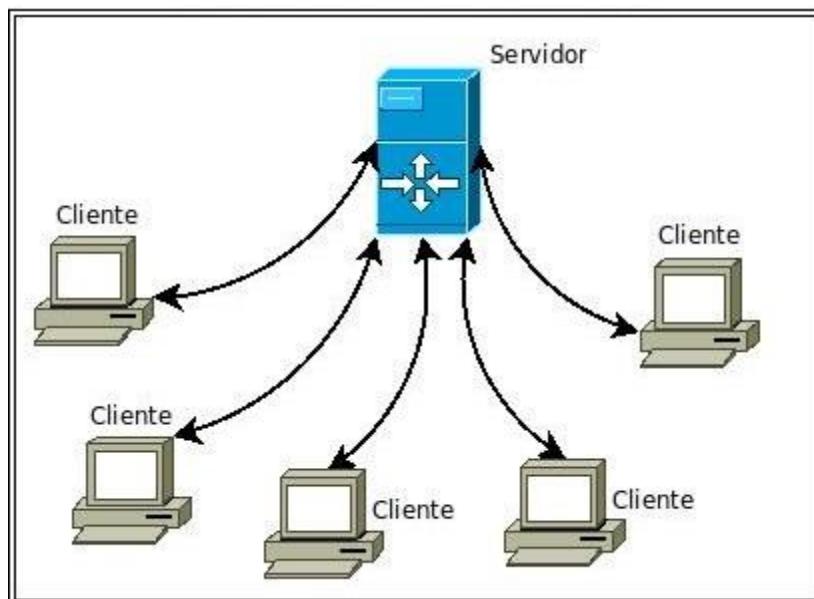
Con este sistema no se requiere un sofisticado servicio de administración de recursos, dado que todos los recursos que se comparten están conectados directamente al servidor.

Sin embargo, agregar un segundo servidor puede complicar las cosas de manera significativa. El problema surge porque cada servidor individual mantiene su propia lista de usuarios y recursos. Veamos un ejemplo:

El servidor A da alojamiento a aplicaciones como documentos de texto y hojas de cálculo; el servidor B aloja el correo electrónico de la compañía, las aplicaciones de contabilidad y la base de datos de ventas. Los usuarios que requieren acceso a la base de datos y utilizar las aplicaciones, necesitan una cuenta en ambos servidores, y deben cerrar e iniciar sesión cada vez que deseen cambiarse de servidor.

Los usuarios también tienen un problema con los diversos servidores individuales. Para usar una impresora, el usuario debe saber cuál servidor tiene la impresora. Para tener acceso a un archivo o programa, el usuario debe conocer cuál servidor lo aloja. A menos que el usuario obtenga herramientas amigables para ubicar los servicios, sería difícil tener acceso a muchas de las capacidades de la red.

Este tipo de redes siguen siendo muy adecuadas en situaciones simples, donde solo existe un servidor y tiene unas funciones muy delimitadas, aunque es una solución no válida para la mayoría de las situaciones actuales, lo que ha hecho que hayan quedado obsoletas.



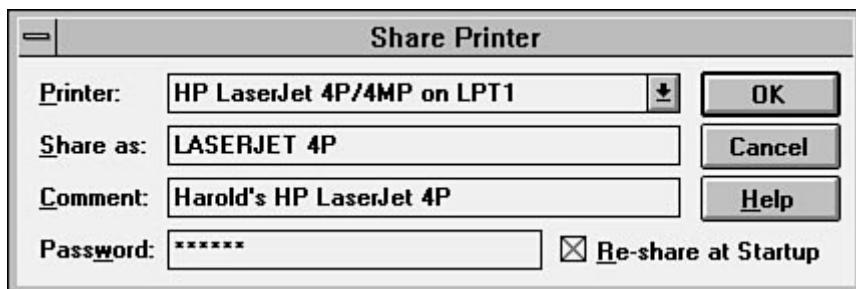
## Grupos de trabajo.

Los grupos de trabajo son conceptualmente opuestos a los servicios individuales. Los servicios individuales son formales y están administrados centralmente en un único servidor; los grupos de trabajo son informales y operados por los usuarios que comparten sus propios recursos locales y no cuentan con ningún servidor. Este tipo de redes se conocen como redes peer to peer, entre pares o entre iguales (y no punto a punto).

Las redes entre iguales se topan con dos problemas en las grandes organizaciones; hay tantos recursos disponibles que los usuarios pueden tener problemas para su localización y los usuarios no disponen de un método fácil para compartir los recursos sólo con un grupo limitado de compañeros.

Microsoft introdujo los grupos de trabajo con el producto Windows for Workgroups (WfW). WfW permite a los usuarios compartir los recursos de su estación de trabajo y los grupos de trabajo facilitan el establecimiento de grupos relacionados que pueden ver y compartir recursos entre ellos.

Después de que alguien se anexa a un grupo de trabajo, tiene acceso a todos los recursos compartidos en ese grupo. Podemos compartir una impresora local, simplemente indicando que queremos compartirla, y si acaso, poniendo una contraseña en dicho recurso compartido. La figura siguiente muestra la forma en que WfW utilizaba para compartir impresora.



Es importante notar que la ventana en la figura anterior permite al propietario de la impresora asignar una contraseña que puede ser utilizada para restringir el acceso a sólo ciertos individuos. Si no existiera la contraseña, cualquier miembro del grupo de trabajo podría utilizar la impresora. Esta es la única seguridad ofrecida por WfW.

Para localizar los recursos en una red, Microsoft utiliza el propio explorador de archivos.

Los grupos de trabajo hacen que el compartir recursos sea una operación muy simple, pero no organizan los servicios en ninguna lista o directorio. Tampoco facilitan la administración de los recursos compartidos de manera eficiente. Las contraseñas pueden ser utilizadas para restringir el acceso a los recursos, pero con una contraseña para cada recurso, éstas proliferan con rapidez. Para cambiar una contraseña debe notificarse a todos los que utilizan dicho recurso. Si cada recurso tiene una contraseña diferente, las cosas se vuelven realmente complicadas. Es difícil mantener un buen nivel de seguridad bajo tales circunstancias.

Cuando diferentes contraseñas son asignadas para usuarios individuales, la cantidad de contraseñas que un usuario debe recordar se multiplica con rapidez. Para facilitar las cosas, los usuarios tienden a elegir contraseñas fáciles de recordar, pero también tienden a ser fáciles de adivinar.

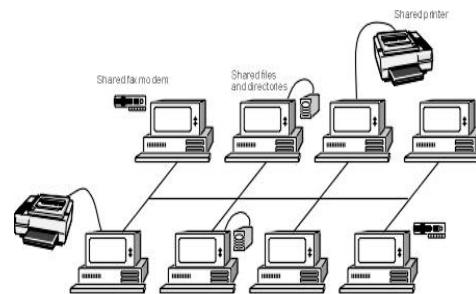
Para empeorar las cosas, imaginad que la red tiene la capacidad de que pueda accederse desde el exterior, mediante la línea telefónica por ejemplo o por una VPN (red privada virtual) a través de internet y un empleado acaba de irse a trabajar con la competencia. Habrá que cambiar todas las contraseñas de manera que el empleado no pueda llamar y obtener datos. Obviamente, cambiar todas esas contraseñas e informar a todos acerca del cambio será un enorme problema.

También podemos usar los grupos de trabajo, sin tener que establecer contraseñas a los recursos. En su lugar, podemos indicar por cada recurso que usuarios pueden acceder al mismo, pero tenemos el problema que sólo podremos escoger usuarios desde nuestra lista de usuarios locales. Esto implica que si queremos acceder desde la red a un recurso compartido en una máquina Windows cliente, tenemos que conocer (o usar) el nombre de usuario y la contraseña de un usuario local de dicha máquina.

También podemos usar acceso anónimo a los recursos, pero esto implicaría que todos en la empresa podrían acceder al recurso, cosa que habitualmente es indeseable.

Las organizaciones grandes o las que quieren más control sobre sus redes requieren algo más que grupos de trabajo. Por ello, Microsoft ha incorporado el concepto de dominio desde Windows NT Server.

Los grupos de trabajo de Windows utilizan SMB (Server Message Block) como software para la conexión en red. Este software SMB corre sobre otro software conocido como NetBIOS (Network Basic Input Output System), y a su vez NetBIOS estaba diseñado para funcionar sobre el protocolo NetBEUI (NetBIOS Extended User Interface) aunque también existen implementaciones de NetBIOS sobre IPX/SPX y sobre TCP/IP que es la más usada hoy en día. Este software NetBIOS al ser muy antiguo (1984) es un protocolo de red bastante inseguro y sobre todo, tremadamente ruidoso (utiliza mucho el broadcast en red).



Todo este “lio” viene provocado por que ni SMB, ni NETBIOS ni NETBEUI son verdaderos protocolos de red “completos”. Veamos cómo se distribuye este sistema entre las 7 capas ISO de red:

Capa	Descripción Capa	Protocolo
7	Nivel de Aplicación	Redirector (parte de SMB)
6	Nivel de Presentación	SMB
5	Nivel de Sesión	NetBIOS
4	Nivel de Transporte	NetBEUI
3	Nivel de Red	NetBEUI
2	Nivel de Enlace	NDIS + NIC driver
1	Nivel Físico	NIC (Network Interface Card)

### Servicio de directorio.

Bajo este sistema, los recursos pueden estar situados en varios equipos, tanto servidores como no servidores, pero se recogen todos en una única lista o directorio. Los recursos pueden agruparse de manera lógica en este directorio para hacerlos más fáciles de ubicar. Los usuarios pueden buscar en el directorio la información que desean, ya sea buscando por tipos de impresoras, capacidades de volúmenes compartidos, etc.



Un servicio de directorio es una especie de guía telefónica exhaustiva que permite a usuarios, administradores y aplicaciones acceder a la información existente de todos y cada uno de los usuarios y sistemas de una red con tan sólo pulsar un botón o a través de programas muy simples.

Como servicios de directorios de red, podemos citar:

- Banyan ofrece el servicio de directorio StreetTalk como parte de su sistema operativo para redes VINES.
- X.500 es un estándar internacional para servicios de directorio, aunque su función se centra en la creación de directorios a nivel global y no en redes locales.
- NetWare Directory Services (NDS, Servicios de directorio NetWare) está incorporado dentro de la línea de productos Novell NetWare 4.x. NDS está basada en X.500, aunque no es totalmente compatible con el estándar.
- LDAP. Es el estándar basado en X.500, pero bastante mejorado y simplificado, y que está diseñado para trabajar sin problemas en TCP/IP.

El concepto de un servicio de directorio es atractivo. En lugar de conectarse a diversos servidores, el usuario se conecta a una red y tiene acceso a los recursos de la red a través del servicio de directorio, sin importar cuál servidor ofrezca el servicio. El usuario ve el directorio de la red de una forma lógica, puede acceder a los recursos sin preocuparse de quien comparte dichos recursos, del mismo modo, puede iniciar sesión una única vez en cualquier servidor, y será reconocido automáticamente por todos los servidores.

Por su importancia actual, veamos más en profundidad el servicio de directorio LDAP.

### LDAP.

LDAP (Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP se considera muchas veces como una base de datos a la que pueden realizarse consultas, aunque en realidad no es una base de datos como tal.

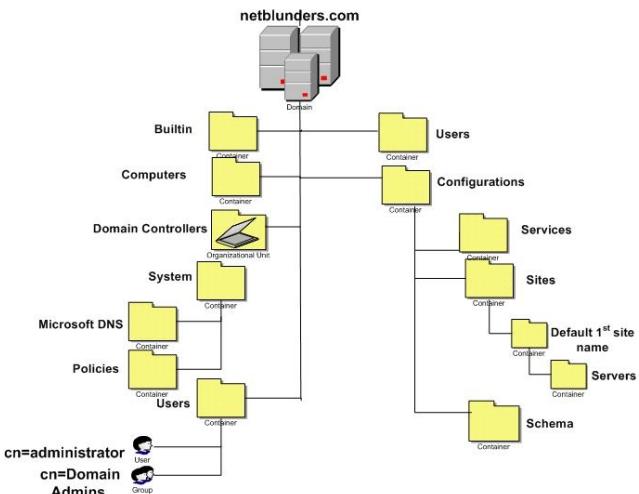
Un directorio es un conjunto de objetos con atributos organizados en una manera lógica y jerárquica. El ejemplo más común es el directorio telefónico, que consiste en una serie de nombres (personas u organizaciones) que están ordenados alfabéticamente, con cada nombre teniendo una dirección y un número de teléfono adjuntos.

Los despliegues actuales de LDAP tienden a usar nombres de Sistema de Nombres de Dominio (DNS por sus siglas en inglés) para estructurar los niveles más altos de la jerarquía. Conforme se desciende en el directorio pueden aparecer entradas que representan personas, unidades organizacionales, impresoras, documentos, grupos de personas o cualquier cosa que represente una entrada dada en el árbol (o múltiples entradas).

Habitualmente almacena la información de autenticación (usuario y contraseña) y es utilizado para autenticarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc.). A manera de síntesis, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red.

Existen diversas implementaciones y aplicaciones reales del protocolo LDAP como pueden ser Active Directory (Directorio Activo), Novell Directory Services, IPNet, OpenLDAP o Red Hat DS.

La implementación que vamos a estudiar en este tema es la de Active Directory, utilizada por Microsoft en sus versiones servidores.



## Active directory.

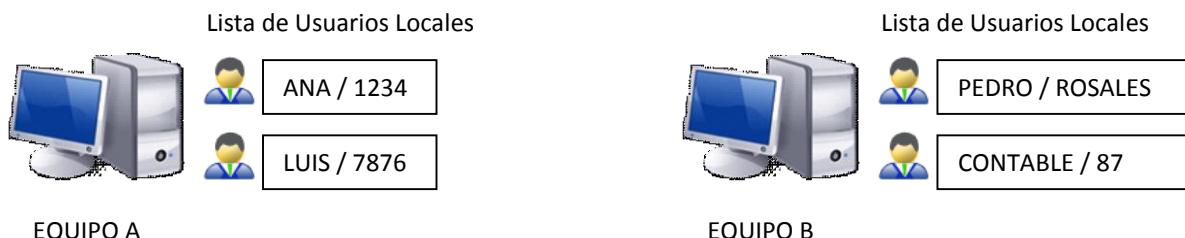
Active Directory es el nombre utilizado por Microsoft (desde Windows 2000) en su servicio de directorio.

Un Servicio de Directorio es un depósito estructurado de la información de los diversos objetos que contiene el Active Directory, en este caso podrían ser impresoras, usuarios, equipos, etc.

Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados) LDAP versión 3, lo cual permite integrar otros sistemas que soporten el protocolo. En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc.

### Rol de servidor. Dominio.

Si estamos usando un grupo de trabajo, y compartimos un recurso, al acceder a la lista de usuarios de dicho recurso hemos visto cómo podemos añadir únicamente usuarios locales, de nuestro propio sistema. Esto quiere decir que no podemos compartir uno de nuestros recursos para un usuario que no sea local en nuestro sistema, a menos que dupliquemos la cuenta de usuario en los demás sistemas.

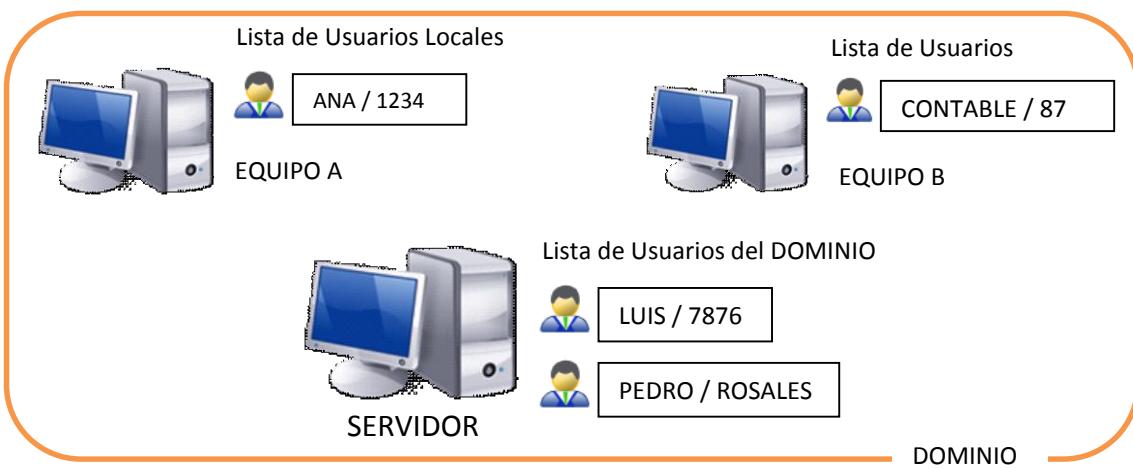


Así, si en el equipo A tenemos un recurso compartido, solo podremos indicar dentro de su ACL, que puede ser usado por ANA (con contraseña 1234) o por LUIS (con contraseña 7876). Si queremos que ese recurso compartido del equipo A sea usado por la cuenta PEDRO del equipo B, no tenemos más remedio que añadir esa cuenta de usuario en el equipo A, para que así PEDRO aparezca en la lista de usuarios locales del equipo A y pueda ser añadido a la lista de acceso del recurso. Obviamente podríamos establecer un acceso anónimo, pero esto no suele ser interesante en una empresa, ya que no es habitual que dejemos un recurso abierto a todo el mundo.

El grupo de trabajo se comporta así porque todas las cuentas de usuario son locales y son almacenadas en cada equipo individual, y al ser una red entre iguales, ningún equipo confía en los demás, por lo que no permite que entre en la máquina un usuario que no esté en su lista de usuarios locales.

Una solución para este problema es crear cuentas globales o comunes, es decir cuentas que no pertenezcan a una sola máquina, sino que sean reconocidas en todas las máquinas de la red.

Para hacer esto, necesitamos establecer un ordenador especial que va a ser el encargado de almacenar todas estas cuentas globales, mientras que las cuentas locales seguirán estando almacenadas en cada equipo normal. Este ordenador especial en el que todos los demás ordenadores confían pasa a ser un servidor y nuestro grupo de trabajo se convierte en un dominio, dado que se ha establecido una relación de dominio de un equipo sobre los demás.



Así conseguimos que la cuenta LUIS no se almacene localmente en el equipo A, sino que sea una cuenta del dominio creada y almacenada en el SERVIDOR del dominio. Ahora, tanto el equipo A como el equipo B cuando vayan a compartir un recurso verán en sus ACL a LUIS, ya que ambos confían en el servidor y por tanto dejan entrar a sus usuarios.

Fijaros como en el grafico anterior vemos que LUIS y PEDRO son usuarios del dominio mientras que los usuarios ANA y CONTABLE son usuarios locales que solo aparecen en las listas de sus propios equipos, y no pueden interactuar con el dominio.

Si queremos trabajar en un dominio, hay que indicar en todos los equipos que dejamos de trabajar en un grupo de trabajo, y queremos conectarnos a un dominio. Podemos decir que los equipos deben decidir dejar de ser "libres" para pasar a ser dominados por el servidor.

Los dominios toman conceptos de los grupos de trabajo y servicios de directorio. Al igual que los grupos de trabajo, los dominios pueden ser bastante informales y cada equipo puede decidir compartir sus propios recursos que estarán disponibles en red al igual que los recursos puestos por el servidor.

Un dominio organiza los recursos de diversos servidores en una estructura administrativa. Los usuarios reciben privilegios de conexión a un dominio más que a un servidor individual. Debido a que un dominio controla los recursos de varios servidores, es más fácil de administrar que una red con muchos servidores individuales.

Los servidores, dentro del dominio, anuncian sus servicios a los usuarios. Los usuarios que se conectan en un dominio obtienen acceso a todos los recursos del dominio para el cual han recibido autorización de acceso, sin importar desde qué servidor se conectaron ni qué servidor está prestando el recurso.

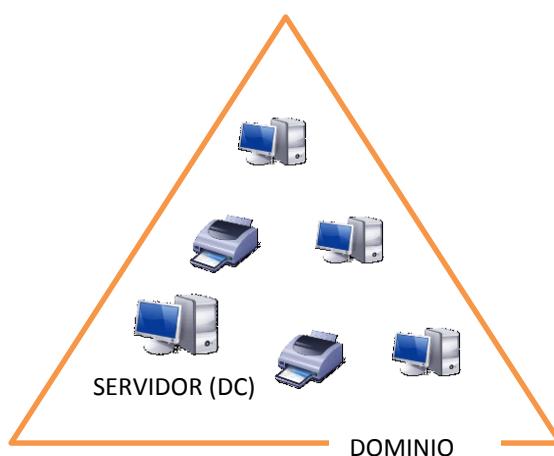
Cuando las redes se vuelven lo suficientemente amplias como para requerir varios dominios, los administradores pueden establecer relaciones de confianza (trust) entre los dominios. Estas relaciones simplifican la administración, ya que un usuario sólo requiere una cuenta en uno de los dominios. Los otros dominios que confían en el dominio de conexión del usuario pueden depender de que el dominio de conexión autentifique dicha conexión.

## Active directory.

Active Directory (AD) es el término que usa Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadores. Utiliza distintos protocolos (como LDAP, DNS, DHCP, Kerberos, etc.). Su estructura jerárquica permite mantener una serie de objetos relacionados con componentes de una red, como usuarios, grupos de usuarios, permisos y asignación de recursos y políticas de acceso.

Active Directory (AD) es usado por las versiones de Windows Server NT, Windows 2000 y Windows 2003. Windows 2008 utiliza una nueva versión de AD conocida como Active Directory Domain Servers (ADDS).

Active Directory se basa en el uso de dominios, cada dominio contiene una serie de máquinas clientes, unos recursos y al menos un servidor que domina a los equipos clientes, este servidor se conoce como Controlador de Dominio (Domain Controller, DC).



Podemos agrupar varios dominios formando estructuras de dominios, donde cada uno de estos dominios cuenta con su propio controlador de dominio. Esta agrupación de dominios se realiza de forma anidada, de la misma forma que anidamos carpetas en un volumen de datos. Cada dominio puede tener dominios padres y dominios hijos, y todos los dominios tienen un dominio padre menos el dominio raíz, que es el primero de todos.

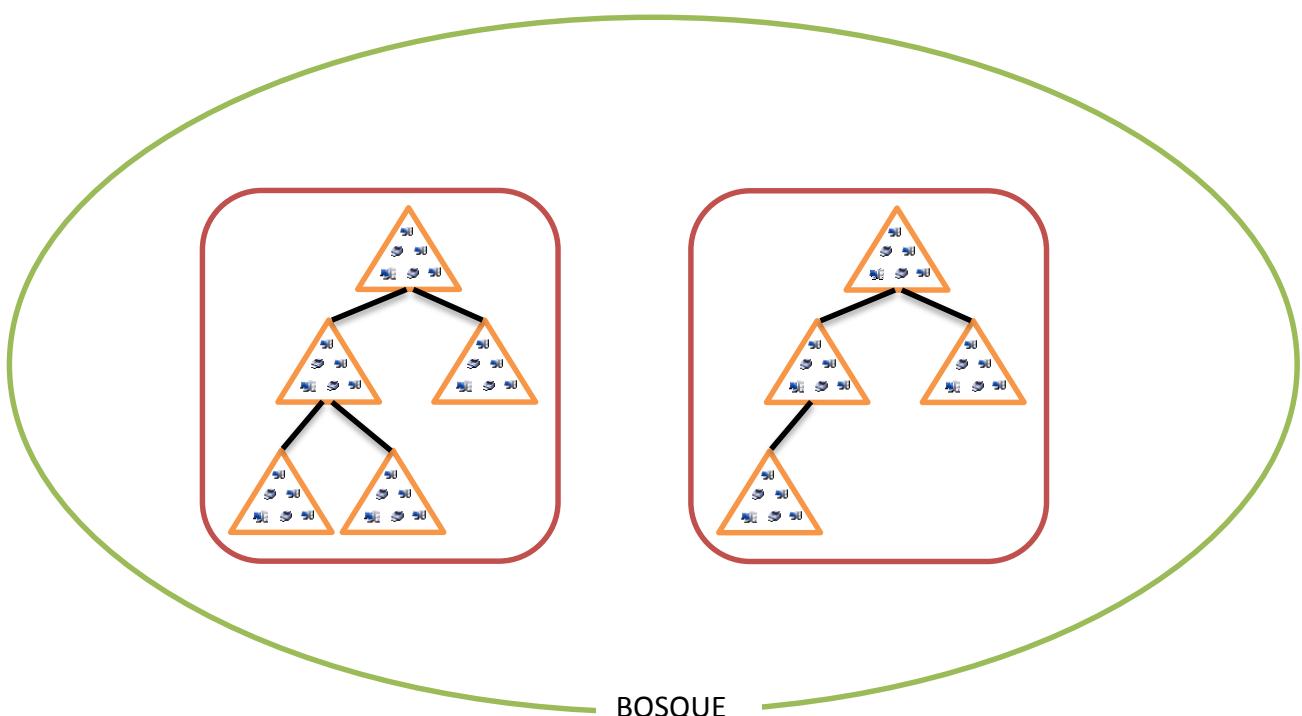
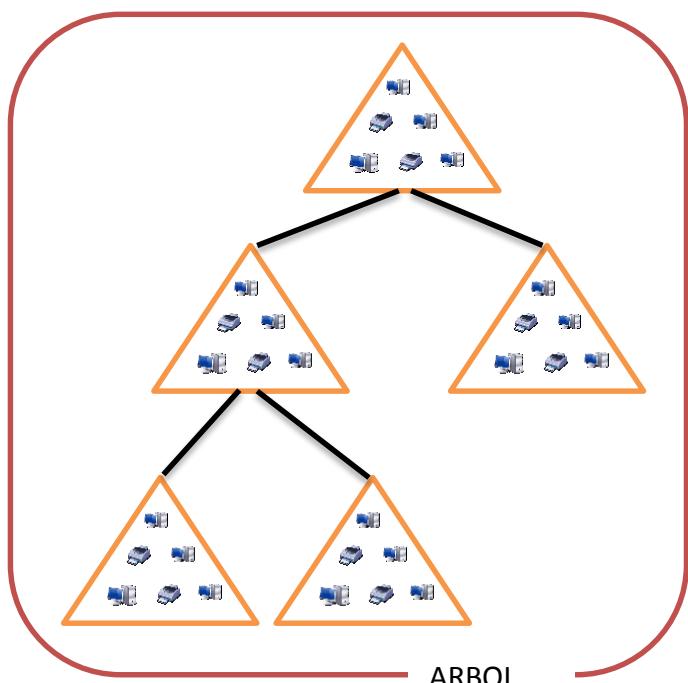
Esta estructura de dominios anidados se conoce como árbol.

En este ejemplo de la derecha, vemos un árbol creado con 5 dominios. Cada uno de estos dominios cuenta con un controlador de dominio (DC) como mínimo, sus equipos clientes, sus recursos locales, su infraestructura de red, etc.

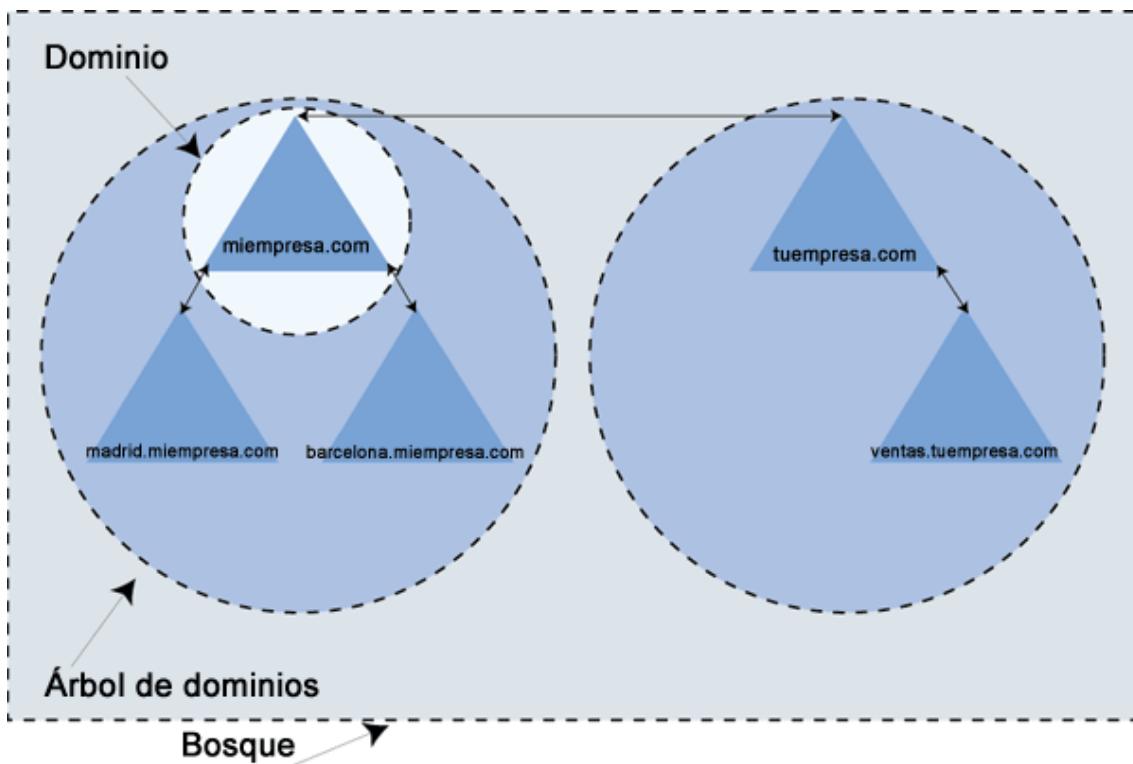
Vemos como el dominio raíz tiene dos dominios hijos, y uno de ellos tiene a su vez dos hijos más.

Al hablar de árbol, podemos decir que el dominio raíz tiene dos ramas, y una de esas ramas tiene a su vez dos ramas más.

Es posible crear una estructura que cuente con más de un árbol, estas estructuras de carácter superior al árbol se conocen como bosque. (Un bosque son varios árboles).



En este ejemplo vemos un bosque formado por dos árboles, uno con 5 dominios y el otro con 4. Cada uno de estos dominios contará con al menos un DC, por lo que al menos en ese bosque existirán 9 Controladores de Dominio.

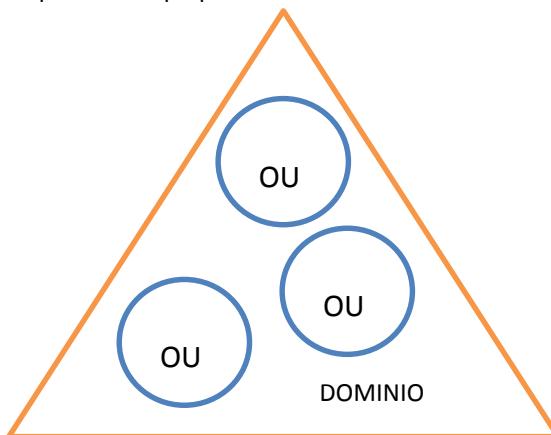


En este ejemplo vemos como hemos unido 5 dominios (`miempresa.com`, `Madrid.miempresa.com`, `Barcelona.miempresa.com`, `tuempresa.com` y `ventas.tuempresa.com`).

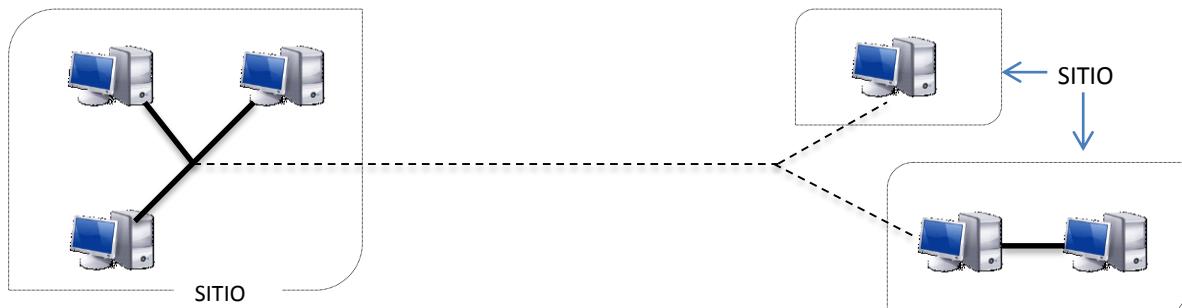
Cada uno de estos dominios contará como mínimo con un controlador de dominio Windows Server, y un gran número de máquinas clientes conectados. Para realizar esto en Windows Server sólo hemos tenido que crear `miempresa.com` (nombre de dominio) como dominio raíz de un árbol de dominios. `Madrid.miempresa.com` y `Barcelona.miempresa.com` se han montado como dominios que cuelgan de la raíz del árbol de dominios formado por `miempresa.com`.

Hemos creado otro dominio `tuempresa.com` que forma una raíz de árbol, y hemos colgado el dominio `ventas.tuempresa.com` de la raíz `tuempresa.com`.

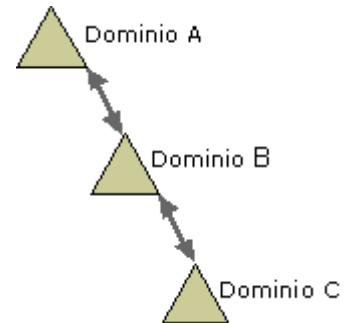
Hemos visto como la estructura que podemos crear usando Active Directory se forma con un bosque, que a su vez se divide en árboles, los cuales se dividen en dominios. Para facilitar la administración podemos a su vez dividir un dominio en partes más pequeñas conocidas como Unidades Organizativas (OU).



Estas divisiones que hemos visto hasta ahora son divisiones “lógicas”, es decir, no tienen en cuenta donde están situados los equipos físicamente. AD también nos permite crear estructuras de equipos “bien conectados”, es decir, equipos que tienen un gran ancho de banda entre ellos. Estas divisiones se conocen como sitios.

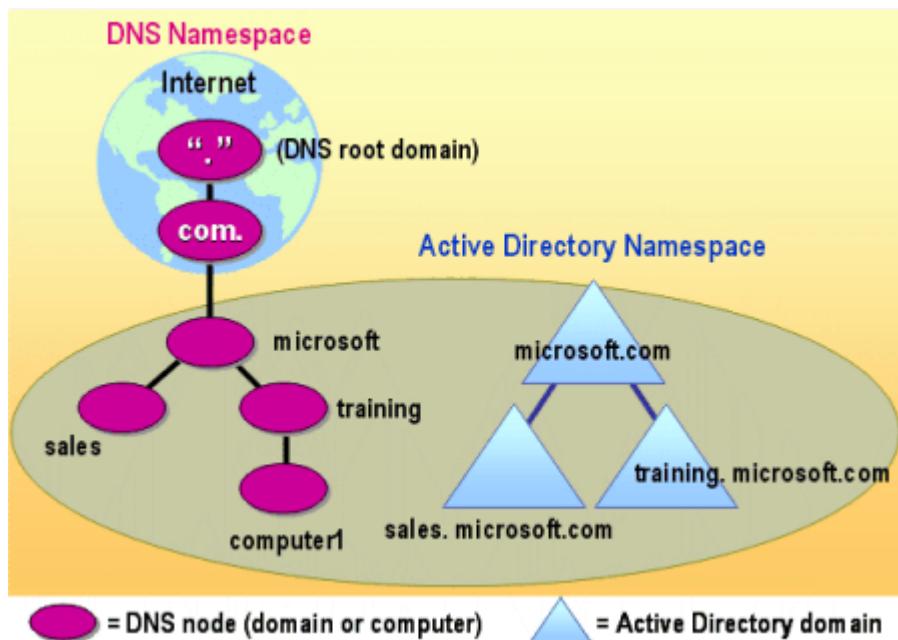


Hemos indicado anteriormente que todos los equipos de un dominio confían totalmente en el controlador de dominio o servidor de ese mismo dominio. Cuando montamos un árbol, tenemos varios dominios interactuando entre ellos, así que tenemos que indicar que dominios confían en qué dominios, o lo que es lo mismo, establecer relaciones de confianza entre los dominios. Por defecto, en los Windows Server posteriores al Windows 2000 se establecen relaciones de confianza biunívocas entre todos los dominios, de modo que todos los DC confían en todos los demás DC. Estas relaciones de confianza pueden ser modificadas si nos interesan.



Si queremos que los usuarios del dominio B puedan acceder a los recursos del dominio A, tendremos que hacer que el dominio A confíe en el dominio B.

Active Directory está estrechamente relacionado con el protocolo DNS, de modo que cuando creamos un árbol AD estamos creando al mismo tiempo un árbol DNS. Esto es importante recordarlo ya que al mismo tiempo que configuramos AD estaremos configurando DNS.

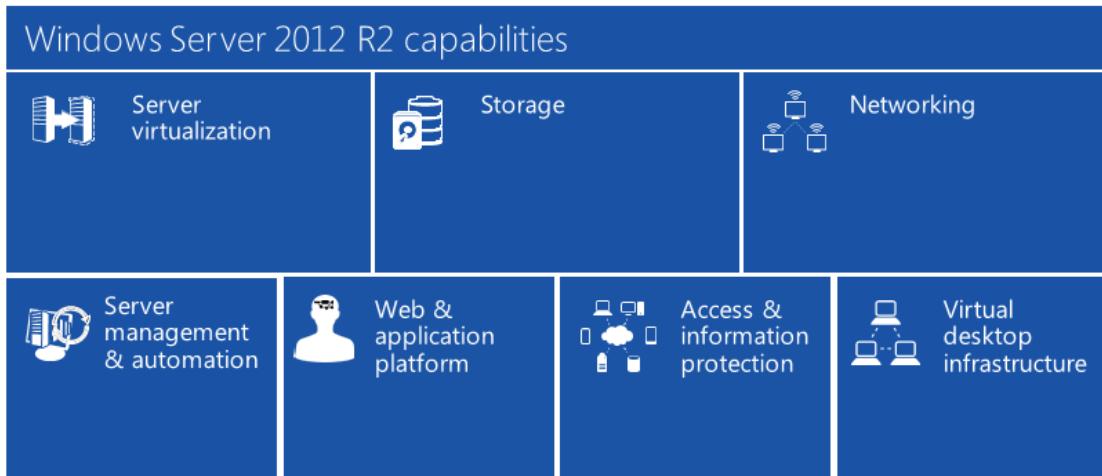


## Windows Server 2012 r2.

### Introducción.

Los requisitos mínimos para la instalación de Windows Server 2012 son 32 GB de disco duro, un procesador de 64 bits y 1,4 GHz y 512 MB de RAM. Podemos actualizar directamente un Windows 2008 a Windows 2012 insertando la imagen ISO del W.2012 en un sistema que este ejecutando Windows 2008.

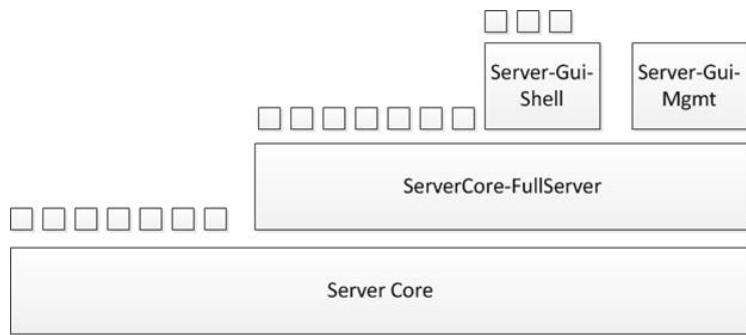
Existen dos versiones principales de Windows Server 2012, la normal y la R2 (revisión 2). La versión R2 es con la que vamos a trabajar nosotros y prácticamente todas sus diferencias con la versión anterior son relativas a Hyper-V el software de virtualización usado por Windows Server.



Todas las versiones de Windows Server cuentan con versiones de evaluación que funcionan durante 180 días sin tener que activarlos, podemos descargarlas directamente desde Microsoft desde la dirección <http://www.microsoft.com/es-es/server-cloud/products/windows-server-2012-r2/try.aspx>. En esta dirección también podemos acceder a laboratorios virtuales que nos permiten conocer distintas soluciones de Microsoft sin tener que instalar nada en nuestro sistema, mediante un cliente Web.

La versión de evaluación podemos bajarla directamente como ISO, como VHD (Virtual Hard Disk) que podemos asignar a una máquina virtual de vmWare directamente, o una máquina virtual completa para ejecutar directamente desde Azure, la plataforma PaaS de Microsoft.

Al instalar Windows Server 2012 R2 podemos elegir entre realizar una instalación normal, o bien instalar solo el núcleo del SO sin el entorno gráfico, de modo que hay que administrarlo usando la línea de comando o bien remotamente.



Las versiones principales que nos podemos encontrar son:

- Windows Server 2012 R2 Datacenter: Para un entorno altamente virtualizado que requiera características de alta disponibilidad, incluida la agrupación en clústeres.
- Windows Server 2012 R2 Standard: Para un entorno no virtualizado o poco virtualizado en el que se desee incluir características de alta disponibilidad, incluida la agrupación en clústeres.
- Windows Server 2012 R2 Essentials: Para pequeñas empresas con hasta 25 usuarios, especialmente aquellas empresas que quieran implementar su primer servidor.
- Windows Server 2012 R2 Foundation: Para pequeñas empresas con hasta 15 usuarios (solo disponible a través de partners OEM directos).

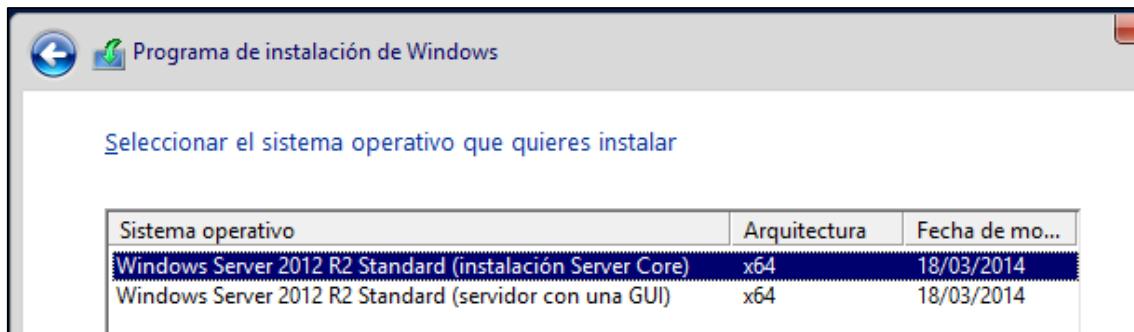
---

### Instalación de Windows Server 2012 r2.

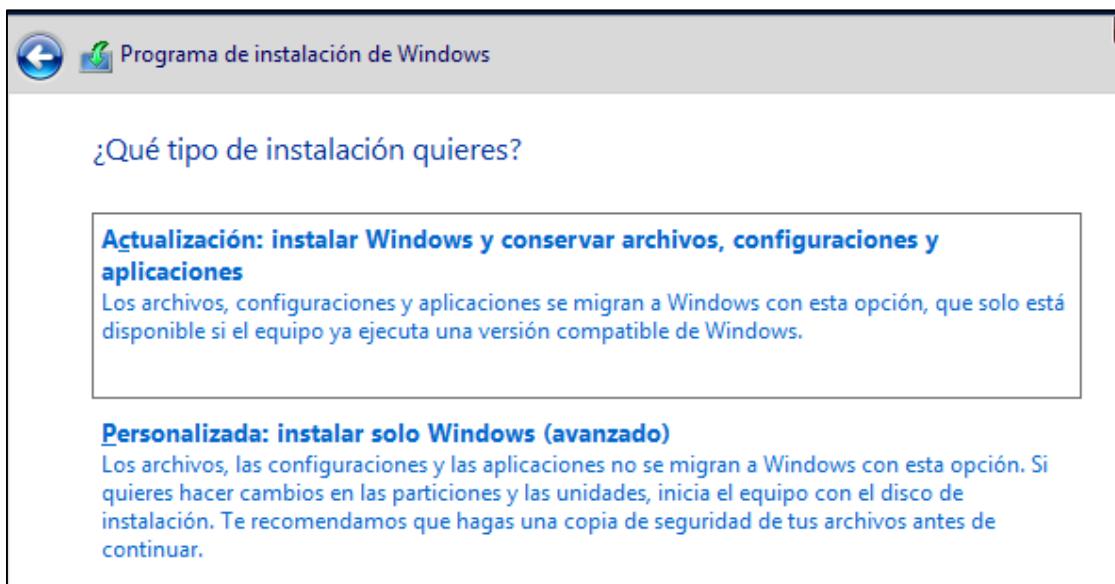
La instalación de Windows Server 2012 R2 es muy parecida a la de otros sistemas operativos Windows que ya hemos visto como instalar. Dado que deseamos hacer una instalación “ limpia”, tendremos que iniciar nuestra máquina arrancando el sistema desde un DVD o USB con una ISO de Windows Server 2012 R2. Dado que nosotros vamos a hacerlo en una máquina virtual, bastará con que introduzcamos la ISO del WS2012 y encendamos nuestra máquina virtual.

No vamos a tratar aquí las pantallas simples, donde se escogen distribución de teclado y demás, sino que vamos a explicar algunas otras que no son tan simples.





En esta pantalla vemos como nos permite seleccionar entre la instalación de la versión Core o bien de la versión con GUI (Interfaz Gráfica de Usuario). Nosotros vamos a instalar la versión gráfica de momento.



En esta pantalla vemos cómo podemos o bien instalar Windows actualizándolo o bien de forma personalizada. Nosotros siempre vamos a instalar nuestros sistemas de forma personalizada, lo que conocemos como forma “ limpia ”.

El proceso de instalación es prácticamente idéntico al de Windows 7 que ya conocemos, una vez terminada la instalación nos solicitará la contraseña para el administrador del sistema (se recomienda utilizar una contraseña fuerte).

Una vez instalado tenemos que ponerle un nombre a nuestra maquina ya que se le asignará uno aleatorio y también tendremos que ponerle una configuración de red, ya que en ningún caso podemos trabajar con un servidor que tenga una configuración dinámica de IP.

Vamos a cambiar el nombre de la máquina desde Power Shell, que viene a ser una terminal de sistema pero mucho más potente que la terminal normal que solemos usar (cmd).



Para abrir una ventana de Power Shell pulsamos el icono de Power Shell que tenemos directamente en la barra de tareas en la parte inferior de la pantalla.

```
PS C:\Users\Administrador>
PS C:\Users\Administrador> Rename-Computer WServ2012
ADVERTENCIA: Los cambios serán efectivos tras reiniciar el equipo
WIN-B25U50VD3UR.
PS C:\Users\Administrador>
```

Vemos como hemos ejecutado el comando `Rename-Computer` y hemos asignado un nombre al equipo, en este ejemplo `WServ2012` (basta con que escribáis `Ren` y pulséis `Intro`). Vemos como nos pide reiniciar el equipo, cosa que podemos hacer con el comando `Restart-Computer`.

Una vez reiniciada la máquina comprobamos que se ha cambiado el nombre del equipo. Ahora pasaremos a cambiar la configuración IP del equipo. Vamos a hacerlo también desde el Power Shell.

En primer lugar vamos a comprobar todos los adaptadores de red de nuestro equipo. Esto lo podemos hacer con el comando `Get-NetAdapter`.

Name	InterfaceDescription	ifIndex	Status	MacAddress	LinkSpeed
Ethernet0	Conexión de red Gigabit Intel(R) 82574L	12	Up	00-0C-29-3A-B2-D4	1 Gbps

Podemos comprobar la IP de nuestro adaptador con el comando `Get-NetIPAddress`.

```
PS C:\Users\Administrador> Get-NetIPAddress -InterfaceAlias Ethernet0 -AddressFamily IPv4

IPAddress      : 192.168.127.144
InterfaceIndex : 12
InterfaceAlias : Ethernet0
AddressFamily  : IPv4
Type           : Unicast
PrefixLength   : 24
PrefixOrigin   : Dhcp
SuffixOrigin   : Dhcp
AddressState   : Preferred
ValidLifetime  : 00:18:40
PreferredLifetime : 00:18:40
SkipAsSource   : False
PolicyStore    : ActiveStore
```

En nuestro ejemplo el adaptador se llama `Ehternet0` y vemos como tiene una configuración dinámica mediante `dhcp`. Vamos a configurar dicho adaptador con el comando `New-NetIPAddress` poniéndole una ip fija.

```
PS C:\Users\Administrador> New-NetIPAddress -IPAddress 192.168.177.100 -InterfaceAlias Ethernet0 -AddressFamily IPv4 -PrefixLength 16

IPAddress      : 192.168.177.100
InterfaceIndex : 12
InterfaceAlias : Ethernet0
AddressFamily  : IPv4
Type           : Unicast
PrefixLength   : 16
PrefixOrigin   : Manual
SuffixOrigin   : Manual
AddressState   : Tentative
ValidLifetime  : Infinite ([TimeSpan]::.MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::.MaxValue)
SkipAsSource   : False
PolicyStore    : ActiveStore

IPAddress      : 192.168.177.100
InterfaceIndex : 12
InterfaceAlias : Ethernet0
AddressFamily  : IPv4
Type           : Unicast
PrefixLength   : 16
PrefixOrigin   : Manual
SuffixOrigin   : Manual
```

Copio aquí la instrucción anterior ya que se corta la pantalla:

```
New-NetIPAddress -IPAddress 192.168.177.100 -InterfaceAlias Ethernet0  
-AddressFamily IPv4 -PrefixLength 16
```

Si queremos cambiar la IP también podemos usar el comando Set-NetIPAddress.

Si queremos obtener ayuda de los comandos de Power Shell (por ejemplo, para añadir la dirección del Gateway o puerta de enlace) podemos pedir ayuda mediante help New-NetIPAddress.

Vamos a asignar también un servidor DNS a nuestro equipo, también desde Power Shell. Para ello usamos el comando Set-DnsClientServerAddress.

```
PS C:\Users\Administrador> Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAdd  
resses 8.8.8.8  
PS C:\Users\Administrador>
```

El comando es

```
Set-DnsClientServerAddress -InterfaceAlias Ethernet0 -ServerAddresses 8.8.8.8.
```

Comprobar con Get-NetIPAdress o con ipconfig /all que las configuraciones de red se han establecido correctamente.

Una cosa que tenemos que hacer para facilitar las comprobaciones posteriores es habilitar que nuestro sistema responda a los pings. Si recordamos este punto de Windows Cliente (1<sup>a</sup> evaluación) recordareis que había que crear una nueva regla avanzada en los cortafuegos y era un proceso engorroso. Lo mismo podemos hacerlo directamente con una línea desde Power Shell.

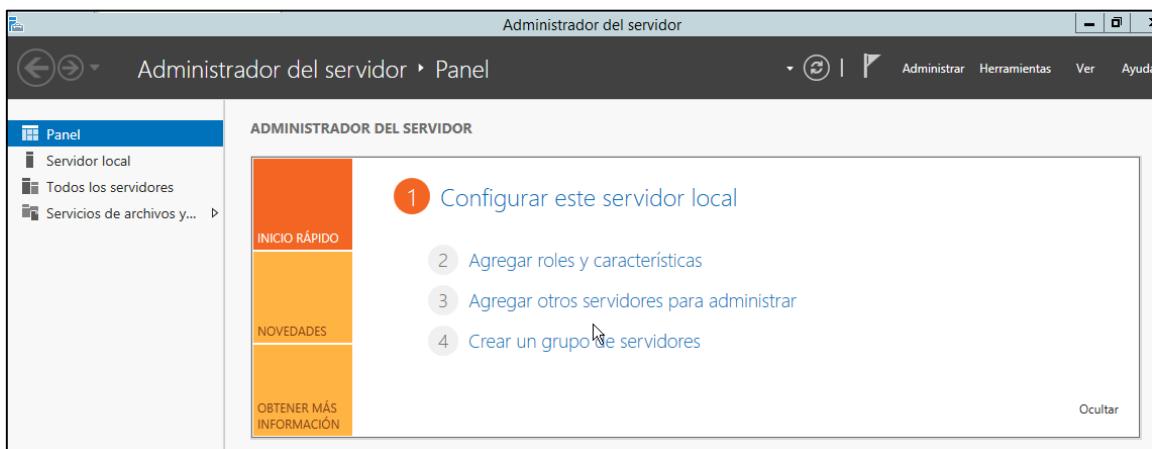
```
PS C:\Users\Administrador> New-NetFirewallRule -Name PingSi -DisplayName PingSi -Protocol  
ICMPv4 -IcmpType 8 -Enabled True -Action Allow
```

Vemos con este ejemplo como si bien parece al principio que usar Power Shell es más complicado que configurar el sistema con el entorno gráfico, a la larga es mucho más rápido y sobre todo automatizable. Repito aquí el comando anterior.

```
New-NetFirewallRule -Name PingSi -DisplayName PingSi -Protocol ICMPv4  
-IcmpType 8 -Enabled True -Action Allow
```

## Instalación de active directory.

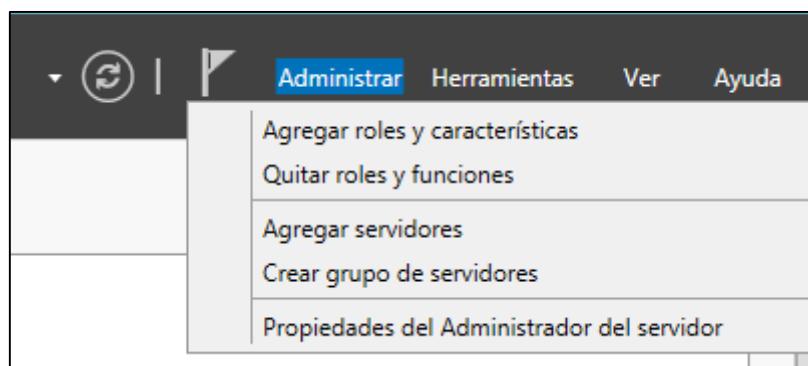
Una vez que hemos instalado nuestro Windows Server 2012 R2 al iniciar el equipo veremos automáticamente el panel del asistente administrador de servidor.



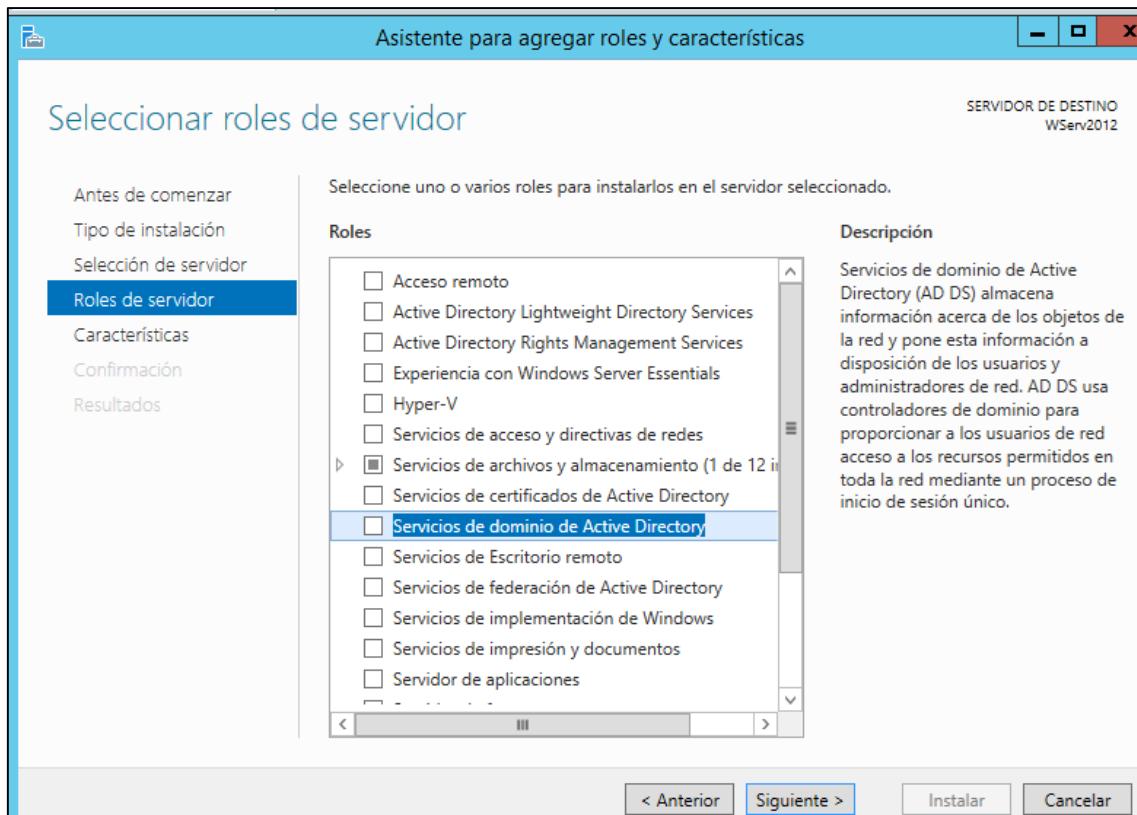
Desde este panel podremos configurar rápidamente nuestro dominio. Vemos como directamente el asistente nos indica los pasos de inicio rápido que nos aconseja dar. Nosotros vamos a realizar estas configuraciones de forma manual, siguiendo nuestra propia planificación.

Como ya hemos visto, para contar con un dominio es necesario establecer un servidor de dominio, conocido como controlador de dominio (DC). Vamos a asignarle a nuestro servidor recién instalado ese rol.

Antes de instalar un DC debemos asegurarnos que el nombre y la configuración IP de nuestra máquina son correctas, ya que una vez promovido nuestro equipo a DC estos campos no deben modificarse. Si está todo bien, lo primero que tenemos que hacer es asignar a nuestro equipo un rol. Para ello debemos escoger el menú Administrar que está arriba a la derecha en nuestro panel de Administrador del Servidor.



Seleccionamos Agregar roles y características y posteriormente indicamos que queremos realizar una instalación basada en roles y características, no en entornos de escritorio remoto. A continuación debemos seleccionar nuestro servidor de la lista de servidores disponibles.



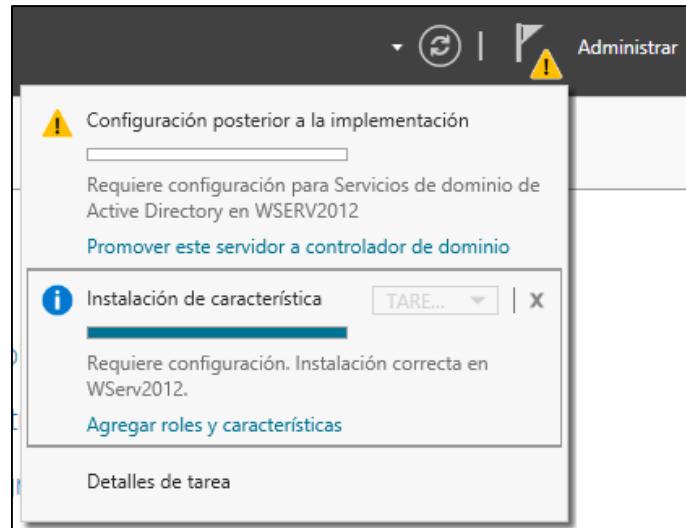
El rol que ahora mismo nos interesa instalar es el de Servicios de dominio de Active Directory (esto sólo habrá que hacerlo una vez, las próximas veces que queramos promover nuestro equipo a DC no tendremos que repetir la instalación de ADDS ya que estará instalado).

Además de dejarnos escoger roles para nuestro servidor, también podemos escoger desde este asistente características para el mismo.

- Roles de servidor: Los roles de servidor son un conjunto de componentes software que establecen servidores para realizar una función (rol) determinada, como puede ser Servicios de Dominio de Active Directory (ADDS).
- Características: Las características son componentes que añaden funcionalidades a nuestro servidor, como puede ser un servidor de copias de seguridad, un cliente ftp, etc.

Una vez que hemos terminado de instalar el rol ADDS en nuestro equipo, ya lo tendremos preparado para montar un Controlador de Dominio (DC). Daros cuenta que en este momento no hemos creado ningún dominio, simplemente hemos instalado ADDS que es la base sobre la cual podemos montar un DC.

Podemos comprobar como en el panel de Administrador del Servidor veremos una banderita amarilla en el ícono de notificaciones. Estos son mensajes importantes del sistema que quiere que veamos. Si hacéis clic en dicho ícono veréis que vemos una notificación inferior indicándonos que la instalación de ADDS terminó correctamente, y una nueva notificación que nos da la opción de promover nuestro equipo a Controlador de Dominio. (No hacerlo de momento).



Si queremos quitar un rol o característica de las que hemos instalado, en el menú de Administrar comprobar cómo no solo aparece la opción de Agregar Roles y Características, sino también aparece debajo la función de Quitar Roles y Funciones (funciones y características son lo mismo).

Podemos comprobar fácilmente los roles y características de nuestro equipo desde el panel de configuración, pero también podemos hacerlo evidentemente desde Power Shell. Para conseguir esta información usamos el comando Get-WindowsFeature

PS C:\Users\Administrador> Get-WindowsFeature -name AD*	Name	Install State
[ ] Active Directory Lightweight Directory Services	ADLDS	Available
[ ] Active Directory Rights Management Services	ADRMS	Available
[ ] Servidor de Active Directory Rights Manageme...	ADRMS-Server	Available
[ ] Compatibilidad con la federación de identidades	ADRMS-Identity	Available
[ ] Servicios de certificados de Active Directory	AD-Certificate	Available
[ ] Entidad de certificación	ADCS-Cert-Authority	Available
[ ] Inscripción web de entidad de certificación	ADCS-Web-Enrollment	Available
[ ] Respondedor en línea	ADCS-Online-Cert	Available
[ ] Servicio de inscripción de dispositivos de red	ADCS-Device-Enrollment	Available
[ ] Servicio web de directiva de inscripción de ...	ADCS-Enroll-Web-Pol	Available
[ ] Servicio web de inscripción de certificados	ADCS-Enroll-Web-Svc	Available
[X] Servicios de dominio de Active Directory	AD-Domain-Services	Installed
[ ] Servicios de federación de Active Directory	ADFS-Federation	Available

Vemos como nos aparece marcado el rol de Servicios de dominio de Active Directory, con el nombre AD-Domain-Services.

También podríamos haber instalado ADDS desde el mismo Power Shell. Para comprobarlo vamos a empezar por quitar este rol desde nuestro panel de Administrador. Darle a Administrar -> Quitar Roles y Funciones y desmarcar la opción ADDS (Servicios de dominio de Active Directory).

Una vez eliminado (comprobarlo con Get-WindowsFeature) vamos a proceder a instalarlo de nuevo pero desde el símbolo de sistema de Power Shell.

Para instalar un rol o característica usaremos el comando de Power Shell Install-WindowsFeature y para eliminarlo usaremos Uninstall-WindowsFeature. En ambos comandos hay que indicar el nombre de lo que queremos instalar como se ve en la columna Name del ejemplo anterior. Existen varios parámetros que podemos asignar a dichos comandos, como –includeallsubfeature –includemanagementtools.

```
PS C:\Users\Administrador> Install-WindowsFeature AD-Domain-Services -includeallsubfeatures  
-includemanagementtools  
Success Restart Needed Exit Code      Feature Result  
----- -----  
True   Yes           SuccessRest... (Servicios de dominio de Active Directory,...  
ADVERTENCIA: Debe reiniciar este servidor para finalizar el proceso de instalación.  
ADVERTENCIA: La actualización automática de Windows no está habilitada. Para asegurarse  
de que la característica o el rol recién instalados se actualicen automáticamente, active  
Windows Update en el Panel de control.
```

Vemos como aquí hemos instalado el ADDS desde línea de comandos de Power Shell. Vamos a desinstalarlo ahora:

```
PS C:\Users\Administrador> Uninstall-WindowsFeature AD-Domain-Services  
Success Restart Needed Exit Code      Feature Result  
----- -----  
True   Yes           SuccessRest... (Servicios de dominio de Active Directory)  
ADVERTENCIA: Debe reiniciar este servidor para finalizar el proceso de eliminación.
```

Una vez desinstalado, reiniciar la máquina para asegurarnos de que se han actualizado todos los procesos pendientes, y volver a instalar por última vez el ADDS. Podéis hacerlo desde el entorno gráfico o bien desde la línea de comandos del Power Shell.

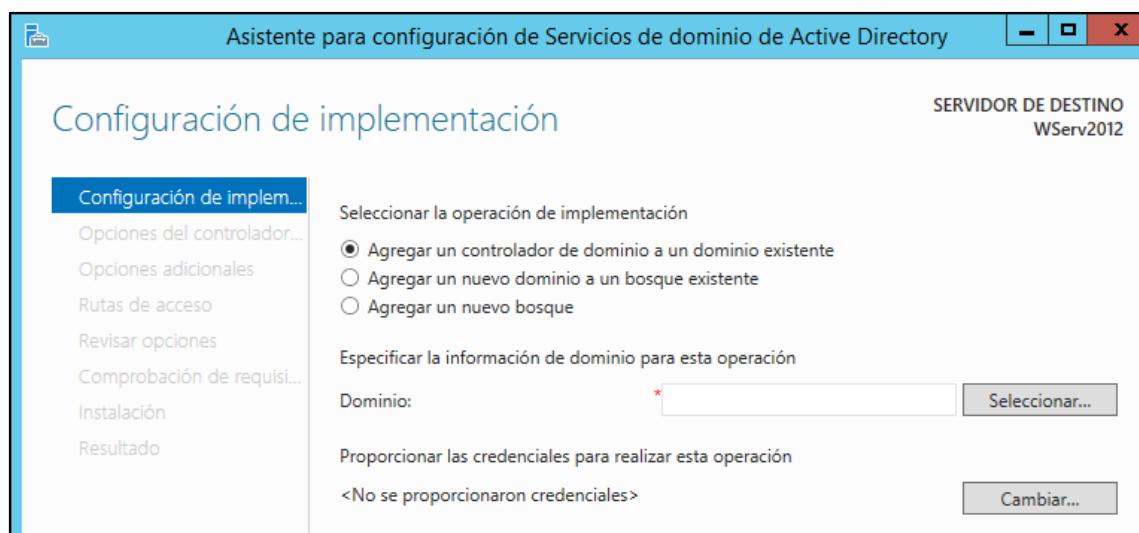
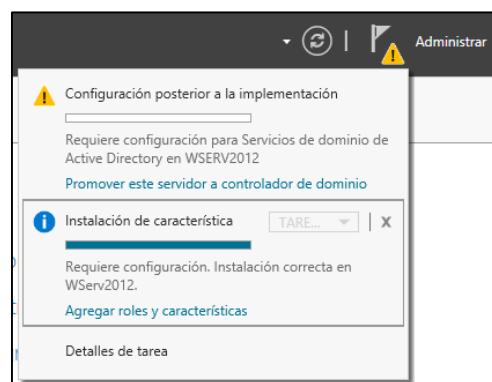
Una vez que tenemos instalado ADDS ya podemos instalar nuestro primer controlador de Dominio, y por lo tanto formar nuestro primer dominio, nuestro primer árbol y nuestro primer bosque.

### Promocionar controlador de dominio.

Una vez instalado ADDS directamente en el centro de configuraciones nos aparecerá la opción de “Promover este servidor a controlador de dominio”.

Vamos a darle a esta opción para montar nuestro primer Controlador de Dominio (DC). Posteriormente veremos cómo lo podemos hacer desde la línea de comandos del Power Shell.

Una vez que pulsemos la opción nos aparecerá el asistente para la configuración de servicios de dominio de Active Directory.



Las opciones que vemos aquí nos indican donde se va a montar nuestro dominio dentro del bosque y del árbol.

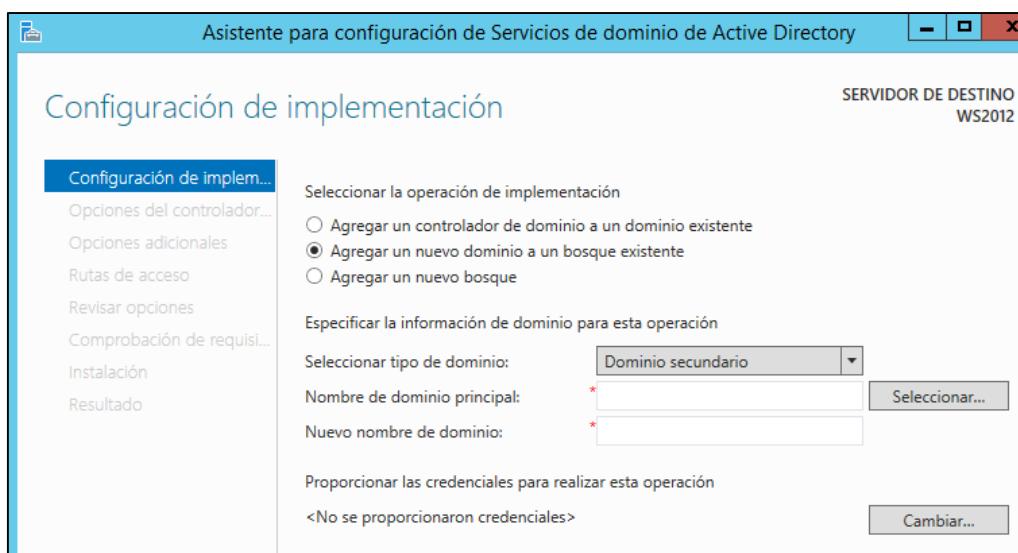
- Agregar un controlador de dominio a un dominio existente. Esta opción convierte nuestro equipo en controlador de dominio, pero **no se va a crear ningún dominio**, sino que se agrega nuestro equipo como controlador **adicional** a un dominio que ya existe. Podemos decir que nuestro equipo va a transformarse en un **ayudante** de un controlador de **dominio que ya existe**. Esta opción solo se debe elegir si en la empresa ya existe algún dominio al que vamos a apoyar.
- Agregar un nuevo dominio a un bosque existente. Esta opción convierte nuestro equipo en controlador de dominio, y **crea un nuevo dominio**, pero no lo crea como raíz de árbol, sino que nuestro dominio **va a colgar de un dominio que ya existe**, es decir, vamos a crear **una rama** en un árbol que ya existe. Esta opción solo se debe elegir si en la empresa ya existen dominios de los que queremos colgar.
- Agregar un nuevo bosque. Esta opción convierte nuestro equipo en controlador dominio, **crea un nuevo dominio** y al mismo tiempo **crea un árbol** del que nuestro dominio será raíz y **crea un**

**bosque** nuevo. Esta opción es la que hay que elegir si en nuestra empresa aún no existe ningún controlador de dominio.

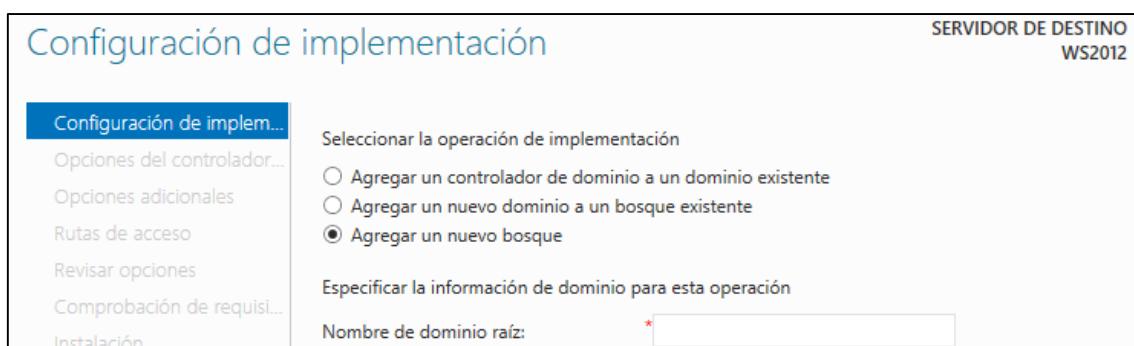
En la misma pantalla nos piden a continuación el nombre de dominio. Recordemos que siempre que estemos en Active Directory trabajamos con DNS, por lo que los nombres de dominio deben ser DNS (jerárquicos separados por punto).

Si escogemos la opción 1 (agregar un controlador de dominio a un dominio existente) evidentemente este nombre de dominio debe existir ya en la red, y de hecho se aconseja elegirlo dándole a seleccionar, no escribiendo el nombre directamente. Vemos un ejemplo de esta pantalla del asistente en la imagen anterior.

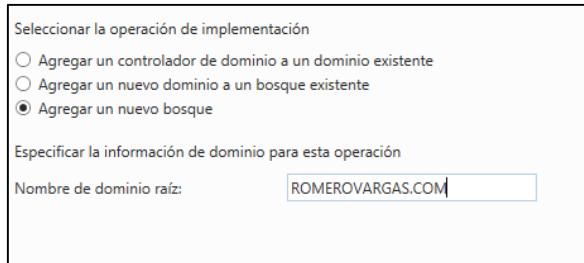
Si escogemos la opción 2 (agregar un nuevo dominio a un bosque existente) este nombre de dominio debe ser nuevo, pero debe colgar de algún dominio ya existente. Así, si nuestro dominio se va a llamar ventas y va a colgar del dominio Colombia.com el nombre de nuestro dominio sería ventas.Colombia.com de modo que el nombre de dominio principal sería Colombia.com y el nombre del nuevo dominio sería ventas. Se recomienda seleccionar el dominio principal, y no escribir su nombre directamente.



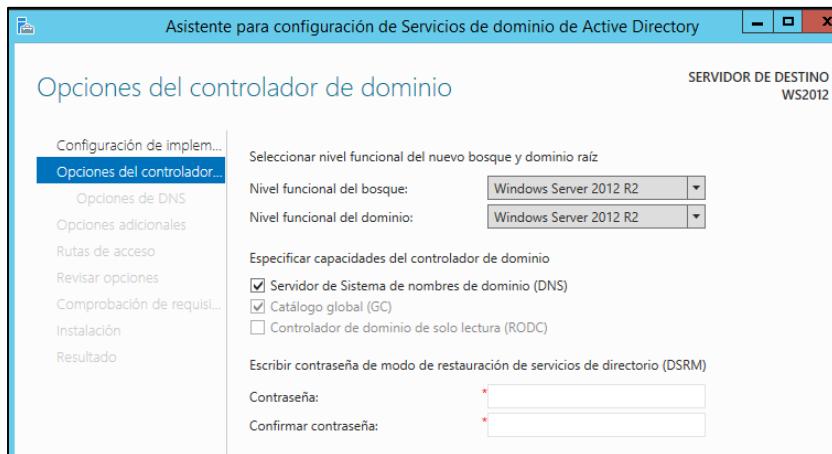
Si escogemos la opción 3 (agregar un nuevo bosque) este nombre de dominio debe ser nuevo y debe ser un dominio raíz ya que va a crear su propio árbol. Así, nuestro dominio podría ser Jerez.com, Jupiter.Net o Huelva.Org.



Como estamos creando nuestro primer dominio, nosotros vamos a escoger la opción de agregar un nuevo bosque y vamos a poner como nombre de dominio raíz ROMEROVARGAS.COM.



A continuación se nos pide el nivel funcional del nuevo bosque y del nuevo dominio. Los niveles funcionales nos permiten indicar la compatibilidad que queremos asignar a nuestro bosque y a nuestro dominio. La opción por defecto es la de WS 2012 R2, este tipo de nivel funcional integra todas las novedades de 2012 R2 pero no es compatible con los servidores Windows 2008. Si en nuestra infraestructura contamos con servidores 2008 tendremos que bajar el nivel funcional, con lo que perderemos algunas características pero ganaremos compatibilidad con este tipo de servidores.



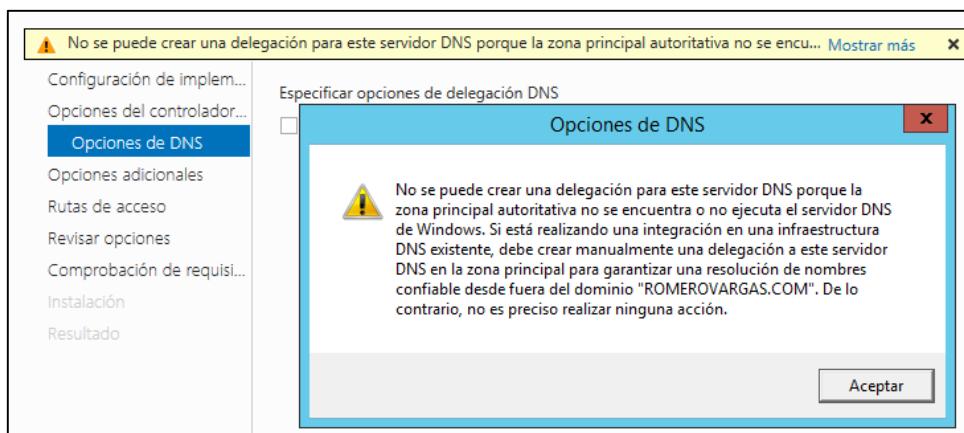
Aquí nos pregunta también algo muy importante, y es si queremos instalar el servidor de sistema de nombres de dominio en este servidor de forma automática durante la instalación del DC o no. Es imposible que tengamos un dominio si no estamos trabajando en DNS, y por lo tanto, no contamos con un servidor propio DNS que sea capaz de trabajar con nuestros nombres. Ahora, este servidor DNS puede que ya esté montado en nuestra empresa, por eso aquí nos pregunta si queremos montar un nuevo DNS automático o no. Como en este momento en nuestra empresa no hay ningún DNS propio funcionando, dejamos esta casilla activada para que instale el DNS de forma automática y lo más importante, lo configure de forma adecuada.

El catálogo global lo trataremos más adelante, pero es obligatorio que exista al menos uno en nuestra infraestructura, y ya que estamos creando el primer DC es obligatorio que cuente con el GC.

El controlador de dominio de solo lectura (RODC) es un tipo de controlador que podemos montar para ayudarnos en nuestro dominio, pero dado que nuestro DC es el primero, no puede ser ayudante, tiene que ser el principal.

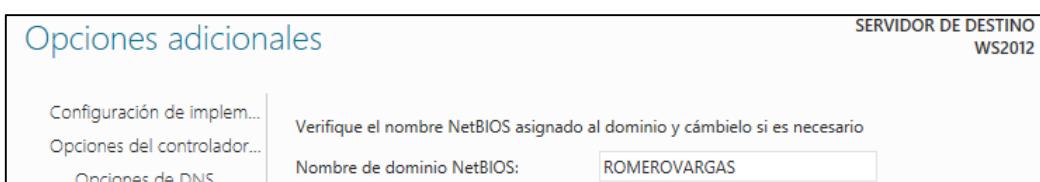
A continuación nos pide la contraseña para el modo de restauración de servicios de directorio (DSRM). Ojo, esta no es la contraseña del administrador del dominio, es una contraseña especial que solo se pide si entramos en modo de restauración.

A continuación y tal como estamos configurando nuestro dominio, recibiremos un mensaje de advertencia, no preocuparnos que es normal.

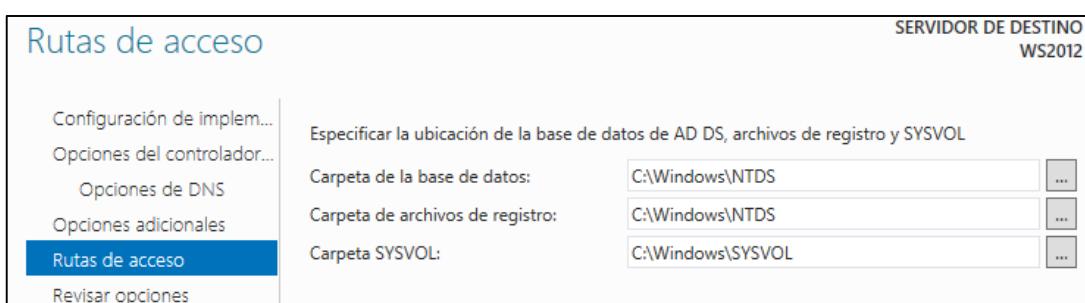


Aquí precisamente nos indica que no existe ningún DNS en la red que conozca la zona ROMEROVARGAS.COM lo que es normal. Nos dice también que no debemos preocuparnos de este error a menos de que tengamos un DNS ya funcionando en la red configurado. En caso de no ser así el solo va crear y configurar un DNS que sepa trabajar con la zona ROMEROVARGAS.COM por lo que no debemos preocuparnos por este mensaje de momento.

Tampoco podemos crear una delegación DNS ya que esto solo se puede hacer si el servidor DNS ya está funcionando y configurado.



El nombre NetBIOS es el nombre que tendrá nuestro dominio en red para trabajar con máquinas que no estén usando DNS. Puesto que dichas máquinas no van a poder hablar con ROMEROVARGAS.COM (nombre DNS por el punto) les indicamos que hablen con nuestro nombre NetBIOS que debe ser un nombre normal no DNS (lo normal es dejar nuestro nombre DNS hasta el punto y eliminar el resto).



Toda la información sobre equipos, cuentas de usuario, contraseñas, configuraciones de seguridad, etc. del directorio activo se almacenan en una base de datos conocida como NTDS, y la carpeta pública SYSVOL es donde se almacenarán todos los perfiles de usuario, scripts de inicio de sesión, etc. El sistema nos pregunta donde deseamos crear dichos elementos. Lo ideal sería colocarlos en discos duros distintos, para que pudiera accederse a ellas más rápidamente y además que dichos HD contarán con una alta velocidad y opciones de recuperación de errores. Nosotros dejamos las opciones por defecto ya que no contamos con tales lujo en clase.

Luego veremos un resumen de todas las opciones que hemos seleccionado para la instalación de nuestro dominio. Una opción interesante es la de ver el script Power Shell que se va a ejecutar.



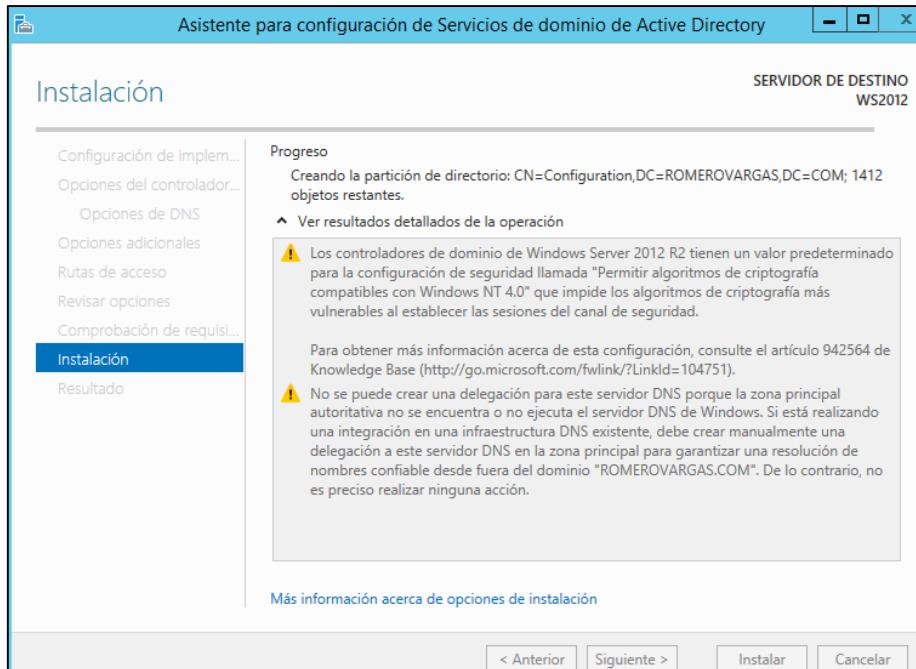
```

#
# Script de Windows PowerShell para implementación de AD DS
#
Import-Module ADDSDeployment
Install-ADDSForest `-
-CreateDnsDelegation:$false `-
-DatabasePath "C:\Windows\NTDS" `-
-DomainMode "Win2012R2" `-
-DomainName "ROMEROVARGAS.COM" `-
-DomainNetbiosName "ROMEROVARGAS" `-
-ForestMode "Win2012R2" `-
-InstallDns:$true `-
-LogPath "C:\Windows\NTDS" `-
-NoRebootOnCompletion:$false `-
-SysvolPath "C:\Windows\SYSVOL" `-
-Force:$true

```

Este script podemos modificarlo, copiarlo, lanzarlo en otras máquinas, etc. Es una forma muy práctica de automatizar las tareas de instalación.

A continuación el sistema realizará una revisión de los requisitos previos para la instalación de AD y comprobará que todo está correcto. Veremos una serie de mensajes de advertencia (warning) que no son especialmente importantes, y si no se encuentra ningún error grave se permitirá que se inicie la instalación para lo cual tendremos que hacer clic en el botón instalar.



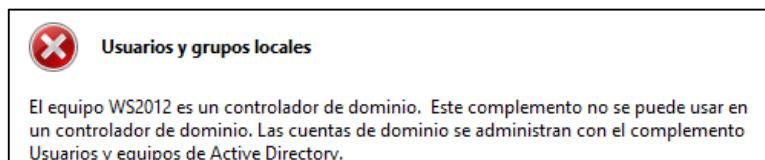
La instalación de un dominio puede ser un proceso lento, esperaremos que se complete y posteriormente el sistema nos presentará una pantalla de resultado. Si hemos escogido la opción de reinicio automático no veremos dicha pantalla y el sistema se reiniciará pero ya como controlador de dominio. El primer inicio de un controlador de dominio puede tardar bastante tiempo, paciencia.

Una vez reiniciado vamos a comprobar que nuestro equipo ya ha formado un dominio nuevo en un árbol nuevo en un bosque nuevo y se ha colocado como DC del mismo. Podemos comprobarlo con el comando Power Shell Get-ADDomainController.

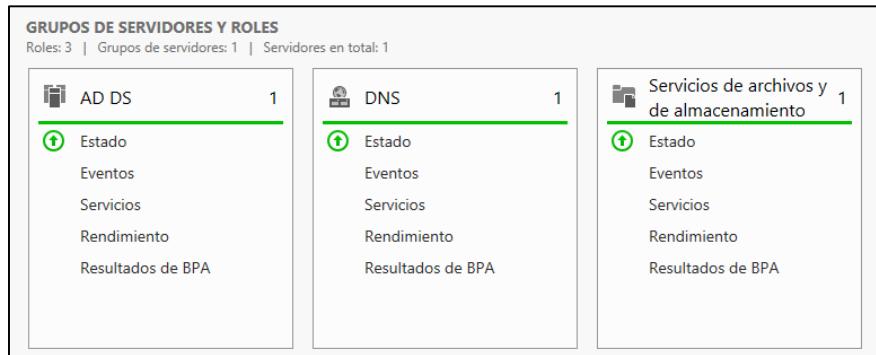
```
PS C:\Users\Administrador> Get-ADDomainController

ComputerObjectDN : CN=WS2012,OU=Domain Controllers,DC=ROMEROVARGAS,DC=COM
DefaultPartition : DC=ROMEROVARGAS,DC=COM
Domain          : ROMEROVARGAS.COM
Enabled         : True
Forest          : ROMEROVARGAS.COM
HostName        : WS2012.ROMEROVARGAS.COM
InvocationId    : 8c7be1de-583f-4f55-ab73-2aa2bf4f652d
IPv4Address     : 192.168.177.100
IPv6Address     : ::1
IsGlobalCatalog : True
IsReadOnly       : False
LdapPort        : 389
Name            : WS2012
NTDSSettingsObjectDN : CN=NTDS Settings,CN=WS2012,CN=Servers,CN=Default-First-Name,CN=Sites,CN=Configuration,DC=ROMEROVARGAS,DC=COM
OperatingSystem  : Windows Server 2012 R2 Standard
```

En este momento nuestro equipo se ha transformado en un DC (Domain Controller, Controlador de Dominio) y deja de ser un equipo normal. Así, por ejemplo, si ejecutáis la consola de administración de usuarios y grupos locales (**lusrmgr.msc**) que ya conocemos de temas anteriores veréis como no puede usarse dado que nuestro equipo ya no puede trabajar con cuentas de usuario o grupos locales.

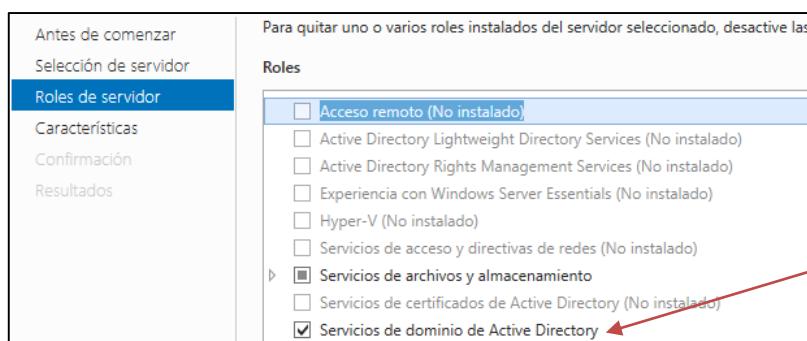
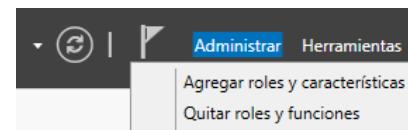


Si nos fijamos en el panel del asistente de administración, veremos cómo nuestro equipo ahora mismo está desempeñando 3 roles distintos, el de ADDS (DC), el de servidor DNS y el de servidor de archivos (ya que nuestro equipo al ser controlador de dominio tiene que compartir carpetas obligatoriamente).

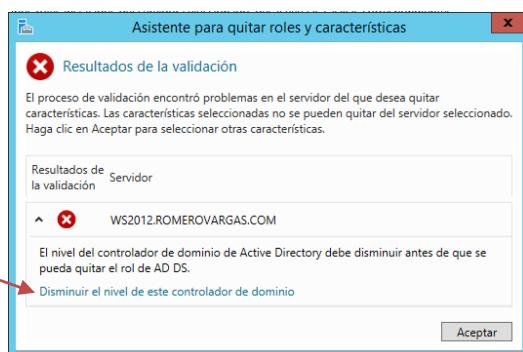


Vamos a proceder ahora a degradar nuestro servidor, de modo que deje de ser controlador de dominio. Dado que nuestro dominio ROMEROVARGAS.COM solo tiene un DC que somos nosotros mismos, al degradarnos también eliminaremos el dominio completo, su árbol y su bosque.

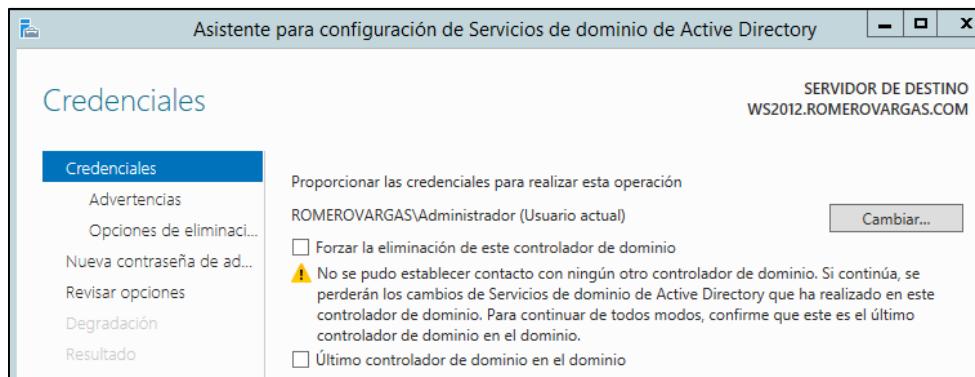
Para degradar nuestro servidor seleccionamos quitar roles y funciones del panel.



Posteriormente en la lista de roles de servidor desmarcamos la opción de Servicios de dominio de Active Directory. Esto realmente no va a eliminar ADDS de nuestro equipo, sino que al ser nuestro equipo DC lo va a degradar eliminando el dominio, pero realmente no elimina ADDS. Si desmarcamos esta casilla cuando nuestro equipo no es DC realmente elimina ADDS. Al desmarcar la opción y tras unos segundos, veremos por pantalla una advertencia como la siguiente:



Aquí elegimos la opción de Disminuir el nivel de este controlador de dominio, que es la opción que realmente degrada nuestro equipo.

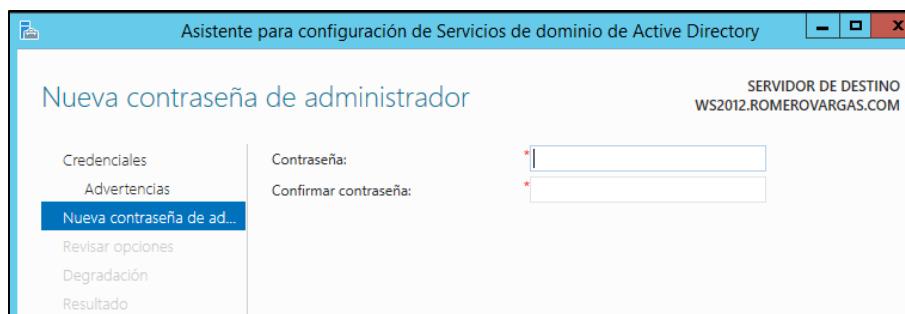


Aquí hay que marcar la opción de forzar la eliminación del controlador de dominio. Podemos seleccionar cambiar si queremos realizar esta acción con las credenciales (permisos) de otro usuario, pero ya que vemos que el usuario actual es Administrador, este debería tener poder suficiente para eliminar este dominio en nuestro ejemplo. (Esto no siempre es así, como veremos más adelante).

Una opción importante que tenemos que marcar es la de Último controlador de dominio en el dominio. Esto le indica al sistema que elimine nuestro dominio ya que no queda ningún controlador de dominio en el mismo, y es algo que tenemos que controlar nosotros. En nuestro ejemplo no existen más servidores creados en nuestro dominio ROMEROVARGAS.COM así que es obligatorio que marquemos dicha opción para que elimine ROMEROVARGAS.COM después de que hayamos degradado el servidor. Habrá ocasiones en que el dominio cuente con varios servidores y será necesario dejar esta casilla sin marcar.

Posteriormente el sistema nos presenta un resumen de todas las cosas que va a eliminar (que son bastantes) y nos pide confirmación del degradado. Le decimos que sí, que continúe con la eliminación.

Las cuentas del dominio van a desaparecer junto con el dominio, y la cuenta de Administrador que estamos usando también va a desaparecer. Nos pide entonces la contraseña que le va a asignar a la nueva cuenta de Administrador del equipo.



Vemos en la siguiente pantalla que nos aparecerá que también podemos generar un script de Power Shell con las instrucciones que hay que ejecutar para realizar el degradado tal como lo hemos elegido.

Para confirmar el degradado seleccionamos Disminuir nivel y veremos cómo empieza el proceso de degradado, eliminación del dominio, del árbol y del bosque. También veremos cómo se borran las zonas del DNS, cosa que estudiaremos más adelante. Nuestro equipo se reiniciará ya sin ser DC.

Vamos a proceder ahora a montar de nuevo el dominio pero esta vez utilizando la consola Power Shell. Ahora mismo no tenemos ni bosque, ni árbol ni dominio, tenemos que crear un bosque, con lo que el sistema creará automáticamente un árbol con un dominio y promocionara nuestro equipo a DC de dicho dominio.

Podemos crear un bosque nuevo con el comando Install-ADDSForest.

```
PS C:\Users\Administrador.WS2012> Install-ADDSForest -domainname "ROMEROVARGAS.COM"
SafeModeAdministratorPassword: *****
Confirmar SafeModeAdministratorPassword: *****

El servidor de destino se configurará como un controlador de dominio y se reiniciará cuando se complete esta operación.
¿Desea continuar con esta operación?
[SI] [O] Si a todo [N] No [T] No a todo [U] Suspender [?] Ayuda <el valor predeterminado es "S">: O
```

Hemos usado el comando `Install-ADDSForest -domainname "ROMEROVARGAS.COM"` para crear directamente nuestro bosque. El sistema automáticamente creará el servidor DNS si lo considera necesario. Este comando toma muchas opciones por defecto, si queremos podemos indicar explícitamente estas opciones mediante parámetros, como por ejemplo `Install-ADDSForest -DomainName ROMEROVARGAS.COM -CreateDNSDelegation -DomainMode Win2008 -ForestMode Win2008R2 -DatabasePath "d:\NTDS" -SYSVOLPath "d:\SYSVOL" -LogPath "e:\Logs"`.

Con este comando ya habremos conseguido instalar toda nuestra infraestructura.

Para degradar nuestro DC y en nuestro eliminar el dominio, el árbol y el bosque tendremos que utilizar el comando de Power Shell `Uninstall-ADDSDomainController`.

```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador.WS2012> Uninstall-ADDSDomainController -Forceremoval -Demoteoperationmasterrole
LocalAdministratorPassword: *****
Confirmar LocalAdministratorPassword: *****
```

En nuestro ejemplo hemos ejecutado el comando con las opciones `Uninstall-ADDSDomainController -Forceremoval -Demoteoperationmasterrole`.

Vemos como es mucho más rápido el realizar estas opciones desde Power Shell que desde el interfaz gráfico de usuario. De hecho la propia Microsoft está intentando que se pase a administrar desde este Power Shell y cada vez introduce más opciones y las quita del interfaz gráfico.

Si queremos ver todos los comandos de los que disponemos en Power Shell para trabajar con Active Directory podemos ejecutar directamente el siguiente comando: `Get-Command -Module ActiveDirectory`.

```
PS C:\Users\Administrador.WS2012.000> Get-Command -Module ActiveDirectory

 CommandType      Name                                     ModuleName
 -----          -----
 Cmdlet          Add-ADCentralAccessPolicyMember           ActiveDirectory
 Cmdlet          Add-ADComputerServiceAccount            ActiveDirectory
 Cmdlet          Add-ADDomainControllerPasswordReplicationPolicy ActiveDirectory
 Cmdlet          Add-ADFineGrainedPasswordPolicySubject   ActiveDirectory
 Cmdlet          Add-ADGroupMember                         ActiveDirectory
 Cmdlet          Add-ADPrincipalGroupMembership          ActiveDirectory
 Cmdlet          Add-ADResourcePropertyListMember        ActiveDirectory
 Cmdlet          Clear-ADAccountExpiration             ActiveDirectory
 Cmdlet          Clear-ADClaimTransformLink              ActiveDirectory
 Cmdlet          Disable-ADAccount                      ActiveDirectory
```

También podemos instalar el ADDS completo desde Power Shell directamente con el comando `Install-windowsfeature -name AD-Domain-Services -IncludeManagementTools` y podemos desinstalarlo con el comando `Uninstall -ADDSDomainController -Forceremoval -Demoteoperationmasterrole`.

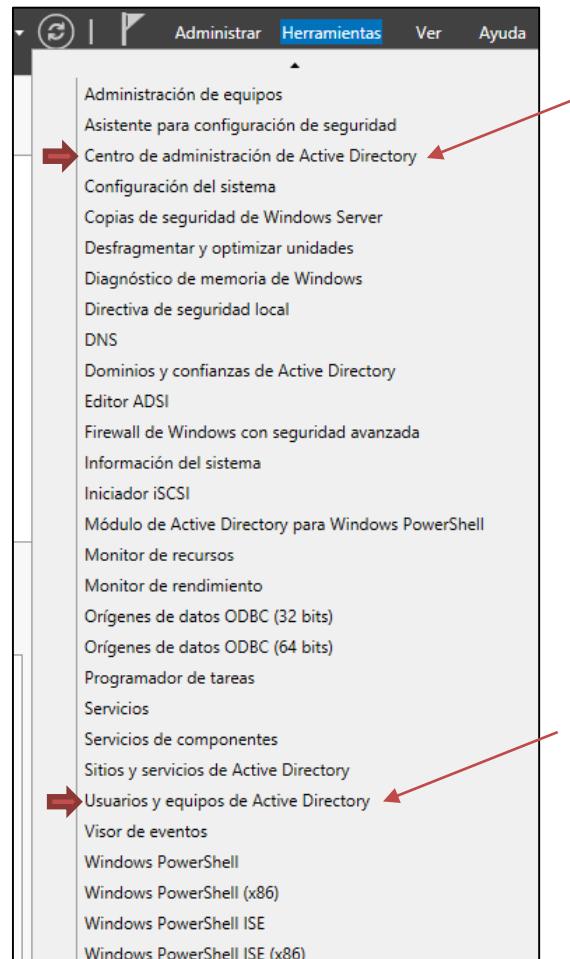
### CREACIÓN DE UNIDADES ORGANIZATIVAS, USUARIOS Y GRUPOS DEL DOMINIO.

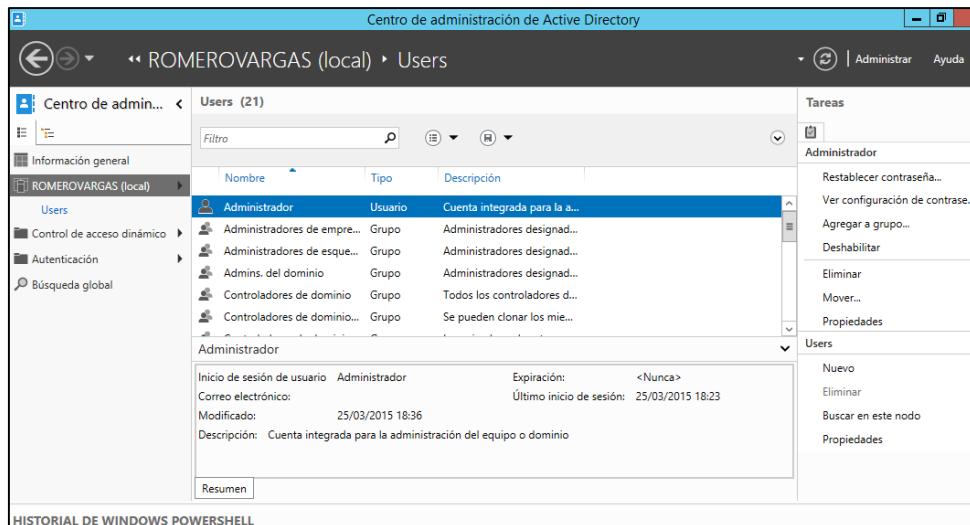
Una vez que hemos creado nuestro dominio, deberemos crear algunas unidades organizativas, algunos usuarios del dominio y algunos grupos del dominio. Esto lo podemos realizar desde dos consolas principales, la más antigua que es Usuarios y Equipos de Active Directory o la más nueva que es Centro de Administración de Active Directory (ADAC, Active Directory Administrative Center).

Microsoft recomienda utilizar el Centro de Administración de Active Directory ya que es donde piensa ir colocando todas las nuevas características, dejando usuarios y equipos de active directory más por compatibilidad que por otra cosa.

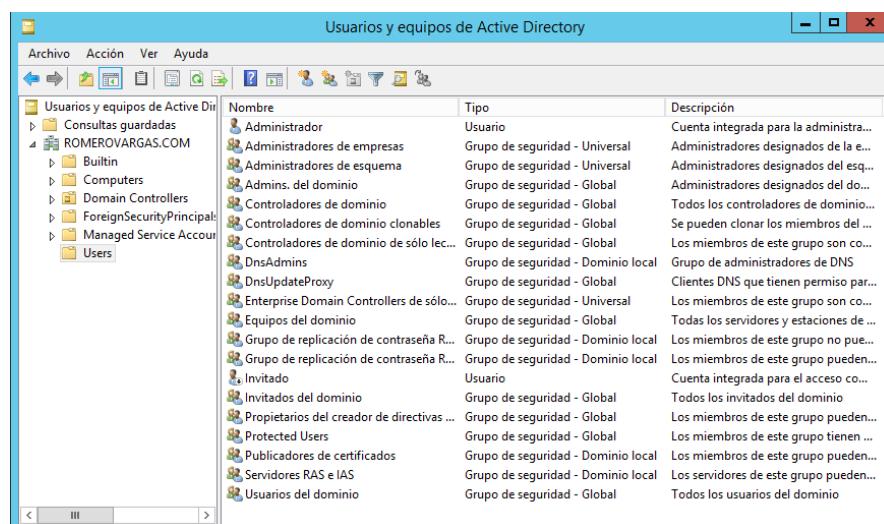
Evidentemente también podremos realizar estas funciones de administración de unidades organizativas, usuarios y grupos del dominio desde la consola Power Shell. La consola es bastante más engorrosa para estas operaciones que las interfaces gráficas de usuario, pero es muchísimo más conveniente cuando queremos crear al mismo tiempo una gran cantidad de objetos, o bien queremos automatizar la administración de los mismos.

Veamos ahora una captura de pantalla del centro de administración de Active Directory.





Aquí podemos ver una captura de pantalla de la consola de Usuarios y Equipos de Active Directory.



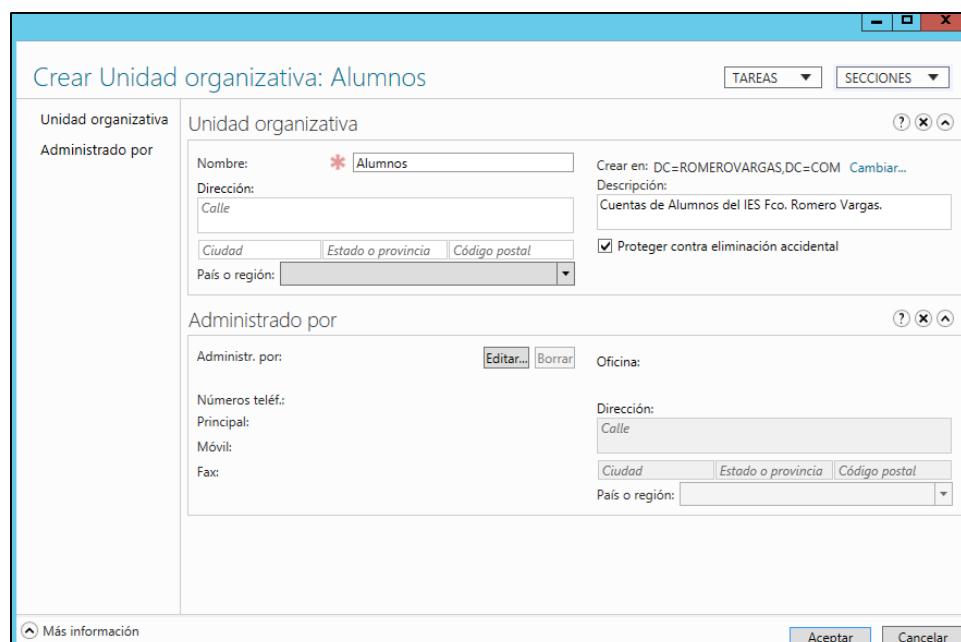
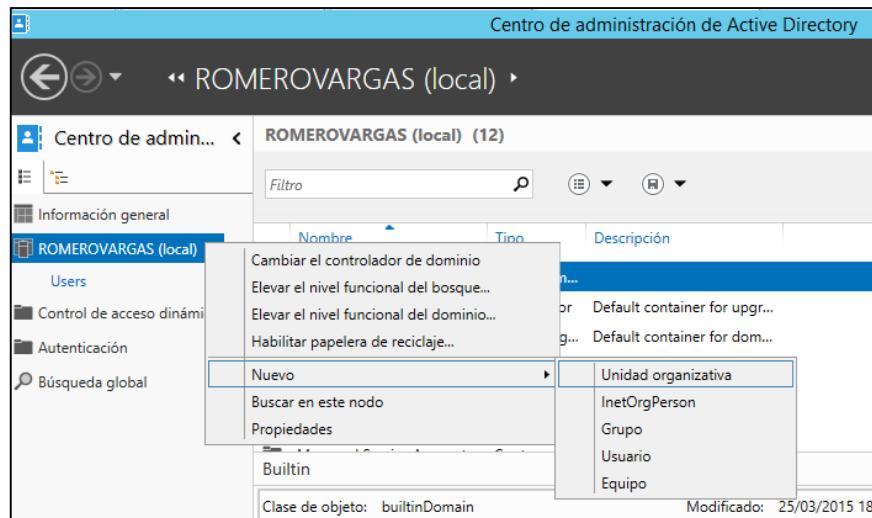
Nosotros durante este curso vamos a usar el centro de administración de Active Directory.

### Unidades organizativas usando ADAC.

Las unidades organizativas se utilizan para organizar los objetos dentro de un active directory. Cualquier objeto (como usuarios, grupos, equipos, etc.) pueden ser colocados dentro de unidades organizativas para administrarlas de una forma más cómoda. Las dos principales razones por los que creamos unidades organizativas son:

- 1) Administrar varios objetos a la vez mediante políticas de grupo.
- 2) Delegar ciertas tareas de administración de varios objetos a un usuario.

Vamos a crear un par de unidades organizativas llamadas Alumnos y Profesores dentro de nuestro dominio ROMEROVARGAS.COM. Para ello lanzamos el centro de administración de Active Directory, damos botón derecho sobre el dominio local ROMEROVARGAS.COM



Una vez creadas ambas unidades organizativas veremos cómo aparecen directamente como elementos de nuestro dominio romerovargas.com.

En Windows 2012 podemos crear OU (Organizational Unit) anidadas, es decir, que ahora dentro de la OU Alumnos podríamos crear otras 3 OU llamadas Informática, Electrónica y Administrativos.

#### LDAP nombres distintivos.

Active Directory utiliza el Lightweight Directory Access Protocol (LDAP) como hemos visto anteriormente. LDAP utiliza los nombres distintivos (Distinguished Name) para identificar de forma única todos los objetos dentro del directorio. Antes de seguir viendo como creamos dichos objetos, tenemos que comprender como funcionan estos nombres distintivos (DN).

El formato DN usa varias parejas `Typo_Objeto=Nombre_Objeto` separadas por coma para identificar cada objeto. Por ejemplo, nuestro dominio `romerovargas.com` tiene dos componentes de dominio (DC) que son `romerovargas` y `com` y su nombre DN sería el siguiente:

`dc=romero, dc=com`

El tipo de una unidad organizativa es OU, así que nuestra unidad organizativa Profesores tendría el siguiente nombre DN.

`ou=Profesores, dc=romero, dc=com`

Vemos como los nombres DN van ordenados de izquierda a derecha, de modo que siempre terminan con el dc.

Los contenedores (Users, Computers) se identifican como de tipo CN (common name, nombre común). Así, el contenedor Users tiene el siguiente nombre DN:

`cn=Users, dc=romero, dc=com`

La diferencia entre contenedores y unidades organizativas son las siguientes:

- Los contenedores se crean automáticamente al crear al promover un servidor a controlador de dominio, mientras que las unidades organizativas tenemos que crearlas manualmente.
- No se pueden aplicar políticas de grupo a los contenedores, pero sí a las unidades organizativas.
- No se pueden crear UO dentro de los contenedores, sí dentro de otras UO.

Los usuarios del sistema también se consideran objetos del dominio, de modo que también tienen su propio nombre DN. El tipo de cuentas de usuario y grupo son cn (common name). Así, si creamos una cuenta de usuario `Jose.Antonio` dentro de nuestra UO profesores, esta cuenta tendrá un nombre DN como el siguiente:

`cn=Jose.Antonio, ou=Profesores, dc=romero, dc=com`

Una cuenta con nombre usuario, creado dentro del contenedor Users, tendría el siguiente nombre DN:

`cn=usuario, cn=Users, dc=romero, dc=com`

Si el nombre DN tiene espacios en blanco tiene que estar encerrado entre comillas, hay que tener cuidado con esto. Los nombres DN no distinguen mayúsculas de minúsculas, por lo que los siguientes nombres DN son los mismos:

```
cn=pedro,ou=Administrativo,ou=Alumnos,dc=romero,dc=com  
CN=Pedro,Ou=ADMINISTRATIVO,Ou=ALUMNOS,DC=Romero,DC=Com
```

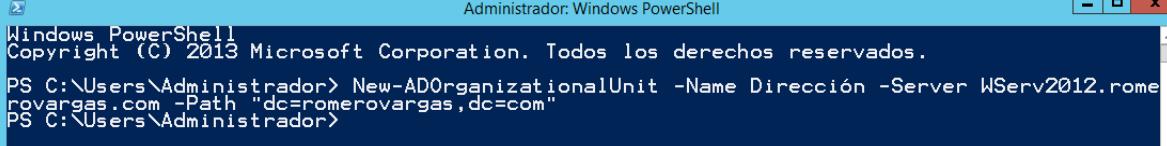
---

#### Unidades organizativas usando PowerShell.

El comando para crear nuevas unidades organizativas desde PowerShell es `New-ADOrganizationalUnit` donde le tenemos que indicar el nombre de la nueva OU, en que servidor se va a crear y el path dentro del directorio donde se va a crear.

La línea completa para crear una OU Dirección dentro de romerovargas.com en nuestro servidor WServ2012 sería la siguiente:

```
New-ADOrganizationalUnit -Name Dirección -Server WServ2012.romerovargas.com -Path "dc=romero,dc=com"
```



Windows PowerShell  
Administrator: Windows PowerShell  
Copyright (C) 2013 Microsoft Corporation. Todos los derechos reservados.  
PS C:\Users\Administrador> New-ADOrganizationalUnit -Name Dirección -Server WServ2012.romerovargas.com -Path "dc=romero,dc=com"  
PS C:\Users\Administrador>

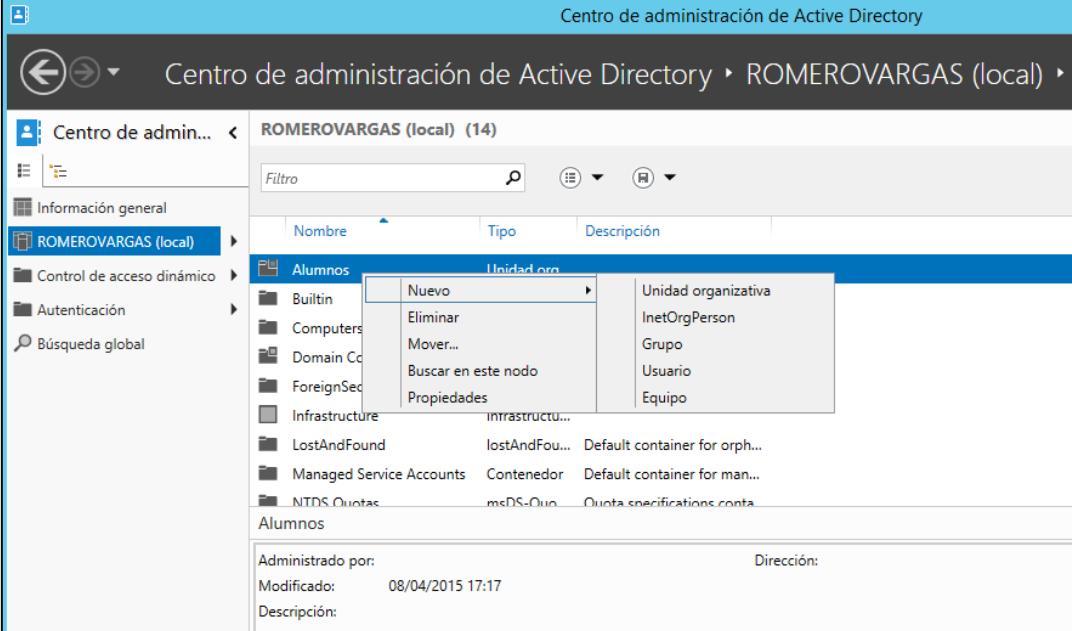
Si queremos ver información sobre una OU utilizaríamos el comando Get-ADOrganizationalUnit y si quisiermos borrar una OU el comando Remove-ADOrganizationalUnit.

#### CUENTAS DE USUARIO UTILIZANDO ADAC.

Tanto los usuarios como los equipos que se conecten a nuestro dominio necesitan una cuenta de dominio creada para poder trabajar. Las cuentas de equipo se crean automáticamente cuando los equipos se conectan por primera vez al dominio, por defecto se crean en el contenedor Computers.

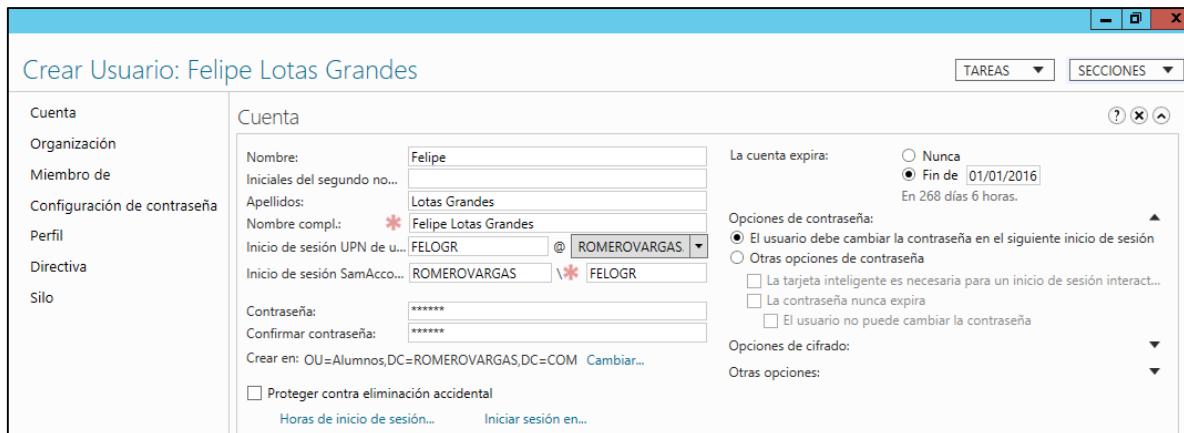
Hasta ahora hemos ejecutado ADAC seleccionándolo desde el menú del Panel de Administración, pero también podemos ejecutarlo directamente ejecutando el comando dsac.exe. Probad a pulsar la tecla Windows y escribir directamente ese comando.

Vamos a crear una cuenta de usuario directamente en la unidad organizativa Alumnos que creamos anteriormente. Para ello pulsamos botón derecho en la OU Alumnos y seleccionamos Nuevo – Usuario.



The screenshot shows the 'Centro de administración de Active Directory' (Active Directory Administrative Center) interface. The left navigation pane shows 'ROMEROVARGAS (local)' selected. In the main pane, under the 'Alumnos' container, a context menu is open over the 'Nuevo' item in the 'Unidad org.' column. The menu options are: Eliminar, Mover..., Buscar en este nodo, and Propiedades. The 'Nuevo' option is highlighted. The 'Nombre' column lists several objects: BuiltIn, Computers, Domain Controllers, ForeignSecurity, Infrastructure, LostAndFound, Managed Service Accounts, and NTDS-Contas. The 'Tipo' column indicates their type: Unidad organizativa, InetOrgPerson, Grupo, Usuario, and Equipo. At the bottom of the main pane, there are fields for 'Administrado por:', 'Modificado:', and 'Descripción:'.

Los primeros datos que pide son el Nombre de pila, las iniciales del segundo nombre de pila si es que lo tiene, los Apellidos, el nombre de inicio de sesión UPN que es el nombre de la cuenta, la contraseña, la expiración de la cuenta, las opciones de contraseña que ya conocemos, las opciones de cifrado, etc.



### Cuentas de usuario utilizando powershell.

El comando de PowerShell que usamos para crear usuarios es NEW-ADUser.

```
PS C:\Users\Administrador> New-ADUser
cmdlet New-ADUser en la posición 1 de la canalización de comandos
Proporcione valores para los parámetros siguientes:
Name: Ricardo
PS C:\Users\Administrador>
```

Como vemos en la pantalla anterior, los comandos de PowerShell los podemos ejecutar sin pasarselos parámetros, con lo que nos pedirá los parámetros obligatorios directamente por teclado. Vemos como el único parámetro que pide para el nuevo usuario es el Nombre, que le hemos indicado que es Ricardo. Vemos ahora como efectivamente hemos creado una cuenta de usuario del dominio con nombre Ricardo, sin ningún otro dato, que cuelga directamente del contenedor Users y que esta deshabilitada, ya que no se puede habilitar una cuenta de Dominio a menos que cuente con una contraseña.

Vamos a eliminar la cuenta Ricardo directamente desde el ADAC y vamos a volver a crearla desde PowerShell pero ya dándole todos los datos mediante parámetros.

```
PS C:\Users\Administrador> New-ADUser -Name Ricardo -Path "OU=Alumnos,DC=RomeroVargas,DC=Com" -Givenname Ricardo -Surname "Borriquero Campo" -UserPrincipalName "RIBOCA@RomeroVargas.Com" -AccountPassword (Read-Host -AsSecureString "Contraseña : ") -Enabled 1 -ChangePasswordAtLogon 1
Contraseña : : *****
PS C:\Users\Administrador>
```

Detallo aquí el comando completo:

#### New-ADUser

- Name Ricardo
- Path "OU=Alumnos,DC=RomeroVargas,DC=Com"
- Givenname Ricardo
- Surname "Borriquero Campo"
- UserPrincipalName **RIBOCA@RomeroVargas.Com**
- AccountPassword (Read-Host -AsSecureString "Contraseña : ")
- Enabled 1
- ChangePasswordAtLogon 1

La mayoría de las opciones es fácil de entender lo que hacen, vamos a detenernos en la de la contraseña. Esa línea le indica que la contraseña de la cuenta debe ser pedida por teclado (Read-Host) que debe pedirse como una cadena segura (no verse por pantalla y guardarse internamente como cadena segura o cifrada) y que el mensaje que verá el usuario será "Contraseña :".

Podríamos de igual modo asignar directamente la contraseña sin pedirla al usuario. Vamos a volver a crear el usuario Ricardo pero esta vez asignándole una contraseña. Para ello en primer lugar eliminamos la cuenta creada Ricardo, pero esta vez voy a hacerlo desde PS (PowerShell).

```
PS C:\Users\Administrador> Remove-ADUser Ricardo
Confirmar
¿Está seguro de que desea realizar esta acción?
Se está realizando la operación "Remove" en el destino
"CN=Ricardo,OU=Alumnos,DC=ROMEROVARGAS,DC=COM"
[S] Sí [0] Sí a todo [N] No [T] No a todo [U] Suspender [?] Ayuda
(el valor predeterminado es "S"):0
PS C:\Users\Administrador>
```

Vamos a volver ahora a crear Ricardo.

```
PS C:\Users\Administrador> New-ADUser -Name Ricardo -Path "OU=Alumnos,DC=RomeroVargas,DC=Com" -Givenname Ricardo -Surname "Borriquero Campo" -UserPrincipalName "RIBOCA@RomeroVargas.Com" -AccountPassword P4ssw0rd -Enabled 1 -ChangePasswordAtLogon 1
New-ADUser : No se puede enlazar el parámetro 'AccountPassword'. No se puede convertir el valor "P4ssw0rd" de tipo "System.String" al tipo "System.Security.SecureString".
En línea: 1 Carácter: 177
+ ... ccountPassword P4ssw0rd -Enabled 1 -ChangePasswordAtLogon 1
+           + CategoryInfo          : InvalidArgument: (:) [New-ADUser], ParameterBindingException
+           + FullyQualifiedErrorId : CannotConvertArgumentNoMessage,Microsoft.ActiveDirectory.Management.Commands.NewADUser
```

Ups, error.

Si leemos el error (cosa que siempre os recomiendo) veremos cómo se queja de que la contraseña que le he indicado (P4ssw0rd) Es de tipo String (cadena) y no puede convertirse en tipo SecureString. Esto es así porque la contraseña debe ser introducida como una cadena segura, como vimos en el anterior ejemplo. La forma de introducir nuestra contraseña como cadena segura es la siguiente:

```
PS C:\Users\Administrador> New-ADUser -Name Ricardo -Path "OU=Alumnos,DC=RomeroVargas,DC=Com" -Givenname Ricardo -Surname "Borriquero Campo" -UserPrincipalName "RIBOCA@RomeroVargas.Com" -AccountPassword (ConvertTo-SecureString P4ssw0rd -AsPlainText -force) -Enabled 1 -ChangePasswordAtLogon 1
PS C:\Users\Administrador>
```

Vemos como el parámetro de password ha quedado como:

-AccountPassword (ConvertTo-SecureString P4ssw0rd –AsPlainText –force)

Con esto hemos conseguido que la cuenta Ricardo tenga como contraseña P4ssw0rd.

En estos apuntes no vamos a ver todos los parámetros posibles de cada orden, ya que son muchos y no se considera necesario saberlos o practicarlos todos, aunque si es necesario saber cómo ver la ayuda de los comandos para cuando los necesitemos. Por ejemplo, quiero que modifiquéis la línea anterior para que el usuario Ricardo se cree pero de forma que la cuenta expire automáticamente el 02 de febrero del 2020.

En primer lugar, escribir desde el PS el comando Help New-ADUser, leer lo que pone e intentad comprenderlo, y posteriormente hacer todo lo necesario para poder obtener la ayuda necesaria (desde el mismo PS) para poder conocer que parámetro necesitamos para indicar la fecha de expiración y como debemos usarla.

Como vemos, al menos en el momento actual, nos encontraremos con un error, dado que la documentación de ayuda sobre estos comandos aún no ha sido traducida totalmente al castellano. Por ello, tendremos que acceder a la ayuda Web y en inglés, para ello tal como indica la ayuda hay que usar el comando Get-Help New-ADUser –Online.

Comprobaremos como este comando tampoco funciona correctamente, y aunque abre el explorador de internet para llevarnos a la página correspondiente, esta no puede ser cargada. Esto es normal y lógico. Si miramos la configuración IP de nuestro servidor veremos que estamos usando nuestro propio equipo como servidor DNS (obligatorio en un AD). Esto está muy bien para trabajar en AD pero evidentemente nuestro DNS no sabe aún como navegar por Internet. Esto lo arreglaremos posteriormente, no intentar bajo ningún concepto añadir un servidor DNS a nuestro servidor a menos que queráis cargaros totalmente el Active Directory. De momento consultar la ayuda desde nuestra máquina anfitrión.

## Grupos.

La razón más frecuente para crear grupos es la de agrupar y organizar las cuentas de los usuarios, y permite darles permisos de forma conjunta. En general, siempre recomendamos asignar permisos a grupos, y nunca a usuarios de forma individual.

En el tema de Windows Cliente que vimos en la primera evaluación ya trabajamos con grupos, pero solo existía un tipo de grupos. En un dominio sin embargo tenemos varios tipos de grupos, que vamos a proceder a ver ahora.

Hay dos tipos de grupo principales en Active Directory: grupos de distribución y grupos de seguridad.

## Grupos de distribución.

- Se utiliza sólo con aplicaciones de correo electrónico
- No está habilitado para seguridad



Estos grupos no cuentan con SID (identificador de seguridad) propio, de modo que no pueden ser introducidos en las ACL (listas de control de acceso a los recursos). Estos grupos solo se suelen utilizar cuando queremos crear un grupo para realizar envíos de correo a varios usuarios habitualmente.

## Grupos de seguridad.

- Se utiliza para asignar derechos y permisos a los grupos de usuarios y equipos
- Se utiliza de forma más eficaz cuando está anidado



Estos grupos si cuentan con SID, de modo que pueden ser utilizados para ser introducidos en las ACL. Por regla general siempre que creamos un grupo lo crearemos de este tipo, de seguridad.

## Ámbito de los grupos.

Todos los grupos tienen un atributo de ámbito que determina dónde se puede utilizar dicho grupo en una red. Así, nos encontramos con los siguientes tipos de grupos:

- Grupos **locales** de dominio.
  - Su **ámbito es local**, es decir, los grupos locales no son visibles fuera del dominio donde se crean.
- Grupos **globales** de dominio.
  - Su **ámbito es global**, es decir, los grupos globales son visibles en todos los dominios que formen parte de nuestro bosque.

- Grupos universales.
  - Su ámbito es global, al igual que en los grupos globales.

### Integrantes de los grupos.

---

Mientras que el ámbito de los grupos es independiente del nivel funcional de dominio (que establece la compatibilidad de Windows Server), la membresía de los grupos depende directamente de dicho nivel funcional.

Así, dependiendo del nivel funcional de nuestro dominio podremos o no introducir miembros determinados dentro de cada tipo de grupo.

Las siguientes reglas se aplican si el **nivel funcional** de dominio es al menos **Windows 2003**.

- Grupos **locales** de dominio.
  - Un grupo local de dominio **puede contener grupos globales** y universales de cualquier dominio del bosque. También **puede contener cuentas de usuario** y equipos **de cualquier dominio** del bosque. También puede contener otros grupos locales pero únicamente del mismo dominio donde se ha creado (evidentemente).
- Grupos globales de dominio.
  - Un grupo global **puede contener** otros **grupos globales del mismo dominio** donde se crea el grupo global. También **puede contener cuentas de usuario** y equipos **del mismo dominio** donde se crea el grupo global.
  - Un grupo global **no puede contener** grupos universales ni **grupos locales**. Tampoco puede contener grupos globales ni cuentas de usuario ni cuentas de equipo de fuera de su propio dominio.
- Grupos universales.
  - Un grupo universal **puede contener** grupos universales, grupos globales, cuentas de usuario y cuentas de equipo de cualquier dominio del bosque.
  - Un grupo universal **no puede contener** grupos locales.

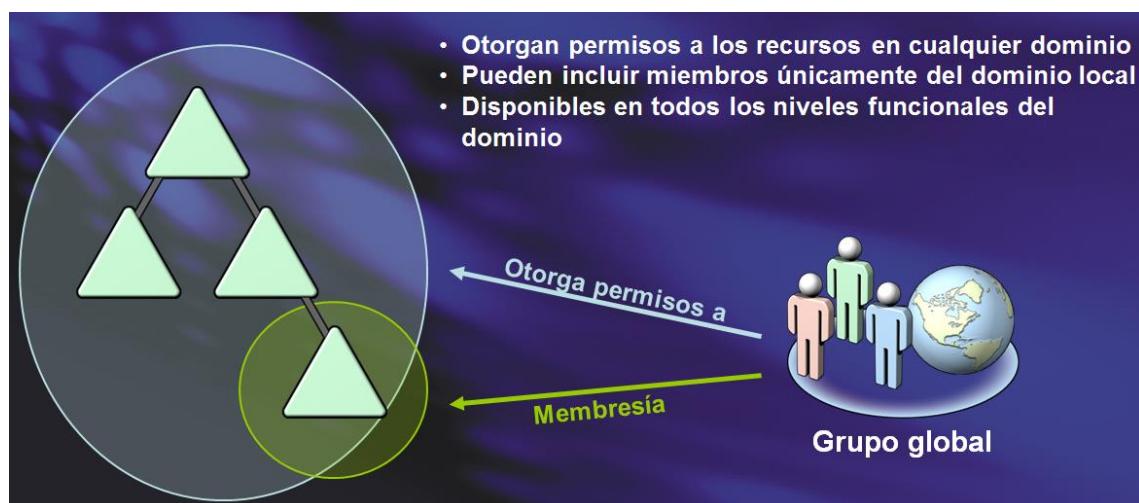
### Tipos de grupos en Windows server.

Un **grupo de dominio local** es un grupo de seguridad o distribución que puede contener grupos universales, grupos globales, otros grupos locales de dominio de su propio dominio y cuentas de cualquier dominio del bosque.

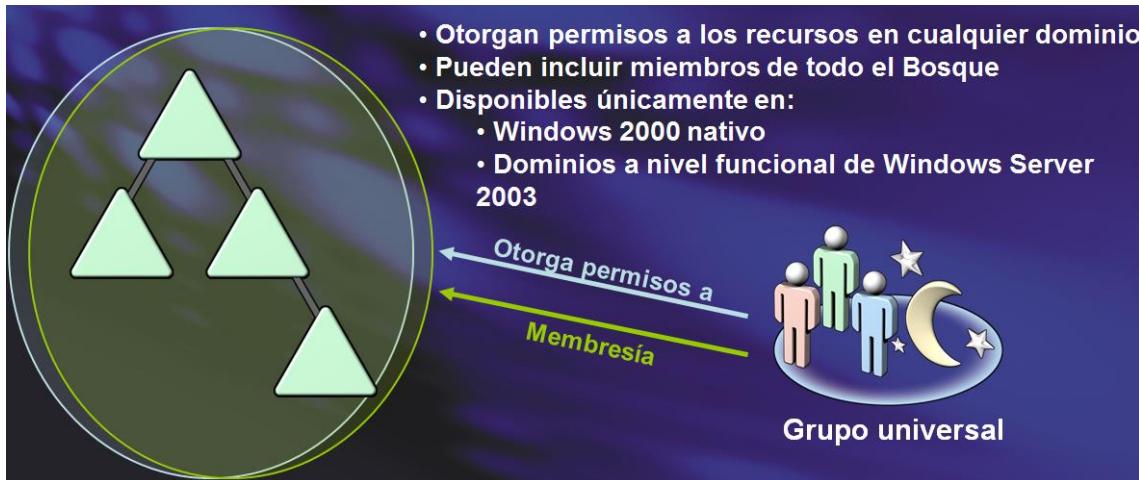
En los grupos de seguridad local, solamente puede otorgar derechos y permisos sobre los recursos que residen en el dominio en el que está ubicado el grupo local de dominio.



Un **grupo global** es un grupo de seguridad o distribución que puede contener usuarios, equipo y grupos globales de su propio dominio. Puede conceder derechos y permisos a los grupos de seguridad global para los recursos de cualquier dominio del bosque.



Un **grupo universal** es un grupo de seguridad o distribución que puede contener usuarios, equipos, grupos universales y grupos globales de cualquier dominio del bosque. Se pueden conceder derechos y permisos a los grupos de seguridad universales sobre los recursos de cualquier dominio del bosque.



### Anidamiento de grupos.

Hay que tener mucho cuidado al anidar grupos (incluir grupos como miembros de grupos) si tenemos el nivel funcional del dominio elevado a Windows 2003 o superior, ya que el sistema permitirá anidar recursivamente, es decir, podemos llegar a formar un bucle infinito de membresías.

Así por ejemplo, imaginad que tenemos el grupo local LOCAL1, e indicamos que un miembro de dicho grupo es LOCAL2, y a su vez indicamos que un miembro de LOCAL2 es LOCAL1.

Para evitar esto no se recomienda introducir dentro de un grupo local otro grupo local, del mismo modo que no se recomienda utilizar grupos universales.

### Cuando utilizar cada tipo de grupo.

Los grupos con ámbito local de dominio nos ayudan a definir y administrar el acceso a los recursos en un solo dominio. Por ejemplo, para conceder a cinco usuarios acceso a una impresora determinada, podemos agregar las cinco cuentas de usuario a la lista de permisos de la impresora. Sin embargo, si más tarde deseamos dar a esos cinco usuarios acceso a una nueva impresora, debemos especificar nuevamente las cinco cuentas en la lista de permisos de la nueva impresora.

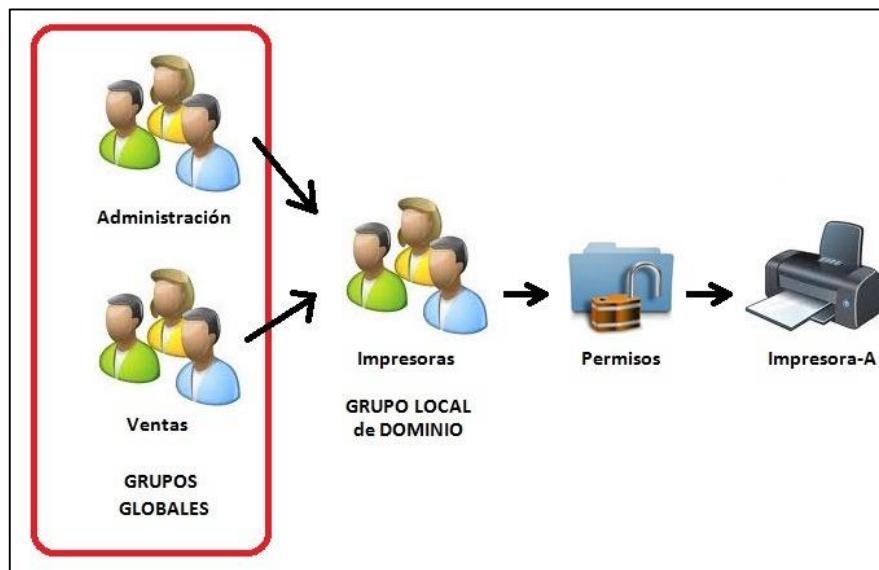
Si planeamos antes los grupos, podemos simplificar esta tarea administrativa rutinaria. Para hacerlo, deberemos crear un grupo de seguridad con ámbito local de dominio y asignarle los permisos necesarios para tener acceso a la impresora. Ahora añadimos a los 5 usuarios como miembros del nuevo grupo con lo cual podrán acceder a la impresora.

Si ahora deseamos dar a esos 5 usuarios acceso a una nueva impresora, basta con añadir a la lista de permisos de esa impresora el grupo local anteriormente creado (1 operación) y no añadir manualmente a los 5 usuarios (5 operaciones).

Además, si queremos que un usuario deje de poder usar las impresoras, bastará con sacar a dicho usuario del grupo, con lo que habremos conseguido que no pueda usar dichos recursos. Si no usamos grupos, no nos quedaría más remedio que ir impresora por impresora e ir quitándole los permisos al usuario por cada una de ellas.

Pero, ¿y si de necesitamos que estos 5 usuarios impriman en una impresora situada en otro dominio del bosque?

Para ello, en lugar de añadir los usuarios a un grupo local de dominio, lo conveniente es colocar las cinco cuentas de usuario en un grupo con ámbito global y agregar este grupo global como miembro del grupo local de dominio que da permisos sobre las impresoras. De este modo, conseguiremos que a nuestros usuarios se les pueda asignar permisos en cualquier dominio del bosque.



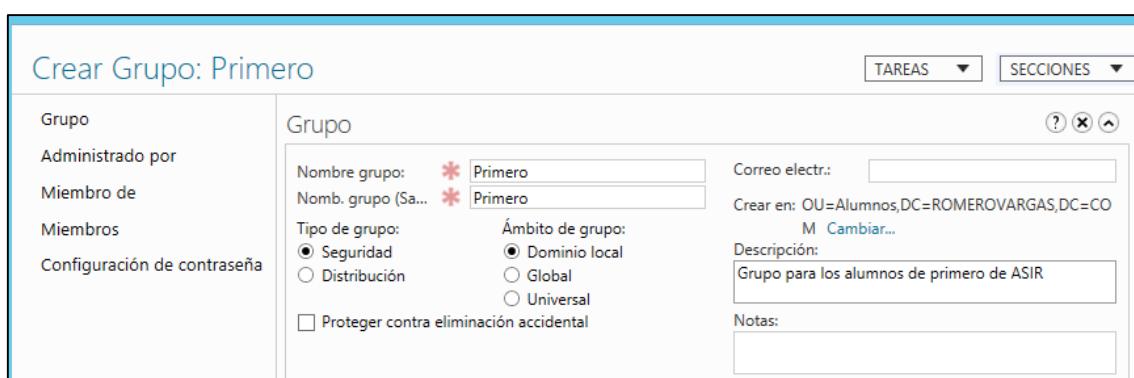
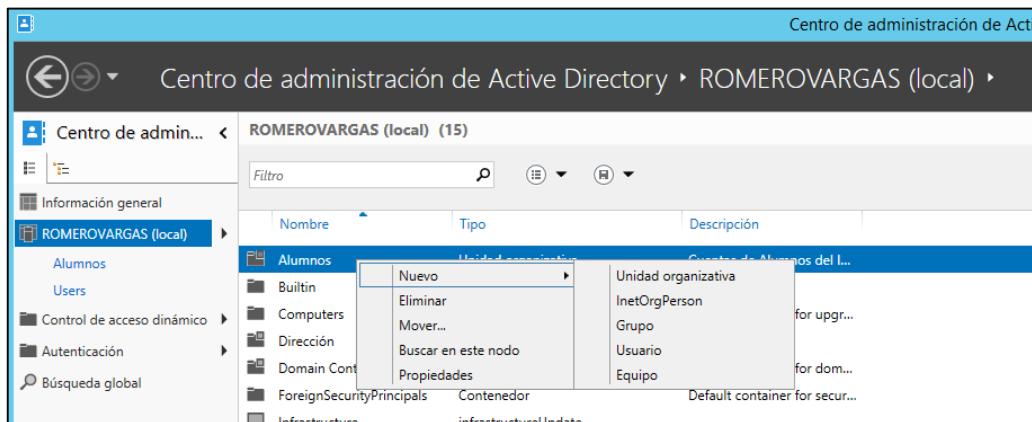
La estrategia que hemos visto aquí se conoce habitualmente como AGDLP, donde A indica Accounts (Cuentas de usuario) G indica grupos Globales, DL indica grupos locales de dominio (Domain Local) y P indica permisos. Es una forma de recordar la estrategia. (Las cuentas de usuario se meten en grupos globales, que a su vez se meten en grupos locales, que es a los que se les asigna los permisos).

Los grupos universales se usan únicamente cuando contamos con infraestructuras con múltiples dominios, y entonces se dice que usamos la estrategia AGUDLP (Cuentas → Grupos Globales → Grupos universales → Grupos Locales → Permisos).

### Gestión de grupos utilizando ADAC.

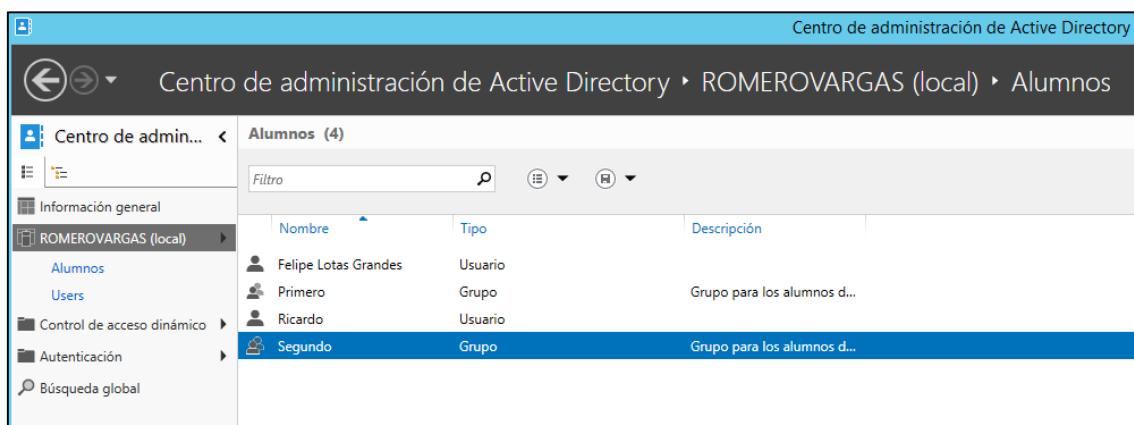
Igual que creábamos cuentas de usuario mediante botón derecho -> nuevo -> Usuario, podemos crear grupos seleccionando nuevo -> grupos.

Como ejemplo, creamos dos grupos de usuarios en Alumnos, uno llamado Primero y otro Segundo. Ambos grupos queremos que sean grupos de seguridad y de ámbito local de Dominio.

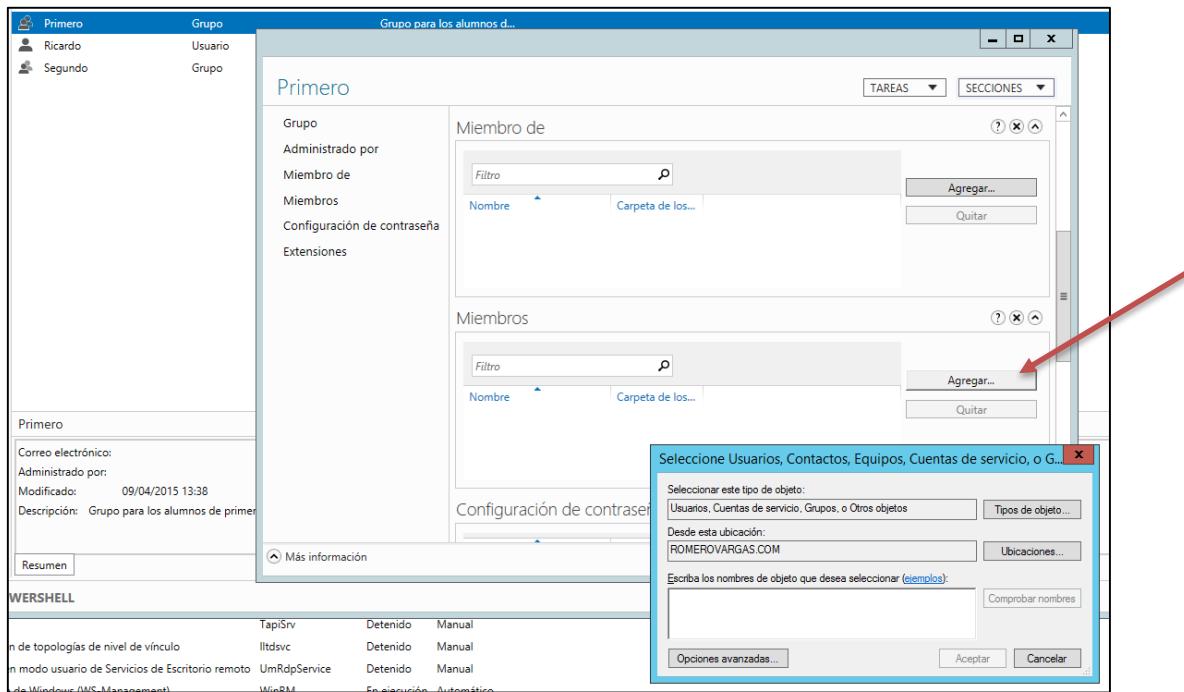


Vemos aquí las pantallas que nos permiten crear el grupo Primero. Haced lo mismo para Segundo.

En este momento nuestra OU Alumnos debería tener los siguientes miembros:



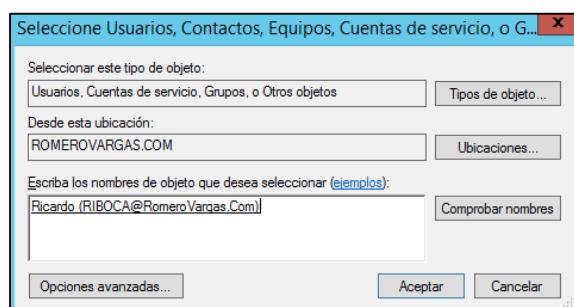
Ahora vamos a añadir a nuestros usuarios Felipe y Ricardo al grupo Primero. Esto lo podemos gestionando la cuenta de los usuarios y haciéndoles miembros del grupo, o gestionando la cuenta del grupo y añadiéndole miembros al mismo. Vamos a hacerlo directamente gestionando la cuenta del grupo Primero.



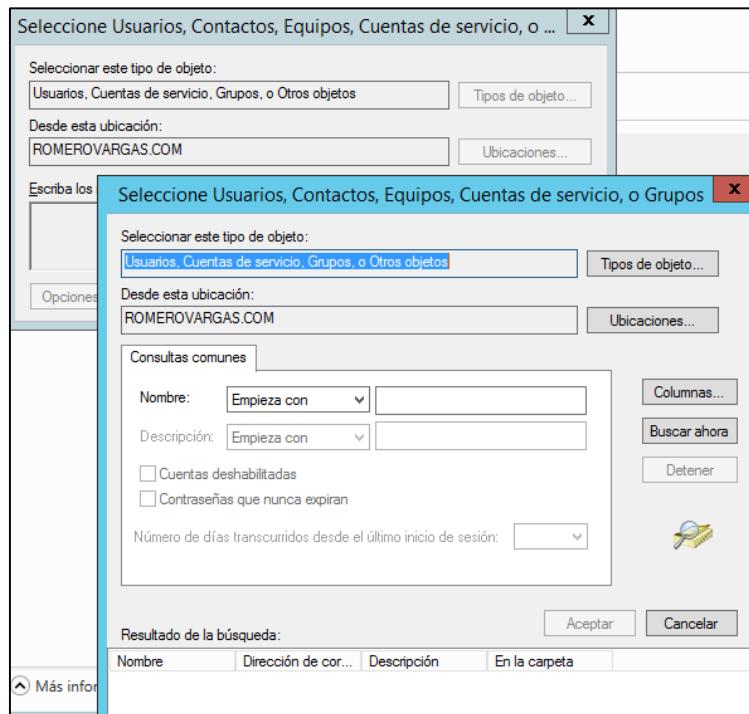
Desde la opción “Miembro de” añadiríamos al grupo primero como miembro de otro grupo, desde la opción “Miembros” indicamos los miembros que va a tener nuestro grupo. Seleccionamos Agregar en Miembros.

Nos aparecerá entonces el formulario de Selección de objetos, que es la pantalla que vemos en el ejemplo anterior. Podemos escribir directamente el nombre de un objeto en el cuadro de texto que nos presenta, y luego pulsar Comprobar nombres para asegurarnos de que encuentra el objeto. Si el objeto aparece subrayado es que lo ha encontrado sin problemas. Vamos a proceder a añadir a Ricardo como miembro de esta forma:

Vemos como al darle a Comprobar nombres automáticamente nos ha puesto el nombre completo de la cuenta y lo ha subrayado. Esto nos indica que ha encontrado el objeto. Ahora simplemente pulsamos Aceptar y ya habremos conseguido que Ricardo sea miembro del grupo Primero.



Ahora vamos a proceder a darle otra vez a Agregar, pero esta vez en el formulario de selección de objetos en lugar de escribir el nombre de Felipe, vamos a buscarlo. Para ello tendremos que pulsar en “Opciones avanzadas”.



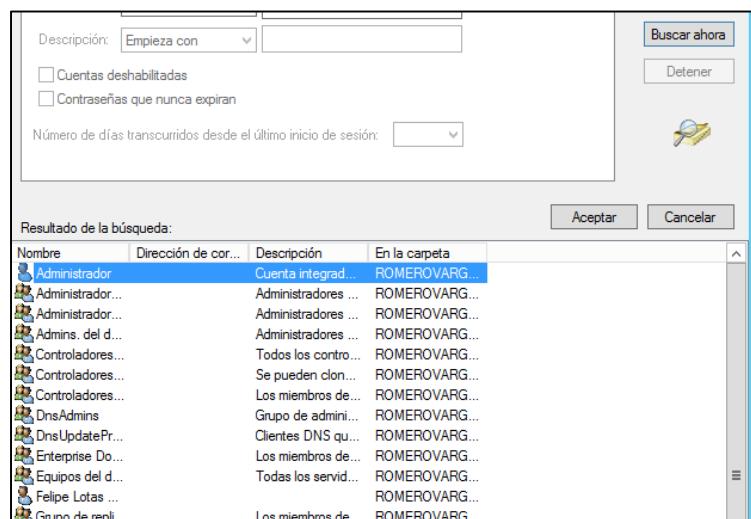
Desde aquí podemos buscar objetos según partes de su nombre, podemos seleccionar el tipo de objetos que queremos buscar (solo usuarios, solo grupos, etc.), podemos indicar la ubicación donde queremos buscarlos (en nuestro ejemplo al solo tener un dominio solo veremos RomeroVargas.Com pero más adelante tendremos más dominios y nos será muy útil esta opción).

Nosotros vamos a seleccionar “Buscar ahora” para que nos muestre todos los objetos disponibles.

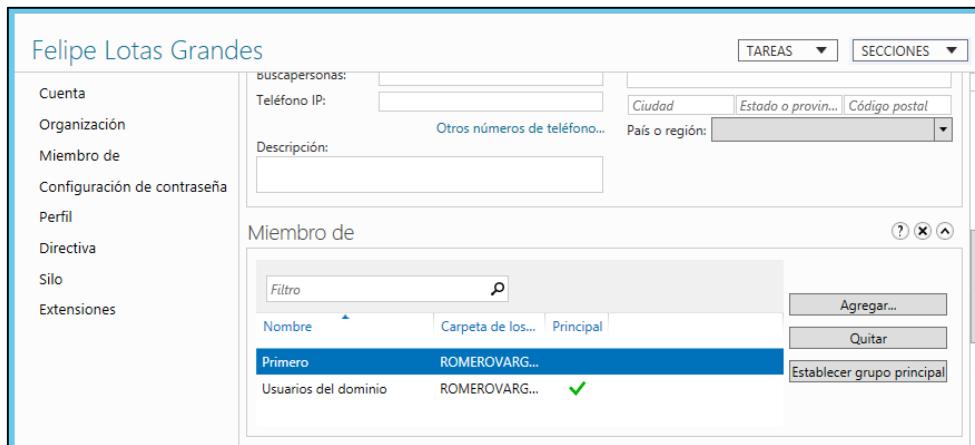
En la lista de objetos seleccionaremos a nuestro usuario Felipe. (Desde aquí podemos seleccionar varios objetos pulsando Control o Mayusculas mientras hacemos click con el ratón).

Una vez que seleccionemos la cuenta de Felipe pulsamos Aceptar.

Veremos como aparece ya Felipe en el formulario al igual que antes aparecía Ricardo, ahora simplemente pulsamos Aceptar de nuevo ya habremos conseguido que Felipe sea miembro de Primero.

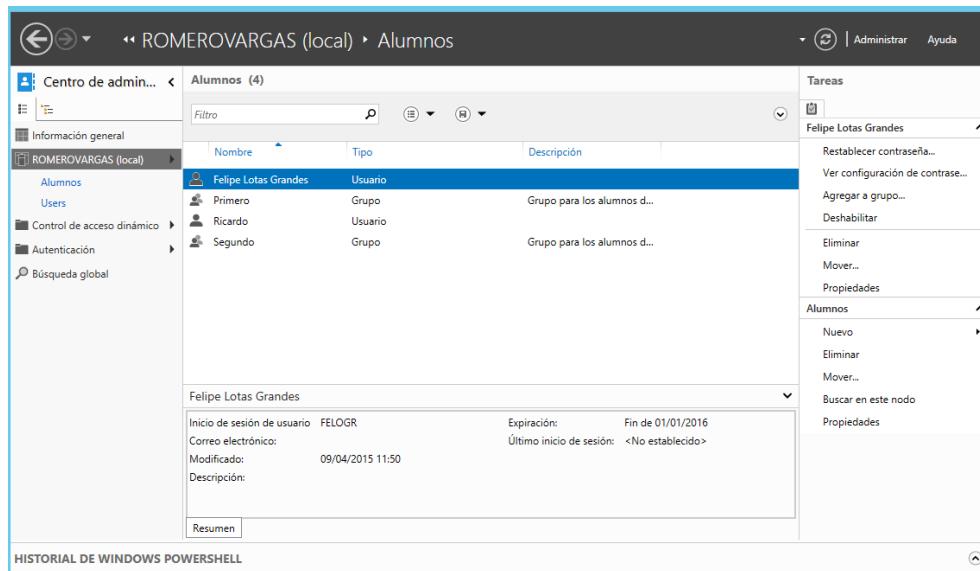


Iros ahora a las propiedades de nuestro usuario Felipe, y comprobar como en la parte de Miembro de nos aparece el grupo Primero. Veremos como también aparece un grupo Usuarios del dominio. Este es un grupo que se crea automáticamente y al que se le asignan todas las cuentas de usuario del dominio que vayamos creando. Además veremos cómo dicho grupo se considera el principal del usuario.



### Gestión de grupos utilizando PowerShell.

Vamos a proceder ahora a gestionar los grupos pero utilizando comandos PowerShell. En este momento ya hemos visto cuáles eran los comandos para crear usuarios, y si pensamos un poco podremos deducir qué comando es necesario utilizar para crear grupos, ya que sigue la misma estructura en el nombre de comando. Sin embargo, vamos a ver una forma mucho más simple de encontrar estos comandos de los que ni siquiera sabemos el nombre. Para ello vamos a echarle un vistazo a nuestra consola ADAC.



Si miráis en la parte inferior, veréis una opción “Historial de Windows PowerShell”. Pulsad en ella.

HISTORIAL DE WINDOWS POWERSHELL						
	Buscar	Copiar	Iniciar tarea	Finalizar tarea	Borrar todo	Marca de tiempo
Cmdlet						09/04/2015 13:38:43
☒	New-ADGroup					09/04/2015 13:40:03
	-Description:"Segundo de ASIR" -GroupCategory:"Security" -GroupScope:"DomainLocal" -Name:"Segundo" -Path:"OU=Alumnos,DC=ROMEROVARGAS,DC=COM" -SamAccountName:"Segundo" -Server:"WServ2012.ROMEROVARGAS.COM"					09/04/2015 13:40:14
☒	Set-ADGroup					09/04/2015 13:55:19
	-Description:"Grupo para los Alumnos de Segundo de ASIR" -Identity:"CN=Segundo,OU=Alumnos,DC=ROMEROVARGAS,DC=CO..."					
☒	Set-ADGroup					
	-Description:"Grupo para los alumnos de Segundo de ASIR" -Identity:"CN=Segundo,OU=Alumnos,DC=ROMEROVARGAS,DC=CO..."					
☒	Set-ADGroup					
	-Add:@{'Member'='CN=Ricardo,OU=Alumnos,DC=ROMEROVARGAS,DC=COM", "CN=Felipe Lotas Grandes,OU=Alumnos,DC=RO..."}					

Vemos como nos aparecen los últimos comandos que el sistema ha ejecutado. Daros cuenta que aunque nosotros hemos creado los grupos y hemos asignado los usuarios a los grupos usando el entorno gráfico, en realidad el sistema se ha limitado a ejecutar los comandos PowerShell necesarios para realizar dichas acciones.

Vemos así como por ejemplo para crear el grupo Segundo, se ha ejecutado el comando New-ADGroup. Pulsad ahora en el símbolo más (+) que aparece a la izquierda de dicho comando:

☒	New-ADGroup
	-Description:"Segundo de ASIR"
	-GroupCategory:"Security"
	-GroupScope:"DomainLocal"
	-Name:"Segundo"
	-Path:"OU=Alumnos,DC=ROMEROVARGAS,DC=COM"
	-SamAccountName:"Segundo"
	-Server:"WServ2012.ROMEROVARGAS.COM"

Ahí tenemos el comando exacto que se ha ejecutado, con todos sus parámetros. Deberíamos ser capaces de entenderlos todos sin problemas (si no es así, volved atrás y leed los apuntes desde el principio). Si tenemos problemas por el inglés hay muchos diccionarios online en Internet ;-).

Ahora que ya conocemos el comando, cread mediante PS dos grupos en la OU Profesores con nombres Técnicos y Prácticos, queremos que ambos sean de seguridad (a partir de ahora ya no lo especificaremos, los grupos siempre serán de seguridad) y de ámbito local de dominio.

Fijaros como en la parte superior de la ventana Historial de Windows PowerShell tenemos un botón de buscar y otro de Copiar. Si seleccionamos el comando completo y pulsamos copiar ya solo lo tendremos que pegar (botón derecho) en nuestra ventana del PS y posteriormente modificar lo que necesitemos.

Ahora cread un usuario en la OU Profesores con nombre Federico. Una vez creado, haced que Federico sea miembro del grupo Técnicos. Tenéis que hacedlo desde PowerShell y el comando que tenéis que usar lo buscáis en el histórico de ADAC, ya que no pienso ponerlo aquí. ;-)

### Delegación usando unidades organizativas.

Una de las razones para crear OU es para delegar el control de ciertas acciones de Administración a usuarios que no son Administradores.

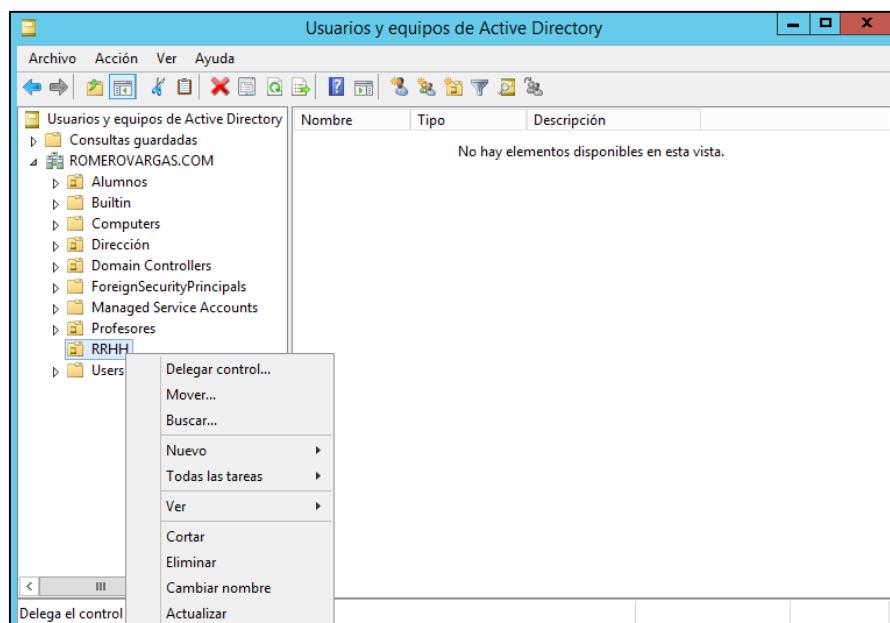
Imaginemos que en el departamento de recursos humanos de nuestra empresa tenemos 3 usuarios: Ana, Andrea y Amparo. Resulta que detectamos que tanto Andrea como Amparo tienen cierta tendencia a “olvidar sus contraseñas” por lo que continuamente se ponen en contacto con nosotros para que se las reseteemos. Si esto pasa muchas veces, llegará un momento que será un engorro para nosotros, y ahí es donde entran las delegaciones. Creamos una OU llamada RRHH y “metemos” dentro a Ana, Andrea y Amparo, y posteriormente deleo el poder de resetear contraseñas en la OU RRHH al usuario Ana. Es el único poder que le estoy dando, y solo se lo estoy dando para la OU RRHH.

Vamos a realizar este ejercicio en la práctica:

- 1) Cread tres cuentas de usuario con UPN Ana, Andrea y Amparo en el contenedor USERS.
- 2) Cread una OU con nombre RRHH
- 3) Moved las tres cuentas de usuario del punto 1 de USERS a RRHH
- 4) Cread un grupo local de dominio en RRHH con nombre ResetContrasRRHH
- 5) Meted a Ana como miembro del grupo recién creado

Ahora vamos a delegar el control de resetear contraseñas en RRHH al grupo ResetContrasRRHH (Fijaros cómo podríamos haber delegado el control directamente a Ana, sin tener que usar el grupo, pero es siempre recomendable hacerlo de esta forma. Hay un dicho en Administración de Sistemas que dice que las cuentas de usuario vienen y van, pero los grupos permanecen).

La consola ADAC que estamos usando no está del todo terminada, de hecho hay un par de cosas que no se pueden realizar aún desde la misma. Una de estas cosas es precisamente la delegación de una unidad organizativa. Para realizar esta acción necesitamos ejecutar la consola “antigua” que es la de Usuarios y Equipos de Active Directory.

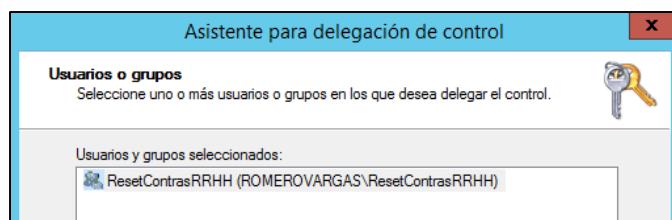


Vemos en la imagen anterior la consola de Usuarios y Equipos de Active Directory abierta, y vemos como al pulsar botón derecho sobre la OU RRHH nos aparece como primera opción la de “Delegar Control”.

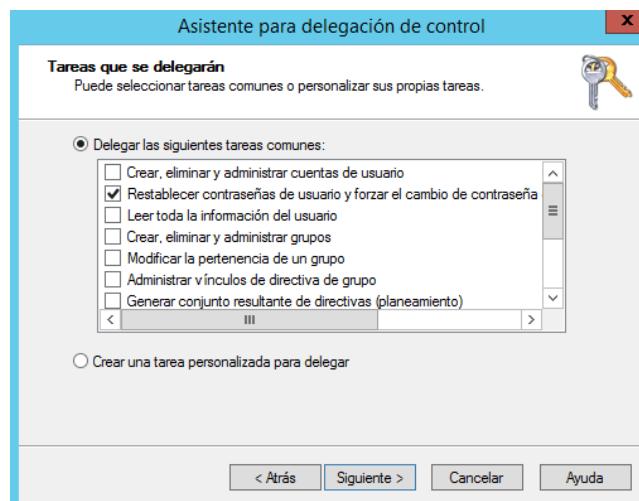
Al pulsar sobre dicha opción nos aparece el asistente para la Delegación de Control.



En dicho asistente tendremos que seleccionar el usuario o grupo al que vamos a delegar, y en nuestro ejemplo seleccionamos el grupo ResetContrasRRHH.



Una vez seleccionado el grupo, pulsamos siguiente y nos preguntará que permisos vamos a delegarle a dicho grupo. En nuestro caso tenemos que delegarle únicamente el permiso para restablecer contraseñas.

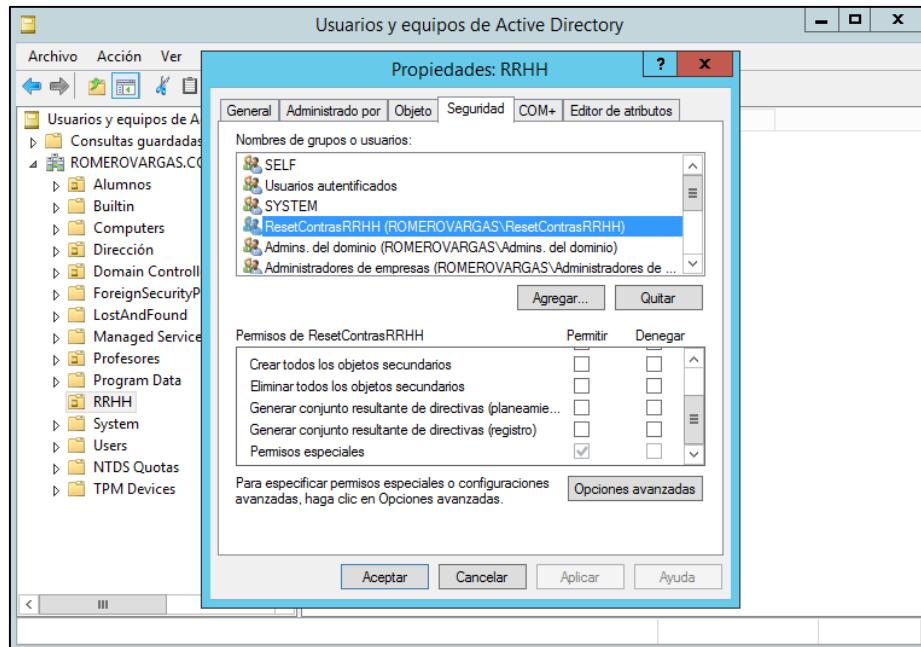


Al pulsar siguiente nos presentará un resumen de lo que vamos a realizar. Confirmar dicho resumen y ya habremos realizado nuestra delegación.

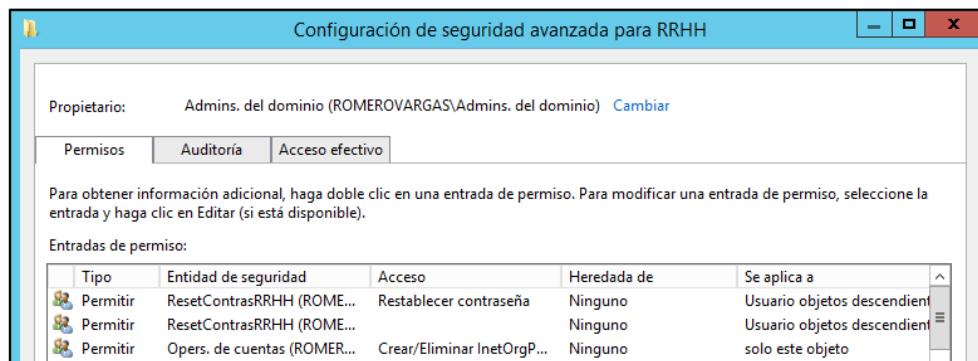
Si vemos la imagen anterior veremos cómo podemos asignar muchas tareas distintas de administración mediante delegación, pero todavía podemos hacer un control más fino de las delegaciones.

Abrid Usuarios y Equipos de Active Directory (ADUC) y pulsar en Ver -> Características Avanzadas. Comprobad como ahora vemos muchos más elementos que antes en ADUC.

Ahora damos botón derecho sobre la OU RRHH y escogemos Propiedades. Una vez en propiedades nos vamos a la pestaña Seguridad.



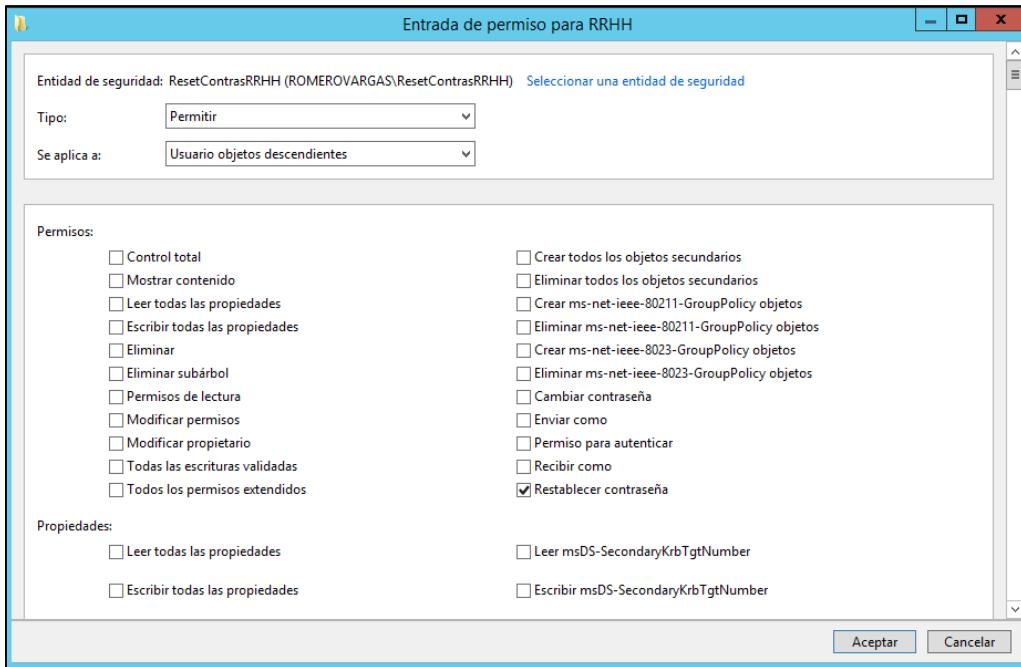
Vemos como nos aparece una entrada en la ACL de RRHH indicando que el grupo ResetContrasRRHH tiene permisos especiales (esta es la delegación que acabamos de llevar a cabo). Como esto no nos dice mucho, pulsad sobre Opciones avanzadas, para ver los permisos en más detalle.



Como vemos, desde aquí si podemos comprobar que el permiso que se la ha asignado a ResetContrasRRHH es el de Restablecer contraseña.

Veremos dos entradas del grupo, una sin permisos (que se crea al delegar directamente) y otra con permisos que se crea una vez que hemos establecido dichos permisos.

Dadle ahora doble clic en la entrada del grupo donde vemos el permiso de Restablecer contraseña. Veremos una pantalla como la siguiente:



Vemos como ahora si vemos muchísimos más permisos que podemos delegar de nuestra UO, y vemos además como tenemos una barra de desplazamiento vertical que nos permite ver aún más opciones de delegación. En total se pueden delegar más de 10.000 permisos para una única OU, y eso contando solo los permisos de Permitir.

Aprovechando que tenemos abierta ADUC (Active Directory Users and Computers, Usuarios y Equipos de Active Directory) vamos a hacer un ejercicio completo que hemos venido realizando bien desde ADAC o bien desde PowerShell, pero utilizando ahora ADUC.

#### Ejercicio:

- Cread un dominio llamado BETTY.BOOP que contará con un DC (Domain Controller, controlador de dominio) con nombre Server1201 con dirección IP 192.168.221.1.
- Cread una OU llamada CONTABILIDAD y dentro las cuentas de usuario de Pedro, Pablo y Paula.
- Cread una OU llamada VENTAS y dentro las cuentas de Sergio y Samanta.
- Cread una OU llamada ALMACEN y dentro las cuentas de Ramiro, Rodolfo y Raimunda.
- Cread un grupo CONTABLES e introducid dentro a Pedro, Pablo y Paula.
- Cread un grupo local de dominio VENDEDORES e introducid dentro a Sergio y Samanta.
- Cread un grupo local de dominio ALMACENEROS e introducid dentro a Ramiro, Rodolfo y Raimunda.
- Cread un grupo global de dominio PLANTILLA e introducid dentro a Pedro, Paula, Sergio, Samanta, Ramiro y Raimunda.
- Cread un grupo global de dominio PRÁCTICAS e introducid dentro a Pablo y a Rodolfo.
- Delegad a Pedro para que pueda cambiar las contraseñas de Pablo y de Paula.
- Delegad a Ramiro para que pueda borrar y crear cuentas de usuarios en ALMACEN.

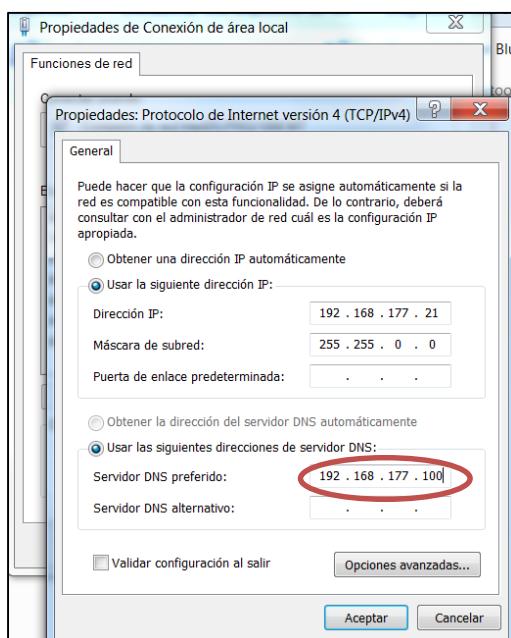
### Conexión de clientes al dominio.

En primer lugar vamos a crear un dominio para poder conectarnos al mismo. Cread un dominio con nombre ROMEROVARGAS.COM, con un DC llamado WServ2012 con IP 192.168.177.100/16.

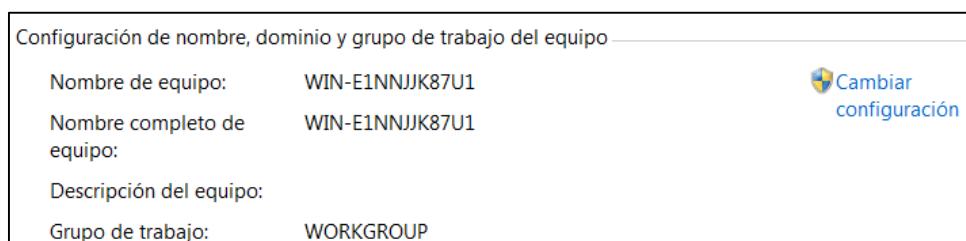
Para comprobar si nuestro recién estrenado dominio funciona correctamente, vamos a añadir a nuestro servidor algunos clientes. Para ello, debemos tener en red local algunos equipos con un sistema operativo que permita conexión a dominios (en la actualidad, prácticamente todos) e indicarles que pasen a trabajar dentro del dominio.

Veamos cómo hacerlo en un Windows 7:

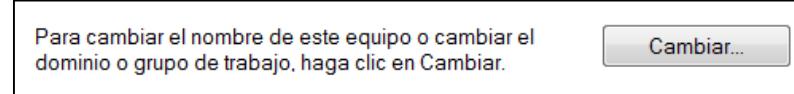
- 1) En primer lugar tenemos que indicar a nuestro Windows 7 que utilice el servidor DNS que ha montado nuestro dominio. En nuestro ejemplo, en las propiedades de Red de XP debemos indicar que use como servidor DNS único la dirección IP de nuestro Controlador de Dominio.



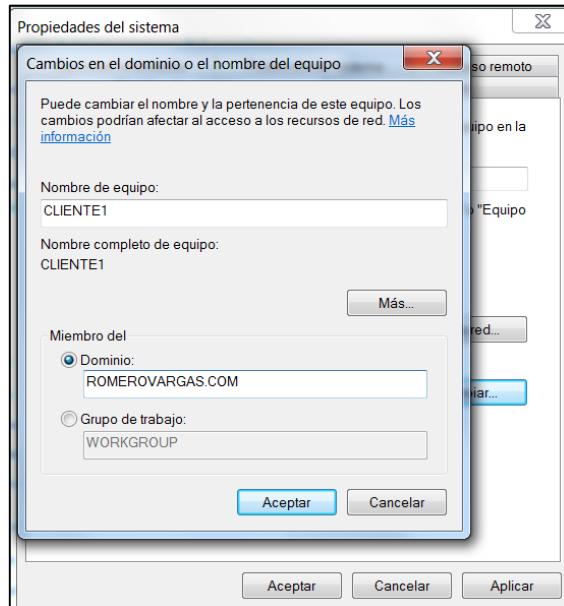
- 2) Accedemos propiedades del sistema (Windows + Pausa) y desde allí entramos en Cambiar configuración para poder cambiar el nombre de equipo y el grupo de trabajo.



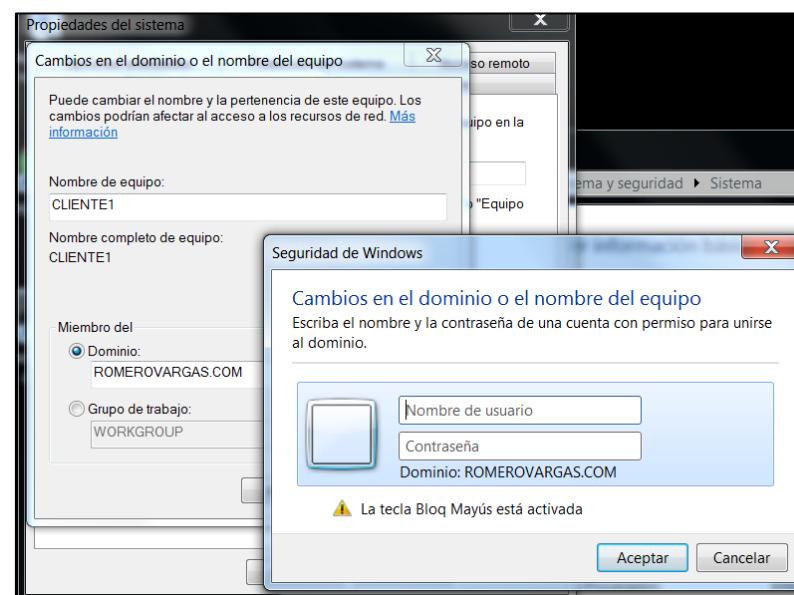
- 3) Vemos como nos indica la pantalla que para unirnos a un dominio hagamos clic en Cambiar.

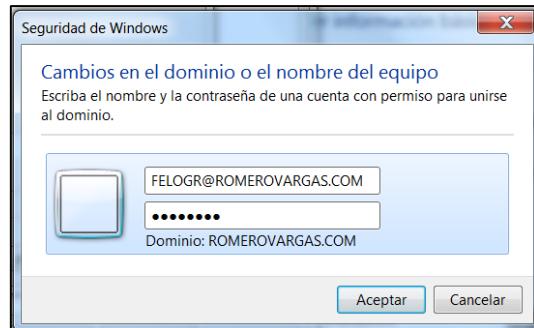


- 4) Desde aquí ponemos un nombre al equipo adecuado y a continuación escribimos el nombre FQDN (nombre DNS) del DOMINIO al que queremos conectarnos y le damos clic a Aceptar. (Si nos indica que no encuentra el dominio, revisar el paso 1).

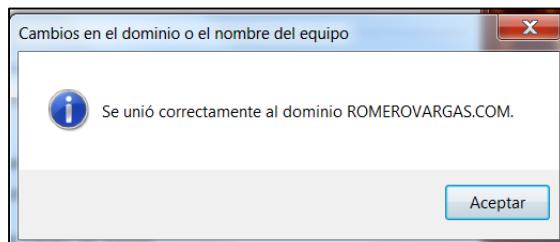


- 5) El cliente se pondrá en comunicación con el DC del dominio y nos pedirá un nombre de usuario y contraseña para demostrar que tenemos credenciales suficientes como para unirnos al dominio. Este usuario debe ser usuario del dominio (no hace falta que sea administrador) creado desde el Controlador de Dominio ADAC, ADUC o PowerShell.





- 6) Si todo funciona bien, recibiremos un mensaje de “Bienvenido al dominio” y nos pedirá que reiniciemos la máquina.



- 7) A partir de ese momento, podremos iniciar sesión en nuestro cliente, tanto de forma individual (usaremos la maquina fuera del dominio con sus usuarios locales), como formando parte del dominio (usando la maquina dentro del dominio con sus usuarios de dominio).

Un primer cambio que notaremos en el cliente es que utiliza el inicio seguro, obligándonos a pulsar una combinación de teclas para iniciar sesión, y desapareciendo la pantalla de bienvenida que veíamos antes de unirnos al dominio.

Presione Ctrl+Alt+Supr para iniciar una sesión

Las cuentas de usuario que indiquemos para abrir sesión pueden ser locales (se iniciará la sesión de modo local) o de dominio (se iniciará la sesión en modo dominio).



En la imagen anterior vemos como usuario1 es un usuario local de CLIENTE1, que es el nombre de la máquina local. Si introducimos la contraseña de usuario1 iniciaremos sesión fuera del dominio, solo en local. Si queremos abrir sesión en el dominio tendremos que pulsar sobre Cambiar de usuario.



A continuación pulsamos sobre Otro usuario.

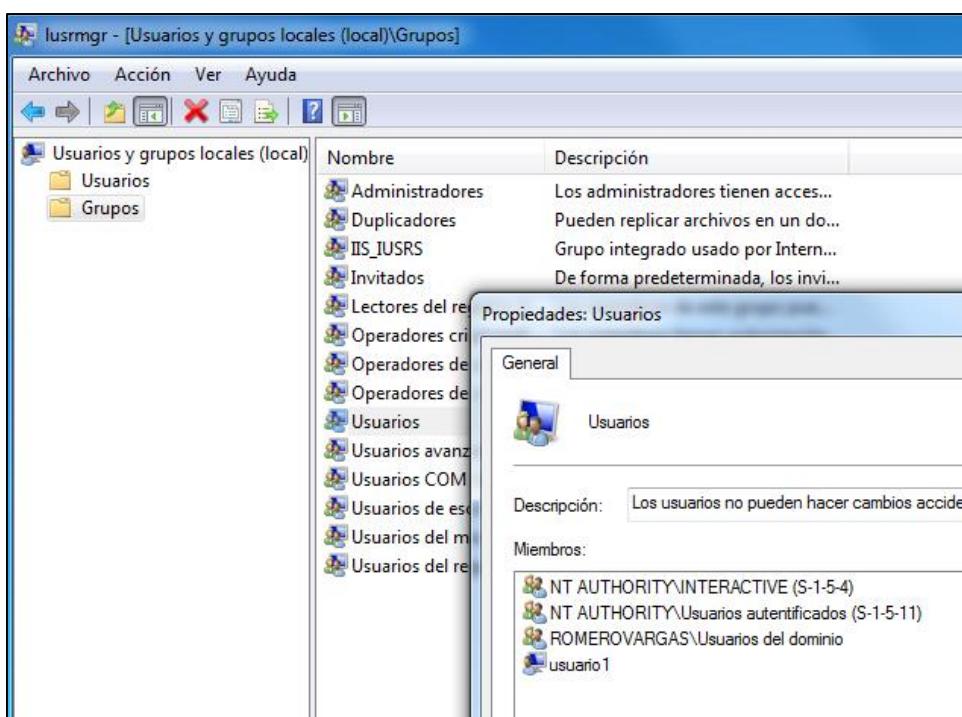
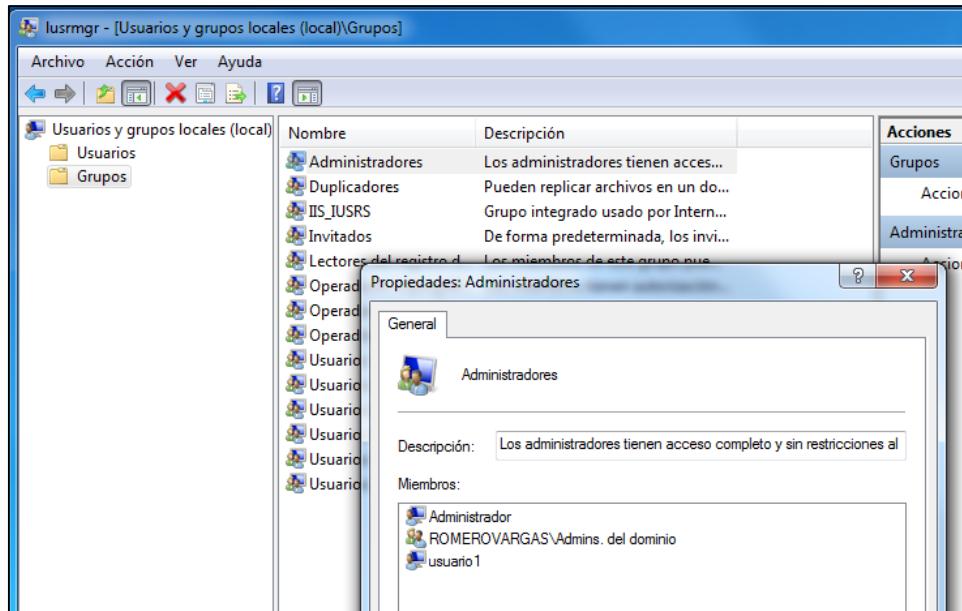


Introducimos el nombre de usuario que queremos utilizar indicándole que es del dominio (con la arroba seguida del nombre del dominio). Ahora ya cuando pulsemos la flecha hacia la derecha para iniciar sesión abriremos dicha sesión en el dominio. Esta cuenta de usuario no estará creada en el equipo local, sino que estará almacenada en el DC del dominio.

La forma de conectarnos que hemos visto es la del Windows 7 pero es prácticamente idéntica a la forma en que se conectan todos los sistemas operativos Windows. La forma de conexión de máquinas con sistemas operativos no Windows es también muy parecida, pero con particularidades en cada SO.

Hemos visto como el equipo una vez conectado al dominio tiene la posibilidad de abrir sesión fuera del dominio, abriendo sesión en el propio equipo. Si no queremos que esto suceda simplemente tenemos que eliminar todas las cuentas de usuario locales del equipo cliente y dejar únicamente la cuenta de administrador local, con una contraseña evidentemente que no conozcan los usuarios de ese equipo. De este modo, obligaremos a que los usuarios solo puedan abrir sesión usando su cuenta de dominio. Por regla general, una vez establecido el dominio todas las personas reciben una cuenta de usuario de dominio, y se evita el trabajar con cuentas locales.

Una de las acciones que se llevan a cabo automáticamente cuando conectamos un equipo a un dominio, es que se integra al grupo “Admins. Del dominio” como miembro del grupo local de la máquina “Administradores”, también se integra al grupo “Usuarios del dominio” como miembro del grupo local de la máquina “Usuarios”. Esto permite que cualquier usuario del dominio es automáticamente usuario de esa máquina, y que cualquier administrador del dominio es automáticamente administrador de esa máquina.



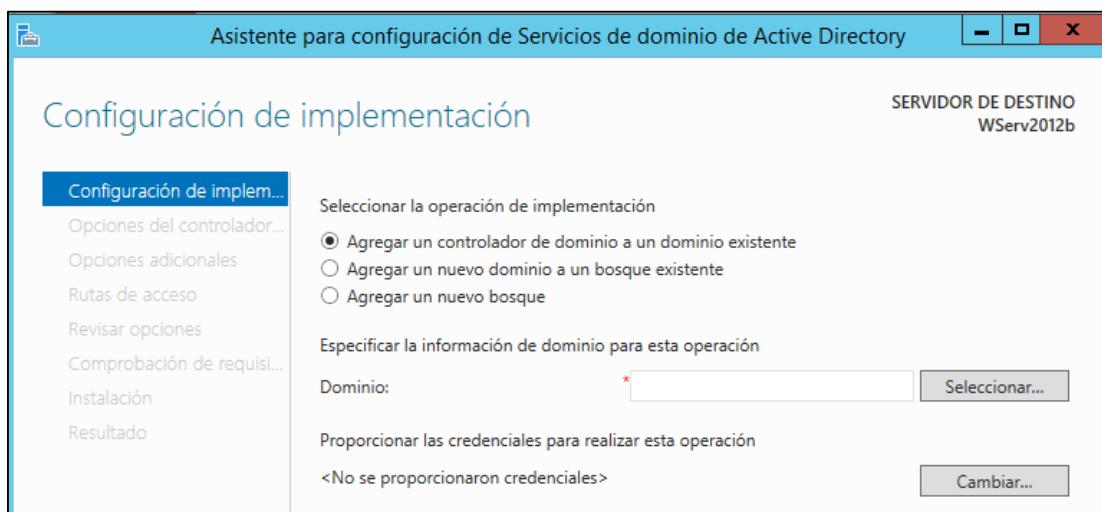
### Instalación de un controlador de dominio adicional.

Si tenemos un dominio de gran tamaño con cientos de máquinas conectadas al mismo, no es aconsejable que todo dependa de un único servidor. Un fallo en este equipo sería catastrófico para toda la infraestructura. En casos así, es aconsejable instalar varios servidores, es decir, contar con varios controladores de dominio en un único dominio.

En versiones anteriores de Windows Server teníamos que establecer controladores de dominios principales y secundarios, pero desde Windows 2003 no es necesario hacer esta diferenciación. Todos los controladores funcionan al mismo nivel y trabajan entre sí de forma automática.

Vamos a realizar ahora la incorporación de un nuevo DC a nuestro dominio, para ello:

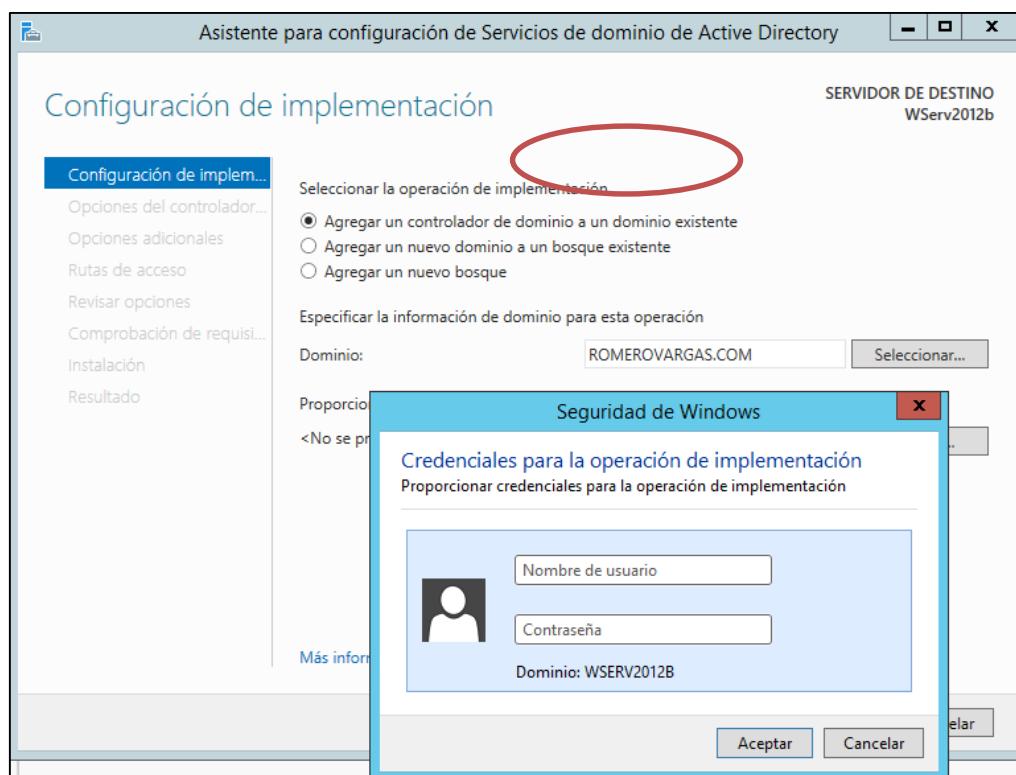
- 1) Debemos contar con un dominio ya creado y con un DC correctamente configurado
- 2) En una nueva máquina con Windows Server indicamos que queremos usar como servidor DNS la dirección del DNS del dominio. También debemos controlar que este equipo cuente con una IP fija y con un nombre de equipo adecuado. No hace falta añadir esta máquina como cliente del dominio. Una buena prueba para asegurarnos de que tenemos el nuevo equipo bien configurado es realizando un PING desde este nuevo equipo al nombre del dominio (RomeroVargas.Com por ejemplo) y comprobando como nos responde con la IP del DC inicial.
- 3) Promocionamos esta nueva máquina a servidor de dominio como hemos visto anteriormente. Recordar que tenemos que instalar ADDS en el servidor nuevo antes de que podamos promocionarlo a DC.
- 4) En este momento el sistema comenzará a hacernos preguntas para saber dónde queremos instalar nuestro DC. Elegimos agregar un controlador de dominio a un dominio existente.



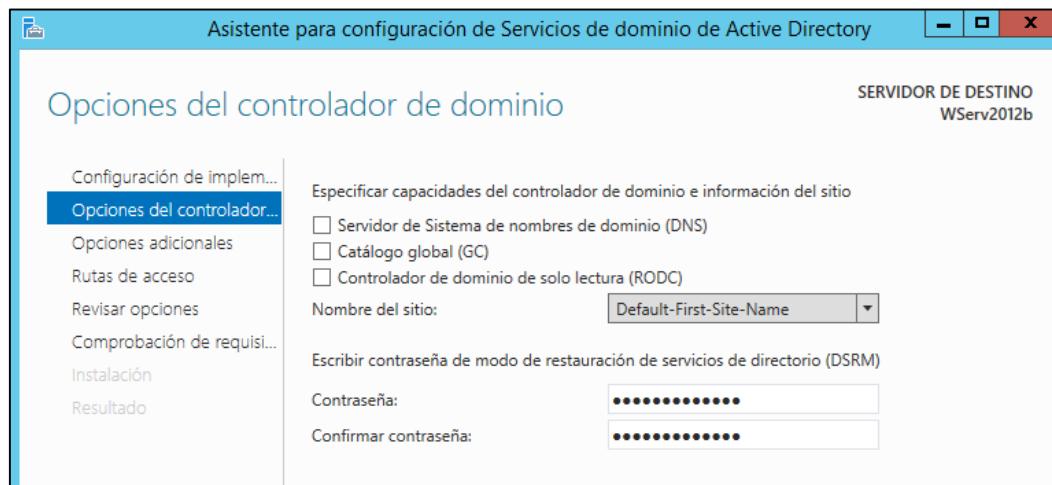
- 5) En el mismo formulario, justo debajo, el sistema nos pedirá que introduzcamos el nombre FQDN (nombre completo DNS) del dominio al que queremos conectarnos como DC adicional.



- 6) Cuando le demos a seleccionar el dominio, tendremos que introducir unas credenciales, es decir, un nombre de usuario y contraseña del dominio donde queremos conectarnos. Obviamente ya que queremos instalar un Controlador de Dominio, la cuenta que usemos debe tener permisos de administrador del domino, ya que no estamos añadiendo un simple equipo, sino un DC completo.

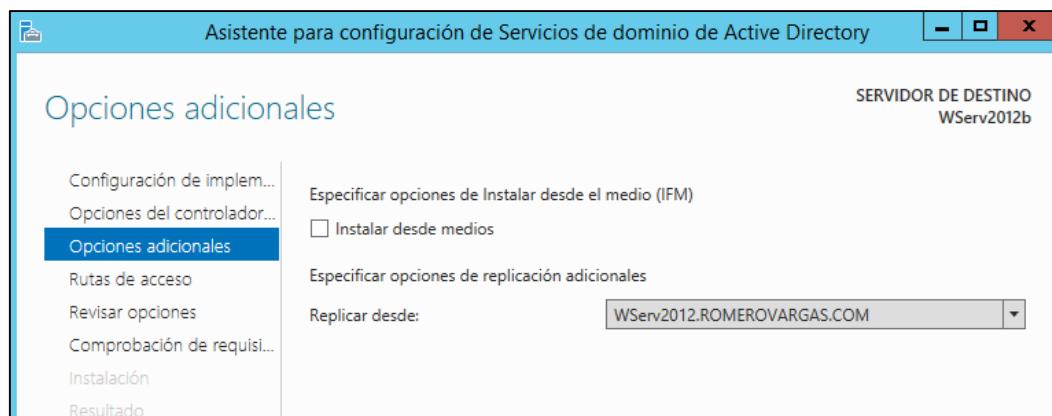


- 7) A continuación, y si la cuenta introducida es reconocida como admin. del dominio, continuará la instalación del DC tal como ya vimos en puntos anteriores. Mucho cuidado que por defecto la cuenta de usuario que introduzcamos se buscará en el equipo nuevo (fijaros en lo que pone en Dominio: en el formulario). Por eso es conveniente escribir el nombre UPN completo del usuario.
- 8) Es importante indicar que en este caso que estamos tratando el servidor DNS ya está instalado en la red, por lo que no tendremos que instalarlo ni recibiremos ningún mensaje de error sobre el mismo como si obtuvimos al instalar el primer DC. Hay que desmarcar pues la opción de instalar DNS y también podemos desmarcar si queremos la opción de Catalogo Global, puesto que dicho catalogo ya está instalado en DC inicial.



Ojo, en este ejemplo no instalamos DNS puesto que solo vamos a tener un DNS en el dominio que ya está instalado en el DC inicial, podemos encontrarnos otros casos donde si queramos instalar varios DNS en el dominio y donde esta opción habría que dejarla marcada. Lo mismo pasa con el Catalogo Global, que de hecho en la mayoría de las ocasiones querremos que este instalado en todo los DC si solo tenemos un dominio.

- 9) En la siguiente pantalla del asistente se nos da la opción para variar el medio de instalación (lo dejamos como está) y para indicar de que DC vamos a “pillar” los datos para replicarlos (cuentas de usuario, grupos, etc). Escogemos el DC inicial.



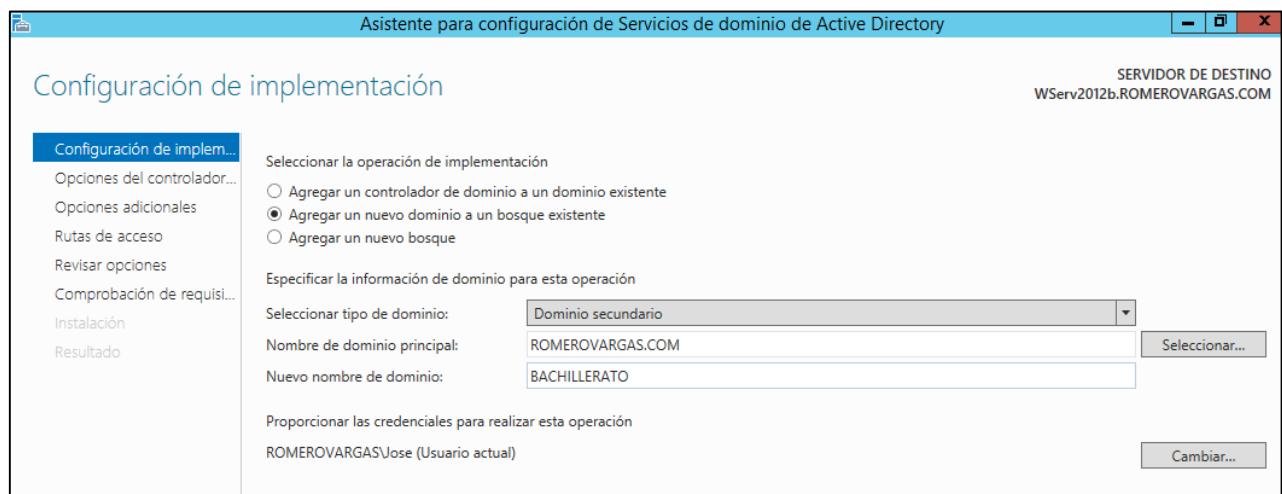
- 10) Escogemos las opciones de ubicación de la BD NTDS y de la carpeta SYSVOL, como explicamos anteriormente.

En este punto ya habremos instalado un Controlador de Dominio adicional a nuestro dominio, de modo que contaremos con dos servidores en el mismo dominio. Para ello el DC 1 tiene que enviar ahora toda la información del dominio al DC 2 (replicación) y a partir de ahora cualquier cambio que hagamos en uno de ellos será inmediatamente replicado en el otro.

### Instalación de un nuevo dominio en un bosque existente.

En este caso vamos a crear una “rama” de un árbol ya existente. Vamos a instalar un dominio nuevo pero que “cuelga” de un dominio ya existente.

Todos los pasos anteriores son válidos, la primera diferencia la encontraremos en el punto 4. En este caso debemos indicar igualmente que queremos crear un dominio en un bosque ya existente, pero no debemos indicar que queremos agregar un controlador de dominio adicional a un dominio ya existente. Para ello escogemos la opción de “Aregar un nuevo dominio a un bosque existente”.



En tipo de dominio tenemos que seleccionar Dominio secundario, ya que vamos a crear una rama hija de un dominio principal. El nombre del dominio principal será el “padre” de nuestro dominio, en nuestro ejemplo RomeroVargas.Com y el nuevo nombre de dominio será el nombre del dominio que vamos a crear, en nuestro caso Bachillerato. En este ejemplo el nombre FQDN completo de nuestro nuevo dominio será Bachillerato.RomeroVargas.Com.

Una cuestión importante es el nivel de credenciales de este comando, es decir, el tipo de usuario que vamos a utilizar para realizar esta operación. No es suficiente como en el caso anterior un miembro del grupo administradores del dominio, ya que estos “mandan” sobre el dominio ROMEROVARGAS.COM pero no sobre el árbol completo. Nos hace falta una cuenta con permisos aún mayores, y esto lo conseguimos con una cuenta de usuario que sea miembro del grupo “Administradores de Empresas.”

Nombres coincidentes:		
Nombre	Descripción	En la carpeta
Administradores		ROMEROVARGAS.COM,
Administradores de empresas	Administradores designados de la empresa	ROMEROVARGAS.COM,
Administradores de esquema	Administradores designados del esquema	ROMEROVARGAS.COM,
Administradores de Hyper-V		ROMEROVARGAS.COM,
Admins. del dominio	Administradores designados del dominio	ROMEROVARGAS.COM,

Una vez pasado este punto, el asistente nos irá pidiendo los datos necesarios para crear un nuevo dominio, tal como vimos anteriormente.

Una decisión importante que tenemos que tomar es si creamos un servidor DNS en este nuevo dominio o si preferimos utilizar el DNS que se instaló en el primer DC que instalamos. De momento vamos a indicar que NO queremos que instale su propio DNS, y por lo tanto seguiremos usando el ya creado.

Con respecto al Catalogo Global, a este primer DC del dominio Bachillerato vamos a decirle que sí, que lo instale.



Una vez reiniciado el servidor contaremos con 2 dominios en un árbol, cada uno será el único DC de su propio dominio.

### Crear un nuevo bosque.

Es muy parecido al punto anterior, ya que también crearemos un nuevo DC, pero en este caso, en vez de crear una rama en un árbol ya existente, crearemos la raíz de un nuevo árbol en un bosque ya existente, es decir, en un bosque donde ya existe un DC que forma la raíz de otro árbol.

Esto lo conseguiremos escogiendo en primer lugar la opción “Aregar un nuevo dominio a un bosque existente” igual que en el punto anterior, pero en lugar de escoger la opción de Dominio secundario en “Tipo de Dominio” escogeríamos la opción de Dominio principal, con lo que creariamos una raíz de un nuevo arbol en nuestro bosque.

Esta opción es muy poco usada, y muy difícil de ver en la realidad, así que no vamos a tratarla en profundidad.

## Instalación de active directory en Windows anteriores a 2012.

Siguiendo el patrón de un asistente estándar, la instalación de Active Directory en un servidor es una cuestión de responder a las solicitudes en una secuencia de pantallas. Windows Server incorpora vínculos al asistente en la página de Active Directory de la página principal de Configurar el servidor de Windows Server. Esta página se muestra en el explorador Microsoft Internet Explorer automáticamente después de la instalación del SO. Esta página Web local está diseñada para guiar al administrador a través de los procesos necesarios para configurar un nuevo servidor mediante preguntas al estilo de los asistentes y vínculos a las herramientas apropiadas para cada tarea.

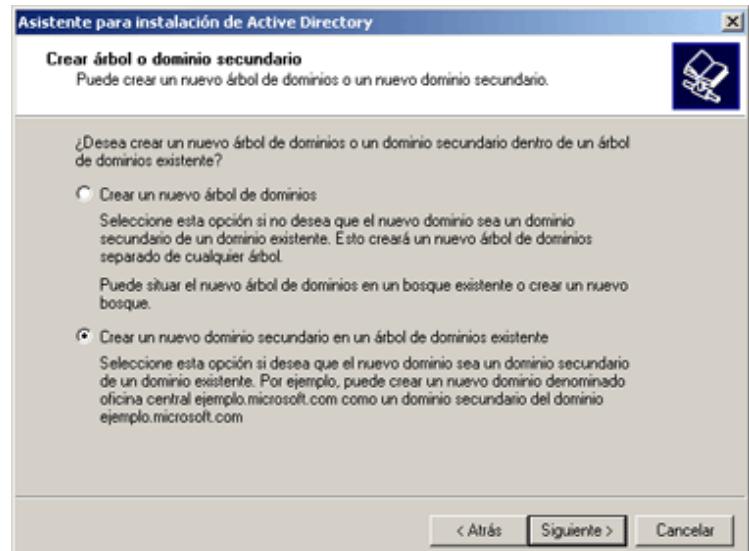
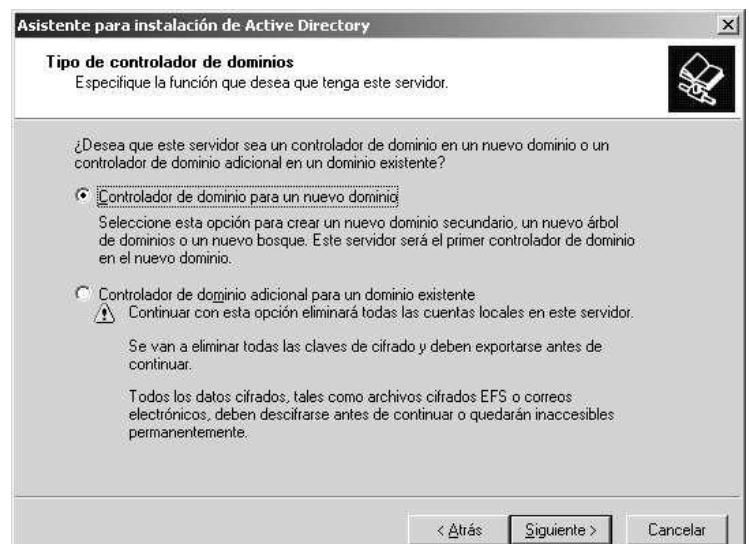
(Atención, en estos apuntes utilizamos imágenes procedentes de Windows 2000. Aunque hay algunas diferencias con Windows Server 2003 y Windows Server 2008 básicamente son iguales en el fondo).

Para instalar el Primer controlador deberemos seguir los siguientes pasos:

Iniciar la Herramienta Configuración del Servidor desde el menú de Herramientas Administrativas. También puede iniciar el asistente directamente ejecutando el archivo ejecutable **Dcpromo.exe** desde el cuadro de dialogo Ejecutar.

Después de una pantalla de bienvenida, el Asistente para instalación pregunta sobre la acción que se va a realizar, basándose en el estado actual de Active Directory en el sistema. Si el servidor ya es un controlador de dominio, el asistente solo proporciona la opción de degradar el sistema de nuevo a servidor independiente o miembro. En un equipo que no es un controlador de dominio, el asistente muestra la pantalla Tipo de controlador de dominios, la cual pide que se seleccione una de las siguientes opciones:

- Controlador de dominio para un nuevo dominio: Instala Active Directory en el servidor y lo designa como el primer controlador de dominio de un nuevo dominio.



- Controlador de dominio adicional para un dominio existente: Instala Active Directory en el servidor y replica la información del directorio desde un dominio existente.

Para instalar el primer servidor Active Directory en la red, se selecciona la opción **Controlador de dominio para un nuevo dominio**. Esto hace que el asistente instale los archivos de soporte de Active Directory, cree el nuevo dominio y lo registre en el DNS

**Crear un árbol o unirse a un árbol.** Deberemos elegir el tipo de dominio que queremos configurar de las dos opciones que se presentan en el siguiente cuadro.

- Crear un nuevo árbol de dominios: Configura el nuevo controlador de dominio para que aloje el primer dominio de un nuevo árbol. Esta es la opción que debemos escoger para instalar nuestro primer servidor.
- Crear un nuevo dominio secundario en un árbol de dominios existente: Configura el nuevo controlador de dominio para que aloje un hijo de un dominio de un árbol que ya existe.

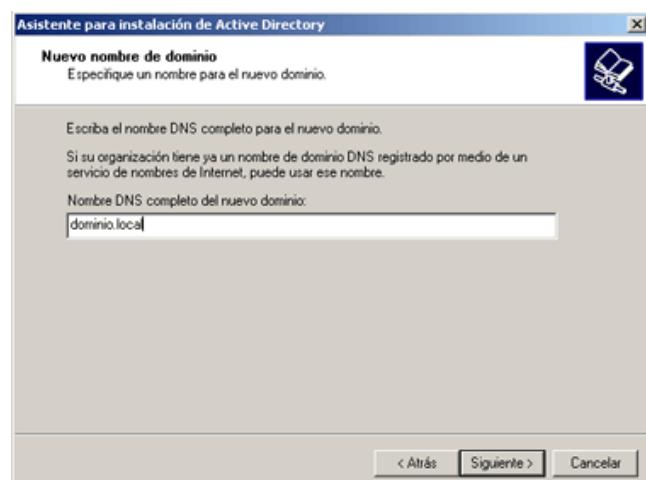
**Crear un bosque o unirse a un bosque**, que permite especificar una de las siguientes opciones:

- Crear un nuevo bosque de árboles de dominios: Configura el controlador de dominio para que sea la raíz de un nuevo bosque de árboles.
- Situar este nuevo árbol de dominios en un bosque existente: Configura el controlador de dominio para que aloje el primer dominio de un nuevo árbol en un bosque que ya contiene uno o más árboles.

En este caso hay que seleccionar Crear un nuevo bosque de árboles de dominios, porque el primer controlador de dominio Windows 2000 de la red será siempre un nuevo dominio, en un nuevo árbol, en un nuevo bosque. A medida que se instalen controladores de dominio adicionales, se pueden utilizar estas mismas opciones para crear otros bosques nuevos o para poblar el bosque existente con árboles y dominios adicionales.

**Nombre de nuevo Dominio:** Para identificar el controlador de dominio en la red se debe especificar un nombre DNS válido para el dominio que se está creando.

Este nombre no tiene por qué ser el mismo que el del dominio que utiliza la empresa para su presencia en Internet (aunque puede serlo). El nombre tampoco tiene que estar registrado en el Centro de información de redes de Internet (InterNIC, Internet Network información), la organización responsable de mantener el registro de los nombres DNS en los dominios de nivel superior com, net, org y edu. Sin embargo, el uso de un nombre de dominio registrado es una buena idea si los usuarios de la red van a acceder a los recursos de Internet al mismo tiempo que a los recursos de red locales, o si los usuarios externos a la organización accederán a los recursos de red locales vía Internet.



**Nombre de dominio NetBIOS.** Después de introducir un nombre DNS para el dominio, el sistema solicita un equivalente NetBIOS para el nombre del dominio para que los utilicen los clientes antiguos que no soporten Active Directory.

Los sistemas Windows Server todavía utilizan el espacio de nombres NetBIOS para sus nombres de equipo, pero Active Directory utiliza la nomenclatura DNS para los dominios. Windows NT 4 y los sistemas Microsoft Windows 9x utilizan nombres NetBIOS para todos los recursos de la red, incluyendo los dominios.

Si se dispone de clientes de nivel inferior en la red (esto es, Windows NT 4, Windows 9x, Microsoft Windows para Trabajo en grupo o Cliente de red Microsoft para sistemas MS-DOS), estos solo serán capaces de ver el nuevo dominio por medio del nombre NetBIOS. La pantalla Nombre de dominio NetBIOS contendrá una sugerencia para el nombre, basándose en el nombre DNS especificado, que se puede utilizar o bien se puede reemplazar con un nombre que se elija que tenga 15 caracteres o menos.

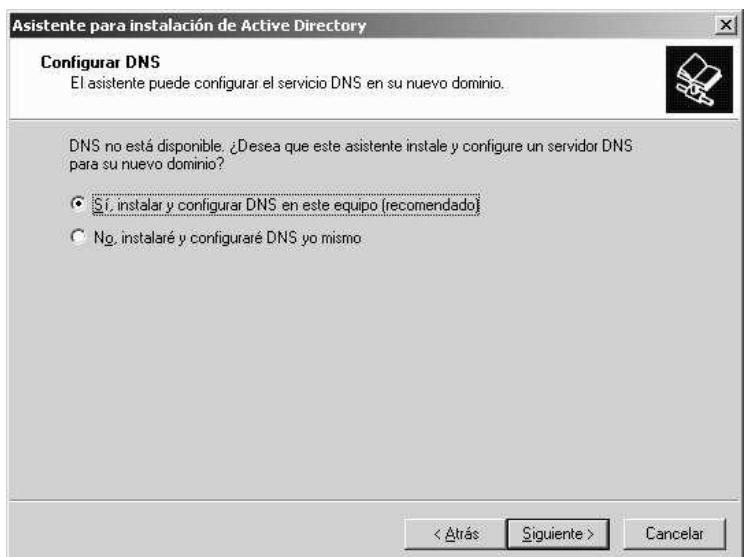
Después de especificar los nombres de dominio, el asistente solicita las ubicaciones de la base de datos, los archivos de registro y el volumen del sistema de Active Directory. La base de datos de Active Directory contendrá los objetos Active Directory y sus propiedades, mientras que los archivos de registro registran las actividades del servicio de directorio. Los directorios para estos archivos se especifican en la pantalla ubicación de la base de datos. La ubicación predeterminada tanto para la base de datos como para los registros es la carpeta %SystemRoot%\Ntds del volumen del sistema, pero se pueden modificar según nuestras necesidades siendo aconsejable que no residan en el mismo disco duro, para optimizar el rendimiento.

La pantalla Volumen del sistema compartido permite especificar la ubicación de lo que se convertirá en el recurso compartido Sysvol del controlador de dominio. El volumen del sistema es un recurso compartido que contiene información del dominio que se replica al resto de controladores de dominio de la red. De forma predeterminada, el sistema crea este recurso compartido en la carpeta %SystemRoot%\Sysvol en la unidad de disco del sistema.

La base de datos, los registros y el volumen del sistema de Active Directory tiene que situarse en volúmenes que utilicen el sistema de archivos NTFS

5. Si el asistente detecta que alguno de los volúmenes escogidos no utiliza NTFS 5, habrá que convertirlos o seleccionar otro volumen antes de poder completar el proceso de instalación de Active Directory. También resulta aconsejable situarlo en otro disco distinto al del sistema operativo

**Instalación de DNS:** En este punto, el Asistente para instalación de Active Directory tiene toda la información de configuración necesaria para instalar Active Directory y promover el servidor a controlador de dominio. El asistente determina ahora si el servidor DNS que se ha indicado en las



propiedades TCP/IP (si es que se ha indicado) es capaz de trabajar con el servidor Windows Server y está activo.

El asistente también determina si el servidor DNS que alojara el dominio soporta el protocolo de Actualización dinámica. Si el sistema no puede contactar con el servidor DNS especificado en la configuración TCP/IP cliente del equipo, o si el servidor DNS especificado no es capaz de dar soporte a un dominio Windows Server, el asistente se ofrece a instalar Microsoft DNS Server y configurarlo para que funcione como servidor autorizado para el dominio.

La pantalla Configurar DNS permite especificar si se desea instalar el servidor DNS o configurar uno personalmente. Si se opta por utilizar otra máquina para el servidor DNS, es preciso instalarlo y configurarlo antes de poder completar la instalación de Active Directory.

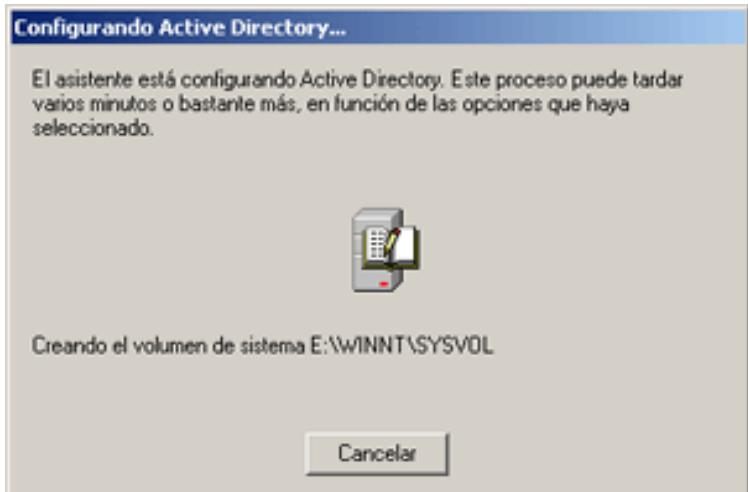
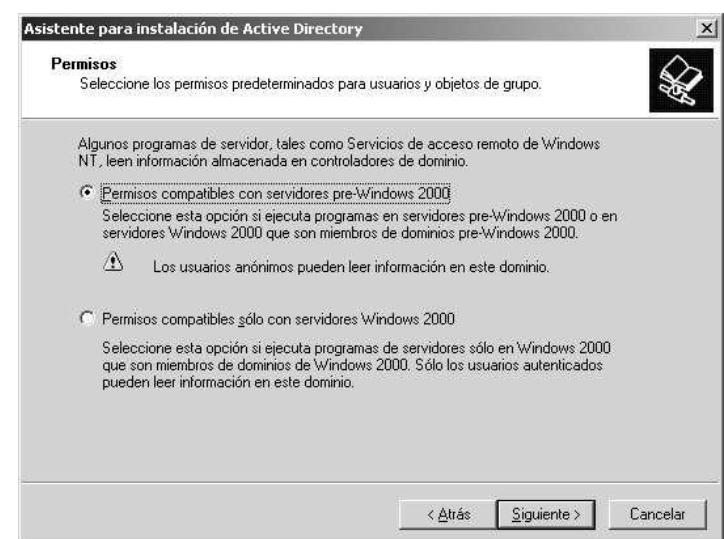
En nuestro caso, escogeremos la opción de **instalar y configurar DNS en este equipo**.

Ahora el asistente nos solicitará que escogamos entre trabajar en modo nativo o en modo mixto. En caso de que tengamos en nuestra red servidores NT y deseemos que estos servidores se conecten al dominio como servidores, tendremos que escoger permisos compatibles con servidores anteriores al Windows Server que se esté instalando.

Siempre que sea posible, escogeremos la opción de permisos compatibles sólo con servidores Windows Server actuales, ya que será la forma más cómoda de trabajar.

A continuación, el asistente nos solicitará una contraseña que tendremos que usar si queremos restaurar el sistema. Tenemos que tener en cuenta que al promocionar nuestro equipo desde servidor individual a servidor de dominio, creamos una cuenta especial; la de Administrador del Dominio, que tendrá la misma contraseña que tenía el Administrador del equipo donde instalamos el Active Directory. Como es obvio, esta contraseña no debe olvidarse bajo ningún concepto. Es muy recomendable usar la misma contraseña para el Administrador del servidor y el Administrador del dominio, así no nos equivocaremos cuando nos la pida el sistema luego.

Finalización de la instalación de Active Directory:  
El asistente registra todas las actividades que se producen durante el proceso de instalación en dos archivos llamados Dcpromo.log y Dcpromoui.log, en la carpeta %SystemRoot%\debug.



La instalación puede durar varios minutos, después de lo cual hay que reiniciar el sistema para que tengan efecto los cambios.

### Instalación de un controlador de dominio adicional en Windows 2003.

Los servidores adicionales proporcionan tolerancia a fallos en un dominio Active Directory, y pueden reducir el tráfico entre redes permitiendo a los clientes de la red autenticarse utilizando un controlador de dominio en el segmento local.

Cuando un controlador de dominio no funciona correctamente o no está disponible por algún motivo, sus réplicas asumen automáticamente sus funciones. Incluso un dominio pequeño necesita al menos dos controladores de dominio para mantener esta tolerancia a fallos.

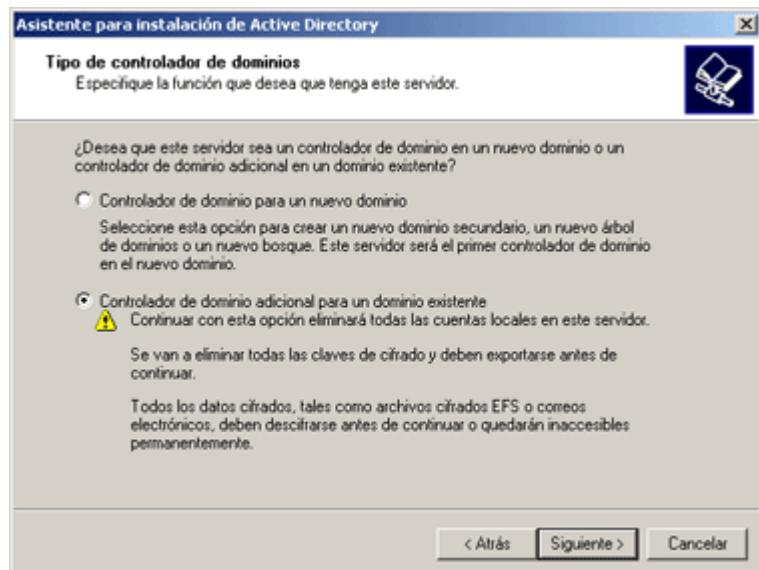
Para crear una réplica de un dominio existente, hay que ejecutar el Asistente para instalación de Active Directory (dcpromo) en un Windows Server recién instalado después de unirse al dominio que se trata de replicar.

Cuando aparece la pantalla Tipo de controlador de dominios en el asistente, hay que seleccionar Controlador de dominio adicional para un dominio existente y especificar el nombre DNS del dominio que se va a replicar. Después hay que suministrar el nombre de usuario, la contraseña y el nombre de dominio de una cuenta con privilegios administrativos en el dominio.

El asistente instala Active Directory en el servidor, crea la base de datos, los registros y el volumen del sistema en las ubicaciones especificadas, registra el controlador de dominio en el servidor DNS y replica la información de un controlador de dominio para ese dominio existente.

Una vez que la réplica del controlador de dominio está en funcionamiento, no es distinguible del controlador de dominio existente, al menos en lo que concierne a la funcionalidad de los clientes. Las réplicas funcionan como iguales, a diferencia de los servidores Windows NT, que están designados como controladores de dominio principales o de reserva. Los administradores pueden modificar el contenido de Active Directory (tanto los objetos como el esquema) de cualquier controlador de dominio, y los cambios se replicarán al resto de controladores de dominio de ese dominio.

Cuando se crea una réplica, el Asistente para instalación de Active Directory configura automáticamente el proceso de réplica entre los controladores de dominio. Se puede personalizar el proceso de réplica utilizando Sitios y servicios de Active Directory.



### Creación de un dc para un dominio secundario en un árbol existente en Windows 2003.

Cuando se crea el primer dominio Windows Server de la red, también se está creando el primer árbol del bosque. Se puede poblar el árbol a medida que se crean dominios adicionales haciéndolos secundarios de dominios existentes. Un dominio secundario es uno que utiliza el mismo espacio de nombres que un dominio principal. Este espacio de nombres se establece por el nombre DNS del dominio principal, al cual el secundario añade un nombre precedente para el nuevo dominio.

Por ejemplo, si se crea un dominio llamado SANA.COM, un dominio secundario de ese dominio podría llamarse algo así como INVESTIGACION.SANA.COM.

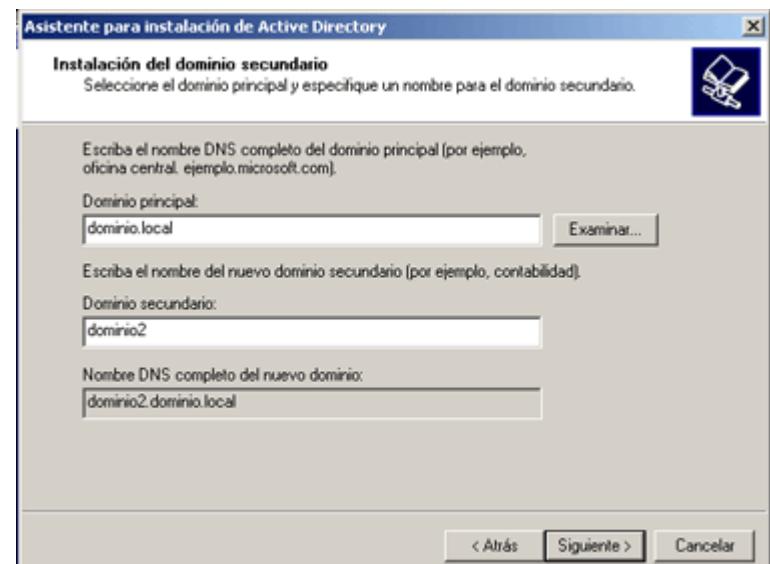
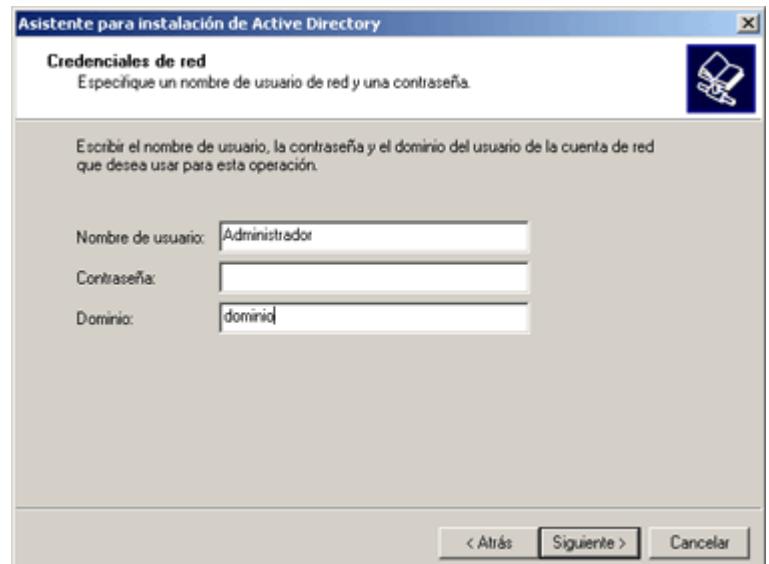
Por regla general, los dominios secundarios reflejan las divisiones geográficas, departamentales o políticas de una organización, pero se puede utilizar cualquier principio para el diseño del árbol que se desee. Un dominio principal puede tener cualquier número de secundarios, y la estructura del árbol puede extenderse a través de cualquier número de generaciones, lo que permite utilizar un único espacio de nombres para crear un árbol de dominios que refleje la estructura de toda la organización.

Para instalar Active Directory y crear un dominio secundario:

Unir el equipo en el que se desea crear el Dominio secundario al dominio principal suministrando las credenciales administrativas o creando manualmente un objeto equipo en el dominio por medio de Usuarios y equipos de Active Directory.

Iniciar sesión en el sistema utilizando la cuenta de administrador local

Ejecutar el Asistente para instalación de Active Directory desde la página Configurar el servidor o ejecutando Dcpromo.exe desde el cuadro de diálogo Ejecutar.



Un dominio secundario no es una réplica; es un dominio completamente independiente situado en el mismo árbol. Por lo tanto, cuando el asistente muestra la pantalla Tipo de controlador de dominios, hay que seleccionar Controlador de dominio para un nuevo dominio. En el cuadro de diálogo Crear árbol o dominio secundario, hay que seleccionar Crear un nuevo dominio secundario en un árbol de dominios existente. El asistente solicita a continuación el nombre DNS del dominio que ha de ser el principal del secundario. Después de suministrar esto, hay que especificar el nombre corto para el dominio secundario. El nombre corto es el nombre que se añadirá al nombre DNS del dominio principal para formar el nombre completo del dominio secundario. Por ejemplo, para crear un dominio secundario llamado Investigacion.miempresa.com, se especifica Miempresa.com como nombre del dominio principal a investigación como nombre corto del secundario.

En la siguiente pantalla nos solicita un nombre NetBIOS para el nuevo dominio de no más de 15 caracteres.

#### Creación de un dc para un nuevo árbol en un bosque ya existente en Windows 2003.

La diferencia fundamental entre la creación de un nuevo árbol y la creación de un nuevo bosque es que los bosques tienen cada uno sus propios esquema y configuración individuales. El escenario más obvio en el que una red debería tener múltiples bosques es cuando dos empresas con instalaciones Active Directory existentes se fusionan, y las suficientes diferencias de esquema y configuración existentes entre las dos hacen que la unión de ambas en un solo bosque sea impracticable. El proceso de crear un nuevo bosque es el mismo que el de la creación del primer dominio de la red.

#### Degradación de controladores de dominios en Windows 2003.

Una diferencia fundamental entre los controladores de dominio Windows 200X y los controladores de dominio Windows NT es que se puede degradar un controlador de dominio Windows 200X a servidor independiente o miembro. Cuando se ejecuta el Asistente para instalación de Active Directory, el programa determina que el sistema ya está funcionando como controlador de dominio y solo proporciona la opción de degradar el servidor. La pantalla Configurar el servidor también detecta el estado del sistema y proporciona una única opción.



La degradación de un controlador de dominio elimina la base de datos de Active Directory de la máquina, borra todas las referencias a ella del servidor DNS y devuelve las cuentas de seguridad del sistema a un estado idéntico al de un servidor Windows 2000 recién instalado. Si el dominio al que pertenece el sistema tiene controladores de dominio de réplica en la red, el servidor permanece como miembro de ese dominio después de la degradación.

Si el servidor es el único controlador de dominio de un dominio particular, la degradación provoca que el dominio se elimine completamente de Active Directory, y que el sistema se convierta en un servidor independiente hasta que se una a otro dominio. Si el servidor es el único controlador del dominio raíz de un bosque, hay que destruir el resto de dominios del bosque antes de que se pueda proceder con la degradación del controlador de dominio raíz. Una vez que se ha degradado un dominio (mediante el asistente por ejemplo), hay que asegurarse de que se cambia la identidad del equipo, para conseguir esto se realizan los siguientes pasos:

- 1) Abrir la herramienta Sistema del Panel de control y pulsar en la pestaña Identificación de red.
- 2) Pulsar el botón Avanzada para abrir el cuadro de diálogo Cambios de identificación.
- 3) Introducir el nuevo nombre para el equipo si es que se desea cambiar, y agregar el equipo a un grupo de trabajo cualquiera. (Si quisiéramos integrarlo como miembro de un dominio, podríamos hacerlo también).
- 4) Pulsar el botón Más y asegurarse de que se borra la casilla donde aparece el nombre de nuestro anterior dominio, que se usa como sufijo en el nombre de máquina. Mucho cuidado de no desactivar la casilla de verificación que indica que se debe usar el sufijo, ya que si lo hacemos será imposible que esa máquina pueda volver a trabar en un dominio.

## Maestros de operaciones.

Hemos comentado anteriormente como en el antiguo Windows NT los controladores de dominio se dividían en controladores principales (uno por dominio) y controladores secundarios. Desde Windows 2000 esto ya no es así, todos los controladores de dominio trabajan al mismo nivel.

Sin embargo, hay controladores de dominio que realizan una serie de operaciones especiales y por lo tanto son más importantes que el resto, estos son los maestros de operaciones.

Las funciones de maestro de operaciones son funciones específicas en las que se organizan las operaciones que utilizan la replicación de maestro único. La replicación de maestro único designa un controlador de dominio como el único controlador de dominio en el que pueden realizarse ciertos cambios en el directorio activo. Esto se hace para evitar conflictos de replicación que pueden presentarse si dos controladores de dominio realizan actualizaciones al mismo tiempo en el mismo atributo de objeto (dos controladores que cambian el nombre de un usuario al mismo tiempo, por ejemplo). Active Directory utiliza la replicación de maestro único para cambios importantes, como la adición de un nuevo dominio o un cambio en el esquema de todo el bosque.

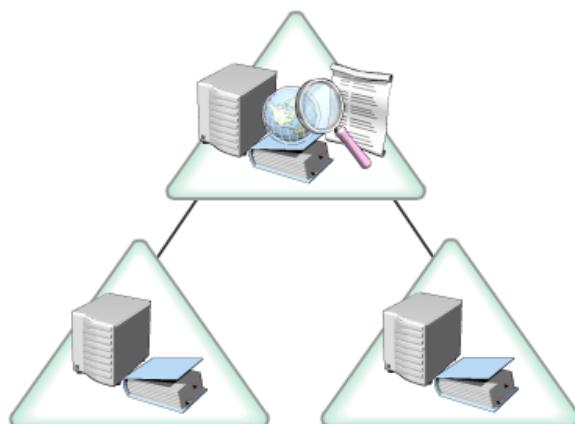
El controlador de dominio que es responsable de una función particular es el maestro de operaciones de esa función. Active Directory almacena la información acerca del controlador de dominio que tiene una función específica. Active Directory define cinco funciones de maestro de operaciones, con una ubicación predeterminada para cada una. Las funciones de maestro de operaciones abarcan todo el bosque o todo el dominio, hay dos funciones que abarcan todo el bosque y tres funciones que abarcan todo el dominio.

### Funciones para todo el bosque

- Maestro de nombres de dominio
- Maestro de esquema

### Funciones para todo el dominio:

- Emulador de PDC
- Maestro de RID
- Maestro de infraestructura

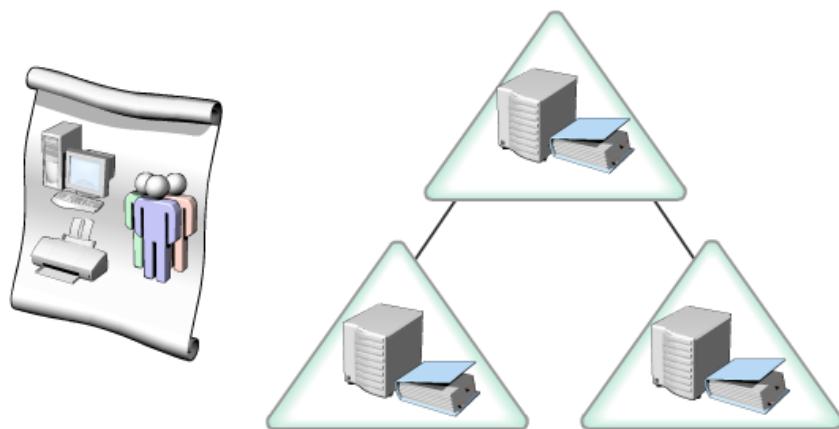


Las funciones que abarcan todo el bosque, incluyen el maestro de esquema que controla todas las actualizaciones del esquema. El esquema contiene una lista general de clases de objetos y atributos que se utilizan para crear todos los objetos de Active Directory como, por ejemplo, usuarios, equipos e impresoras.

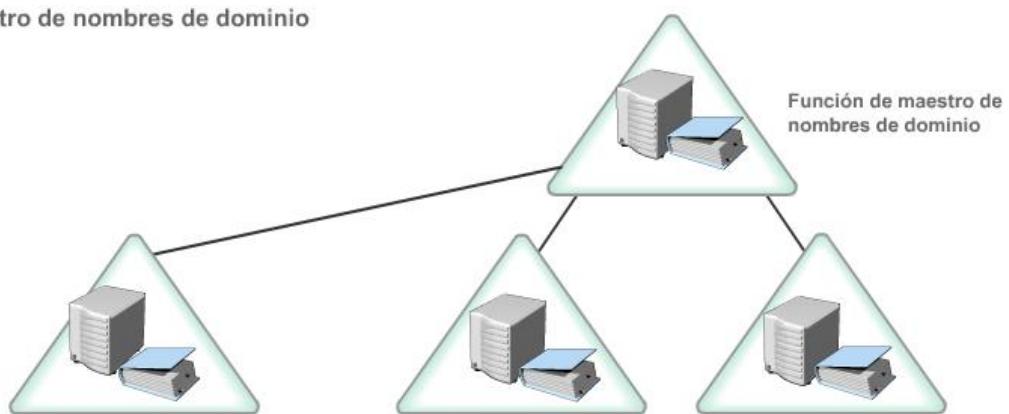
La otra función que abarca todo el bosque, el maestro de nombres de dominio, controla la adición o eliminación de dominios en el bosque. Sólo el controlador de dominio que tiene la función de maestro de nombres de dominio puede agregar un nuevo dominio. Sólo existe un maestro de esquema y un maestro de nombres de dominio en todo el bosque.

**Funciones para todo el bosque:**

- Maestro de esquema



- Maestro de nombres de dominio



Las funciones para todo el dominio son exclusivas de cada dominio en un bosque. Las funciones que abarcan todo el dominio son el emulador del controlador principal de dominio (PDC), el maestro de identificadores relativos (RID) y el maestro de infraestructura. Cada dominio de un bosque tiene su propio emulador de PDC, maestro de RID y maestro de infraestructura.

El emulador de PDC, el primer controlador de dominio que se crea en un nuevo dominio, acepta los controladores de dominio de reserva (BDC) que ejecutan Microsoft Windows NT® dentro de un dominio de modo mixto. Este tipo de dominio tiene controladores de dominio que ejecutan Windows NT® 4.0.

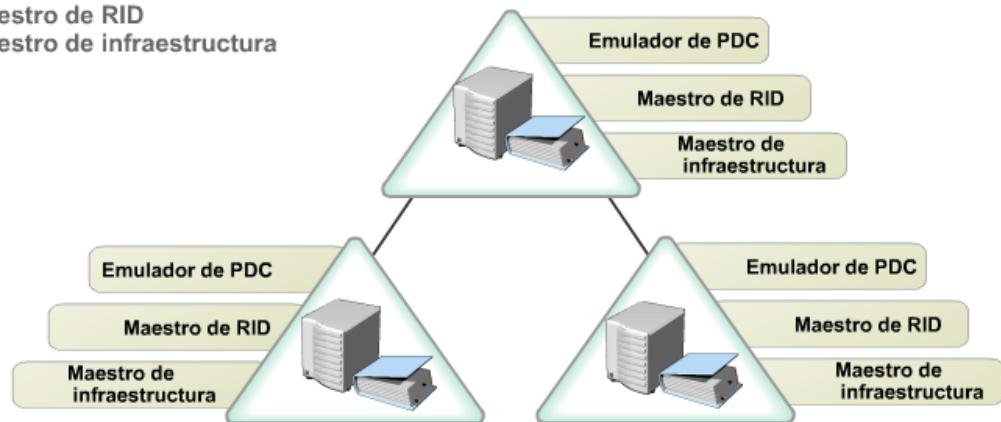
El maestro de RID asigna bloques de identificadores relativos a cada controlador de dominio en el dominio.

Cuando se mueven objetos de un dominio a otro, el maestro de infraestructura actualiza las referencias a objetos en su dominio que apuntan al objeto en el otro dominio. La referencia al objeto contiene el identificador único global (GUID) y un identificador de seguridad (SID). Active Directory actualiza

periódicamente el nombre completo y el SID en la referencia al objeto para que se reflejen los cambios realizados en el objeto propiamente dicho, como los movimientos dentro de los dominios y entre éstos y la eliminación del objeto.

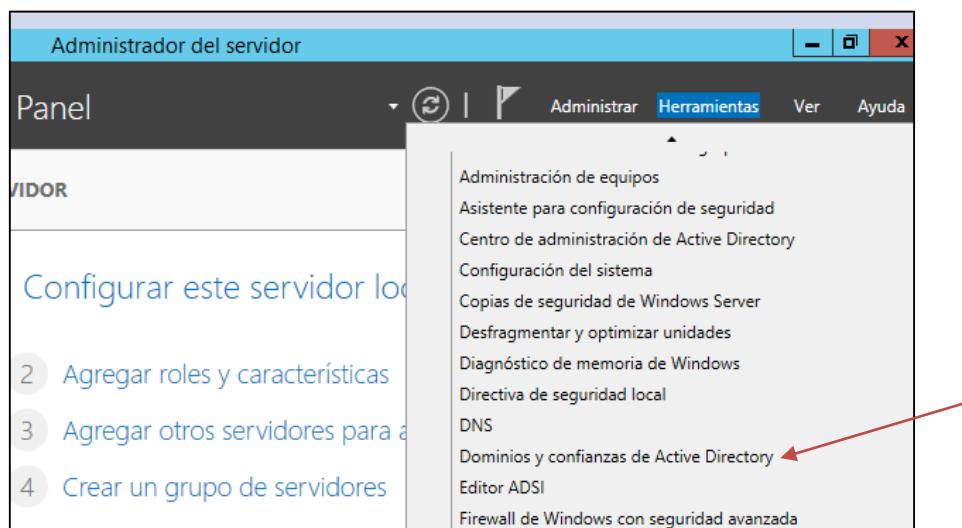
### Funciones para todo el dominio:

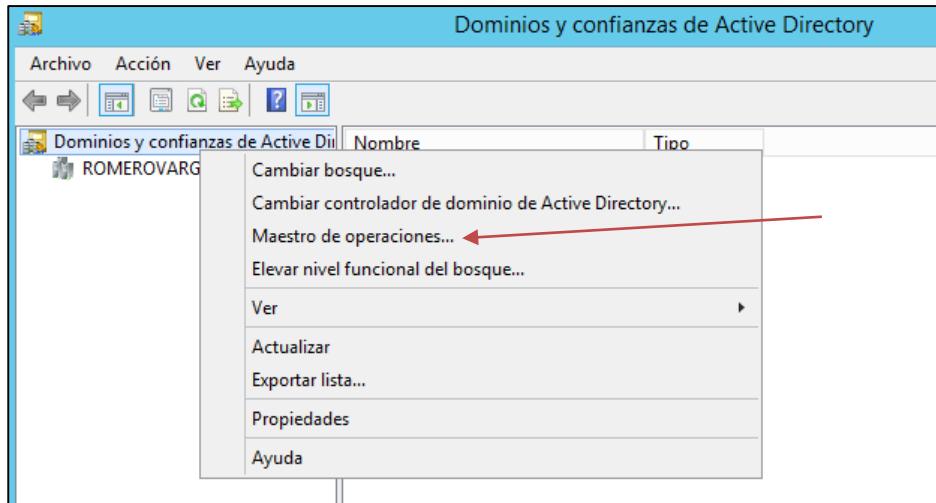
- Emulador de PDC0
- Maestro de RID
- Maestro de infraestructura



### Cambiar el maestro de operaciones para nombres de dominio.

Windows Server irá asignando estas funciones de maestros de operaciones a los primeros controladores de dominio creados. Si queremos modificar estas asignaciones podemos hacerlo desde la consola MMC de Dominios y Confianzas de Active Directory. Para ello pulsamos con botón derecho sobre Dominios y confianzas de Active Directory y escogemos la opción Maestro de Operaciones, que nos permitirá cambiar el CD que realiza la función de maestro de nombres de dominio.



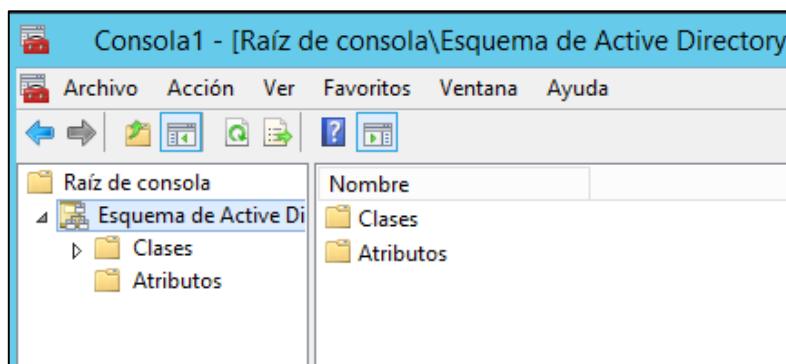


La función de maestro de nombres de dominio recordemos que es la encargada de añadir y eliminar dominios de nuestro árbol, por lo que es muy importante tener controlado que CD realiza esta función, ya que si dicho CD está apagado, no se podrán añadir ni eliminar ramas a nuestro árbol, o arboles a nuestro bosque.

Para llevar a cabo este procedimiento, debemos ser miembros del grupo Administradores de dominio o del grupo Administradores de organización de Active Directory.

#### Cambiar el maestro de operaciones para maestro de esquema.

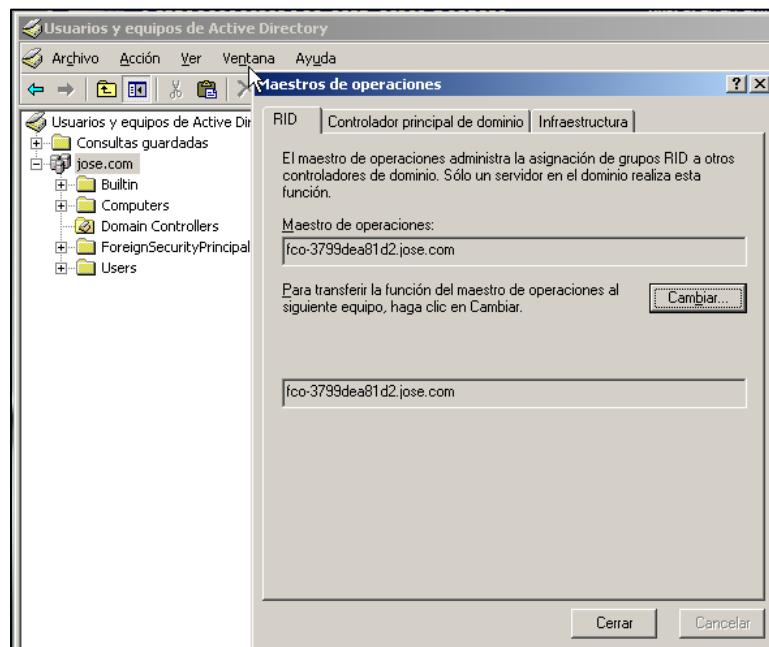
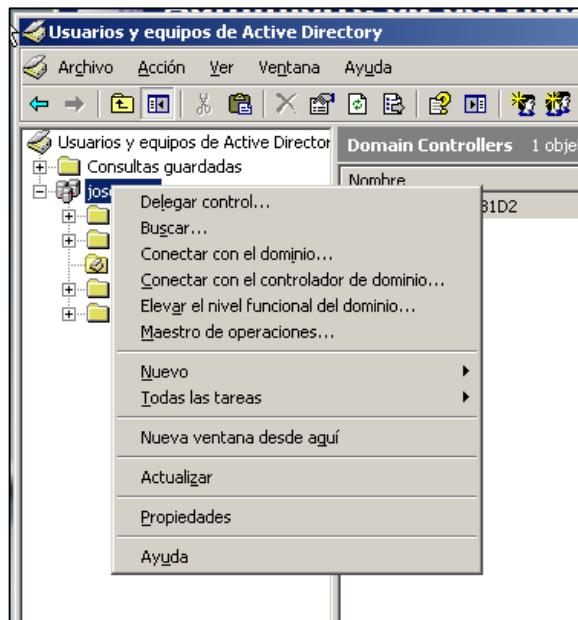
Se realiza dicho cambio desde la MMC de Esquema de Active Directory. Recordamos que dicha MMC no se instala por defecto, ya explicamos anteriormente como instalarla, ejecutando en una terminal el comando **regsvr32 schmmgmt.dll**. Una vez hecho nos aparecerá un mensaje de éxito en pantalla, volveremos a Inicio -> Ejecutar y una vez allí ejecutaremos "mmc" lo que nos abrirá una consola vacía, navegamos a Archivo -> Agregar o quitar complemento.. y seleccionar Esquema de Active Directory.



Una vez hecho esto, pulsamos botón derecho sobre Esquema de Active Directory y escogemos la opción de cambiar el maestro de operaciones.

Cambiar el maestro de operaciones para emulador de pdc, maestro de rid y maestro de infraestructura.

Para cambiar estas funciones que trabajan a nivel de dominio, tenemos que ejecutar la consola Usuarios y Equipos de Active Directory. Pulsamos con botón derecho sobre el nombre de nuestro dominio y escogemos la opción maestro de operaciones.



Veremos cómo nos aparece un formulario que nos permite cambiar el maestro de RID, el Controlador principal de dominio que realiza las funciones de emulador de PDC y el maestro de infraestructura.

### Catalogo global.

El primer controlador de dominio Windows Server de un bosque es automáticamente un servidor de Catálogo global. El Catálogo global (CG) contiene una réplica completa de todos los objetos de directorio del dominio en que se aloja además de una réplica parcial de todos los objetos de directorio de cada dominio del bosque. El objetivo de un CG es proporcionar autenticación a los inicios de sesión. Además, como un CG contiene información sobre todos los objetos de todos los dominios del bosque, la búsqueda de información en el directorio no requiere consultas innecesarias a los dominios. Una única consulta al CG produce la información sobre donde se puede encontrar el objeto.

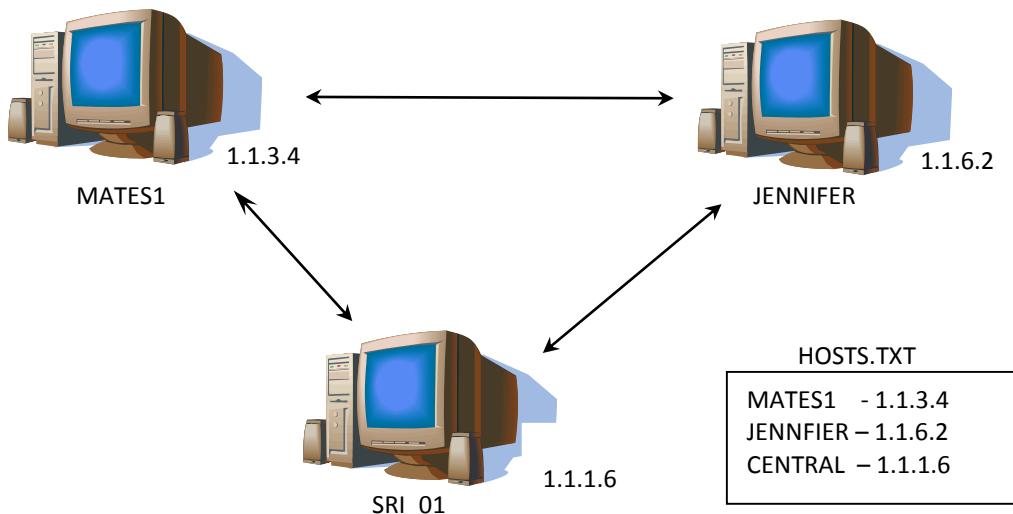
De forma predeterminada, habrá un CG, pero cualquier controlador de dominio se puede configurar como servidor de Catalogo global. Si se necesitan servicios de inicio de sesión y búsqueda adicionales, se pueden tener múltiples servidores de Catalogo global en el dominio.

## Servidores DNS y DHCP en Windows server.

### Servidor DNS.

Todos los hosts con TCP/IP tienen una dirección de IP única que se utiliza para la comunicación con otros equipos de la red. Un equipo trabaja fácilmente con direcciones IP, pero estas direcciones son muy difíciles de usar para las personas, ya que los usuarios suelen identificar los sistemas por un nombre. Para facilitar una comunicación efectiva y eficiente, los usuarios deben poder referirse a los equipos por un nombre y permitir que su equipo use su dirección de IP transparentemente.

En los primeros días de ARPANET, el antecesor de la Internet actual, sólo existía un pequeño número de equipos conectados a la red. El Centro de Información de Red (NIC), ubicado en el Instituto de Investigaciones de Stanford, SRI (Stanford Research Institute), era el responsable de compilar en un único archivo, HOSTS.TXT, los nombres y direcciones de todos los equipos. Los administradores debían mandar un mensaje al SRI, quien actualizaba el archivo HOSTS.TXT. A continuación, los usuarios de ARPANET debían descargar la nueva versión del archivo HOSTS.TXT mediante el Protocolo de transferencia de archivos (FTP).



Con el crecimiento de ARPANET, resultaba obvio que este método no era práctico, ya que:

- El ancho de banda consumido para transmitir las versiones actualizadas de un archivo de host de ARPANET sería proporcional al cuadrado del número de hosts en la ARPANET. Con un número de hosts creciendo exponencialmente, el impacto a largo plazo probablemente sería de una sobrecarga que ningún host podría mantener. (Para 4 hosts, había que mandar un archivo de 4 KB a 4 equipos lo que ocuparía un ancho de banda de 16 KB, con 100 hosts había que mandar un archivo de 100 KB a 100 equipos, lo que ocuparía un ancho de banda de 10.000 KB).
- El archivo de host plano y estático significaría que no podría haber dos equipos en la ARPANET con la misma dirección. Al crecer el número de hosts, crece el riesgo de añadir nombres duplicados, así como la dificultad de intentar un control centralizado.

- La naturaleza de la red subyacente estaba cambiando, los grandes equipos de tiempo compartido con que se había construido ARPANET se estaban viendo desplazados por miles de estaciones de trabajo y cada una necesitaba un nombre de host único. Empezaba a ser imposible controlar todos estos nombres centralizadamente desde un único equipo.

Con el crecimiento de ARPANET, resultaba más claro que se necesitaba una solución mejor. Se generaron varias propuestas según el concepto de servicio de nombres distribuido, que se basaban en un espacio de nombres jerárquico. Nacieron las RFC 882 y 883, donde se describe el diseño de un sistema de nombres de dominio, basado en una base de datos distribuida que contiene información generalizada de recursos. Este diseño evolucionó, y las RFC 1034 y 1035 describen el servicio del Sistema de nombres de dominio (DNS) que se usa hoy en Internet.

---

#### Descripción general de DNS en Microsoft Windows server.

Para facilitar las comunicaciones entre equipos se les puede dar un nombre en un espacio de nombres. El espacio de nombres concreto define las reglas para dar nombre a un equipo y cómo se resuelve un nombre en una dirección de IP. Cuando un equipo se comunica con otro debe resolver, o convertir, un nombre de equipo en una dirección de IP según las reglas del espacio de nombres utilizado. Esta resolución se puede realizar mediante un servicio de resolución de nombres.

Existen dos espacios de nombres principales y métodos de resolución de nombres que se usan en Windows Server: NetBIOS, implementado por el Servicio de Nombres de Internet de Windows (WINS) y DNS. WINS es tan inefectivo que es obligatorio montar y usar DNS, aunque se permite usar también WINS por motivos de compatibilidad, pero siempre y cuando DNS ya esté en funcionamiento.

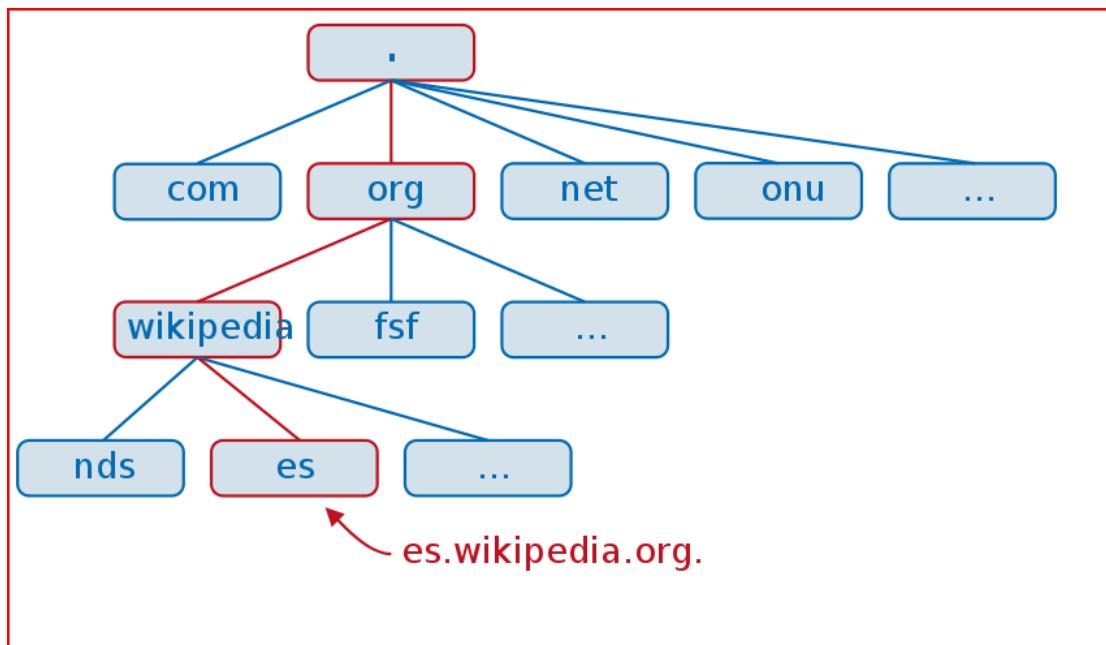
---

#### Términos clave DNS.

DNS es un servicio de nombres estándar. El servicio de DNS permite que un equipo cliente de la red registre y resuelva nombres de dominio de DNS. Estos nombres se utilizan para encontrar y acceder a recursos de otros equipos de la red o de otras redes como Internet. Los tres componentes principales de DNS son los siguientes:

- Los Clientes DNS: Un programa cliente DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS (Por ejemplo: ¿Qué dirección IP corresponde al nombre [www.eufrasia.com](#) ?).
- Los Servidores DNS: Que contestan las peticiones de los clientes. Los servidores recursivos tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada. (Así, el servidor DNS respondería al ejemplo anterior: El nombre [www.eufrasia.com](#) tiene registrada la IP 10.1.2.15).
- Zonas de autoridad, que son porciones del espacio de nombres de dominio que almacenan los datos. Cada zona de autoridad abarca al menos un dominio y posiblemente sus subdominios, si estos últimos no son delegados a otras zonas de autoridad.

El espacio de nombres de dominio está estructurado de manera jerárquica en un árbol que empieza en una raíz sin nombre para todas las operaciones de DNS. En el espacio de nombres de DNS cada nodo y cada hoja en el árbol del espacio de nombres de dominio representan un dominio con nombre. Cada dominio puede tener dominios hijos adicionales.



#### Nombre de dominio.

Cada nodo en el árbol de DNS tiene un nombre distinto, llamado etiqueta que puede tener entre 1 y 63 caracteres. El dominio raíz no tiene caracteres (.) .

Un nombre de dominio concreto es la lista de etiquetas en la ruta desde el nodo nombrado hasta la raíz del árbol de DNS. La convención de DNS es que las etiquetas que componen un nombre de dominio se leen de izquierda a derecha, desde lo más concreto hasta la raíz, por ejemplo, ventas.europa.cocacola.com. Este nombre completo también se denomina nombre de dominio completo o FQDN (Fully Qualified Domain Name).

Los nombres de dominio se pueden almacenar en mayúsculas o en minúsculas indistintamente, ya que todas las comparaciones y funciones de dominios se definen como insensibles a mayúsculas y minúsculas. Por tanto, www.midominio.com es idéntico a WWW.MIDOMINIO.COM para las operaciones DNS.

Un nombre de dominio usualmente consiste en dos o más etiquetas, separadas por puntos cuando se las escribe en forma de texto. Por ejemplo, www.theoatmeal.com o es.Wikipedia.org

Como vemos en el gráfico anterior, el raíz del árbol es el punto (.) que es la primera parte del nombre DNS (los nombres DNS se “escriben” de derecha a izquierda). Este punto normalmente nunca se representa ni se escribe para simplificar los nombres.

A la etiqueta ubicada más a la derecha (sin contar el punto) se le llama dominio de nivel superior (Top Level Domain). Como **com** en www.theoatmeal.**com** o **es** en www.Wikipedia.**es**

Cada etiqueta a la izquierda especifica una subdivisión o subdominio. (No hay que confundir los “dominios y subdominios” DNS con los dominios y subdominios de Windows). En teoría, esta subdivisión puede tener hasta 127 niveles, y cada etiqueta contiene hasta 63 caracteres, pero restringido a que la longitud total del nombre del dominio no exceda los 255 caracteres, aunque en la práctica los dominios son casi siempre mucho más cortos.

Finalmente, la parte más a la izquierda del dominio suele expresar el nombre de la máquina (hostname). Más a la izquierda aún se puede colocar un prefijo como www, ftp, etc. Estos prefijos no forman parte real del nombre DNS y solo se utilizan para indicar qué tipo de protocolo se va a usar para la conexión, no tienen ninguna utilidad adicional.

---

### Dominios superiores.

Un dominio superior es un dominio de DNS directamente debajo de la raíz (el punto final de cualquier host DNS aunque normalmente no se representa). Resulta difícil crear nombres adicionales, al menos en Internet. Las tres categorías de dominios superiores son las siguientes:

- <ARPA>. Es un dominio especial, se usa en la actualidad para búsqueda inversa de nombres.
- Dominios de 3 letras. Existen siete dominios superiores de 3 caracteres. (en la actualidad, estos nombres se han incrementado con algunos más).
- Nombres de 2 letras para los países. Estos dominios con código de país se basan en los nombres de país de la Organización Internacional de Normalización (ISO) y se usan, principalmente, por empresas y organizaciones fuera de los EE.UU.

---

### Registros de recursos de DNS.

Un registro de recurso es un registro que contiene información relacionada con un dominio que puede contener la base de datos de DNS y que puede solicitar y usar un cliente de DNS. Por ejemplo, el RR de host de un dominio concreto mantiene la dirección de IP de tal dominio (host); un cliente de DNS podrá utilizar este RR para conseguir la dirección de IP para el dominio.

Cada servidor de DNS contiene los RR relacionados con aquellas porciones del espacio de nombre de DNS para el que es autoridad, o para el que puede responder las solicitudes por un host.

Cuando un servidor de DNS es autorizado para una porción del espacio de nombres de DNS, dicho servidor es el responsable de asegurar que la información sobre esa porción del espacio de nombres de DNS es correcta. Para aumentar la eficiencia, un servidor de DNS dado puede hacer caché de los RR relativos a un dominio de cualquier parte del árbol de dominios.

Cada RR contendrá un conjunto de información común, como la siguiente:

- Propietario. Indica el dominio de DNS en el que se encuentra el registro de recurso.
- TTL. Tiempo que utilizan otros servidores de DNS para determinar durante cuánto tiempo se hace caché de la información de un registro antes de descartarla. Para la mayoría de los RR, este campo es opcional. El valor de TTL se mide en segundos, con un valor de 0 que indica que el RR contiene datos volátiles que no se deben guardar en caché. Por ejemplo, los registros SOA tienen

un valor de TTL predeterminado de 1 hora. De esta forma se evita que otros servidores mantengan en caché estos registros durante largos períodos de tiempo, lo que podría retrasar la propagación de cambios.

- Clase. Para la mayoría de los RR, este campo es opcional. Cuando se utiliza, contiene un texto mnemónico que indica la clase de un RR. Por ejemplo, una clase con IN indica que el registro pertenece a la clase Internet (IN). Alguna vez existieron muchas clases, como CH para Chaos Net, pero en la actualidad sólo se usa la clase IN.
- Tipo. Este campo es requerido y mantiene un texto que indica el tipo del RR. Por ejemplo, la letra A indica que el RR guarda la información de dirección (Address) del host.
- Datos específicos del registro. Es un campo de tamaño variable que contiene información que describe el recurso. Este formato de información varía de acuerdo con el tipo y clase del RR.

Los archivos de zona de DNS estándar contienen el conjunto de RR de dicha zona en un archivo de texto. En este archivo de texto, cada RR se encuentra en una línea separada y contiene todos los elementos de datos anteriores, como un conjunto de campos de texto separados por espacios en blanco.

```
$TTL 86400 ; 1 day
$ORIGIN example.com.
@           IN      SOA    linux01.example.com.    hostmaster.example.com.
@           IN      NS     linux01.example.com.
@           IN      NS     linux02.example.com.

;-----
; Hosts in the Primary Data Centre - 192.168.1.0/24
;-----
router01 IN      A      192.168.1.1
linux01  IN      A      192.168.1.10
router02 IN      A      192.168.2.1
linux02  IN      A      192.168.2.10
router03 IN      A      192.168.3.1
router03 IN      A      192.168.4.1
linux03  IN      A      192.168.4.10
```

---

#### Registros de recursos que admite Windows server.

Existen numerosos tipos de RR definidos. La mayoría de los tipos de RR ya no se necesitan ni se usan, aunque todos esos están disponibles en Windows Server. Los RR usados más habitualmente, son:

- Dirección de host (A) Address 32 bits. Este RR contiene la dirección de host que hace corresponder un nombre de dominio de DNS con una dirección de IPv4 de 32 bits.
  - Ejemplo:      LINUX03 IN        A        192.168.4.10
- Dirección de host (AAAA) Address de 128 bits. Este RR contiene la dirección de host que hace corresponder un nombre de dominio DNS con una dirección de IPV6 de 128 bits.
  - Ejemplo:      LINUX03 IN        A        4321:0:1:2:3:4:567:89ab

- Nombre canónico (CNAME) canonical name. El RR nombre canónico (CNAME) permite crear alias (sobrenombres) para un host.
  - Ejemplo: SERVIDOR3 CNAME LINUX03
- Puntero (PTR) Pointer reverse. Este RR se usa para los mensajes de búsqueda inversa de nombre, es decir, en vez de buscarse un nombre y devolver su dirección IP, se busca una dirección IP y se devuelve el nombre. Normalmente, se usa el árbol de dominio in-addr.arpa para la búsqueda inversa de la correspondencia dirección-nombre.
  - Ejemplo: 192.168.4.10 IN PTR LINUX03
- Localizador de servicio (SRV) [Server] El RR SRV (Service Locator) permite a un equipo localizar un host que disponga de un cierto servicio, como el Controlador de dominio del Active Directory de Windows Server.
- Servidores de Nombre (NS). El RR NS permite a un equipo localizar a los servidores de nombre, es decir, a los propios servidores DNS.

Especial atención debemos prestar cuando usemos Windows Server a los RR PTR dado que estos registros deben estar en una zona de búsqueda inversa, y dicha búsqueda no se crea automáticamente en Windows Server, tendremos que crearla manualmente cada vez que instalamos un servidor DNS que funcione en una zona integrada de Active Directory.

### Operación de solicitud de DNS.

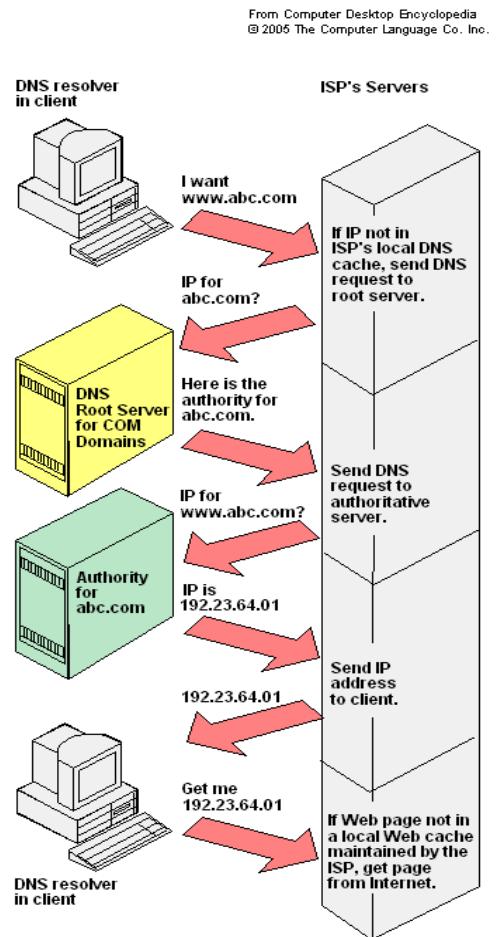
Como vemos en el gráfico de la derecha, nuestra máquina necesita resolver un nombre de dominio (por ejemplo [www.bekkoame.co.jp](http://www.bekkoame.co.jp)). Para conocer su dirección IP, le enviará una petición de un registro de recurso (RR) de tipo A a nuestro servidor DNS (el que tengamos configurado en las propiedades de red).

Si nuestro servidor DNS tiene un RR de tipo A de nuestra petición nos enviará directamente el RR, con lo que sabremos que su dirección ip es 202.11.252.20.

Pero es bastante habitual que nuestro servidor DNS no tenga ningún registro sobre ese nombre (sería imposible e indeseable que en un solo servidor estuvieran almacenados todos los RR de todos los nombres de todas las máquinas de internet).

En estos casos, nuestro servidor DNS manda una petición de ayuda a un servidor root de Internet (hay 13 root-servers principales en internet). El servidor root normalmente no devuelve la dirección IP de nuestra petición, sino que busca la dirección IP del servidor DNS que tiene autoridad (SOA, Start of Authority) sobre nuestra petición. En nuestro caso, y como nuestra petición [www.bekkoame.co.jp](http://www.bekkoame.co.jp) pertenece a Japón (jp) nos devolvería la dirección a un servidor con autoridad sobre Japón.

Ahora solicitamos al nuevo servidor DNS de Japón un RR de tipo A sobre [www.bekkoame.co.jp](http://www.bekkoame.co.jp) y normalmente nos responderá sin problemas. Si este servidor tampoco es capaz de encontrar el host, obtendríamos el mensaje de host inexistente.



### Solicitud inversa.

Una solicitud inversa es aquella en la que se solicita a un servidor de DNS el nombre de dominio de DNS de un host con una determinada dirección de IP. Los mensajes de Solicitud de búsqueda inversa son, realmente, solicitudes estándar, pero relacionadas con las zonas de búsqueda inversa.

Las zonas de búsqueda inversa se basan en el nombre de dominio in-addr.arpa y mantiene, principalmente, los RR de PTR.

En este tipo de solicitudes lo que se manda al servidor DNS no es un nombre de host del que queremos saber su IP, sino lo inverso o contrario, le mandamos una IP y queremos que nos devuelva el nombre.

### Clases de solicitudes de DNS.

Las solicitudes de DNS pueden ser de dos clases: recursivas o iterativas.

Una solicitud **recursiva** es una solicitud de DNS que se envía a un servidor de DNS en la que el host solicitante pregunta al servidor de DNS para que le proporcione una respuesta completa a la solicitud, aunque ello signifique que tenga que ponerse en contacto con otros servidores para obtener la respuesta.

Una solicitud **iterativa** es una solicitud de DNS que se envía a un servidor de DNS en el que el host solicitante pide que se devuelva la mejor respuesta que el servidor de DNS pueda proporcionar sin buscar ayuda adicional de otros servidores de DNS.

En general, los equipos envían solicitudes recursivas. Los equipos suponen que el servidor de DNS conoce la respuesta a la solicitud, o puede encontrarla.

Por otra parte, un servidor de DNS normalmente enviará solicitudes iterativas a otros servidores de DNS si no puede responder a la solicitud con la información de que dispone.

---

### Operación de actualización de DNS.

Una operación de actualización de DNS la envía un cliente a un servidor de DNS para actualizar, añadir o eliminar algunos o todos los RR de información relacionada con un determinado dominio, por ejemplo, para actualizar el registro de host del equipo con nombre kona.midominio.com para que apunte a 10.10.1.100. La operación de actualización también se denomina actualización dinámica.

---

### Resolución de nombres: resolutor de DNS.

En Windows, el resolutor de DNS es un componente del sistema que realiza solicitudes de DNS a otro u otros servidores de DNS. La pila de TCP/IP de Windows se configura, normalmente, con la dirección de IP de al menos un servidor de DNS al que el resolutor envía una o más solicitudes de información de DNS.

En Windows, el resolutor forma parte del servicio Cliente de DNS. Este servicio se instala automáticamente cuando se instala TCP/IP y se ejecuta como parte del proceso Services.Exe.

---

### Caché del resolutor de DNS.

Un host de IP podría necesitar ponerse en contacto periódicamente con otro host y por tanto necesitaría resolver un nombre concreto de DNS muchas veces, como por ejemplo el nombre del servidor de correo electrónico.

Para evitar tener que enviar solicitudes a un servidor de DNS cada vez que el host quiere resolver el nombre, Windows Server implementa una caché especial de información de DNS.

El servicio Cliente de DNS hace caché de los RR recibidos en las respuestas a las solicitudes de DNS. La información se mantiene durante un Período de vida, TTL (Time To Live), y se puede utilizar para responder solicitudes posteriores. De forma predeterminada, la caché utiliza el valor de TTL recibido en la respuesta de solicitud de DNS. Cuando se resuelve una solicitud, el servidor autoridad de DNS en el dominio resuelto define el TTL para un RR dado.

```
G:\>IPCONFIG /DISPLAYDNS
Configuración IP de Windows 2000
localhost.

Nombre de registro...: localhost
Tipo de registro...: 1
Tiempo de vida...: 31532890
Longitud de los datos: 4
Sección...: Answer
Un registro (Host)...: 127.0.0.1

1.0.0.127.in-addr.arpa.

Nombre de registro...: 1.0.0.127.in-addr.arpa
Tipo de registro...: 12
Tiempo de vida...: 31532890
Longitud de los datos: 4
Sección...: Answer
Registro PTR...: localhost
```

Puede utilizar el comando IPCONFIG con la opción /DISPLAYDNS para mostrar el contenido actual de la caché del resolutor.

#### Caché negativa.

El servicio Cliente de DNS también utiliza una caché negativa. La caché negativa ocurre cuando no existe un RR de un nombre de dominio solicitado o cuando el propio nombre de dominio no existe, en cuyo caso se guarda la falta de resolución. La caché negativa evita repetir solicitudes adicionales de RR o dominios que no existen.

Si se realiza una solicitud a un servidor de DNS y la respuesta es negativa, las siguientes solicitudes al mismo nombre de dominio se responden negativamente durante un tiempo predeterminado de 300 segundos.

Para evitar guardar en la caché información negativa anticuada, cualquier información de solicitud respondida negativamente se mantiene durante un período de tiempo inferior al que se utiliza para las respuestas positivas. Con la caché negativa se reduce la carga en los servidores de DNS, pero estarán disponibles los RR relevantes, y se podrán enviar solicitudes posteriores para obtener la información.

Si se realiza una solicitud a todos los servidores de DNS y no está disponible ninguno durante un tiempo predeterminado de 30 segundos, las solicitudes posteriores por nombre fallarán inmediatamente en lugar de esperar los plazos. De esta forma se puede ahorrar tiempo en servicios que utilizan DNS durante el proceso de arranque, sobre todo cuando se arranca de la red.

La orden IPCONFIG puede ser usada con el parámetro /FLUSHDNS para vaciar la caché del resolutor, con lo que también eliminamos la caché negativa.

#### Delegación de zona.

DNS es una base de datos distribuida de información diseñada específicamente para superar las limitaciones de la resolución de nombres anterior con el archivo HOSTS.TXT.

La función que permite a DNS manejar grandes espacios de nombres/redes, como Internet, es su capacidad para delegar la administración de dominios. Se produce una delegación de zona cuando la

responsabilidad de los RR de un subdominio se traslada del propietario del dominio principal al propietario del subdominio.

En el núcleo de Internet existen 13 servidores raíz, denominados de A.ROOTSVERERS.NET a M.ROOT-SERVERS.NET. Los servidores raíz están extensamente distribuidos. Mantienen datos de todos los dominios de nivel superior, como los .com, .org y .net, así como para los dominios geográficos como .uk y .jp. Estos servidores raíz permiten a los hosts de Internet tener un acceso a toda la base de datos de DNS. Por debajo de los dominios raíz y superior están los dominios y subdominios de las organizaciones individuales. En algunos dominios superiores existen niveles jerárquicos adicionales. Por ejemplo, en el dominio .uk existe un subdominio co.uk para las compañías de UK (por ejemplo, psp.co.uk) y ac.uk para las instituciones académicas (por ejemplo, ic.ac.uk para el Imperial Collage).

La delegación ocurre como una división del DNS en las responsabilidades para los dominios debajo de la división que se delega del dominio superior. En el dominio midominio.com está el subdominio jh.midominio.com. La responsabilidad para el dominio subordinado se ha delegado a un servidor diferente.

Para implantar la delegación, la zona superior debe tener tanto un RR A como un registro de Servicio de nombre (NS), ambos apuntando a la nueva raíz de dominio delegado.

---

#### Cliente de actualización dinámica de DNS.

En grandes redes, conseguir toda la información de RR necesaria en el DNS y mantenerla actualizada puede ser una tarea agotadora. El mantenimiento de los registros de hosts, en algunos entornos, puede ser un trabajo a tiempo completo para una o más personas. Para simplificar esta tareas, Windows Server incluye la actualización dinámica de DNS.

Mediante el DNS dinámico, los clientes envían un mensaje de registro de DNS al servidor de DNS, indicándole que actualice el registro (A) para el host. Además, si el cliente es también cliente de DHCP, cada vez que ocurre un suceso de dirección, por ejemplo, una concesión de una nueva dirección o una renovación de dirección, como parte del proceso de administración de las concesiones de DHCP, el cliente de DHCP envía la Opción 81 al servidor de DHCP junto con su nombre completo. La Opción 81 indica al servidor de DHCP que registre el RR PTR por él.

Este mecanismo, donde el cliente actualice el registro (A) y el servidor de DHCP actualice el registro PTR, es el elegido porque sólo el cliente conoce qué direcciones de IP en el host se corresponden con el nombre del host. El servidor de DHCP puede que no sea capaz de realizar correctamente el registro del RR (A) debido a un conocimiento parcial. Si resulta apropiado también se puede configurar el servidor de DHCP para registrar ambos registros en el DNS.

## Instalación y configuración de un servidor DNS.

Los servidores DNS son una parte esencial de una red basada en TCP/IP además de una parte esencial del Active Directory. Microsoft recomienda la instalación de DNS en cada controlador de dominio cuando se utilice Active Directory.

Esta solución permite al servidor DNS dinámico de Windows Server utilizar Active Directory para almacenar información de la zona, permitiendo de este modo la réplica con múltiples maestros completa de la zona por medio de Active Directory, simplificando la tarea de conseguir la tolerancia a fallos y haciendo menos difícil la administración del DNS.

Es fundamental instalar DNS en el controlador primario que forme la raíz del árbol en un bosque nuevo.

Si no se instaló DNS en el controlador de dominio durante la instalación de Windows Server, será necesario usar uno que ya esté instalado en la empresa y habrá que configurarlo para que trabaje con nuestro dominio. También es posible instalar el servidor DNS en nuestro servidor después de instalar nuestro dominio, pero es una operación complicada y engorrosa.

## Configuración del servicio DNS.

Las zonas son los cerebros del DNS; por lo tanto, el servidor DNS es inútil hasta que se configuren las zonas del dominio. Las zonas permiten almacenar porciones del espacio de nombres del DNS de forma que un único servidor DNS pueda servir una porción del espacio de nombres. Así, si creamos un dominio INSTITUTO.LOCAL tendremos que crear una zona INSTITUTO.LOCAL en un servidor DNS.

Cuando se configuran los dominios, hay que comenzar por el dominio de nivel más alto. Despues hay que crear los subdominios y delegar el control de los dominios a otros servidores DNS si fuese necesario. Podemos elegir si INFORMATICA.INSTITUTO.LOCAL es una zona DNS dentro del mismo servidor DNS que ya tenemos instalado, o bien instalar un nuevo servidor DNS que tendrá delegada la zona INFORMATICA y dependerá del servidor DNS de la zona principal INSTITUTO.LOCAL.

Los dos tipos de zonas que es necesario tomar en consideración son las zonas de búsqueda directa y las zonas de búsqueda inversa.

- Las zonas de búsqueda directa son los tipos de zonas que se asocian normalmente con servidores DNS; ellas devuelven una dirección IP cuando se les proporciona un nombre DNS. Estas zonas se suelen crear automáticamente cuando instalamos el Active Directory, de modo que no tendremos que crearlas a mano. Sin embargo, su creación no es inmediata, y suelen necesitar que exista cierta actividad dentro del dominio antes de que se creen correctamente.
- Las búsquedas inversas se utilizan menos a menudo, aun siendo importantes de todos modos. Proporcionan la capacidad de asignar un nombre DNS a una dirección IP, algo que los Servicios de Internet Information Server (IIS) también utilizan para sus archivos de registro y herramientas de solución de problemas como Nslookup. Es importante destacar que estas zonas de búsqueda inversa no se crean automáticamente, y tendremos que crearlas siempre a mano.

### Creación de una nueva zona.

Para crear una nueva zona de búsqueda directa en el servidor DNS para que los clientes puedan obtener la dirección IP de un nombre DNS, hay que seleccionar DNS en la carpeta Herramientas administrativas, Seleccionar el servidor DNS en el árbol de la consola.

Escoger entonces Crear una zona nueva en el menú Acción para iniciar el Asistente para crear zona nueva. Hay que pulsar Siguiente para comenzar a utilizar el asistente.

**Tipo de Zona:** En esta ventana hay que escoger una de las siguientes opciones y pulsar entonces Siguiente para continuar:

**Active Directory integrado:** Se debe utilizar si todos los controladores de dominio ejecutan Windows Server. Esta opción también se puede utilizar en una red mixta si los servidores UNIX son compatibles con el DNS de Microsoft.

**Principal estándar:** Se debe utilizar si el servidor DNS ejecuta Windows Server pero no es un controlador de dominio.

**Secundaria estándar:** Se debe utilizar si el servidor DNS está alojado en servidores UNIX. También se debe utilizar si este servidor va a tener privilegios de sólo lectura en la zona para toda la información obtenida del servidor DNS principal.

**Zona de búsqueda directa o inversa.** Esta ventana nos permite escoger el tipo de zona que queremos crear.

**Zona de búsqueda directa:** Es la que permite a los clientes buscar los equipos de la red a través de los nombres, convirtiendo los nombres DNS a direcciones IP.

**Zona de búsqueda inversa:** Las zonas de búsqueda inversa permiten a los clientes obtener el nombre DNS de un host a partir de una dirección IP, lo que resulta útil para herramientas de solución de problemas como Nslookup. Y realizar una búsqueda inversa junto con los archivos de registro de IIS permite el registro de un nombre DNS en lugar de una dirección IP. Para crear una zona de búsqueda inversa tenemos que indicar la parte fija de las direcciones IP de nuestra red. Normalmente en nuestro caso siempre creamos la zona de búsqueda inversa como 192.168.x.x.



Nombre de Zona: Introducir el nombre DNS para la zona en el cuadro de texto Nombre y pulsar Siguiente

Si se ha escogido la instalación de una Zona Active Directory Integrada, se creará ahora. Si se está creando una Zona principal estándar, seguirá el proceso de instalación. Para una Zona secundaria estándar se abre la ventana Servidores maestros DNS. Hay que introducir las direcciones IP de los servidores maestros de los cuales se desea copiar la información de zona, pulsando Agregar después de introducir cada una. Se puede utilizar el botón Examinar para buscar servidores. Se pueden utilizar los botones Arriba y Abajo para organizar las direcciones IP en el orden en el que se deseen contactar. Hay que pulsar Siguiente cuando se haya terminado y pulsar después Finalizar para completar la configuración de la zona secundaria.



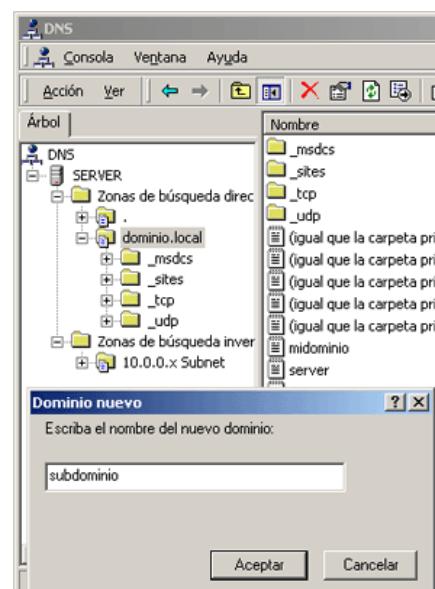
Archivo de Zona: Nos permitirá elegir el archivo que queremos utilizar para la Zona DNS que estamos creando.

Cree un archivo nuevo con este nombre de archivo: introducir el nombre que se le quiere dar al archivo de zona o utilizar el que se proporciona.

Usar este archivo: Para utilizar un archivo de zona existente para almacenar la información de la zona, hay que copiar el archivo a la carpeta %SystemRoot%\System32\DNS. Esta es la opción a elegir si estamos importando una Zona DNS desde otro sistema.

#### Creación de subdominios y delegación de autoridad.

En muchos entornos de red grandes es necesario crear subdominios y delegar su administración a otras zonas DNS que estén alojadas en otros servidores DNS. Este paso elimina la situación de tener un enorme espacio de nombres alojado en una única zona de un único servidor. Por lo tanto, se debería tener una zona que contuviera el dominio raíz dominio.com además del subdominio marketing.dominio.com; sin embargo, se debería tener el subdominio subdominio.dominio.com y sus subdominios delegados a una zona separada administrada por otro servidor DNS.



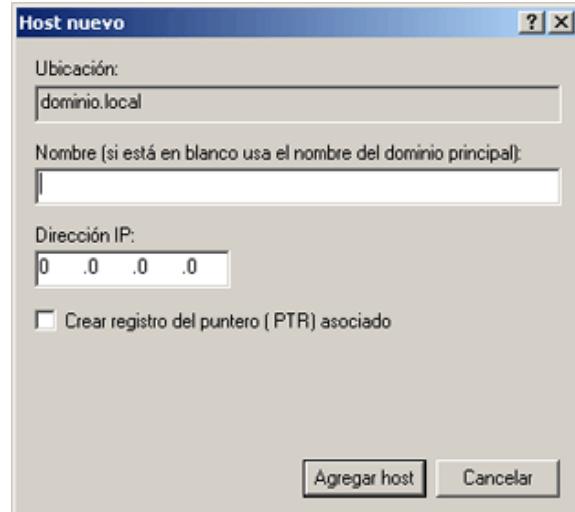
Hay que asegurarse de que se tiene un registro de host creado para el servidor DNS en la Zona de búsqueda directa y un registro del puntero para el servidor DNS en la Zona de búsqueda inversa. Puede que el DNS no los cree automáticamente (especialmente el registro del puntero), por lo que conviene verificar ambos; en otro caso el servidor podría no funcionar.

Conviene observar que las zonas deben tener un espacio de nombres contiguo, por lo que no es posible combinar subdominios de diferentes ramas del espacio de nombres y situarlos en una única zona: sería necesario crear zonas separadas para cada parte no contigua del dominio.

#### Agregación de registros de recursos del host.

Después de crear las zonas y los subdominios se deberían añadir registros de recursos (RR) para el servidor del dominio y cualquier otro servidor con direcciones IP estáticas o reservas de IP (servidores DHCP, servidores WINS, enrutadores, etc.). El servidor DNS no funcionará adecuadamente sin un registro de host y un registro del puntero, este último no se creará de forma automática.

- Seleccionar la zona y dominio o subdominio al cual pertenece el host y escoger entonces Host nuevo en el menú Acción. Escoger el tipo de RR que queremos crear. (En este caso Tipo A).
- Introducir el nombre del host o dejar el cuadro Nombre en blanco para utilizar el nombre del dominio principal. Hay que introducir la dirección IP del host.
- Seleccionar Crear registro del puntero (PTR) asociado para crear un RR para el host en la zona de búsqueda inversa.
- Pulsar Agregar host y llenar después los campos para cualquier registro de host adicional que se quiera crear o pulsar Realizado.



Cuando instalamos el DNS por primera vez, veremos cómo aparecen algunos hosts del tipo A con nombre de host y que sin embargo no están creados en la zona de búsqueda inversa. Estos host hay que borrarlos de la zona directa y volver a crearlos de la forma que se ha explicado, marcando la casilla Crear registro del puntero PTR asociado.

Para actualizar manualmente el archivo de zona, hay que seleccionar la zona que se desea actualizar y escoger entonces Actualizar archivo de datos del servidor en el menú acción.

#### Interoperación con otros servidores DNS.

De forma predeterminada, el servidor DNS de Windows Server realiza transferencias de zona rápidas con compresión de datos y envío de múltiples registros de recursos en cada mensaje. Este método de transferencia de zona funciona con todos los servidores DNS de Windows y servidores DNS BIND versión 4.9.4 o posterior. Si se necesita realizar transferencias de zona con servidores BIND anteriores a la versión 4.9.4, será necesario desactivar este método de transferencia de zona rápida. Hay que seleccionar el servidor DNS en el árbol de la consola y escoger propiedades en el menú Acción. Después hay que pulsar la pestaña Avanzado y desactivar la casilla de verificación Enlazar secundarios.

## Administración del servidor DNS.

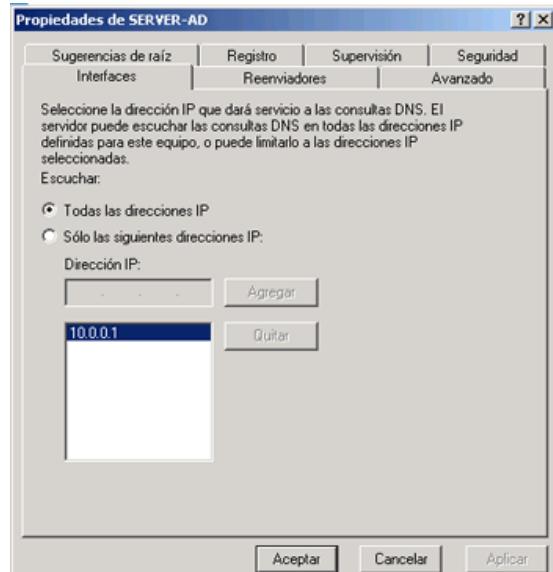
### Pestaña interfaces.

En el caso de los servidores DNS multitarjeta (que funcionan en ordenadores con varias tarjetas de red), puede configurar el servicio DNS para habilitar de forma selectiva y enlazar sólo con las direcciones IP que especifique con la consola DNS. De forma predeterminada, el servicio DNS enlaza con todas las interfaces IP configuradas para el equipo. Esto puede incluir:

Cualquier dirección IP adicional configurada para una conexión de red única.

Direcciones IP individuales configuradas para cada conexión diferente donde haya instaladas más de una conexión de red en el equipo servidor.

En el caso de los servidores DNS multitarjeta, puede restringir el servicio DNS para las direcciones IP seleccionadas. Cuando se utilice esta característica, el servicio DNS sólo atenderá y responderá a las peticiones DNS que se envíen a las direcciones IP especificadas en la ficha Interfaz de las Propiedades del servidor.

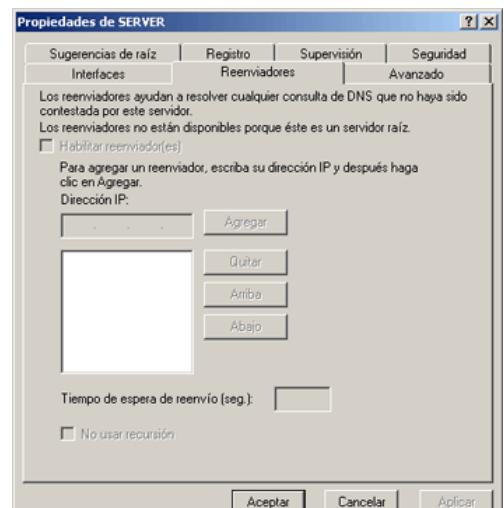


### Pestaña Reenviadores

Ningún servidor de nombres será capaz de responder a las consultas de todos los clientes; algunas veces los clientes solicitarán un nombre DNS que no se encuentra en ninguna de las zonas administradas por el servidor DNS. En estos casos, se puede configurar un servidor DNS para que reenvíe la petición a otro servidor DNS con más probabilidad de tener el registro en su zona o archivo caché. Esta capacidad se necesita más frecuentemente para resolver nombres externos a la red en la que residen los clientes.

Cuando un cliente quiere resolver un nombre fuera de la red interna, se puede configurar un servidor DNS interno para que reenvíe la consulta a un servidor DNS externo a la red, quizás al otro lado de un cortafuego. Este servidor de nombres externo puede entonces realizar consultas más a fondo fuera de la red si es necesario y devolver los resultados al servidor DNS reenviador. Para configurar el servidor DNS de forma que reenvíe las consultas no resueltas a otro servidor DNS, hay que seguir estos pasos:

(Por razones de seguridad, un único servidor DNS reenviará por regla general las peticiones de la red interna a un servidor DNS al otro lado de un cortafuego. El resto de los servidores DNS internos reenvían sus consultas al reenviador designado para que sean pasadas al servidor de nombres externo (o resueltas a partir del archivo caché del reenviador).



1. En el árbol de la consola, hay que seleccionar el servidor DNS sobre el que se desea activar el reenvío, y escoger después propiedades en el menú Acción.
2. Escoger la ficha Reenviadores y seleccionar la casilla de verificación Habilitar reenviador(es).
3. Introducir las direcciones IP del servidor o servidores DNS a los cuales se desea reenviar las consultas no resueltas, pulsando el botón Agregar tras introducir cada una.

Antes de avanzar al siguiente servidor de la lista de servidores a los que reenviar consultas, hay que introducir la cantidad de tiempo que se desea emplear en contactar con un servidor DNS.

Para configurar el servidor DNS como un servidor esclavo -un servidor que no trata de resolver ninguna consulta a partir de sus propios archivos de zona o caché- hay que seleccionar la casilla de verificación No usar recursión

### Pestaña Avanzadas

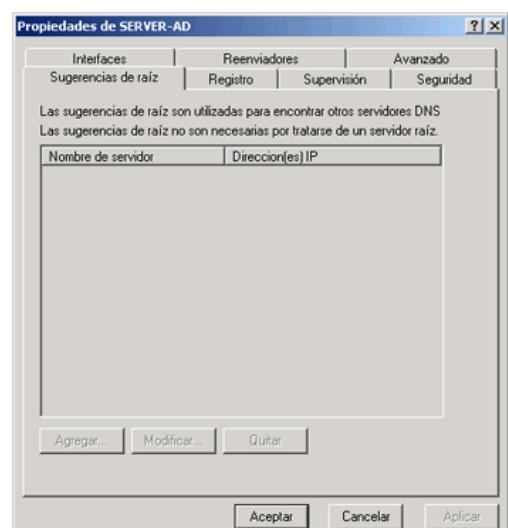
Cuando se inicia el servicio, los servidores DNS de Windows Server utilizan los valores de configuración del servidor obtenidos de los parámetros establecidos en el archivo de información de inicio, en el Registro de Windows Server o en los valores predeterminados que proporciona la integración de Active Directory.

En la mayoría de las situaciones, los valores predeterminados de la instalación son aceptables y no deberían necesitar modificaciones. Sin embargo, cuando sea necesario puede utilizar la consola DNS para ajustar los siguientes parámetros avanzados, que permiten adaptarse a las situaciones y necesidades especiales de distribución.

### Pestaña sugerencias de raíz

Las sugerencias de raíz se utilizan para preparar los servidores autoritativos para zonas que no sean de raíz, a fin de que puedan aprender y descubrir servidores autoritativos que administran dominios de un nivel superior o de otros subárboles del espacio de nombres del dominio DNS. Estas sugerencias son esenciales para los servidores autoritativos de niveles inferiores del espacio de nombres cuando localicen y busquen servidores en estas condiciones.

Por ejemplo, suponga que un servidor DNS (Servidor A) tiene una zona llamada sub.ejemplo.microsoft.com. En el proceso de respuesta a una consulta de un dominio de nivel superior, como el dominio

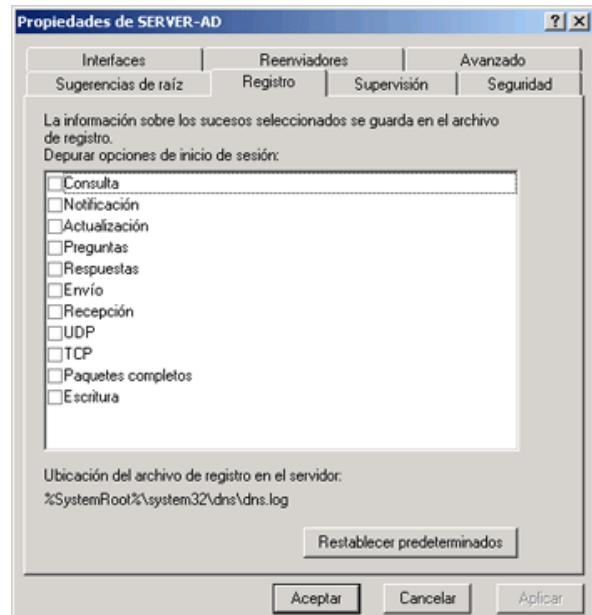


microsoft.com, el Servidor A necesita ayuda para ubicar un servidor autoritativo (como el Servidor B) de este dominio.

Para que el Servidor A encuentre al Servidor B o cualquier otro servidor autoritativo para el dominio microsoft.com, es necesario que pueda consultar a los servidores raíz del espacio de nombres DNS.

Los servidores raíz pueden remitir el Servidor A a los servidores autoritativos del dominio com. A su vez, los servidores del dominio com pueden ofrecer referencia al Servidor B u otros servidores autoritativos para el dominio microsoft.com.

Las sugerencias de raíz utilizadas por el Servidor A deben tener sugerencias útiles para los servidores raíz a fin de que este proceso localice al Servidor B (u otro servidor autoritativo), como se pretende.



### Pestaña registros

Para los servidores DNS de Windows Server se pueden utilizar las siguientes opciones de registro de depuración:

- Consulta: Registra consultas recibidas por el servicio del Servidor DNS desde los clientes.
- Notificar: Registra mensajes de notificación recibidos por el servicio del Servidor DNS desde otros servidores.
- Actualización: Registra actualizaciones dinámicas recibidas por el servicio del Servidor DNS desde otros equipos.
- Preguntas: Registra el contenido de la sección de preguntas de cada mensaje de consulta DNS procesado por el servicio del Servidor DNS.
- Respuestas: Registra el contenido de la sección de respuestas de cada mensaje de consulta DNS procesado por el servicio del Servidor DNS.
- Envío: Registra los distintos mensajes de consulta DNS enviados por el servicio del Servidor DNS.
- Recepción: Registra los distintos mensajes de consulta DNS recibidos por el servicio del Servidor DNS.
- UDP: Registra las distintas solicitudes DNS recibidas por el servicio del Servidor DNS a través de un puerto UDP.
- TCP: Registra las distintas solicitudes DNS recibidas por el servicio del Servidor DNS a través de un puerto TCP.
- Paquetes completos: Registra los distintos paquetes completos escritos y enviados por el servicio del Servidor DNS.

- Escritura: Registra los distintos paquetes escritos completamente por el servicio del Servidor DNS y devueltos a la zona.

De forma predeterminada, todas las opciones de inicio de registro de depuración están deshabilitadas. Cuando se habilitan de forma selectiva, el servicio del Servidor DNS puede realizar un registro adicional a nivel de seguimiento de tipos seleccionados de sucesos o mensajes para solucionar problemas generales y depurar el servidor.

El registro de depuración puede emplear muchos recursos; esto afectará al rendimiento global del servidor y consumirá espacio en disco. Por lo tanto, sólo debe utilizarse temporalmente cuando se necesite información más detallada acerca del rendimiento del servidor.

Dns.log contiene actividad de registro de depuración. Se encuentra en la carpeta windir\System32\DNS.

### Ficha inicio de autoridad (SOA) y ficha servidores de nombres

---

Las zonas se basan en el concepto de autoridad de servidor. Cuando se configura un servidor DNS para cargar una zona, utiliza dos tipos de registros de recursos para determinar las propiedades autorizadas de la zona.

Primero, el registro de recursos de inicio de autoridad (SOA) indica el nombre de origen de la zona y contiene el nombre del servidor que es el origen principal de información acerca de la zona. También indica otras propiedades básicas de la zona.

Muestra los servidores de nombres (NS) configurados para el servidor o la zona de la manera siguiente:

Cuando esta lista se muestra en la ficha Sugerencias de raíz, que se encuentra en las propiedades de servidor DNS correspondientes, presenta sugerencias de raíz que contienen los servidores raíz que el servidor debe utilizar y a los que debe hacer referencia para resolver nombres. En los servidores raíz, este campo debe estar en blanco.

Cuando esta lista se muestra en la ficha Servidores de nombres, que se encuentra en las Propiedades de zona correspondientes, presenta los servidores DNS configurados actualmente como autoridades para la zona. En la mayor parte de los casos, esto incluye todos los demás servidores que están configurados como secundarios de la zona.

### Ficha WINS

---

El Servicio de nombres Internet de Windows (WINS) se puede usar para buscar nombres DNS que no se pueden resolver mediante la consulta del espacio de nombres de dominio DNS. Para ejecutar la búsqueda WINS, se utilizan dos tipos de registros de recursos específicos que se pueden habilitar para cualquier zona cargada mediante el servicio DNS:

El registro de recursos WINS, que se puede habilitar para integrar la búsqueda WINS en las zonas de búsqueda directa

El registro de recursos WINS-R, que se puede habilitar para integrar la búsqueda inversa WINS en las zonas de búsqueda inversa

Los servicios WINS y DNS se utilizan para proporcionar la resolución de nombres para el espacio de nombres NetBIOS y el espacio de nombres de dominio DNS, respectivamente. Aunque DNS y WINS pueden proporcionar un servicio de nombres útil e independiente a los clientes, WINS se necesita, principalmente, para proporcionar compatibilidad con los clientes y programas antiguos que requieren compatibilidad con los nombres NetBIOS.

Sin embargo, el servicio DNS puede funcionar con WINS para proporcionar búsquedas de nombres combinados en los dos espacios de nombres cuando en una información de zona no se encuentra la resolución de un nombre de dominio DNS. Para proporcionar esta interoperabilidad, se ha definido un nuevo registro (el registro WINS) como parte del archivo de base de datos de zonas.

El registro de recursos WINS es específico para Windows Server y versiones anteriores de Windows NT Server, y se puede conectar sólo al dominio de origen de una zona. La presencia de un registro de recursos WINS puede indicar al servicio DNS que utilice WINS para buscar las consultas directas de nombres de host o nombres que no se encuentran en la base de datos de zonas. Esta funcionalidad es especialmente útil en la resolución de nombres que requieren los clientes que no admiten WINS (por ejemplo, UNIX) para los nombres de los equipos que no se registraron con DNS, como los equipos con Windows 95 o Windows 98.

**Usar búsqueda directa WINS:** Para impedir que el registro WINS sea replicado a cualquier servidor secundario por motivos de compatibilidad (los servidores DNS no Microsoft no soportan registros WINS-R), hay que seleccionar la casilla de verificación No replicar este registro.

**Dirección IP:** Introducir la dirección IP de cada servidor WINS que se quiera consultar, pulsando Agregar tras introducir cada una.

## Servidor DHCP.

Para que un host con TCP/IP se comunique correctamente con otro, ambos deben estar configurados apropiadamente. Requieren una dirección de IP válida y única, una máscara de subred y una dirección de pasarela predeterminada, aunque se puede omitir si el host sólo se va a comunicar en la subred local. Para redes mayores se necesita configurar otros elementos, como la dirección de IP de un servidor de DNS, la dirección de IP de un servidor WINS y los tipos de nodo NetBIOS.

En grandes redes, asegurar que todos los hosts se han configurado correctamente puede ser una tarea de administración y gestión importante, especialmente en redes dinámicas con usuarios móviles con ordenadores portátiles. La configuración manual o la reconfiguración de un gran número de equipos es una tarea que lleva mucho tiempo y un error en la configuración de un host puede hacer que sea imposible que se comunique con el resto de la red.

DHCP es un protocolo cliente-servidor que simplifica la administración de la configuración de los clientes de IP y la asignación de los datos de configuración de IP. Mediante DHCP, el administrador define todos los parámetros de configuración necesarios en un servidor central, quien proporciona a los hosts toda la información de configuración de IP.

DHCP proporciona tres ventajas clave en la planificación, diseño y mantenimiento de una red de IP:

- Administración centralizada de las configuraciones de IP. El administrador de DHCP puede administrar de manera centralizada toda la información de configuración de IP. De esta forma se elimina la necesidad de configurar manualmente los hosts individualmente cuando se implanta por primera vez TCP/IP o cuando se necesitan cambios en la infraestructura de IP.
- Sencillez en la configuración de IP de host. Mediante DHCP se asegura que los clientes de DHCP obtienen parámetros de configuración de IP precisos y en tiempo, sin intervención del usuario. Como la configuración es automática se elimina gran parte de los problemas.
- Flexibilidad. Utilizando DHCP, el administrador aumenta su flexibilidad para el cambio de la información de configuración de IP, lo que permite que el administrador cambie la configuración de IP de manera sencilla cuando se necesitan los cambios.

Todos los Windows Server (incluyendo 2000, 2003 y 2008) incluyen el servicio Servidor de DHCP, que se instala como opcional. Todos los clientes de Microsoft Windows instalan automáticamente el servicio cliente de DHCP como parte de TCP/IP.

## Funcionamiento de dhcp.

Los hosts utilizan el protocolo DHCP para obtener una concesión inicial, renovar una existente y detectar servidores de DHCP no autorizados.

### Obtención de una concesión inicial.

La adquisición de una concesión inicial ocurre la primera vez que un cliente de DHCP arranca.

1. El cliente de DHCP difunde, en primer lugar, el mensaje DHCPDISCOVER para buscar un servidor de DHCP. Como el host no tiene dirección de IP, se comunica con el servidor de DHCP mediante un mensaje de difusión en el área local.
2. Si hay más de un servidor de DHCP que puede proporcionar al cliente de DHCP una dirección de IP válida, es posible que el cliente reciba una o más respuestas DHCPOFFER. Si ocurre esto, el cliente elige la «mejor» de ellas, que en Windows Server será la primera recibida. Para ayudar al cliente a decidir cuál es la mejor oferta, el mensaje DHCPOFFER contiene valores para las opciones que el cliente había solicitado y que se configuran en el servidor de DHCP que la entrega. Cualquier servidor de DHCP que recibe un mensaje DHCPDISCOVER y puede asignar al cliente de DHCP una concesión, enviará un mensaje DHCPOFFER con la dirección de IP ofrecida y valores de opción.
3. Si el cliente puede aceptar esta concesión, envía una DHCPREQUEST al servidor de DHCP, solicitando la dirección de IP ofrecida. Esta solicitud también contendrá todas las opciones de configuración que el cliente de DHCP desea obtener.
4. El mensaje final, DHCPACK, se envía desde el servidor de DHCP hasta el cliente de DHCP para confirmar que el cliente tiene la dirección de IP y los valores de las opciones solicitadas que especificó el administrador de DHCP en el servidor.

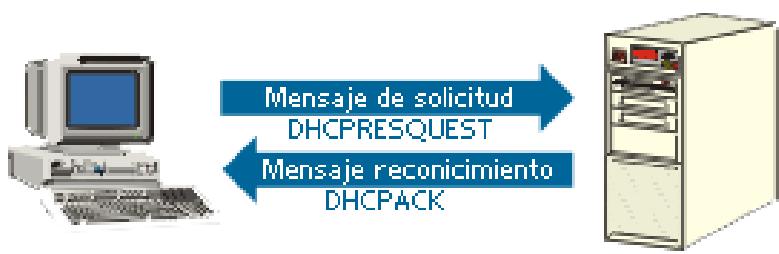


### Renovación de una concesión.

Los clientes de DHCP intentarán renovar la concesión tras cada reinicio o a intervalos regulares después del inicio del cliente de DHCP.

La renovación de una concesión supone sólo dos mensajes de DHCP, DHCPREQUEST y DHCPACK.

Si el cliente de DHCP renueva una concesión mientras se reinicia, se usan paquetes de IP de difusión para enviar estos mensajes. Si la renovación de la concesión se realiza mientras se está ejecutando el cliente de DHCP, el cliente y el servidor de DHCP se comunican mediante dirección IP unicast.



Cuando un cliente obtiene una concesión, DHCP proporciona los valores para las opciones de configuración solicitadas por el cliente.

Reduciendo el tiempo de concesión, el administrador fuerza a los clientes a solicitar periódicamente una renovación de la concesión y obtener detalles actualizados de configuración. Puede ser útil cuando el administrador desea cambiar la configuración de IP de una subred.

Un cliente de DHCP intenta en primer lugar volver a conseguir su concesión a la mitad del tiempo de concesión, conocido como T1. Si falla el cliente intentará de nuevo una nueva renovación de la concesión al 87,5 por 100 del tiempo de concesión, conocido como T2. Si no se consigue obtener la concesión antes de que expire (por ejemplo, si el servidor de DHCP no está accesible), en cuanto expira la concesión el cliente libera la dirección de IP e intenta conseguir una nueva concesión.

#### Cambios en subredes y servidores.

Si el cliente de DHCP solicita una conexión mediante un mensaje DHCPREQUEST y el servidor de DHCP no puede cumplir (por ejemplo, cuando se traslada un portátil a una subred distinta), el servidor de DHCP envía un mensaje DHCPNAK al cliente. El cliente conseguirá una nueva concesión usando el proceso de adquisición de concesión inicial.



Cuando arranca un cliente de DHCP difunde un mensaje DHCPREQUEST para renovar su concesión. Esto le asegura que la solicitud de renovación de DHCP se envía al servidor de DHCP que proporciona direcciones de DHCP para la subred en la que se encuentra ahora el cliente, que puede ser distinta de la del servidor de DHCP que proporcionó la concesión inicial. Cuando el servidor de DHCP recibe la difusión, compara la dirección del cliente de DHCP solicitante con el ámbito configurado en el servidor. Si es imposible satisfacer la solicitud del cliente, el servidor de DHCP envía un DHCPACK y el cliente consigue una nueva concesión.

Si el cliente de DHCP no es capaz de localizar ningún servidor de DHCP cuando se reinicia, para renovar su concesión envía una difusión de ARP (Address Resolution Protocol, Protocolo de Resolución de Direcciones) para la pasarela predeterminada que se obtuvo anteriormente, si la hubo. Si la dirección de IP de la pasarela predeterminada se resuelve correctamente, el cliente de DHCP supone que se encuentra situado en la misma red donde obtuvo su concesión actual que continúa usando.

Si la difusión de ARP del cliente enviada para la pasarela predeterminada no recibe respuesta, el cliente supone que el cliente se ha trasladado a una red que no dispone actualmente de servicios de DHCP, como la red de casa, y se auto configura él mismo mediante APIPA (Automatic Private IP Addressing, Dirección privada IP automática (169.254.x.x)). Una vez auto configurado a sí mismo, el cliente de DHCP intentará, cada 5 minutos, localizar un servidor de DHCP.

#### Detección de servidores de dhcp no autorizados.

Como parte de la inicialización del servicio de DHCP, todos los servidores de DHCP realizan una detección de servicios rogue. Si el servidor no está autorizado en el Active Directory, se apaga.

La detección de servidor rogue comienza con la inicialización del servidor de DHCP enviando una solicitud DHCPINFORM para determinar si existen otros servidores de DHCP inicializados en cualquier red conectada. Si es así, estos servidores responden con un mensaje DHCPACK que contiene el nombre del dominio en el que tienen autorización.



Si se encuentran otros servidores de DHCP, el servicio de DHCP de Windows Server que está arrancando se conecta con el Active Directory y envía una serie de llamadas LDAP para descubrir si está autorizado o no. Si el servidor no está autorizado, el servicio termina. Esta detección se lleva a cabo una vez cada hora por el servidor de DHCP para detectar nuevos servidores no autorizados.

Si está activado el registro de sucesos de DHCP, se escribe un mensaje en el registro de sucesos de DHCP.

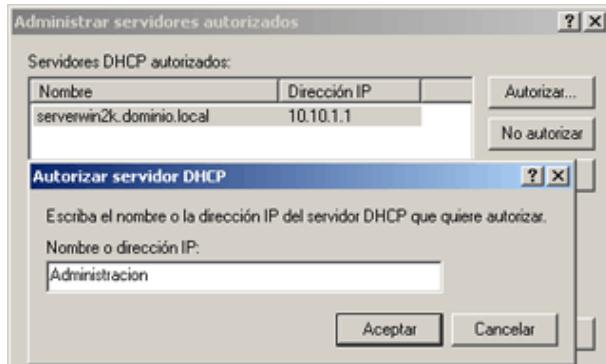
#### Configurando un servidor dhcp.

El servidor DHCP reduce enormemente la tarea administrativa de configurar estaciones de trabajo con una dirección IP y la configuración TCP/IP apropiada para la red. Antes de instalar el servidor DHCP hay que determinar el esquema de direcciones IP. También se deben completar estos pasos adicionales antes de instalar DHCP:

1. Determinar el intervalo de direcciones IP libres y únicas que manejará el servidor DHCP además de cualquier dirección IP que sea necesario excluir para soportar hosts con direcciones IP estáticas.
2. Hacer una lista de los servidores para los que se desea reservar una IP (como servidores DNS y WINS).
3. Configurar manualmente las direcciones estáticas en el equipo donde se instalará el servicio DHCP

Para instalar el servidor DHCP, hay que seguir estos pasos:

- Si se desea instalar el servicio DHCP en un servidor que no sea controlador de dominio, será necesario comunicárselo a Active Directory. Después de la instalación hay que abrir DHCP desde el menú Herramientas administrativas. Hay que resaltar DHCP en el árbol de la consola y escoger después Examinar servidores autorizados en el menú Acción. Hay que pulsar Agregar y escribir después el nombre o la dirección IP del servidor DHCP a autorizar.

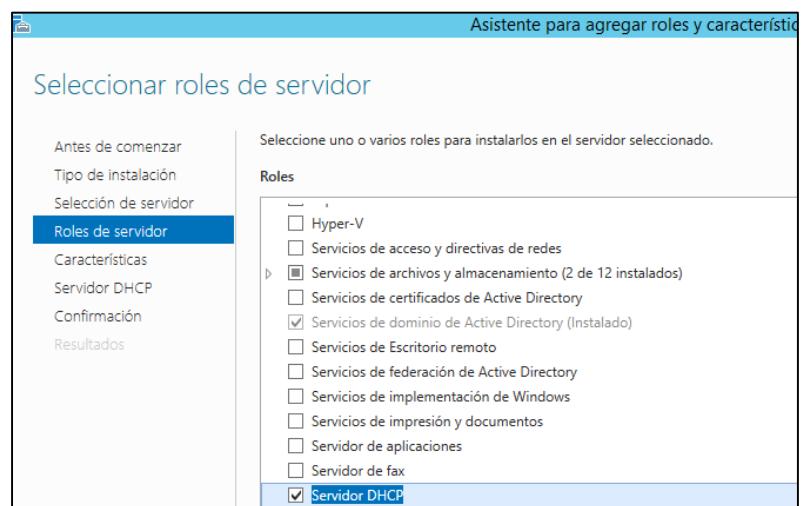


Si se piensa utilizar múltiples servidores DHCP en una subred para realizar equilibrio de carga y tener redundancia, hay que configurar un superámbito en cada servidor DHCP que contenga todos los ámbitos válidos de la subred como ámbitos miembro. Hay que configurar entonces el ámbito miembro en cada servidor para que tenga excluidas las direcciones de los otros servidores de forma que no aparezcan direcciones en ninguna de las colas de direcciones de los servidores. Una buena división consiste en darle el 80 por 100 de las direcciones al servidor DHCP principal y el 20 por 100 al servidor secundario.

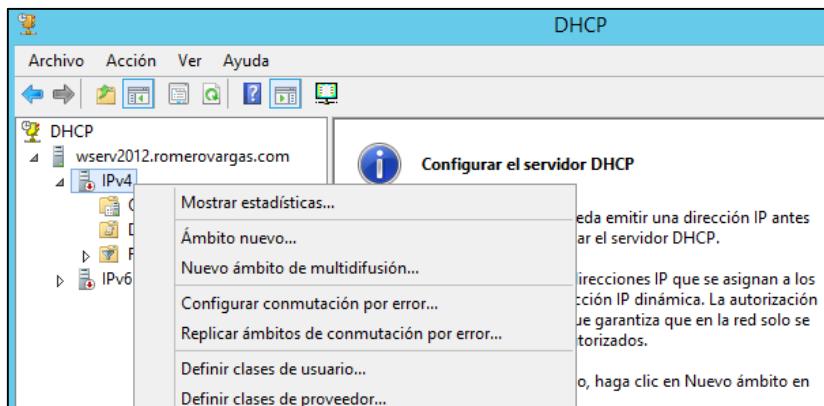
#### Creación de un nuevo ámbito.

Ahora ya se puede ejecutar el Administrador DHCP y crear un nuevo ámbito de direcciones IP para que las gestione el servidor DHCP. Pero antes de hacer esto, hay que asegurarse de que se conoce el intervalo de direcciones IP aprobado, qué direcciones IP son necesarias excluir para los sistemas con direcciones IP estáticas y qué direcciones son necesarias reservar para servidores DNS o WINS. Para abrir el Administrador DHCP y crear el nuevo ámbito, hay que seguir los siguientes pasos:

Escoger DHCP del menú Herramientas administrativas. (Si no aparece DHCP en el menú de Herramientas, es porque no hemos instalado el rol de servidor DHCP, habrá que instalarlo como ya hemos visto en puntos anteriores).



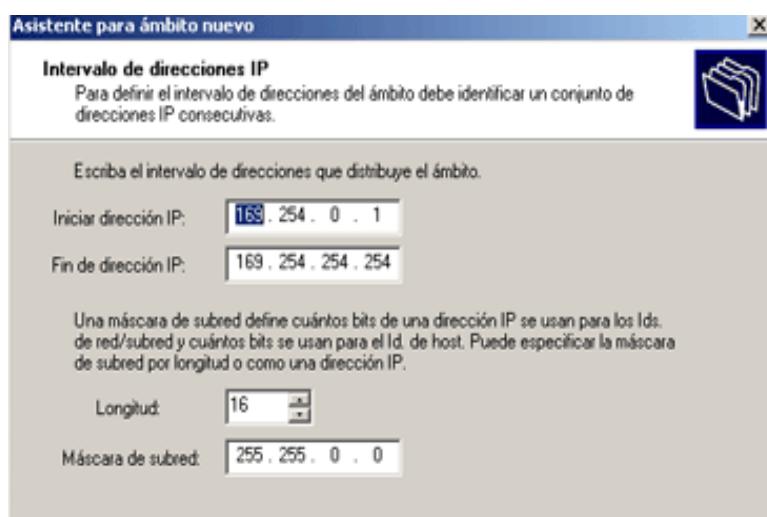
Seleccionar el servidor DHCP en el árbol de la consola. Seleccionar el menú Acción y escoger Ámbito nuevo para ejecutar el Asistente para ámbito nuevo.



Introducimos el nombre y la descripción del ámbito que servirán para distinguir este ámbito de otros.



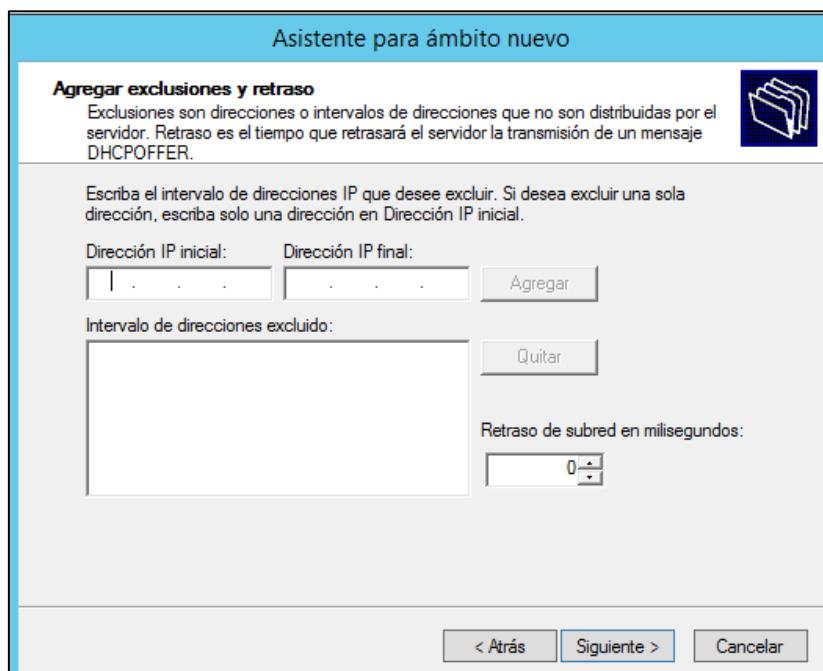
Introducir la dirección IP por la que se desea que comience el ámbito en el campo Iniciar, e introducir la dirección IP por la que se desea que finalice el ámbito en el campo Fin.



Introducir la máscara de subred de la red en el cuadro Máscara de subred, o utilizar el cuadro Longitud para ajustar la longitud de la máscara de subred. Después, pulsar Siguiente.

Para excluir un intervalo de direcciones del ámbito, en el cuadro Iniciar dirección IP, hay que introducir la dirección IP de comienzo para el intervalo de exclusión; en el cuadro Fin de dirección IP hay que introducir la dirección IP final del intervalo de exclusión. Después hay que pulsar Agregar.

Desde aquí también podemos indicar un tiempo que retrasará el servidor la transmisión de un mensaje DHCPoffer.



Especificar la duración de la concesión a los clientes y pulsar Siguiente. Conviene utilizar concesiones más largas en redes sin servidores DHCP redundantes para permitir más tiempo de recuperación de un servidor DHCP sin conexión antes de que los clientes pierdan sus concesiones, o para minimizar el tráfico de red a expensas de una renovación de direcciones menos frecuente. También se pueden utilizar concesiones más largas si las direcciones del ámbito son abundantes (al menos un 20 por ciento disponible), la red es estable y los equipos rara vez se mueven. Por el contrario, los ámbitos que soportan clientes que acceden telefónicamente pueden tener concesiones más cortas y, por lo tanto, funcionar bien con menos direcciones.

Para configurar las opciones de DHCP, hay que pulsar Configurar estas opciones ahora; en otro caso, hay que pulsar Configuraré estas opciones más tarde. Si se selecciona Configuraré estas opciones más tarde hay que pulsar Finalizar para completar la instalación del ámbito.

Si se decide especificar las opciones de DHCP, hay que introducir las puertas de enlace (enrutadores) que se desea que utilicen los clientes en el cuadro Dirección IP, pulsando el botón Agregar después de introducir cada uno. Cuando se haya terminado de introducir puertas de enlace hay que pulsar Siguiente.

Introducir el nombre de dominio del dominio en el cuadro Dominio primario, y añadir las direcciones IP de los servidores DNS en el cuadro Dirección IP, pulsando Agregar tras introducir cada una. Hay que pulsar Siguiente cuando se haya terminado.

En el cuadro Dirección IP de Servidores WINS, hay que introducir las direcciones de todos los servidores WINS que se hayan configurado en la red para asignar direcciones IP a los nombres NetBIOS de los clientes de nivel inferior. No es habitual tener este tipo de servidores instalados en la red. Pulsar Siguiente.

Para activar el ámbito inmediatamente, hay que pulsar Activar este ámbito ahora; en caso contrario, hay que pulsar Activaré este ámbito más tarde. Hay que pulsar Siguiente y pulsar después Finalizar para completar la configuración del ámbito.

---

Autorización del servidor dhcp y activación de los ámbitos.

Después de configurar el servidor DHCP y crear los ámbitos, es necesario activar los ámbitos antes de que cualquier cliente pueda utilizar el servidor para obtener direcciones IP. Antes de que se puedan activar los ámbitos, el servidor tiene que ser autorizado a realizar concesiones, a menos que se haya instalado DHCP en un controlador de dominio, en cuyo caso el servidor DHCP será autorizado automáticamente la primera vez que se añada el servidor a la consola Administrador DHCP.

La autorización de un servidor DHCP es una opción importante que proporciona Windows Server para reducir la capacidad de los hackers de configurar servidores DHCP corrompidos: servidores no autorizados configurados para proporcionar direcciones IP falsas a los clientes. Para autorizar el servidor DHCP después de instalar el servicio, hay que seguir los siguientes pasos:

1. En el Administrador DHCP hay que seleccionar DHCP en la raíz del árbol de la consola.
2. Escoger Administrar servidores autorizados en el menú Acción.
3. Seleccionar Autorizar en el cuadro de diálogo Administrar servidores autorizados.
4. Introducir el nombre o la dirección IP del servidor en el cuadro de texto proporcionado y pulsar Aceptar.
5. Verificar que la información es correcta en el cuadro de diálogo que se muestra y entonces pulsar Sí. Hay que pulsar Aceptar para cerrar el cuadro de diálogo Administrar servidores autorizados.
6. Para activar un ámbito hay que seleccionarlo en el árbol de la consola y escoger después Activar en el menú Acción.

No se debe activar un ámbito hasta que se hayan terminado de seleccionar todas las opciones deseadas. Una vez activado un ámbito, el comando Activar del menú cambia a Desactivar. No se debe desactivar un ámbito a no ser que vaya a ser retirado permanentemente de la red.

### Reservando direcciones.

Las reservas son elementos prácticos que se pueden utilizar en lugar de las direcciones IP estáticas (que requieren exclusiones) para todos los servidores (excepto servidores DHCP) que necesiten mantener una dirección IP específica, como servidores DNS y WINS. Al utilizar reservas en lugar de direcciones estáticas se garantiza que un servidor tendrá una dirección IP consistente proporcionando al mismo tiempo la capacidad de recuperar la dirección IP en el futuro si el servidor es retirado de la circulación o movido. Se debería crear la reserva en todos los servidores DHCP que podrían servir potencialmente al cliente reservado.

Para añadir una reserva de dirección a un ámbito:

1. Pulsar con el botón derecho del ratón en la carpeta Reservas bajo el ámbito deseado y escoger Reserva nueva en el menú contextual.
2. Introducir el nombre de la reserva en el cuadro Nombre de reserva.
3. Introducir la dirección IP para el cliente en el cuadro Dirección IP e introducir la dirección MAC del cliente en el cuadro Dirección MAC.
4. Introducir una descripción para la reserva en el cuadro Descripción.
5. Determinar a qué tipo de cliente se desea permitir que utilice la reserva seleccionando Sólo DHCP, Sólo BOOTP o Ambos. A continuación, pulsar Agregar.



Para obtener la dirección MAC hay que ir al equipo cliente y escribir ipcongig /all en el símbolo del sistema. La dirección MAC se muestra como dirección física.

### Activación de las actualizaciones dinámicas de un servidor DNS

Los servidores DHCP y DNS de Windows Server soportan ahora actualizaciones dinámicas con un servidor DNS, una característica que cualquier administrador que haya tenido que gestionar un servidor DNS de Windows NT 4 estático (o similar) apreciará. Los clientes Windows Server pueden actualizar dinámicamente sus registros de búsquedas directas ellos mismos con el servidor DNS después de obtener una nueva dirección IP de un servidor DHCP.

Además, el servidor DHCP de Windows Server soporta también actualización dinámica de registros DNS para clientes anteriores a Windows Server que no lo puedan hacer ellos mismos. Esta característica sólo funciona actualmente con los servidores DHCP y DNS de Windows Server.

Para permitir que un servidor DHCP actualice dinámicamente los registros DNS de sus clientes, hay que seguir los siguientes pasos:

1. Seleccionar el ámbito o el servidor DHCP en el cual se desea permitir actualizaciones dinámicas.
2. En el menú Acción, escoger Propiedades y pulsar después la pestaña DNS.

3. Seleccionar la casilla de verificación Actualizar automáticamente la información del cliente DHCP en DNS.
4. Para actualizar los registros DNS de un cliente basándose en el tipo de petición DHCP que hace el cliente y sólo cuando sea solicitado, hay que seleccionar la opción Actualizar DNS sólo a la petición del cliente DHCP
5. Para actualizar siempre los registros de búsqueda directa e inversa de un cliente, hay que seleccionar la opción Actualizar siempre DNS.
6. Seleccionar la casilla de verificación Descartar las búsquedas directas al caducar la concesión para permitir que el servidor DHCP borre el registro de recurso Host de un cliente cuando su concesión DHCP caduque y no sea renovada.
7. Seleccionar la casilla de verificación Habilitar actualizaciones para clientes DNS que no sean compatibles con actualizaciones dinámicas para permitir que el servidor DHCP actualice los registros de búsqueda directa e inversa de los clientes que no pueden actualizar sus propios registros de búsqueda directa. Si no se selecciona esta casilla de verificación, el servidor DHCP no actualizará dinámicamente los registros DNS de los clientes que no sean Windows Server.

Si se tienen servidores DNS estáticos como los de Windows NT 4, estos servidores no podrán interactuar dinámicamente cuando las configuraciones de los clientes DHCP cambien. Esta incompatibilidad puede provocar búsquedas fallidas en los clientes DHCP. Para evitar este problema, hay que actualizar los servidores DNS estáticos con un DNS que soporte DNS dinámico (Windows Server). Es decir, vuelvo a desaconsejar fervientemente que se monten redes mixtas con servidores NT y 200X trabajando en el mismo entorno.

---

#### Uso de ipconfig para liberar, renovar o verificar una concesión.

En un equipo que ejecuta Windows con DHCP activado se puede ejecutar una utilidad de línea de comandos para liberar, renovar o verificar la concesión de dirección del cliente. En el símbolo del sistema (o en la ventana Ejecutar) hay que utilizar alguno de los siguientes comandos:

Para liberar una concesión de un cliente, hay que escribir ipconfig/release.

Para renovar una concesión, hay que escribir ipconfig /renew.

Para verificar la concesión del cliente, hay que escribir ipconfig /all.

Con clientes Windows 95/98 hay que utilizar winipcfg con los mismos parámetros. El programa ipconfig es útil a la hora de solucionar problemas porque muestra cada detalle de la configuración TCP/IP actual.

## Cuentas de usuario y grupo en Windows server.

### Tipos de cuentas.

Podemos crear tres tipos de cuenta en Active Directory: cuentas de usuario, cuentas de grupo y cuentas de equipo. Las cuentas de usuario y equipo de Active Directory representan una entidad física, como un equipo o una persona. Las cuentas de grupo sirven como contenedores de los otros 2 tipos de cuenta.

#### Cuentas de usuario.

Cada persona que quiera acceder al dominio necesita que se le cree una cuenta de usuario del dominio. Una cuenta de usuario hace posible lo siguiente:

- Autentificar la identidad de la persona que se conecta a la red.
- Controlar el acceso a los recursos del dominio.
- Auditlar las acciones realizadas utilizando la cuenta.

Windows Server sólo crea dos cuentas de usuario predefinidas: la cuenta **Administrador**, que otorga al usuario todos los derechos y permisos, y la cuenta **Invitado**, que tiene derechos limitados. El resto de las cuentas las crea un administrador y son cuentas de dominio (validas a lo largo de todo el dominio de forma predeterminada). Un controlador de dominio no puede crear cuentas locales, como se puede comprobar si intentamos ejecutar lusrmgr.msc (gestión de usuarios locales) en un controlador de dominio.

#### Nombre principal de usuario (UPN).

Un nombre principal de usuario es un nombre de inicio de sesión que se utiliza para conectarse a una red de Windows Server. Este nombre también se denomina nombre de inicio de sesión de usuario. Un nombre principal de usuario tiene dos partes separadas por el signo @ (como si fuera una cuenta de correo electrónico). Ejemplos de nombres UPN son [godofredo@iesromerovargas.local](mailto:godofredo@iesromerovargas.local) o [floripondio@dominio.com](mailto:floripondio@dominio.com).

De forma predeterminada, el nombre del usuario lo otorga un administrador al crear la cuenta de usuario, mientras que el sufijo principal (lo que va detrás de la arroba) es el nombre del dominio que se ha creado en nuestro controlador de dominio.

#### Estrategias para nombrar cuentas.

Crear nombres de cuentas de usuario parece una tarea trivial, y efectivamente lo es cuando tenemos que crear un par de usuarios, pero se transforma en una tarea mucho más complicada cuando queremos crear cientos, o incluso miles de cuentas de usuario.

Pongamos por ejemplo que queremos crear una cuenta de usuario para cada alumno del instituto Francisco Romero Vargas, que cuenta con unos 900 alumnos. Evidentemente no podemos usar el nombre (sin apellidos) como nombre de cuenta, o acabaremos con cuentas como Jennifer32, dado que habrá muchos usuarios con el mismo nombre.

Es importante crear una estrategia de denominación de cuentas para nuestros bosques y dominios, creando unas convenciones para nombrar cuentas. Ejemplos validos de estrategias podrían ser por ejemplo:

- Usar los 2 primeros caracteres del nombre, los 2 caracteres primeros del 1º apellido y los 2 caracteres primeros del 2º apellido.
- Usar 3 caracteres para indicar el curso del alumno, los 3 caracteres primeros del nombre y los 2 caracteres primeros del 1º apellido.
- Usar los 4 caracteres primeros del nombre del alumno, la inicial del 1º apellido, la inicial del 2º apellido y los 2 últimos números del DNI del alumno.

Fijaros como la 2ª estrategia tiene la ventaja de que la simple cuenta de usuario nos da información sobre el curso del alumno, por lo que tenemos más control que en los otros dos casos.

A parte de facilitar la creación de las cuentas de usuario, estas estrategias tienen la gran ventaja de que nos permiten crear programas para crear automáticamente cuentas de usuario. Así, podemos llegar a una empresa que cuenta con 200 empleados a los que tenemos que crear una cuenta de usuario. Podemos crear un script o programa que leyendo una lista de los nombres de los usuarios nos cree directamente las cuentas, usando nuestra estrategia definida para nombrar las cuentas.

---

### Contraseñas.

Todos los usuarios deberían tener contraseñas bien escogidas y se les debería requerir que las cambiaren periódicamente. Las cuentas deberían establecerse de forma que se bloquearan cuando se introdujeran contraseñas incorrectas. (Se pueden permitir tres intentos, para dejar margen a errores tipográficos.) Una buena contraseña tiene las siguientes características:

- No es una rotación de los caracteres del nombre de inicio de sesión.
- Contiene al menos un carácter alfabético en mayúsculas, uno en minúsculas y uno numérico.
- Tiene una longitud de al menos seis caracteres.
- No es el nombre o las iniciales del usuario, las iniciales de sus hijos, u otro dato significativo o cualquiera de esos elementos combinado con otra información personal comúnmente disponible como la fecha de nacimiento, el número de teléfono o el nombre del cónyuge.

Entre las mejores contraseñas se encuentran los acrónimos alfanuméricos de frases que tienen un significado para el usuario pero que no es probable que conozcan otros. Esto hace que la contraseña sea fácil de recordar para el usuario, mientras que al mismo tiempo sea difícil de adivinar por una persona de fuera. Por ejemplo, usamos la frase “hasta luego Lucas” y de ella sacamos la contraseña H4st4luegoluc4S (sustituimos las a por el número 4 y ponemos en mayúsculas la primera y última letra).

En Windows Server está activo por defecto la opción de seguridad que obliga a que todas las contraseñas cumplan los requisitos de complejidad. Podemos desactivarla si es necesario desde la consola de políticas de seguridad como ya vimos en temas anteriores.

Conviene educar a los usuarios sobre las contraseñas y su privacidad, pero, sobre todo, merece la pena hacer caso de los propios consejos: hay que asegurarse de que la contraseña seleccionada para administración es una buena contraseña y cambiarla frecuentemente. Hacer esto ayudara a evitar las consecuencias de que alguien se introduzca en el sistema y cause estragos. Si los usuarios se conectaran telefónicamente a la red desde casa a otros sitios remotos, debería incluirse más seguridad que la autorización por contraseña de nivel de dominio.

Los administradores deberían tener dos cuentas en el sistema: una cuenta administrativa y una cuenta de usuario normal. Se debería utilizar la cuenta de usuario normal a menos que se estén realizando tareas administrativas.

## Perfiles de usuario en Windows server.

En Windows, un perfil de usuario consiste en un espacio de almacenamiento donde se guardan los documentos del usuario, distintas preferencias, la organización de su escritorio, los favoritos del navegador web, las configuraciones del registro de sistema de dicho usuario, etc.

Cuando trabajamos con un sistema operativo cliente, este perfil se almacena localmente, es decir, en la maquina donde trabajemos, y en una carpeta determinada:

- Documents and Settings\Nombre del usuario en Windows XP
- Users\Nombre del usuario en Vista, Windows 7, Windows 8.

Una de las ventajas de montar un dominio, es que podemos utilizar perfiles que no se almacenen localmente. En un dominio podemos utilizar:

- Perfiles de usuario locales
- Perfiles de usuario móviles
- Perfiles de usuario obligatorios

### Perfiles de usuario locales.

Estos perfiles son los habituales, cada usuario guarda su perfil en un directorio de la maquina local donde inicia sesión. Es un tipo de perfil que precisa que los usuarios siempre usen el mismo ordenador si quieren poder acceder a sus documentos. Si en nuestro dominio los usuarios suelen cambiarse de ordenador, vamos a tener problemas con los perfiles de usuario locales.

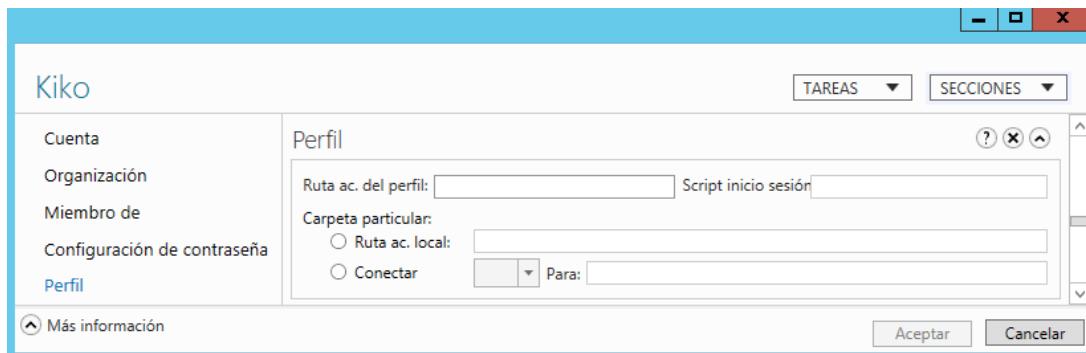
Imaginemos que el usuario JOCADI abre sesión un lunes en el EQUIPO13, trabaja en un documento y cierra sesión al finalizar el día. Si este mismo usuario abre sesión el martes en un equipo distinto, pongamos EQUIPO28, no podrá acceder obviamente al perfil que dejó grabado en el EQUIPO13, y se creará un nuevo perfil local sin ningún contenido en el EQUIPO28.

Obviamente los usuarios pueden ir almacenando sus documentos en memorias USB e irlos pasando de un ordenador a otro, pero esto no quita que sea una fuente de errores importante. Además, un perfil guarda mucha más información aparte de los documentos.

Otro problema con los perfiles de usuario locales, es la perdida de datos por avería o cualquier otro motivo. Puesto que el perfil está grabado en el ordenador local, si este se estropea o tiene que ser cambiado, el usuario se encontrará con que ha perdido sus datos si no los tenía almacenados en algún otro sitio de respaldo.

Las copias de seguridad de la empresa, también se ven muy afectadas por los perfiles de usuario locales. Cada vez que queramos hacer una copia de seguridad de todo, tendremos que ir ordenador por ordenador copiando sus perfiles, y nos encontraremos con muchas versiones de un mismo fichero.

Para utilizar perfiles de usuario locales no hay que hacer nada. Es la opción por defecto del dominio y si no lo configuramos, es la opción que utilizaremos.

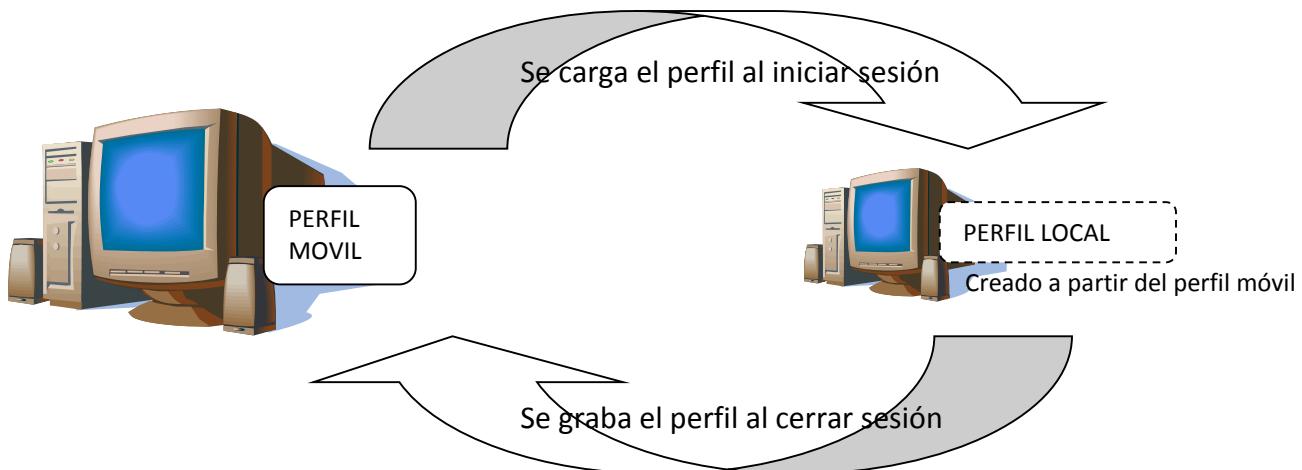


Vemos en la imagen anterior la consola ADAC centrada en la parte que se encarga del perfil del usuario. Si en la ruta de acceso del perfil no ponemos nada, se configura el perfil como local y se almacena en el propio equipo local del usuario como hemos comentado.

### Perfiles de usuario móviles.

En un perfil de usuario móvil, el perfil no se almacena en la máquina local donde se conecta el usuario, sino que se queda almacenado en una carpeta de red, normalmente ubicada en el mismo controlador de dominio.

Siguiendo el ejemplo anterior, el usuario JOCADI abre sesión un lunes en el EQUIPO13, trabaja en un documento y cierra sesión. Su perfil no queda grabado en el EQUIPO13, sino que queda almacenado en el controlador de dominio. Si este usuario llega el martes y abre sesión en el EQUIPO28, comprobará que puede seguir trabajando en el documento del lunes. Da la impresión de que el perfil se “mueve” entre los ordenadores siguiendo al usuario, es por ello que se le da el nombre de perfil móvil.



Como vemos en el gráfico anterior, cuando un usuario abre sesión en una máquina cliente de nuestro dominio, se carga el perfil móvil de dicho usuario desde nuestro servidor, y se guarda una copia en la máquina cliente.

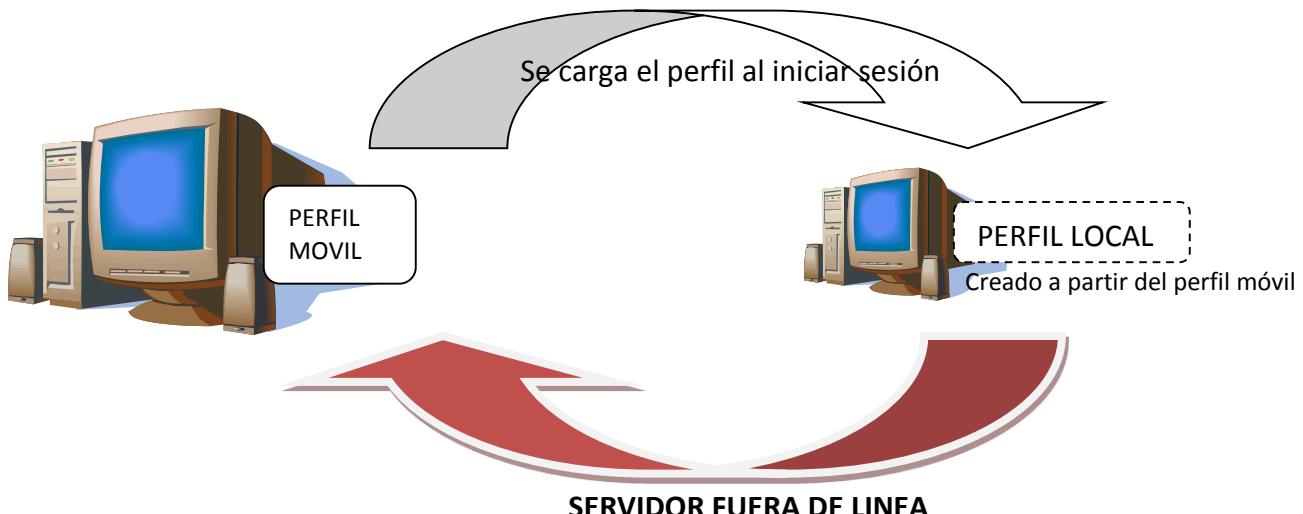
El usuario trabaja en la máquina cliente, y trabaja sobre ese perfil que se ha cargado desde el servidor, por lo que en realidad se comporta como si fuera un perfil local, es decir, cuando guarda un documento lo guarda localmente, no en el servidor.

Esto es así para no sobrecargar la red ni el dominio, si el usuario trabajara sobre el perfil móvil del servidor directamente, habría que estar continuamente enviando información entre la máquina y el servidor y sería muy lento desde el punto de vista del usuario. Otro motivo para trabajar con el perfil local, es que esto nos permite trabajar aunque el servidor deje de estar operativo momentáneamente.

Una vez que el usuario cierra sesión, el perfil local se sincroniza con el perfil que está almacenado en el servidor, añadiendo todos los nuevos documentos y configuraciones, cambiando los que se hayan modificado, etc.

Por lo tanto, en la máquina donde el cliente ha estado trabajando, se queda grabado un perfil local, que es (supuestamente) una copia del perfil móvil que está almacenado en el servidor.

¿Porque decimos lo de supuestamente?



Como vemos en este gráfico, se puede dar el caso de que se inicie sesión en el dominio, se cargue el perfil móvil a la máquina local, el usuario trabaje y modifique dicho perfil, pero cuando llega el momento de cerrar sesión y actualizar los datos del perfil en el servidor, el servidor no está operativo y sea imposible actualizar el perfil móvil almacenado en el servidor.

Como es lógico, esto hará que tengamos dos perfiles distintos para un mismo usuario, uno en el servidor (más antiguo) y otro en la máquina local (más reciente). ¿Qué ocurrirá la próxima vez que el usuario abra sesión en esa máquina, estando ya el servidor operativo?

Lo que ocurre es que cada vez que un usuario inicia sesión, Windows Server no se limita a copiar el perfil móvil en el perfil local, machacando todo lo que hubiera en el equipo cliente, sino que realiza una combinación o **sincronización** de ambos perfiles, machacando los archivos y documentos siempre con el que tenga una fecha posterior, y combinando los archivos únicos de ambos perfiles.

Esto puede conllevar varios comportamientos “extraños” en los perfiles, sobre todo si existen varios usuarios que usen una misma cuenta de usuario, y esta se configura con perfil móvil. Por ello, hay que intentar siempre conceder perfiles móviles únicamente a las cuentas que sepamos que son usadas por una única persona. Si no lo hacemos así, tendremos problemas con los perfiles de esos usuarios compartidos.

Veamos ahora cómo podemos crear un perfil móvil para un usuario.

Accedemos a las propiedades del usuario al que queremos crearle un perfil móvil, usando la consola de Usuarios y Equipos de Active Directory. Desde esta hoja de propiedades accedemos a la pestaña Perfil.

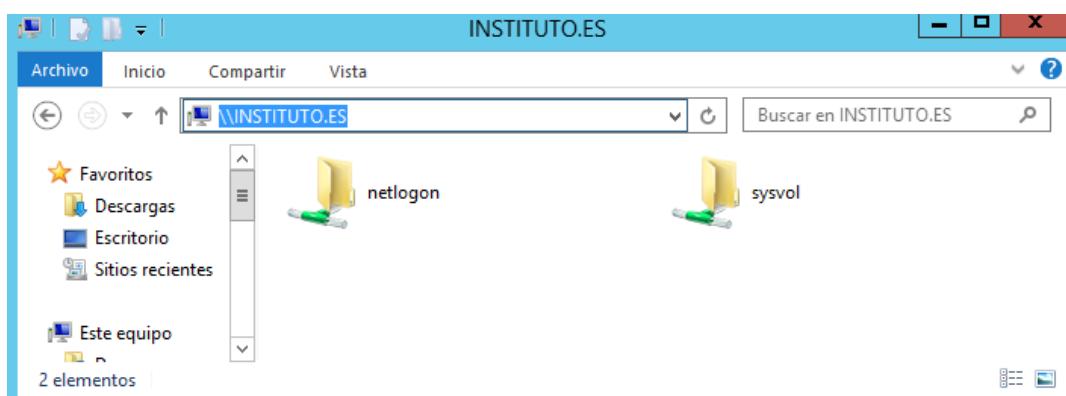


En las propiedades de un usuario del dominio, tenemos que indicar simplemente una ruta en “Ruta de acceso al perfil” que indicará en qué sitio se tiene que almacenar el perfil de dicho usuario. Si no ponemos nada, el perfil se creará en la máquina del usuario, por lo que será un perfil local. Basta con que pongamos cualquier ubicación para poder considerar que el perfil es móvil.

Evidentemente, el usuario debe poder acceder a esta ruta desde una máquina cliente, por lo que debe ser una ruta de red, no tendría sentido grabar el perfil en una ubicación local.

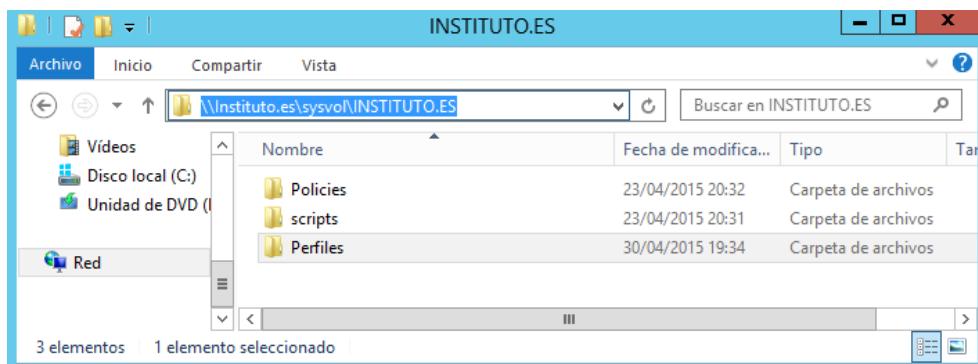
Así, si ponemos como ruta “C:\PERFILES\PEDRO” el usuario guardará su perfil en el disco duro local C: es decir, el disco duro de la máquina cliente donde esté sentado, no en el disco duro del servidor. Lo mismo ocurre si utilizamos la ip 127.0.0.1 por ejemplo.

Si en un explorador de archivos, escribimos \\nombre\_completo\_del\_servidor veremos como aparece una carpeta que directamente está compartida por nuestro servidor en la red, SYSVOL.



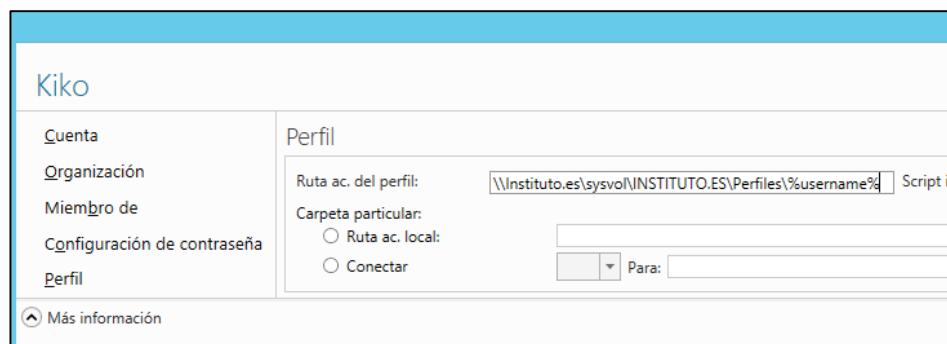
Esta carpeta, que localmente está almacenada en el controlador de dominio en el directorio %WinDir%\SYSVOL\SYSVOL es una carpeta que ya está preparada para ser compartida en red, para almacenar perfiles, scripts, etc. Tiene establecidos todos los permisos adecuados para que todos los usuarios puedan acceder a ella desde la red.

Dentro de esta carpeta sysvol veremos una carpeta con el nombre de nuestro dominio, dentro de esta carpeta crearemos una carpeta para almacenar los perfiles, a la que denominaremos por ejemplo PERFILES. Ahora, dentro de esta carpeta habrá que ir creando una carpeta para cada uno de los usuarios a los que queremos darle un perfil móvil, retocando los permisos tanto de compartición de la carpeta como de seguridad de la misma para asegurarnos que solo el usuario puede acceder a dicha carpeta desde la red.



La carpeta perfil es fácil crearla, pero crear una carpeta para cada usuario con perfil móvil dentro de la misma puede ser un engorro, así que vamos a utilizar un truco, y es indicar al sistema que cree una carpeta con nombre igual a su nombre de usuario automáticamente cuando el usuario inicie sesión por primera vez en el dominio, para ello usaremos la variable de sistema %username% que es la que almacena el nombre del usuario que ha abierto sesión.

De esta forma conseguimos que cada usuario automáticamente cree su propia carpeta, con lo que se establecerán los permisos justamente como nos interesa.



La ruta completa en la imagen anterior sería <\\Instituto.es\sysvol\Instituto.es\Profiles\%username%>

De esta manera, cuando el usuario abra sesión por primera vez en el dominio, el sistema creará una carpeta en la ubicación de red indicada. Esta carpeta, como se crea por el propio usuario automáticamente tendrá los permisos establecidos de modo que él será la única persona que podrá acceder a dicha carpeta y su contenido desde la red, que es precisamente lo que andamos buscando.

Evidentemente nadie nos obliga a crear los perfiles en sysvol, podemos usar cualquier otra carpeta compartida que deseemos, tanto en el controlador de dominio como en cualquier otro punto de la red. Igualmente no tenemos por qué usar la variable username, y podemos dar cualquier nombre a la carpeta donde se almacenará el perfil del usuario.

#### Posibles errores en un perfil móvil.

Si el sistema nos indica al abrir sesión con un usuario que cuenta con perfil móvil que **no encuentra el perfil**, normalmente es debido a que la carpeta que hemos introducido como ruta de perfil, o bien no existe o bien no puede ser accedida por el usuario, debido a permisos mal establecidos. Una forma rápida de comprobarlo, es abrir un explorador de archivos una vez que el usuario abra sesión y escribir la

dirección exacta que hemos puesto en la ruta del perfil. Normalmente comprobaremos como recibimos un error al acceder a dicha carpeta, error que habrá que corregir.

Si el sistema nos indica al abrir sesión con un usuario que cuenta con perfil móvil que le resulta **imposible leer el perfil**, es normalmente debido a que el usuario no tiene permisos de lectura sobre la carpeta que hemos introducido como ruta de perfil. Lo comprobamos de la misma forma que en el punto anterior.

Si el sistema nos indica al **cerrar sesión** con un usuario que cuenta con perfil móvil que le resulta **imposible grabar el perfil**, es debido a que el usuario no tiene permisos de escritura sobre la carpeta que hemos introducido como ruta de perfil, o bien a que la carpeta ha dejado de estar compartida por alguna razón.

Como vemos, es muy importante leer la información del error en pantalla. Ya sabéis, hay que intentar resistir la extraña fuerza que os impulsa a cerrar los mensajes de error inmediatamente sin leerlos antes.

### Perfiles de usuario obligatorios.

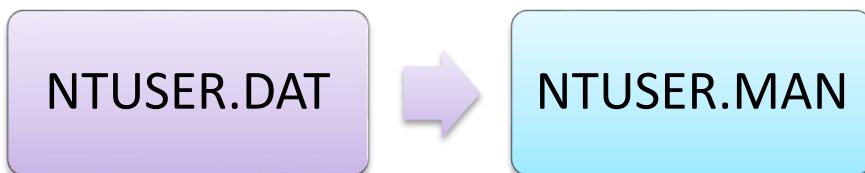
Un perfil de usuario obligatorio es en realidad un perfil móvil que asignamos a los usuarios, pero sin darles permiso para que graben el perfil en el servidor al terminar la sesión.

Al no permitir que el usuario sincronice el perfil en el servidor al cerrar sesión, conseguimos que el usuario use un perfil de “solo lectura”. No importa lo que haga con el perfil de usuario, cuando cierre y vuelva a abrir sesión el perfil volverá siempre al mismo estado.

Es un perfil que se usa mucho en bibliotecas, cibercafé, y en general en cualquier situación donde queremos que un usuario pueda abrir sesión en nuestro dominio, pero no queremos que modifique nada o deje grabado nada en las máquinas.

Estos perfiles obligatorios ademán suelen ser compartidos por múltiples usuarios, de modo que tendremos un número amplio de usuarios utilizando un único perfil obligatorio.

Para conseguir que un perfil se transforme en obligatorio, simplemente hay que ir a la carpeta donde se almacena su perfil y buscar un archivo que se denomina NTUSER.DAT que es el archivo donde se almacenan todas las modificaciones del usuario en el registro del sistema. Basta con modificar la extensión de este fichero, de .DAT a .MAN, es decir, renombrar el fichero NTUSER.DAT a NTUSER.MAN. Con esto conseguiremos que dicho perfil sea obligatorio y que el usuario no lo pueda modificar.



Para poder modificar este fichero, necesitamos acceder al perfil del usuario como usuario administrador, el problema es que dicha cuenta no puede acceder a los perfiles del usuario. Para conseguir este acceso, tenemos que hacer al **grupo Administradores** propietario de la carpeta del perfil del usuario (recordando activar la herencia para subcontenedores) y posteriormente modificar la seguridad del perfil para que pueda ser accedido tanto por el usuario para el que se creó el perfil inicialmente como por el grupo administradores. Es importante no asignar la propiedad del perfil a nadie que no sea el grupo administradores, ya que de lo contrario el perfil se corrompería.

Para generar un perfil obligatorio en primer lugar hay que crear un perfil local de usuario, posteriormente hay que modificar dicho perfil renombrando el fichero NTUSER.DAT a NTUSER.MAN, tenemos también que borrar algunas carpetas del perfil para que pueda ser utilizado como obligatorio, y además tendremos que modificar los permisos de dicho perfil, tanto en seguridad, como en permisos de red, como en el registro del sistema. Una vez realizado todo esto y preparado el perfil podremos utilizarlo con múltiples usuarios.

Una vez que tengamos un perfil obligatorio bien realizado debemos comprobar que realmente el perfil es obligatorio (de solo lectura). Podemos comprobarlo de la siguiente manera:

1. Abrimos sesión
2. Modificamos el perfil (poniendo accesos directos en el escritorio por ejemplo)
3. Cerramos sesión

4. Abrimos sesión y comprobamos que los cambios no se han grabado.

Veamos cómo podemos crear un perfil obligatorio:

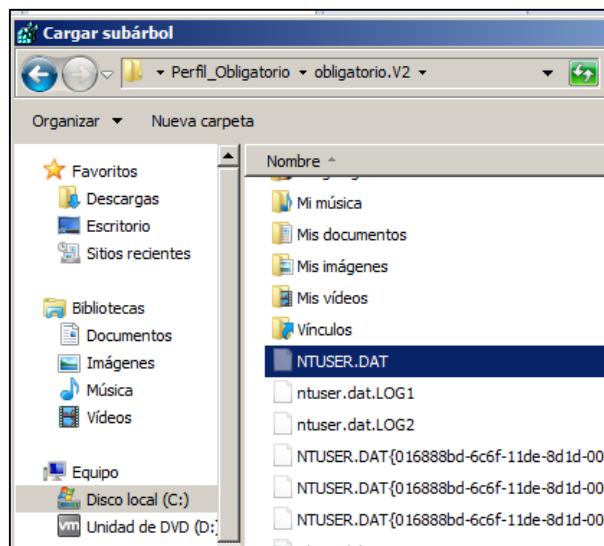
- 1) Creamos un usuario en el servidor Windows 2012 R2. (Por ejemplo con nombre Obligatorio).
- 2) Hacemos a ese usuario miembro del grupo de Administradores de nuestro servidor.
- 3) Iniciamos sesión con dicho usuario en el servidor y lo configuramos para que quede el perfil como deseemos. (Aquí es donde configuramos los accesos directos del escritorio, los programas de la barra de tareas, etc).
- 4) Cerramos sesión y abrimos una nueva sesión con nuestra cuenta habitual con permisos de administrador.
- 5) Creamos una carpeta compartida en el servidor (podemos usar SYSVOL o bien crear un recurso compartido nuevo). Los permisos hay que dejarlos de modo que todo el mundo tenga control total en el permiso de red, y en los permisos NTFS dejad los permisos de modo que los usuarios que vayan a tener perfil obligatorio puedan leer. (Por ejemplo, cread un grupo Perfil\_Obligatorio y dadle permisos de lectura).
- 6) Desactivar el cache de ese recurso compartido. (Permisos de red)
- 7) Ahora debemos copiar el perfil que se habrá creado en C:\Users del usuario creado en el punto 1 (Obligatorio) al directorio que hemos creado y compartido en el punto anterior.
- 8) Borramos las carpetas Local y LocalLow que encontraremos dentro del perfil copiado en el directorio oculto AppData.
- 9) Renombra el directorio del perfil del usuario añadiéndole la extensión V2. (Así, si creamos el usuario Olegario y hemos copiado la carpeta Olegario tenemos que renombrar dicha carpeta a Olegario.V2). Esto es debido a que los perfiles de los nuevos Windows Server utilizan esta extensión para distinguirlos de los perfiles de Windows 2003.
- 10) IMPORTANTE. Hemos modificado los permisos de la carpeta del perfil y subcarpetas (comprobádlo por si acaso) pero al ser un perfil compartido, tendremos que modificar también los permisos internos del fichero NTUSER.DAT que en realidad es una rama del registro de Windows. Para conseguir esto tenemos que hacer lo siguiente:
  - a) Ejecutamos el comando regedit.exe
  - b) Seleccionamos la carpeta HKEY\_USERS



- c) En el menú Archivo, hacemos clic en la opción cargar subárbol



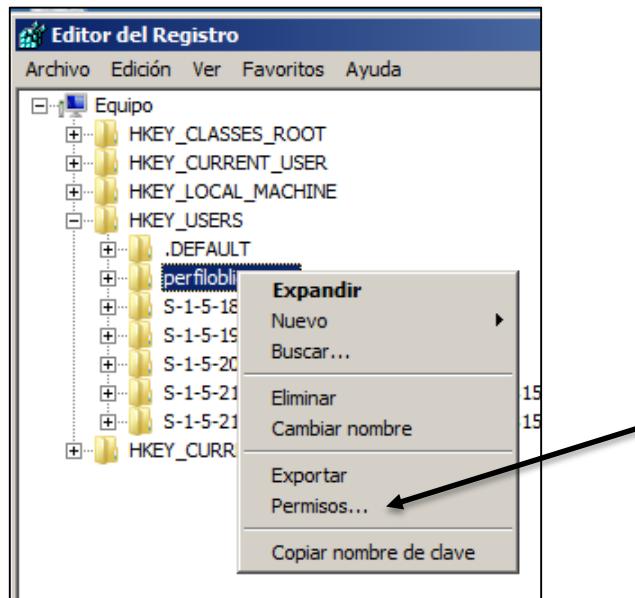
- d) Escogemos el fichero NTUSER.DAT de nuestro perfil (el que hemos renombrado añadiéndole .V2)



- e) Le ponemos un nombre a la rama cuando nos lo pida, por ejemplo perfilobligatorio.



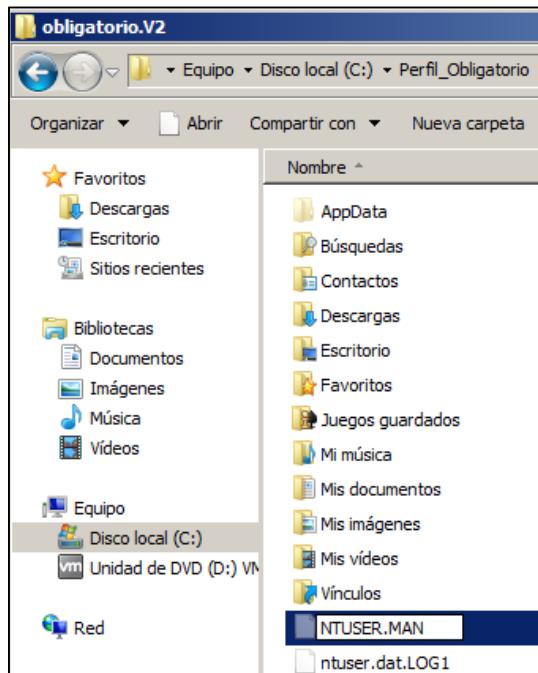
- f) Damos botón derecho en perfil obligatorio y escogemos permisos.



- g) Le damos permiso de CONTROL TOTAL a los usuarios que vayan a usar dicho perfil (en nuestro ejemplo, el grupo Perfil\_Obligatorio) y nos aseguramos de que la herencia se aplique hacia abajo.
- h) Descargamos el árbol del registro (menú Archivo – Descargar subárbol).



- 11) Ahora ya podemos renombrar el fichero NTUSER.DAT a NTUSER.MAN.



- 12) Y después de estos pasos, ya hemos conseguido crear un perfil obligatorio que puede ser compartido por múltiples usuarios. Ahora bastaría con crear un usuario, hacerlo miembro del grupo Perfil\_Obligatorio, y en su pestaña perfil ponerle la ruta de red necesaria para llegar a nuestro perfil (en nuestro ejemplo, Obligatorio.V2).

Importante: Cuando especifiquemos el perfil obligatorio al usuario, hemos de indicarle que su perfil es el nombre de la carpeta sin la extensión V2.

### Perfiles de usuario súper obligatorios.

Un perfil súper obligatorio es similar al perfil obligatorio que acabamos de ver, con la diferencia de que el usuario al que asignemos un perfil súper obligatorio no podrá abrir sesión en el dominio si el servidor donde se almacena su perfil no está disponible.

Los perfiles obligatorios si pueden abrir sesión aunque el servidor donde se almacena el perfil este fuera de línea, en cuyo caso cargan una copia temporal del perfil que se almacena en la propia máquina local.

Para transformar un perfil obligatorio en súper obligatorio, simplemente tenemos que modificar el nombre del directorio del perfil de modo el nombre (y solo el nombre) del directorio acabe en .man. Así, un perfil Olegario.V2 habría que renombrarlo a Olegario.MAN.V2. Cuando introduzcamos este perfil en la configuración del usuario, tendremos que indicar que el nombre del directorio es Olegario.MAN, sin él .V2.

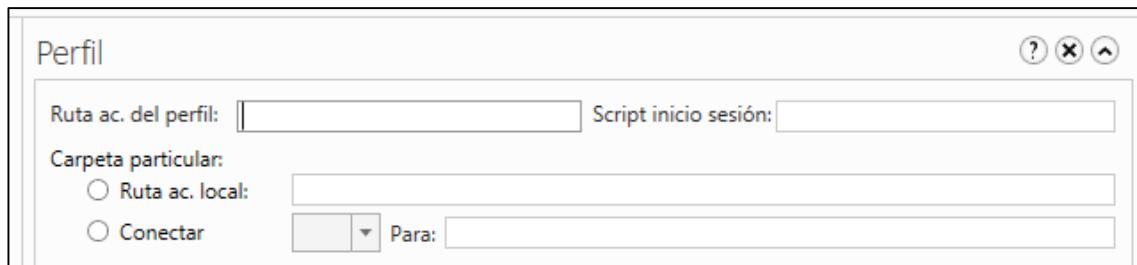
### Perfiles de usuario temporales.

Un perfil temporal de usuario se crea cada vez que se produce un error que evita que el perfil del usuario se cargue correctamente desde el servidor.

Los perfiles temporales se borran automáticamente cuando el usuario cierra la sesión, y cualquier cambio que el usuario haya realizado a sus ficheros, configuraciones o escritorio se pierden cuando el usuario cierre dicha sesión.

### Carpeta particular del usuario.

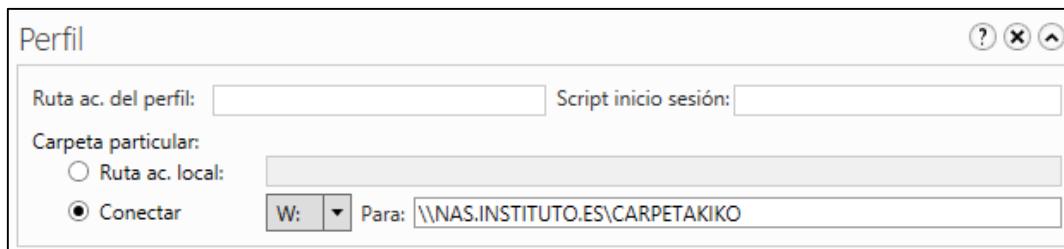
Como podemos comprobar, en la pestaña Perfil de las propiedades del usuario en la consola Usuarios y Equipos de Active Directory aparecen 3 opciones más aparte de la ruta del perfil.



La opción de **Script inicio sesión** nos permite indicar el nombre de un script (pequeño programa) que se ejecutará cada vez que el usuario inicie sesión localmente. Esta opción no suele ser utilizada y su función se realiza mediante el uso de una GPO como veremos en temas posteriores.

Las opciones de Carpeta particular si vamos a verlas con detenimiento.

Estas opciones nos permiten montar una unidad de red en el equipo local donde el usuario abra sesión, e incluso asignarle una letra con la opción Conectar. Veamos un ejemplo.



Con estas opciones, le estamos indicando al sistema que cada vez que el usuario inicie sesión en una máquina del dominio automáticamente acceda a la carpeta compartida en red con nombre CARPETAKIKO y situada en el equipo NAS.INSTITUTO.ES y la monte en el equipo local del usuario como un volumen de datos con la letra Z.

Si abrimos ahora sesión con dicho usuario en una maquina cliente, y abrimos el explorador de archivos, comprobaremos como efectivamente aparece una letra Z que es un volumen de datos montado sobre la carpeta compartida.

En esta prueba hemos utilizado la opción de conectar, no la de ruta de acceso local. Ambas opciones son excluyentes entre sí y realizan exactamente la misma función. La única diferencia es que si escribimos la ruta en Ruta de acceso local en lugar de en conectar, no se le asignará una letra al volumen de datos montado en el cliente.

#### Ejercicio sobre perfiles.

En un dominio crear 5 cuentas de usuario, con nombre PIPA, PIPE, PIPI, PIPO y PIPU.

Preparar PIPA y PIPE para que tengan perfil móvil.

Preparar PIPI y PIPO para que tengan perfil obligatorio (común). Queremos que en su escritorio tengan accesos directos al block de notas y a la calculadora.

Preparar PIPU para que tenga perfil local.

Conectar 2 máquinas clientes a nuestro dominio, y comprobad como PIPA y PIPE pueden abrir sesión en cualquier ordenador sin perder su perfil.

Comprobad como PIPI y PIPO no pueden realizar cambios en su perfil y aunque borren los accesos directos al block de notas y a la calculadora, cuando abren sesión de nuevo vuelven a aparecer.

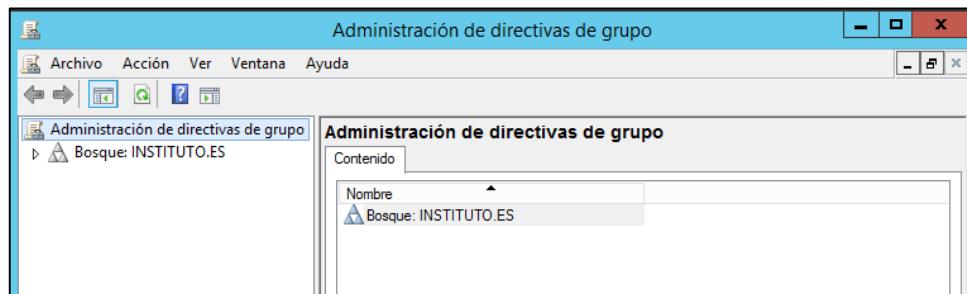
Comprobad como PIPU puede abrir sesión en cualquier ordenador, pero su perfil es distinto en cada máquina.

Queremos que PIPA tenga en su equipo un volumen con letra J que en realidad será una carpeta compartida en el controlador principal del dominio. Queremos que tenga control total sobre dicho volumen J.

## Políticas de grupo (group policy).

### Conceptos

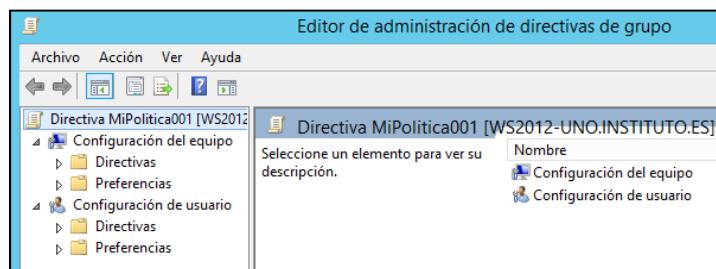
Un Active Directory se configura mediante la creación y despliegue de una serie de objetos de políticas de grupo (Group Policy Objects, GPOs) que pueden ser aplicados a usuarios y equipos seleccionados. Los objetos de política de grupo (GPO) se crean utilizando la consola GPMC o de Administración de Directivas de Grupo. En una sola GPO podemos establecer clientes de configuraciones de seguridad que pueden aplicarse a todos los usuarios, a un grupo de los mismos, solo a uno, a uno o varios equipos, etc.



Una GPO se divide en dos partes principales:

Configuración del equipo. Desde aquí podemos gestionar configuraciones específicas para los equipos, como puede ser una cuota de disco duro, una auditoría de seguridad, un gestor de eventos, etc.

Configuración del usuario. Desde aquí podemos gestionar configuraciones específicas para los usuarios, como configuración de aplicaciones, gestión del menú inicio, carpetas, elementos del escritorio, etc.



Hay muchas ocasiones en que ambos tipos de configuraciones se solapan y podemos encontrar la misma política en ambos sitios.

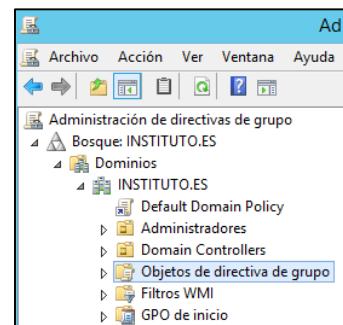
Las GPO no se aplican a grupos de usuario a pesar del nombre, sino que se aplican a sitios, dominios y unidades organizativas. Esta aplicación se conoce como enlace (linking). Una GPO que se le asigna a una OU se aplicará automáticamente a todos los usuarios que sean miembros de esa OU, al igual que si se aplica a un dominio se aplicará a los miembros del dominio, etc.

Las políticas de grupo se aplican a todos los equipos afectados por ella cada cierto tiempo, este periodo de refresco se establece por regla general cada 90 minutos. Esto quiere decir que una vez creada una GPO puede que hasta la hora y media no veamos cómo dicha GPO se asigna a determinados equipos. Veremos cómo podemos forzar dicho refresco.

Las políticas de grupo (GPO) se almacenan en un contenedor especial conocido como Objetos de Directiva de Grupo, y desde allí se enlazan o linkan con las partes de AD donde queremos que se apliquen.

Cada GPO puede contener cientos de posibles configuraciones establecidas, muchas de ellas de forma activa y otras de forma inactiva.

Una vez que enlazamos una GPO a un sitio (un dominio completo, por ejemplo) se le aplicaran automáticamente todas las configuraciones establecidas, no hay forma de indicar que solo queremos que se apliquen un conjunto de las mismas.



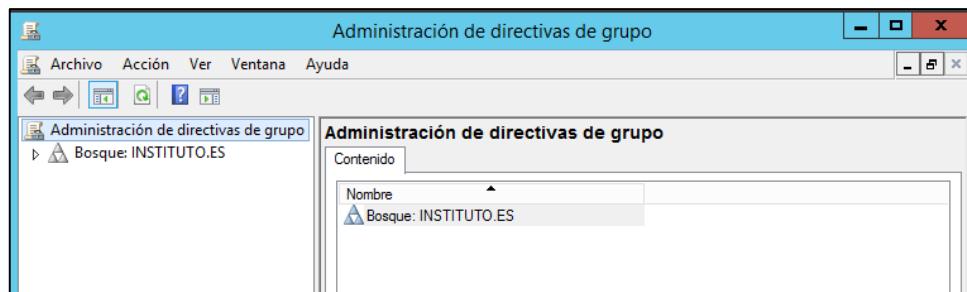
Imaginemos por ejemplo que creamos un GPO con todas las configuraciones establecidas para que los usuarios no puedan ejecutar ningún intérprete de comandos, y enlazamos dicha GPO con el dominio INSTITUTO.ES. Por defecto se les aplicará a todos los usuarios del dominio, y se aplicaran todas las configuraciones. Esto implica que si tenemos un grupo de técnicos llamado ITEC a este grupo también se le aplicará dicha configuración, cosa que no nos interesa. Podemos solucionarlo de dos formas distintas:

- Creamos un OU llamada Usuarios Normales y dentro metemos a todas las cuentas de usuario menos las del grupo ITEC. Luego enlazamos nuestra GPO a dicha OU en lugar de a todo el dominio.
- Podemos asignar la GPO a todo el dominio, pero establecemos un filtro que evitará que se le aplique la GPO al grupo ITEC.

Las políticas son acumulativas y cuentan con herencia. Por ejemplo, si enlazamos al dominio INSTITUTO.ES una GPO para configurar las contraseñas, y luego en una UO de nombre contables enlazamos otra GPO que configura los bloqueos de cuenta, a todos los integrantes de la UO contables se le aplicarán las dos GPO. Por regla general, se suelen configurar a nivel de dominio configuraciones generales, mientras que configuraciones más específicas se realizan a niveles inferiores.

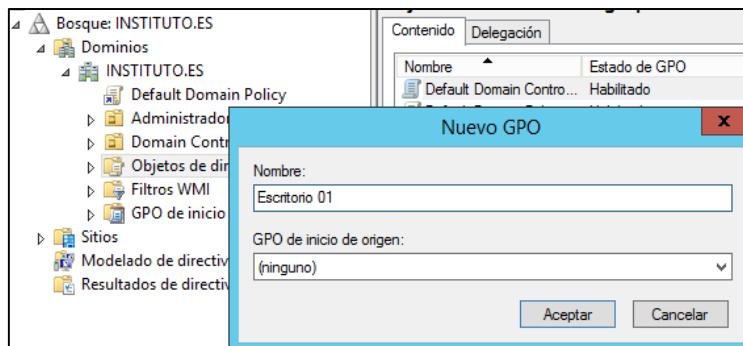
### Políticas locales y objetos de políticas de grupo (GPO)

Ya vimos anteriormente la consola que nos permite gestionar las políticas locales (gpedit.msc). Sin embargo, para trabajar con Objetos de Política de Grupo que están pensadas para ser aplicadas bajo Active Directory necesitamos ejecutar la consola Group Policy Management Editor (Administrador de Directivas de Grupo). Esta consola tiene bastantes más funcionalidades que la local.



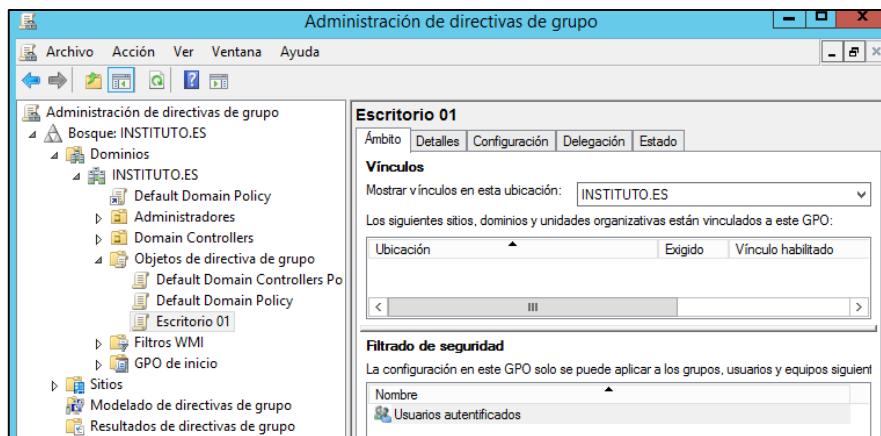
### Creación de una GPO.

Vamos a crear una nueva GPO en nuestro dominio. En primer lugar vamos a ejecutar la consola de Administración de Directivas de Grupo (desde el panel, menú Administrar). Ahora seleccionamos nuestro dominio y abrimos el árbol, damos botón derecho en el contenedor Objetos de Directiva de Grupo y escogemos Nuevo para crear una nueva GPO. Como nombre vamos a ponerle Escritorio 01.



Esto creará una nueva GPO en blanco llamada Escritorio 01 que no está enlazada a ningún sitio, y por lo tanto no está en funcionamiento. Vamos a establecer algunas políticas o configuraciones en la GPO y luego tendremos que enlazarla en algún punto para activarla.

De momento vamos a introducir algunas configuraciones. Hacemos doble clic sobre la GPO Escritorio 01 que se habrá creado dentro del contenedor Objetos de Directiva de Grupo y veremos cómo se despliega nuestra GPO en la ventana de la derecha y veremos 5 pestañas (Ámbito, Detalles, Configuración, Delegación y Estado).

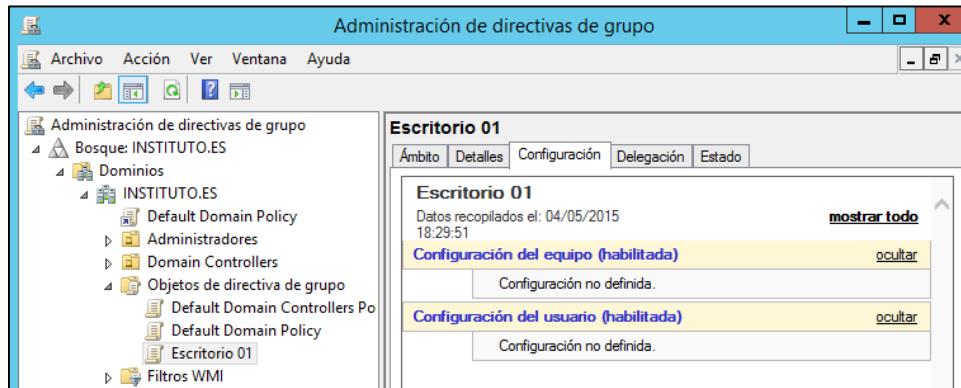


Desde Ámbito podemos ver la localización donde se encuentra nuestra GPO y si esta enlazada o no. En nuestro caso no veremos nada en localización ya que no la tenemos enlazada en ningún sitio.

También en Ámbito podemos ver el Filtrado de Seguridad, que nos indica a quienes se les aplicará nuestra GPO en el momento en que la enlazemos. Vemos como por defecto se les aplica a todos los usuarios autenticados (un grupo automático al que pertenecen todos los usuarios con contraseña del sistema).

Los filtrados WMI son bastante especiales y no los vamos a tratar de momento.

Desde la pestaña Detalles podemos ver datos diversos sobre la GPO como fecha de creación, etc.



Desde Configuración podemos ver las configuraciones que hemos activado en nuestra GPO. De momento veremos como no aparece ninguna configuración como definida. Esta ventana se muestra como una página HTML y es procesada por el internet Explorer, por lo que es posible que la primera vez que la veamos nos pida que configuremos la seguridad del mismo.

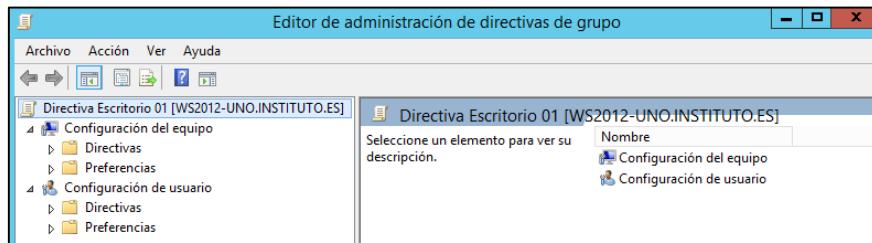
Nombre	Permisos válidos	Heredado
Administradores de empresas (I...)	Editar configuración, eliminar, modificar ...	No
Admins. del dominio (INSTITU...)	Editar configuración, eliminar, modificar ...	No
ENTERPRISE DOMAIN CON...	Lectura	No
SYSTEM	Editar configuración, eliminar, modificar ...	No
Usuarios autenticados	Lectura (de Filtrado de seguridad)	No

La pestaña Delegación nos permite ver la seguridad de la GPO, desde la cual podemos indicar quien puede editar la configuración a quien se le aplica (cualquiera que pueda leerla), etc. Desde aquí podemos comprobar el filtrado de seguridad que hemos establecido en Ámbito.

Por ultimo desde la pestaña Estado (si es que aparece) podremos ver el estado de la GPO referente a la sincronización entre varios servidores en el caso de que los tengamos.

### Editar la GPO.

Para editar la GPO simplemente tenemos que pulsar botón derecho sobre la GPO en la consola GPMC y seleccionamos la primera opción que es Editar. Esto nos abrirá el editor de administración de directivas de grupo (GPME).



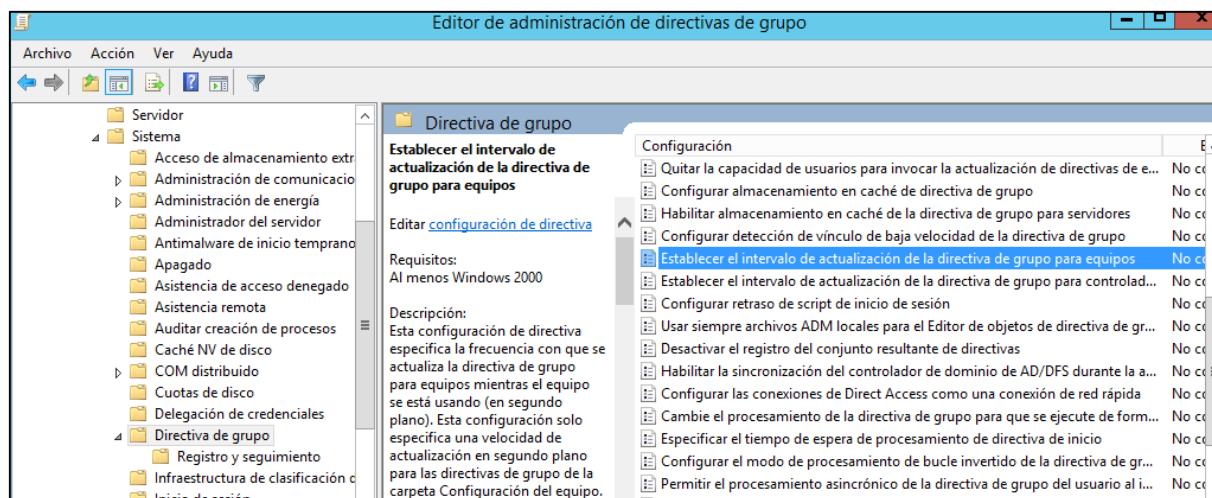
Desde aquí podemos ver dos grupos principales de configuraciones como hemos visto anteriormente, la de usuarios y la de equipos.

La de equipos se aplica a los equipos cada vez que se inician y al cumplirse el intervalo de refresco de las políticas de grupo.

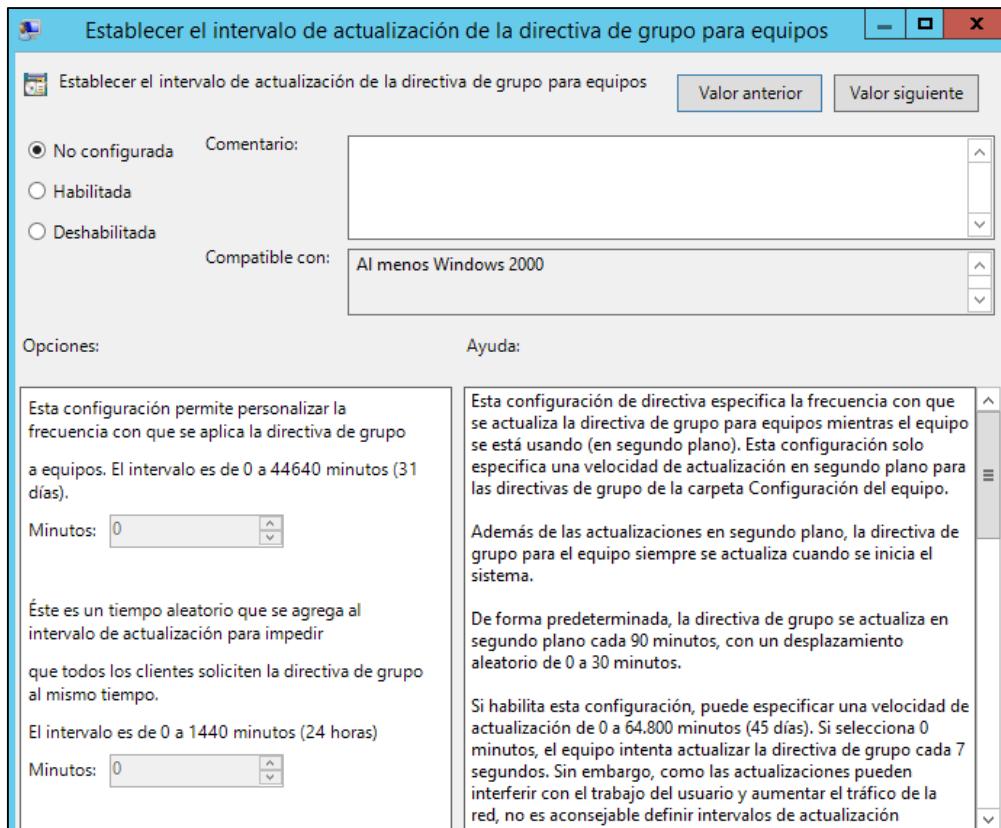
La de usuarios se aplica a cada usuario cuando estos inician sesión y también en el intervalo de refresco.

Una vez que hemos establecido el valor para algunas configuraciones simplemente tenemos que cerrar esta consola GPME para que se apliquen automáticamente, no hay un botón aplicar ni nada parecido para la GPO.

Como ejemplo, vamos a editar directamente la configuración que nos permite indicar el intervalo de refresco automático para las configuraciones de GPO. Para ello vamos a navegar en el árbol de GPMC hasta la configuración "Configuración del equipo > Directivas > Plantillas administrativas > Sistema > Directivas de Grupo > Establecer el intervalo de actualización de la directiva de grupo para equipos".



Una vez encontrada la configuración o política que queremos configurar damos doble clic sobre la misma (o botón derecho editar) y pasaremos al editor de dicha política en concreto.



Vemos como una política puede tener tres estados distintos:

- No configurada
- Habilitada
- No Habilitada

No configurada indica que no vamos a tocar esta configuración desde esta GPO, se puede decir que "pasamos" de ella. Esto permite configurarla desde otra GPO o bien que se aplique su valor por defecto.

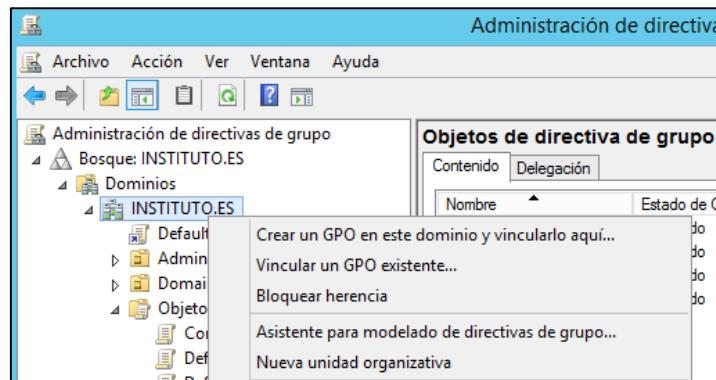
Habilitada indica que vamos a configurar dicha política. En nuestro ejemplo, habilitad la política y poned que el refresco se haga cada 45 minutos y el tiempo aleatorio que se le suma a dicho refresco es de 10 minutos.

Deshabilitada indica que vamos a configurar dicha política, pero negándola. En nuestro caso si deshabilitamos nuestra política eliminaremos el refresco en segundo plano de las políticas de grupos, es decir, que las políticas no se refrescaran automáticamente para los equipos.

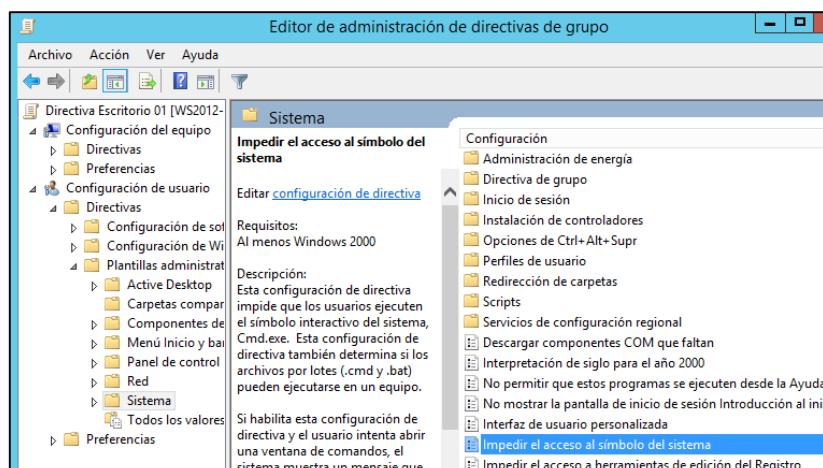
Vemos como junto con la política que nos permite establecer el refresco para los equipos, vemos que hay otra política que nos permite establecer el refresco para los controladores de dominio. Existe otra política que nos permite establecer el refresco para los usuarios, pero esta política no la veremos junto con las otras, puesto que la ruta para llegar a ella es "Configuración de usuario > Directivas > Plantillas administrativas > Sistema > Directivas de Grupo > Establecer el intervalo de actualización de la directiva de grupo para equipos".

No vamos a explicar cada una de las configuraciones o políticas posibles (son miles) ni vamos a explicar que posibilidades de configuración tienen editándolas, pero si os habéis fijado cada política tiene una ayuda en castellano bastante importante con la que debería bastarnos para poder entender que es lo que hace y como configurarla. Si no entendéis la ayuda de una política, es un indicador bastante claro de que no deberíais estar configurándola.

Vamos a ver otro ejemplo de creación y edición de una GPO.

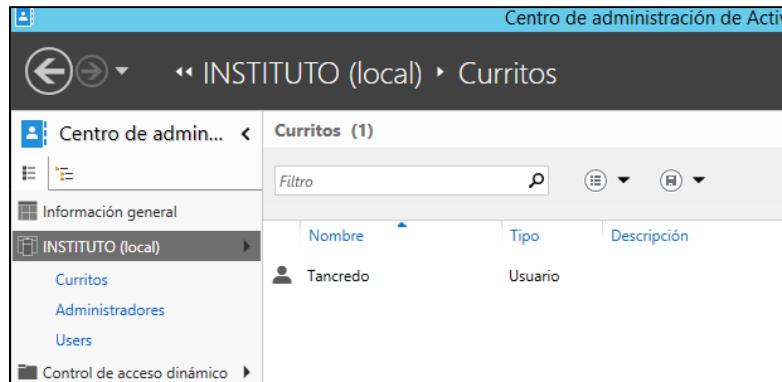


- Cread una GPO en el contenedor Objetos de directiva de grupo llamada NoCLI y pasad a editarla.
- Editar la política "Impedir el acceso al símbolo del sistema" que encontraremos en "Configuración de usuario > Directivas > Plantillas administrativas > Sistema".

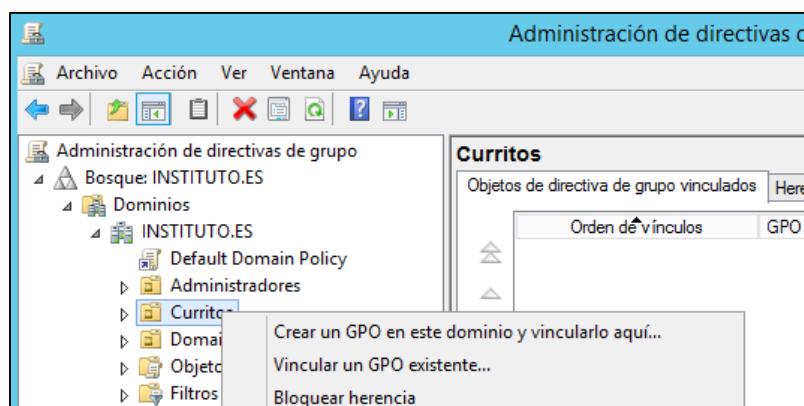


- Configurar dicha política, de forma que se impida que los usuarios puedan acceder al símbolo del sistema y también que no puedan ejecutar scripts.
- Cerrar el editor de administración de directivas de grupo.
- La GPO ya está configurada, pero como no está enlazada en ningún sitio, no se aplica. Vamos a proceder a enlazarla.

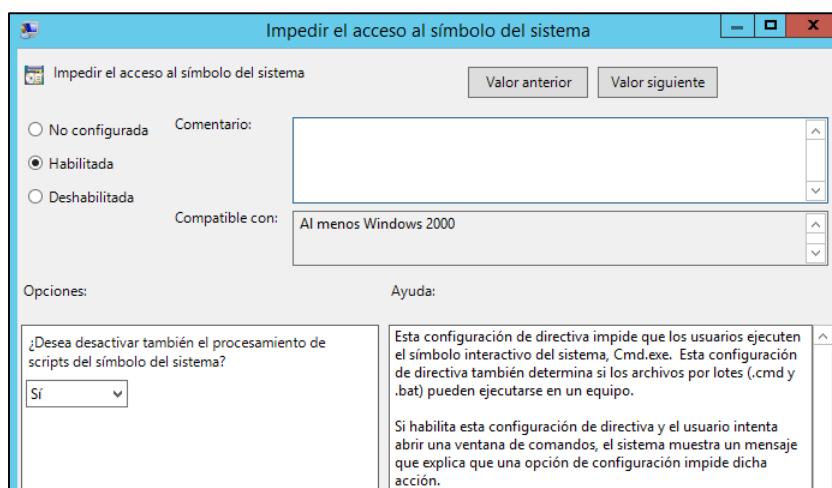
- Cread una OU en el dominio llamada Curritos. Cread dentro un usuario llamado Tancredo.



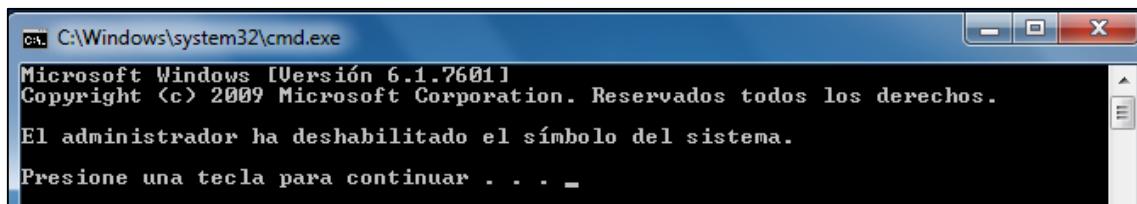
- En la consola GPMC buscad el contenedor llamado Curritos (si no aparece, cerrad GPMC y volved a abrirla) dad botón derecho en la OU Curritos y escoger la opción de Vincular una GPO ya existente.



- Escoged la GPO NoCLI.
- Comprobad como la GPO aparece ahora en el árbol justo debajo del contenedor Curritos. Dadle doble clic sobre la GPO y comprobad como aparece que está vinculada correctamente. Desde la pestaña configuración de la GPO podemos ver los parámetros que hemos configurado.



Ahora la GPO Escritorio 01 se está aplicando a toda la OU Curritos, y por lo tanto afecta a Tancredo. Abrid sesión desde un equipo cliente con Tancredo e intentad acceder al símbolo de sistema.



### Aplicación de GPO.

Imaginemos un dominio en el que tenemos dos GPO, una que establece la longitud de la contraseña para los usuarios en 6 caracteres mínimo, y otra que establece la longitud de la contraseña para los usuarios en 2 caracteres mínimo.. Incluso podríamos tener una tercera GPO que indica que los usuarios no necesitan usar contraseña. ¿Cuál de todas ellas se aplica?

Por defecto, las políticas de grupo se ejecutan de abajo a arriba, de modo que la que está más abajo es la primera que se lee y se aplica, luego se lee la que este más arriba y se aplica, hasta terminar con la que este en la parte superior de la lista. Esto hace que la que más "manda" siempre es la superior, ya que podrá machacar las configuraciones de las que estén por debajo.

Tenemos que tener en cuenta que el orden en que se aplican las GPO no es el que vemos en el árbol de la consola GPMC, sino el que vemos en las propiedades del contenedor.

Vamos a crear un par de GPO para comprender esto mejor.

1) Cread una GPO llamada Fondo\_Pantalla en Objetos de Políticas de Grupo.

2) Editadla configurando la política "Configuración de usuario > Directivas > Plantillas Administrativas > Active Desktop > Active Desktop > Tapiz del escritorio". En esta política nos pide el nombre del fondo de pantalla que se va a aplicar a los usuarios afectados por la GPO. Evidentemente el nombre no puede ser local al equipo, sino que debe ser una URL de red. Utilizad la siguiente URL "\\\INSTITUTO.ES\SYSVOL\INSTITUTO.ES\IMAGENES\INSTITUTO.JPG". En lugar de INSTITUTO.ES hay que utilizar el nombre de vuestro dominio, y la carpeta IMAGENES tenéis que crearla, al igual que tenéis que grabar dentro una imagen con el nombre de INSTITUTO.JPG.

3) Enlazad dicha GPO al OU Curritos.

4) Cread un nuevo usuario en la OU Curritos. Abrid sesión desde un cliente con dicha cuenta de usuario y comprobad como le hemos ajustado el fondo de pantalla con la foto instituto.jpg.

Objetos de directiva de grupo en INSTITUTO.ES					
Contenido	Delegación				
Nombre	Estado de GPO	Filtro WMI	Modificado	Propietario	
Contraseñas	Habilitado	Ninguno	05/05/2015 18:1...	Admins. del domi...	
Default Domain Contro...	Habilitado	Ninguno	23/04/2015 20:3...	Admins. del domi...	
Default Domain Policy	Habilitado	Ninguno	23/04/2015 20:4...	Admins. del domi...	
Escritorio 01	Habilitado	Ninguno	05/05/2015 18:2...	Admins. del domi...	
Fondo_Pantalla	Habilitado	Ninguno	05/05/2015 19:3...	Admins. del domi...	

Imagenes

Nombre Fecha de modifica... Tipo Tamaño

instituto 05/05/2015 19:36 Imagen JPEG 113 KB

Imagenes

Nombre Fecha de modifica... T

instituto 05/05/2015 19:36 Im

Editor de administración de directivas de grupo

Directiva Fondo\_Pantalla [WS2012-UNO.INSTITUTO.ES]

- Configuración del equipo
- Preferencias
- Configuración de usuario
- Directivas**
  - Configuración de software
  - Configuración de Windows
  - Plantillas administrativas: definiciones de directiva (archivos)
    - Active Desktop
      - Active Desktop
      - Active Directory
      - Carpetas compartidas
      - Componentes de Windows
      - Menú Inicio y barra de tareas

Active Desktop

**Tapiz del escritorio**

Editar [configuración de directiva](#)

Requisitos: Al menos Windows 2000

Descripción: Especifica el fondo de escritorio ("papel tapiz") que se mostrará en los escritorios de todos los usuarios.

Esta opción le permite especificar el papel tapiz que aparecerá en los escritorios de los usuarios e

Configuración

- Habilitar Active Desktop
- Deshabilitar Active Desktop
- No permitir cambios
- Tapiz del escritorio**
- Prohibir agregar elementos
- Prohibir cerrar elementos
- Prohibir eliminar elementos
- Prohibir modificar elementos
- Deshabilitar todos los elementos
- Agregar o quitar elementos
- Permitir solo papel tapiz de mapa de bits

Tapiz del escritorio

Valor anterior Valor siguiente

No configurada Comentario: La foto se carga de \\Instituto.es\sysvol\INSTITUTO.ES\Imagenes\instituto.jpg

Habilitada

Deshabilitada Compatibile con: Al menos Windows 2000

Opciones:

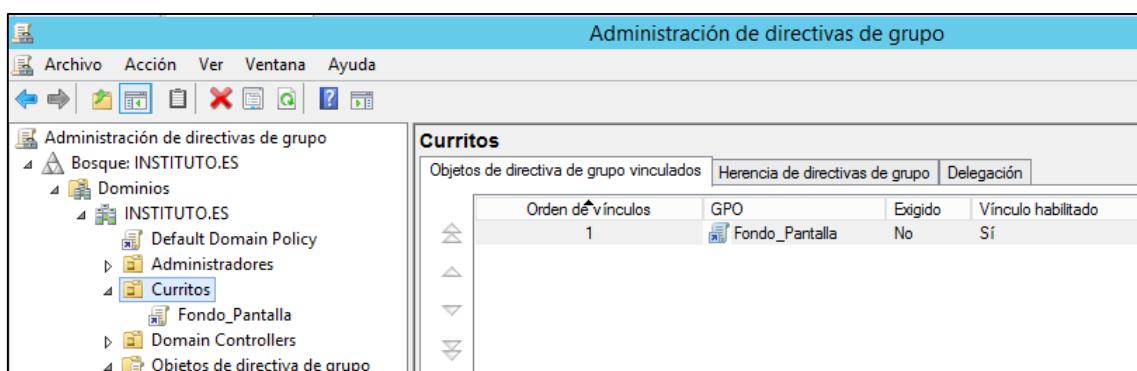
Nombre del papel tapiz: o\INSTITUTO.ES\Imagenes\instituto.jpg

Ejemplo: con una ruta de acceso local: C:\windows\web\wallpaper\inicio.jpg

Ejemplo: con una ruta de acceso UNC: \\Servidor\RecursoCompartido\Corp.jpg

Estilo del papel tapiz: Ajustar

Ayuda: Especifica el fondo de escritorio ("pape Esta opción le permite especificar el pa los usuarios puedan cambiar la imager como un archivo de mapa de bits (\*.br Para usar esta opción, escriba el nombr imagen del papel tapiz. Puede escribir e una ruta UNC como \\servidor\reco



### Principales políticas de una GPO.

Como hemos visto, cada GPO consta de un árbol de políticas que se dividen en dos ramas principales denominadas configuración de equipos y configuración de usuario. Cada una de estas ramas a su vez se dividen en dos ramas: Directivas y Preferencias.

- 1) Directivas. Esta rama incluye tres apartados:
  - a. Configuración de software. Opciones para la instalación automática de software.
  - b. Configuración de Windows. Encontramos opciones de seguridad, ejecución de scripts y redirección de carpetas.
  - c. Plantillas Administrativas. Políticas basadas en la modificación de valores del registro de Windows.
- 2) Preferencias. Esta rama incluye dos apartados:
  - a. Configuración de Windows. Opciones de configuración como por ejemplo creación de variables de entorno, creación de accesos directos, mapeo de unidades de red, etc.
  - b. Configuración de Panel de Control. Opciones de configuración como por ejemplo instalación de dispositivos, configuración de opciones de energía, tareas programadas, servicios, etc.

**Plantillas administrativas.**

Este grupo contiene todas las configuraciones de política basadas en el registro de Windows, incluyendo aquellas que controlan el funcionamiento y apariencia del escritorio, de los componentes de Windows y de algunas aplicaciones que utilizan estas políticas, como por ejemplo la mayoría de las aplicaciones de la propia Microsoft.

Desde estas plantillas podemos configurar cosas como la longitud de las contraseñas de todos los usuarios del bosque, de un dominio o de una UO. Podemos configurar que un usuario no pueda ejecutar el símbolo de comandos, podemos configurar que se desactive el rastreador de sucesos de apagado, etc.

## Directivas de auditoria. Visor de eventos.

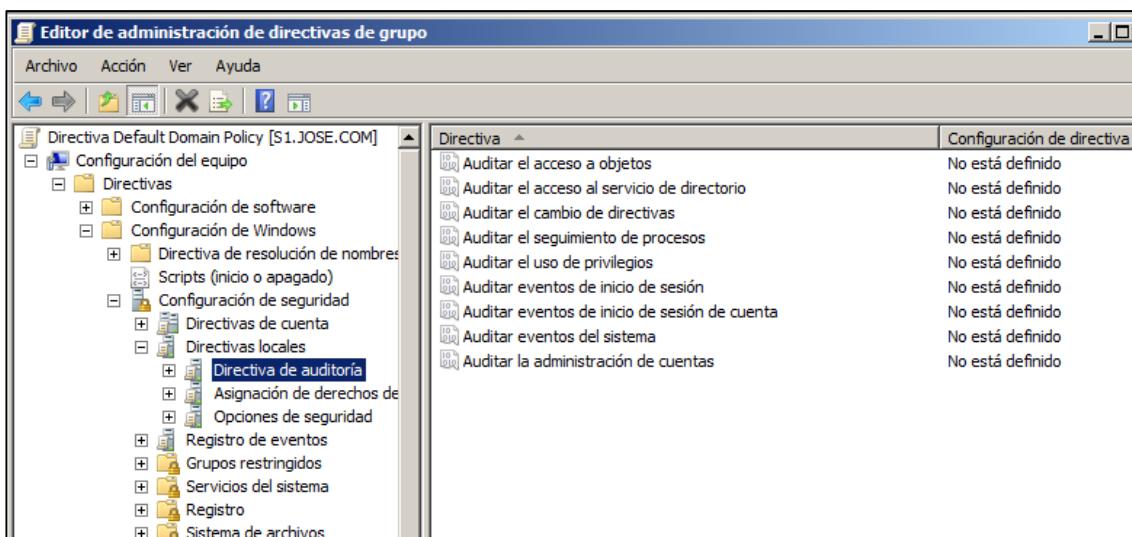
En Windows podemos generar directivas de auditoria, que nos permiten realizar un seguimiento de las actividades de los usuarios sobre los recursos, registrando estas actividades en el registro de seguridad del sistema.

Estas auditorías del sistema son una herramienta muy útil cuando nos encontramos con actividades extrañas en el directorio. Imaginad por ejemplo que un día comprobamos que el espacio de almacenamiento que utilizamos para SYSVOL se ha reducido considerablemente, ya que algún usuario se ha dedicado a subir archivos a una carpeta que presenta permisos de lectura y escritura para todos los usuarios.

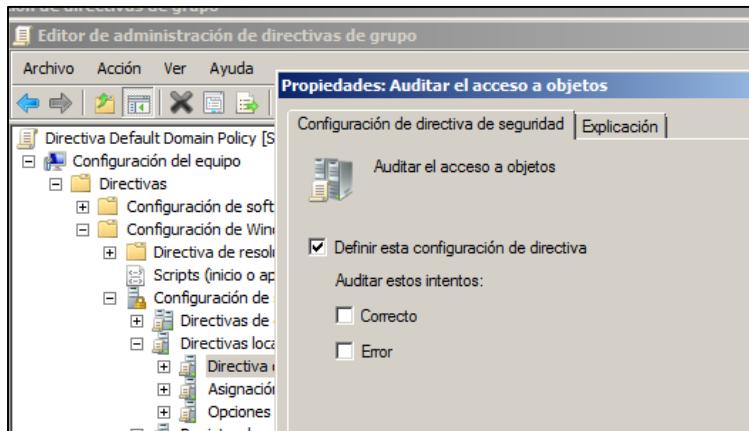
En un caso así, nos interesa conocer al culpable, y ahí es donde entran en juego las auditorias del sistema. Podemos establecer una auditoria sobre la carpeta donde se almacenan estos archivos, y registrar en el log de seguridad del sistema el nombre de cada usuario que acceda a dicha carpeta para grabar ficheros, así como el nombre del fichero, la hora, etc.

Para activar el servicio de auditorías del sistema debemos realizar los siguientes pasos:

- 1) Accedemos a la consola “Administración de directivas de grupo”
- 2) Editamos la GPO “Default Domain Policy”
- 3) Seleccionamos “directiva de auditoría” que está en la ruta “Configuración de equipo” – “Directivas” – “Configuración de Windows” – “Configuración de seguridad” – “Directivas locales” – “Directiva de auditoría”



Aquí podremos definir el tipo de auditorías que queremos activar. Si por ejemplo queremos auditar el acceso de los usuarios a una carpeta, tendríamos que activar “Auditar el acceso a objetos”

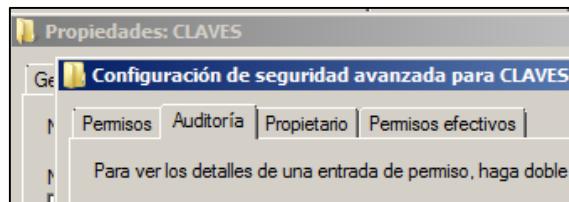


Podemos definir que se auditen tanto los intentos correctos de acceder al objeto (que lean la carpeta, por ejemplo) como los intentos incorrectos o errores (que intenten leer la carpeta y no puedan porque no tienen permisos suficientes). En nuestro ejemplo definimos la configuración y activamos las dos opciones.

Si quisiéramos por ejemplo que nos avisara cuando un usuario se cambia la contraseña, tendríamos que definir la configuración de la directiva “Auditar la administración de cuentas”.

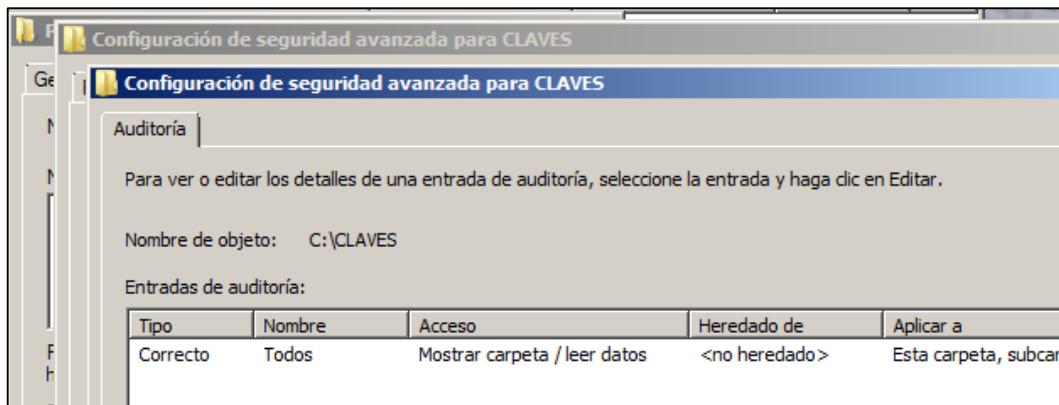
Cerramos la administración de directivas de grupo y en este punto ya tenemos activadas las auditorías para acceso a objetos, pero aún no estamos auditando nada. Tenemos que elegir ahora qué es lo que queremos auditar. Para ello tenemos que irnos al objeto que queremos auditar y activar la auditoría. Este objeto en nuestro caso será una carpeta.

- 1) Cread una carpeta CLAVES en el directorio raíz de vuestro volumen C:\
- 2) Ahora nos vamos a la pestaña seguridad de dicha carpeta, y activamos las opciones avanzadas.
- 3) Veremos como una pestaña de la ventana nos permite gestionar su auditoría.



- 4) Ahora nos preguntará para que usuario o usuarios queremos crear la auditoría. Como en nuestro ejemplo queremos ver quien lee o intenta leer la carpeta CLAVES sin importar quien sea, añadimos el grupo Todos.

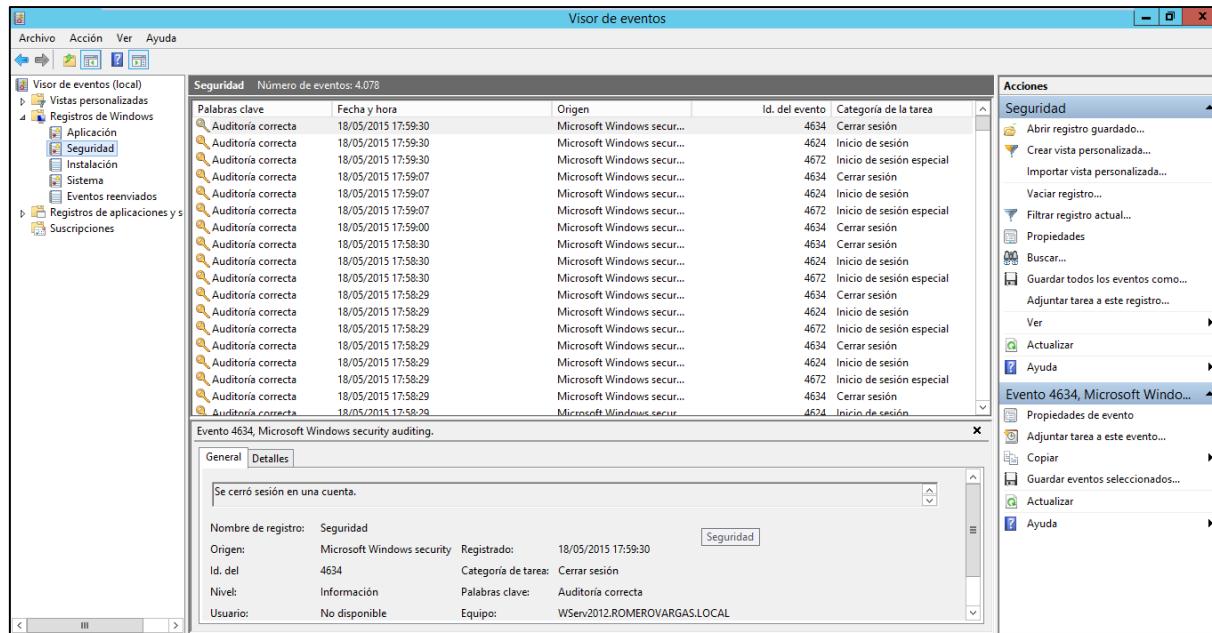
- 5) Ahora nos pregunta qué en concreto queremos auditar. En nuestro ejemplo seleccionamos solo la opción mostrar carpeta/leer datos. Una vez hecho esto vamos dando aceptar hasta salir de las propiedades de la carpeta.



Bien, ya hemos activado las auditorías del sistema para acceso a objetos, y hemos preparado una auditoría para cualquier usuario que intente leer la carpeta CLAVES. Ahora debemos comprobar si todo esto funciona.

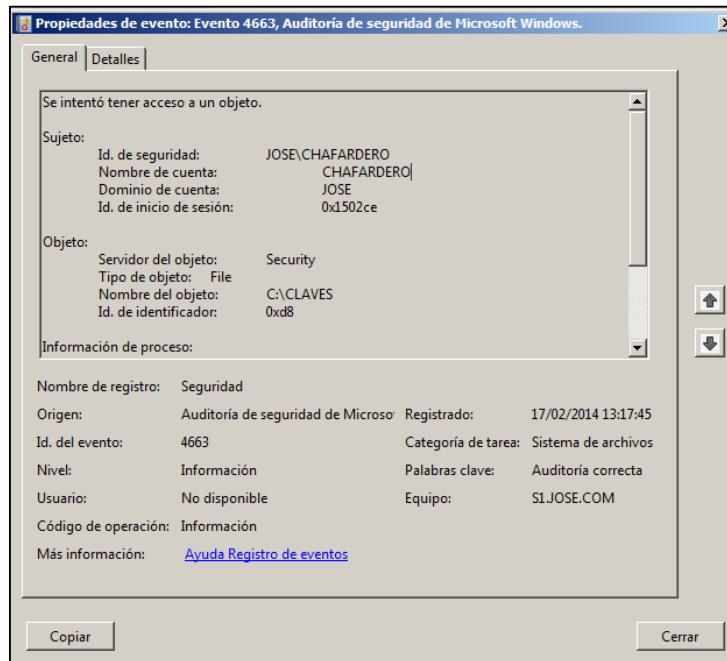
- 1) Crear un par de ficheros dentro de la carpeta CLAVES.
- 2) Cread un usuario con nombre chafardero, abrid sesión con dicho usuario en el propio servidor (o bien lo hacéis miembro del grupo administradores, o bien configuráis la directiva del sistema donde se indica quien puede abrir sesión interactiva local en el equipo).
- 3) Accedid con dicho usuario a la carpeta CLAVES y leer los ficheros.

Con esto habremos generado unas cuentas entradas de auditoría. Para poder ver estas entradas tenemos que ejecutar el visor de eventos (eventvwr.exe).



Una vez en el visor de eventos, debemos abrir “Registros de Windows” – “Seguridad”. Veremos que se han creado una gran cantidad de registros de auditoría

En nuestro caso, nos interesan varios registros, como por ejemplo los que tienen como Id 4663. Buscad los más recientes y dadle doble clic sobre ellos para ver la descripción completa del registro de auditoría.



Vemos como en dicho registro se indica la fecha y hora en la que el usuario CHAFARDERO del dominio JOSE ha intentado tener acceso al objeto C:\CLAVES.

Igual que hemos creado una auditoría para el acceso a un objeto, podéis crear auditorías para acciones tales como crear usuarios, borrar ficheros, editar las configuraciones del sistema, abrir o cerrar sesión, etc. Y cada una de ellas podemos crearlas para todos los usuarios, o solo para vigilar a algún usuario en concreto.