Tema 6: La administración de dominios

Contenido

6.1. CONCEPTOS PREVIOS

6.1.1. La estructura de trabajo en grupo

Los grupos de trabajo son conceptualmente contrarios a los servicios de directorio.

Los servicios de directorio se administran de forma centralizada y los grupos de trabajo son dirigidos por los usuarios cuando reúnen los recursos de sus ordenadores.

Con una conexión en red, los usuarios comparten los recursos de sus ordenadores con otros usuarios (así, éstos pueden utilizar los archivos, las impresoras, compartir un módem o un Cd-Rom de todos y cada uno de los ordenadores del grupo de trabajo.

Los usuarios individuales administran los recursos de sus ordenadores, indicando qué recursos pueden ser compartidos y cuáles van a tener un uso restringido.

Este tipo de redes puede tener dos problemas en grandes organizaciones:

- Algunos recursos compartidos son difíciles de localizar para los usuarios.
- Los recursos se comparten con un grupo limitado de colaboradores.

Microsoft introdujo el concepto de trabajo en grupo con *Windows* 3.11 para Trabajo en Grupo y permitía establecer grupos que podían fácilmente ver y compartir sus recursos (la única seguridad de la que estaba provisto era el uso de contraseñas para restringir el uso de determinados recursos a usuarios específicos). Para localizar recursos en la red se utilizaban servicio de exploración.

Posteriormente, se suministraron tres utilidades (Entorno de Red, Mis sitios de red y Red), que permitían explorar la red e identificar recursos a los que conectarse.

6.1.2. La estructura cliente-servidor

Al principio de la utilización de las redes, se conectaban los ordenadores entre sí para compartir los recursos de todos los ordenadores que estaban conectados.

Con el paso del tiempo, los usuarios fueron necesitando acceder a mayor cantidad de información y de forma más rápida, por lo que fue surgiendo la necesidad de un nuevo tipo de ordenador: **el servidor**.

Un servidor es un ordenador que permite compartir sus recursos con otros ordenadores que están conectados a él. Los servidores pueden ser de varios tipos y entre ellos se encuentran los siguientes:

- **Servidor de archivos.** Mantiene los archivos en subdirectorios privados y compartidos para los usuarios de la red.
- **Servidor de impresión.** Tiene conectadas una o más impresoras que comparte con los demás usuarios.
- **Servidor de comunicaciones**. Permite enlazar diferentes redes locales o una red local con grandes ordenadores o miniordenadores.
- **Servidor de correo electrónico.** Proporciona servicios de correo electrónico para la red.
- **Servidor web.** Proporciona un lugar para guardar y administrar los documentos *HTML* que pueden ser accesibles por los usuarios de la red a través de los navegadores.
- **Servidor FTP.** Se utiliza para guardar los archivos que pueden ser descargados por los usuarios de la red.
- **Servidor proxy.** Se utiliza para monitorizar y controlar el acceso entre las redes. Cambia la dirección *IP* de los paquetes de los usuarios para ocultar los datos de la red interna a Internet y cuando recibe contestación externa, la devuelve al usuario que la ha solicitado. Su uso reduce la amenaza de piratas que visualicen el tráfico de la red para conseguir información sobre los ordenadores de la red interna.

Según el sistema operativo de red que se utilice y las necesidades de la empresa, puede ocurrir que los distintos tipos de servidores residan en el mismo ordenador o se encuentren distribuidos entre aquellos que forman parte de la red.

Así mismo, los servidores de archivos pueden establecerse como dedicados o no dedicados, según se dediquen sólo a la gestión de la red o, además, se puedan utilizar como estación de trabajo. La conveniencia de utilizar uno u otro va estar indicada por la cantidad de estaciones de trabajo de que se vaya a disponer: cuanto mayor sea el número de ellas, más conveniente será disponer de un servidor dedicado.

No es recomendable utilizar un servidor no dedicado como estación de trabajo, ya que, en caso de que ese ordenador tenga algún problema, la totalidad del sistema puede dejar de funcionar, con los consiguientes inconvenientes y pérdidas irreparables que se pueden producir.

El resto de los ordenadores de la red se denominan estaciones de trabajo o clientes, y desde ellos se facilita a los usuarios el acceso a los servidores y periféricos de la red.

Cada estación de trabajo es, por lo general, un ordenador que funciona con su propio sistema operativo. A diferencia de un ordenador aislado, la estación de trabajo tiene una tarjeta de red y está físicamente conectada por medio de cables con el servidor.

6.1.3. Introducción al concepto de directorio y dominio

En el sentido más amplio, un directorio no es más que una lista detallada de objetos. Por ejemplo, una guía de teléfonos es un tipo de directorio que guarda información sobre personas, empresas y otras entidades. De cada uno de los elementos representados, se almacena su nombre, dirección y número de teléfono.

En muchos sentidos, Active Directory Domain Services (AD DS) es muy

parecido a una guía telefónica, aunque resulta más flexible. Se basa en el concepto de dominio que introdujo Windows NT con el fin de facilitar la administración. Sin embargo, ahora el objetivo es crear una estructura dinámica y fácilmente accesible, a través de la que se puede almacenar la información de toda la organización, tanto relativa a la estructura del propio directorio como de su administración, y acceder a ella de forma centralizada.

Active Directory está basado en una serie de estándares establecidos por la *Unión Internacional de Telecomunicaciones* (UIT) llamados *X.500*.

El protocolo LDAP se creó como una versión ligera de X.500

AD DS puede almacenar información sobre la organización, sitios, ordenadores, usuarios, objetos compartidos y cualquier otra cosa que pueda formar parte de la infraestructura de red. A diferencia de los elementos de una guía telefónica, los elementos almacenados en un Directorio Activo pueden ser diferentes unos de otros (usuarios, grupos, políticas de acceso, permisos, asignación de recursos, etc), por lo que la información concreta que se almacena variará según la naturaleza del objeto. Toda esta información se guarda en una base de datos jerárquica.

El motor de esta base de datos es el mismo que incorpora Microsoft Exchange Server y permite la replicación de controladores de dominio. Es decir, se puede enviar la información contenida en la base de datos a diferentes controladores de dominio a través de la red. De esta forma, un usuario creado en un determinado controlador de dominio, podría iniciar sesión en cualquier cliente unido a otro controlador de dominio diferente sin ninguna complicación.

Además de administrar políticas que serán válidas en toda la organización, Active Directory permite realizar operaciones como la instalación de programas, de forma simultánea y centralizada, en multitud de clientes o aplicar actualizaciones críticas en toda la organización.

Cuando utilizamos Active Directory, tenemos a nuestra disposición herramientas de administración para establecer políticas de grupo, para incluir unos grupos dentro de otros en diferentes niveles, un acceso sencillo al árbol de usuarios, ordenadores, impresoras y contactos, etc.

Obviamente, podemos utilizar Windows Server sin usar Active Directory, pero estaremos prescindiendo de un amplio conjunto de capacidades.

En cuanto a la estructura del servicio de directorio, lo primero que debemos saber es que existen dos tipos de componentes en Active Directory: los componentes físicos y los componentes lógicos. Veámoslos representados en la siguiente tabla:

Componentes de AD DS	
Componentes Físicos	Componentes Lógicos
• Controlador de dominio • Sitios • Subredes	• Dominios • Bosques • Árboles • Unidades Organizativas

Por otro lado, Active Directory resulta útil tanto en redes pequeñas como en instalaciones con millones de elementos relacionados.

6.1.4. Conceptos básicos en una estructura de Directorio Activo

Una vez que disponemos de una idea global del concepto de directorio y de lo que son los dominios, es conveniente que hagamos un repaso de la terminología que vamos a emplear cuando hablemos de *Active Directory Domain Services*. Esto es lo que haremos a continuación:

Directorio

Como ya hemos mencionado antes, un *Directorio* es un repositorio único para la información relativa a los usuarios y recursos de una organización. *Active Directory* es un tipo de directorio y contiene información sobre las propiedades y la ubicación de los diferentes tipos de recursos dentro de la red. Usándolo, tanto los usuarios como los administradores pueden encontrarlos con facilidad.

Una de las ventajas que ofrece *Active Directory* es que puede utilizar *LDAP* (*Lightweight Directory Access Protocol*, en español, *Protocolo Ligero de Acceso a Directorios*), un protocolo de acceso estándar que permitirá la consulta de información contenida en el directorio. Sin embargo, también puede utilizar *ADSI* (*Active Directory Services Interface*, en español, *Interfaces de Servicio de Active Directory*), un conjunto de herramientas ofrecidas por *Microsoft*, que tienen una interfaz orientada a objetos y que permiten el acceso a características de *Active Directory Domain Services* que no están soportadas por *LDAP*.

Dominio

Un Dominio es una colección de objetos dentro del directorio que forman un subconjunto administrativo. Pueden existir diferentes dominios dentro de un bosque, cada uno de ellos con su propia colección de objetos y *unidades organizativas*.

Para poner nombre a los dominios se utiliza el protocolo *DNS*. Por este motivo, *Active Directory* necesita al menos un *servidor DNS* instalado en la red. Más adelante, en este mismo apartado, definiremos los conceptos de bosque y unidad organizativa.

Objeto

La palabra *Objeto* se utiliza como nombre genérico para referirnos a cualquiera de los componentes que forman parte del directorio, como una impresora o una carpeta compartida, pero también un usuario, un grupo, etc. Incluso podemos utilizar la palabra *objeto* para referirnos a una unidad organizativa.

Cada objeto dispondrá de una serie de características específicas (según la clase a la que pertenezca) y un nombre que permitirá identificarlo de forma precisa.

Como veremos más adelante, las características específicas de cada tipo de objeto quedarán definidas en el *Esquema* de la base de datos.

En general, los objetos se organizan en tres categorías:

- Definición de usuario: Desde un punto de vista informático, un usuario es un conjunto de *permisos* y de *privilegios* sobre determinados recursos. En este sentido, un usuario no tiene que ser, necesariamente, una persona.
    1. *Usuarios*: identificados a través de un nombre (y, casi siempre, una contraseña), que pueden organizarse en grupos, para simplificar la administración.
    2. *Recursos*: que son los diferentes elementos a los que pueden acceder, o no, los usuarios según sus *privilegios*. Por ejemplo, carpetas compartidas, impresoras, etc.
    3. *Servicios*: que son las diferentes *funciones* a las que los usuarios pueden tener acceso. Por ejemplo, el correo electrónico.

Existen objetos que pueden contener a su vez otros objetos, como es el caso de los *grupos de usuarios* y de las *unidades organizativas*.

Controlador de dominio

Cuando instalamos *Active Directory*en un ordenador con *Windows Server*, convertimos a ese ordenador en un *Controlador de dominio*.

Un *Controlador de dominio* (*domain controller*) contiene la base de datos de objetos del directorio para un determinado dominio, incluida la información relativa a la seguridad. Además, será responsable de la autenticación de objetos dentro de su ámbito de control (facilitarán la apertura y el cierre de sesión, las búsquedas en el directorio, etc.).

En un dominio dado, puede haber varios controladores de dominio asociados, de modo que cada uno de ellos represente un rol diferente dentro del directorio. Sin embargo, a todos los efectos, todos los controladores de dominio, dentro del mismo dominio, tendrán la misma importancia.

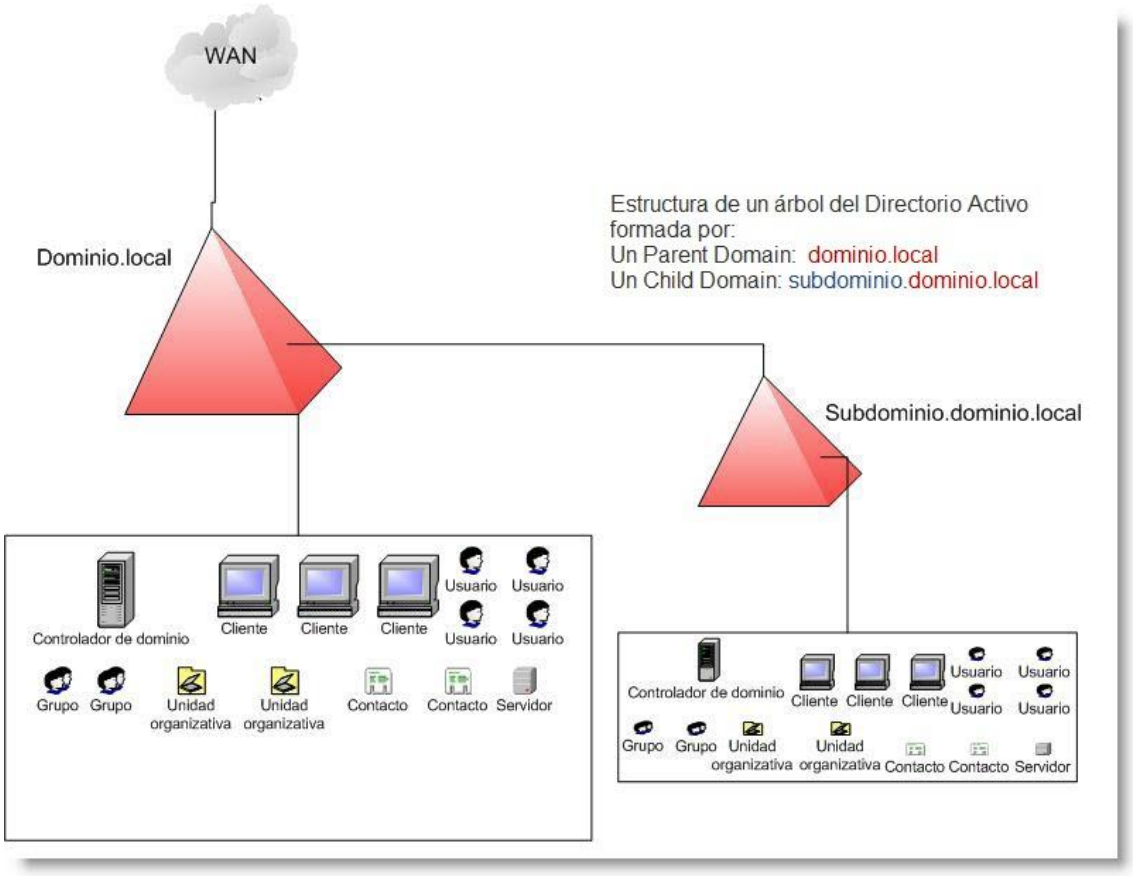
Árboles

Un *Árbol* es simplemente una colección de dominios que dependen de una raíz común y se encuentra organizados como una determinada jerarquía. Dicha jerarquía también quedará representada por un *espacio de nombres DNS* común.

De esta forma, sabremos que los dominios iesaljada.es e aula84.iesaljada.es forman parte del mismo árbol, mientras que juancarlosI.com y iesaljada.es no.

El objetivo de crear este tipo de estructura es fragmentar los datos del *Directorio Activo*, replicando sólo las partes necesarias y ahorrando ancho de banda en la red.

Si un determinado usuario es creado dentro de un dominio, éste será reconocido automáticamente en todos los dominios que dependan jerárquicamente del dominio al que pertenece.



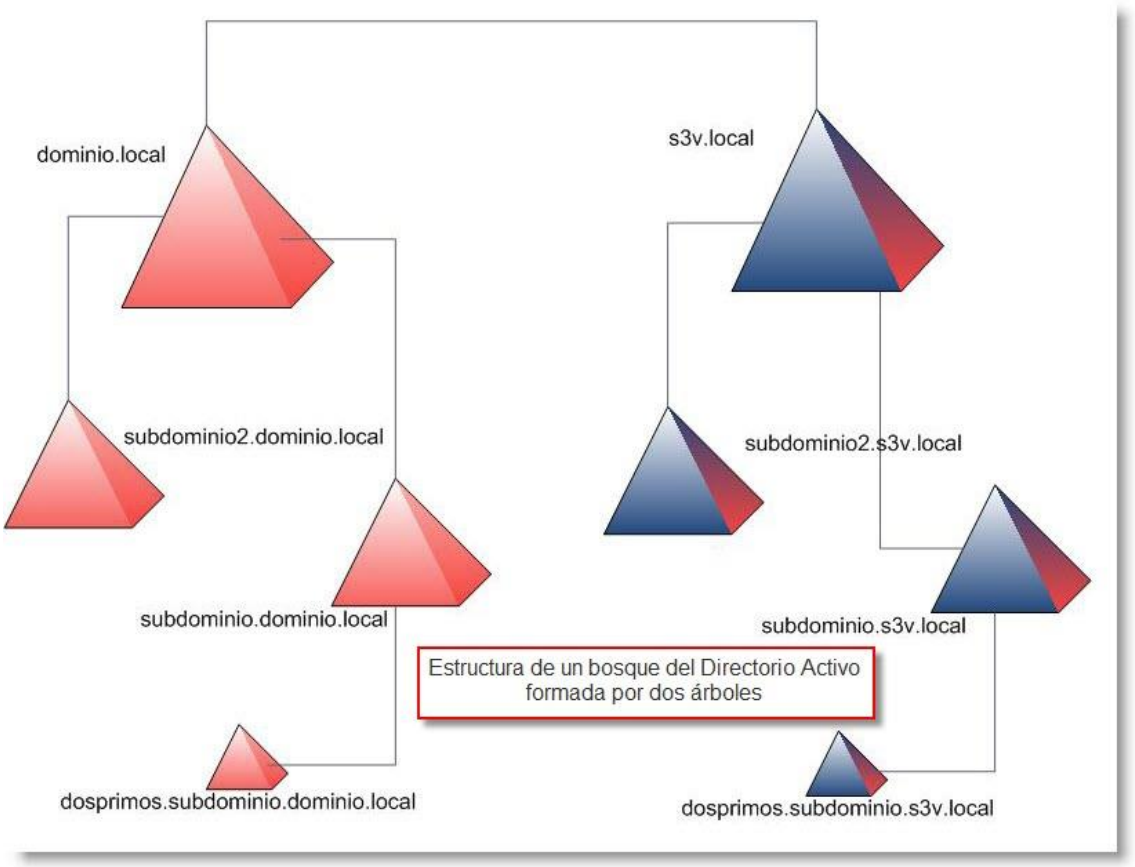
Bosque

El *Bosque* es el mayor contenedor lógico dentro de *Active Directory*, abarcando a todos los dominios dentro de su ámbito. Los dominios están interconectados por *Relaciones de confianza* transitivas que se construyen automáticamente. De esta forma, todos los dominios de un bosque confían automáticamente unos en otros y los diferentes árboles podrán compartir sus recursos.

Como ya hemos dicho, los dominios pueden estar organizados jerárquicamente en un árbol que comparte un *espacio de nombres DNS* común. A su vez, diferentes árboles pueden estar integrados en un bosque. Al tratarse de árboles diferentes, no compartirán el mismo espacio de nombres.

De forma predeterminada, un bosque contiene al menos un dominio, que será el *dominio raíz del bosque*. En otras palabras: cuando instalamos el primer dominio en un ordenador de nuestra red que previamente dispone de *Windows Server*, además del propio dominio, estamos creando la raíz de un nuevo árbol y también la raíz de un nuevo bosque.

El *dominio raíz del bosque* contiene el *Esquema* del bosque, que se compartirá con el resto de dominios que formen parte de dicho bosque.



Unidad Organizativa

Una *Unidad Organizativa* es un contenedor de objetos que permite organizarlos en subconjuntos, dentro del dominio, siguiendo una jerarquía. De este modo, podremos establecer una estructura lógica que represente de forma adecuada nuestra organización y simplifique la administración.

Otra gran ventaja de las unidades organizativas es que simplifican la delegación de autoridad (completa o parcial) sobre los objetos que contienen, a otros usuarios o grupos. Esta es otra forma de facilitar la administración en redes de grandes dimensiones.

Esquema

En Active Directory Domain Services se utiliza la palabra *Esquema* para referirse a la estructura de la base de datos. En este sentido, utilizaremos la palabra atributo para referirnos a cada uno de los tipos de información almacenada.

Sitio

Un *Sitio* es un grupo de ordenadores que se encuentran relacionados, de una forma lógica, con una localización geográfica particular.

En realidad, pueden encontrarse físicamente en ese lugar o, como mínimo, estar conectados, mediante un enlace permanente, con el ancho de banda adecuado.

En otras palabras, un controlador de dominio puede estar en la misma zona

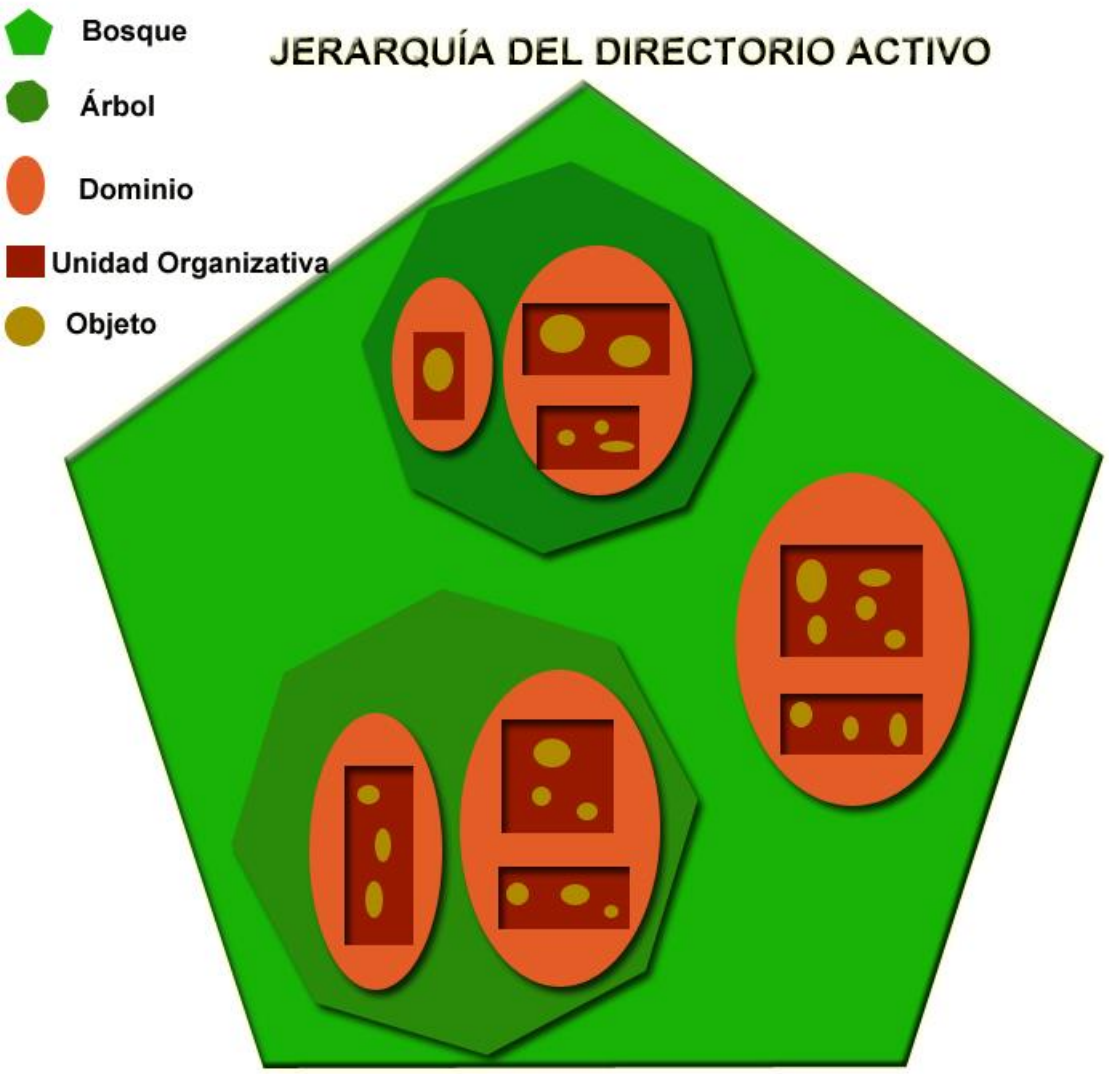
geográfica de los clientes a los que ofrece sus servicios o puede encontrarse en el otro extremo del planeta (siempre que estén unidos por una conexión adecuada). Pero en cualquier caso, todos juntos formarán el mismo *sitio*.

Relaciones de confianza

En el contexto de *Active Directory*, las *Relaciones de confianza* son un método de comunicación seguro entre dominios, árboles y bosques. Las relaciones de confianza permiten a los usuarios de un dominio del *Directorio Activo* autenticarse en otro dominio del directorio.

Existen dos tipos de relaciones de confianza: *unidireccionales* y *bidireccionales*. Además, las relaciones de confianza pueden ser *transitivas* (A confía en B y B confía en C, luego A confía en C).

6.1.5 Jerarquía de Directorio Activo



6.2.- Instalar un dominio básico desde la interfaz gráfica

En realidad, la instalación de un dominio en *Windows Server* se divide en dos subtareas: primero tendremos que instalar el rol *Servicios de dominio de Active Directory* en el servidor y después convertiremos (*promocionaremos*) el servidor en un controlador de dominio.

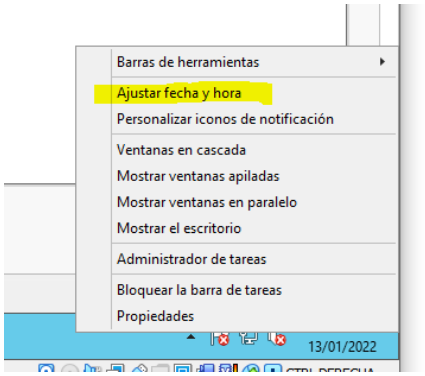
Pasos previos:

A. Configurar la zona horaria en Windows Server 2012 R2 con escritorio.

La configuración predeterminada de la zona horaria, los formatos de fecha y hora y la sincronización del reloj con un servidor NTP a través de Internet, que encontraremos tras instalar Windows server 2012 R2 suele ser correcta. Sin embargo, es interesante saber cómo modificar sus parámetros para ajustarlo a nuestros gustos o, incluso, para realizar los ajustes necesarios si necesitamos trasladar el servidor a una localización diferente.

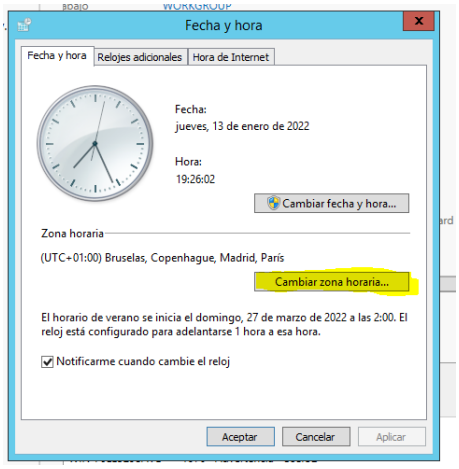
Aunque para establecer la zona horaria podemos recurrir a la herramienta Administrador del servidor, aquí veremos una forma más sencilla, que consiste en hacer clic con el botón derecho del ratón sobre la zona de la Barra de tareas donde aparecen la fecha y la hora.

1.- En el menú de contexto que aparece, elegimos la opción Ajustar fecha y hora.



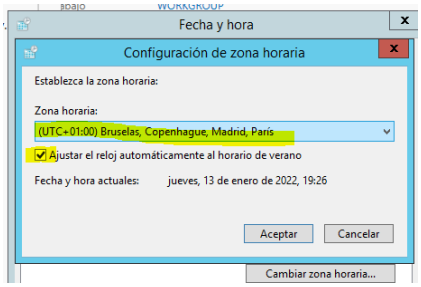
En la ventana que aparece, podremos cambiar la fecha, la hora y establecer la zona horaria del punto geográfico en el que nos encontramos.

2.- Para cambiar la zona horaria, hacemos clic sobre el botón con dicho título.



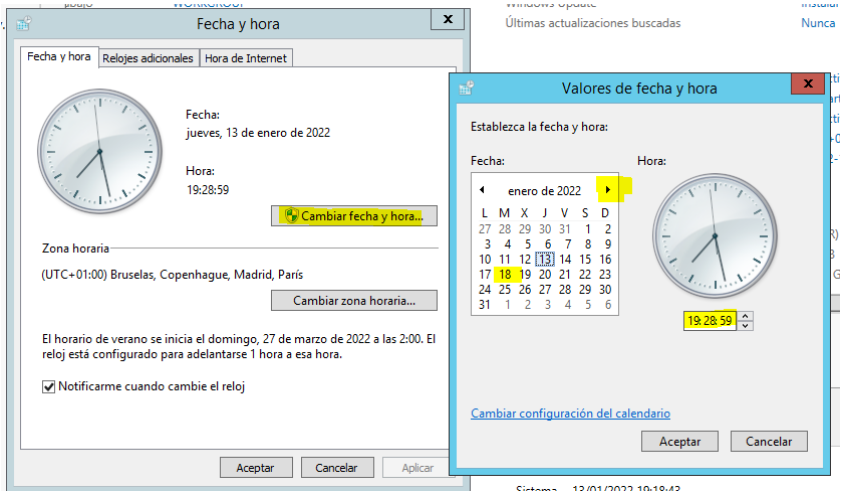
En la ventana que aparece, titulada Configuración de zona horaria, podemos elegir de una lista desplegable la zona horaria a la que pertenecemos e indicar si queremos que el reloj se ajuste automáticamente cuando se produzca el cambio del horario de verano al de invierno y al contrario.

3.- Cuando hayamos establecido nuestras preferencias, hacemos clic en el botón Aceptar.



También podemos utilizar el botón Cambiar fecha y hora para realizar un cambio manual de dichos parámetros. Como puedes ver en la imagen, disponemos de unos botones para elegir el mes y el año, podemos hacer clic sobre un día concreto y podemos utilizar tanto botones como escritura directa para cambiar la hora.

4.- De nuevo, indicamos nuestras preferencias y hacemos clic en el botón Aceptar.



Si preferimos que la hora se ajuste de forma automática, podemos utilizar la solapa Hora de Internet. Aquí podemos ver cuándo se sincronizó nuestro sistema por última vez con el servidor

horario y podemos cambiar la configuración.

En la ventana Configuración de la hora de Internet, podemos establecer si queremos que dicha sincronización se realice o, por el contrario, queremos ajustar siempre el reloj de forma manual. En el caso de que habilitemos la opción de sincronización, podemos elegir el servidor que utilizaremos (de forma predeterminada se utiliza un servidor de Microsoft, pero podemos elegir cualquier otro de la lista).

También disponemos de un botón para actualizar la hora en este instante.

5.- Finalmente, cuando la configuración sea correcta, haremos clic en el botón Aceptar.

B. Configurar las funciones de red en Windows Server 2012 R2 con escritorio

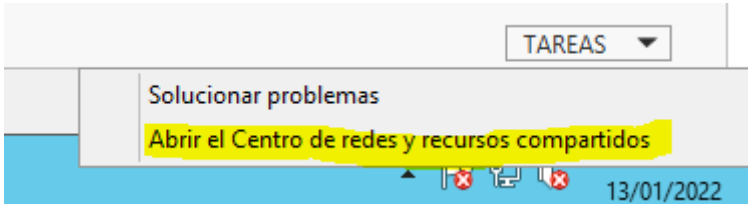
Durante el proceso de instalación de *Windows Server 2012 R2* apenas se solicita información. Esto significa que el asistente toma decisiones que competen a la configuración del equipo, realizando una configuración genérica que utiliza valores predeterminados.

Uno de los aspectos para los que se ha seguido este criterio es la obtención de una *dirección IP* para el equipo. Según la configuración predeterminada, el sistema obtendrá la *dirección IP* a través de *DHCP* (*Dynamic Host Configuration Protocol*).

Sin embargo, lo normal es que los servidores de red tengan valores fijos, que no cambien con cada arranque, para facilitar su localización en la red. Esto es lo que aprenderemos a realizar en el artículo de hoy. Y no sólo estableceremos un valor fijo para la *dirección IP*. También para la máscara de subred, la puerta de enlace e incluso el servidor DNS para el servidor.

Aunque podemos recurrir a la herramienta *Administrador del servidor*, la forma más sencilla consiste en hacer clic con el botón derecho del ratón sobre el icono que representa la conexión de red en la *Barra de tareas*.

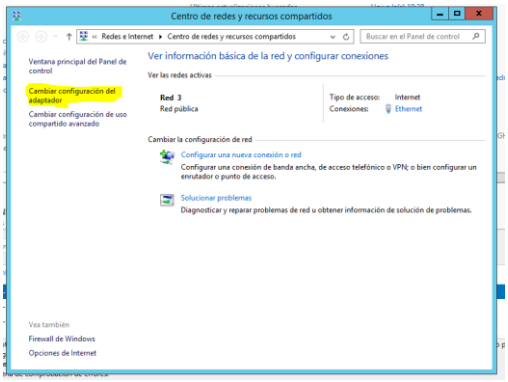
1.- En el menú de contexto que aparece, elegimos Abrir el Centro de redes y recursos compartidos.



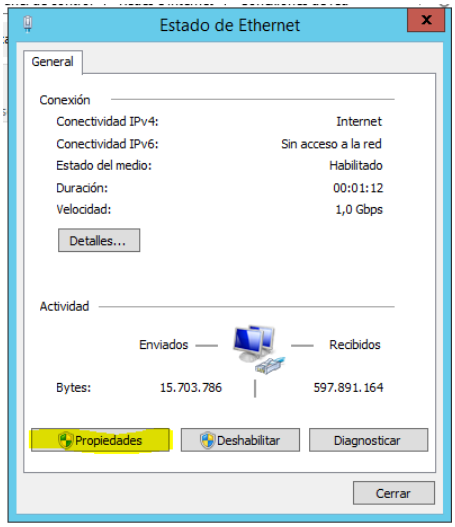
Como cabe esperar, se abre una ventana titulada *Centro de redes y recursos compartidos*.

2.- En ella, hacemos clic sobre el enlace Cambiar configuración del adaptador.

Aparecerá la ventana *Conexiones de red* con un elemento por cada conexión disponible (en nuestro caso, sólo una).



3.- Hacemos doble clic sobre la conexión que vamos a configurar (en este caso, Ethernet)



Aparece la ventana *Estado de Ethernet* con toda la información sobre la conexión. Observa que la entrada *Conectividad IPv6* indica que no tiene acceso a la red. El motivo es que la red local en la que estamos trabajando no dispone de conectividad para el protocolo TCP/IPv6.

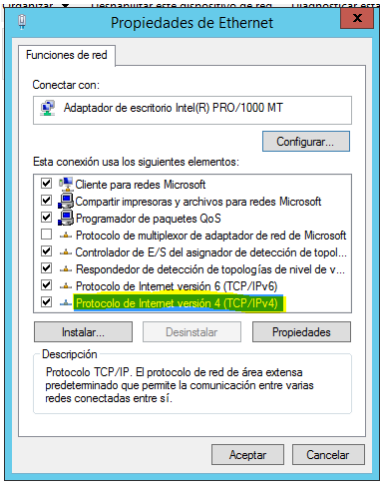
También podemos ver el tiempo que lleva habilitada la conexión (que en este caso coincide con el tiempo desde que iniciamos el sistema), su velocidad y la cantidad de información transmitida.

4.- Para modificar la configuración, hacemos clic en el botón Propiedades.

De esta forma, conseguimos que se muestre la ventana *Propiedades de Ethernet*, donde podemos encontrar (y también configurar) el tipo de tarjeta de red que estamos utilizando y todos los elementos disponibles para esta conexión.

Como hemos visto más arriba que no disponemos de conectividad IPv6, comenzamos por hacer clic sobre la casilla de verificación que hay junto a la entrada *Protocolo de Internet versión 6 (TCP/IPv6)* para deshabilitarlo. De esta forma, evitamos consumir recursos del sistema de forma innecesaria.

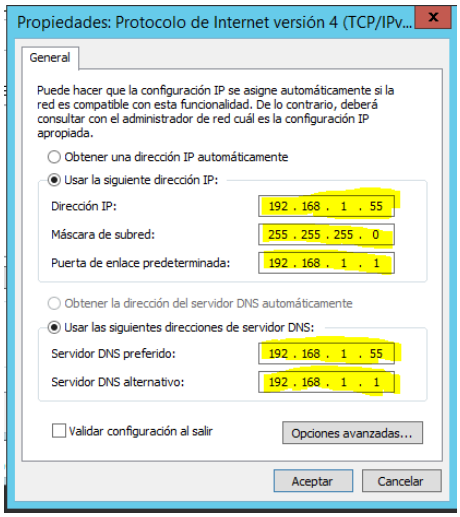
5.- Después, seleccionamos la entrada Protocolo de Internet versión 4 (TCP/IPv4) y hacemos clic sobre el botón Propiedades para configurarlo.



En la ventana de *Propiedades del Protocolo de Internet versión 4 (TCP/IPv4)* fijamos los valores adecuados para nuestra red local.

6.- Cuando todo sea correcto, haremos clic en el botón Aceptar.

En el caso de que sí fuésemos a utilizar el protocolo TCP/IPv6, repetiríamos los pasos 5 y 6 para configurarlo.



C. Proporcionar un nombre de equipo en Windows Server 2012 R2 con escritorio.

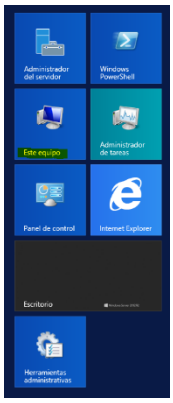
Para llevar a cabo esta tarea, recurriremos al elemento *Este equipo*, que encontramos en el menú *Metro*.

1.- Para comenzar, hacemos clic sobre el icono del menú Inicio.

Veremos que la pantalla cambia para mostrarnos el menú *Metro*, que ya conocemos de apartados anteriores.

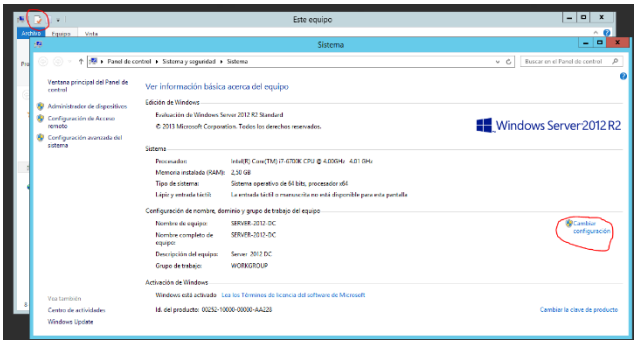
2.- Hacemos clic sobre el elemento Este equipo.

La ventana del *Explorador de archivos* que se muestra a continuación, dispone de un nuevo botón llamado *Propiedades del sistema*.



3.- Hacemos clic sobre él

Al hacerlo, aparece la ventana *Sistema*, que aglutina una gran cantidad de información sobre nuestro equipo, como el tipo de procesador, la cantidad de memoria o el tipo de procesador.

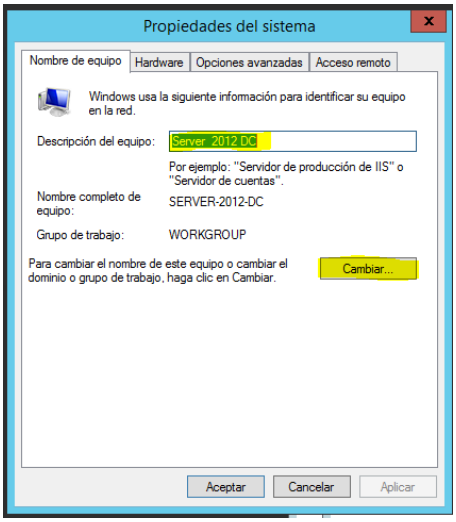


También aparecen datos sobre la configuración, como el nombre del equipo o el del grupo de trabajo al que pertenece.

4.- En esta zona, aparece un enlace titulado Cambiar configuración. Hacemos clic sobre él.

Veremos que aparece una ventana con el título *Propiedades del sistema*. En ella podemos ver el nombre que se está utilizando actualmente y también podemos escribir una breve descripción textual.

5.- Para cambiar el nombre del equipo haremos clic en el botón Cambiar…



En la ventana *Cambios en el dominio o el nombre del equipo* podemos escribir el nuevo nombre. Para este ejemplo, usaremos **`Server 2012 DC`**.

De momento, no tenemos definido ningún dominio, por lo que no tendría sentido poner un nombre de dominio. En todo caso, podríamos cambiar el nombre del grupo de trabajo del que pueda formar parte el Servidor. Sin embargo, de momento no lo haremos.

Más adelante, cuando definamos el dominio, estableceremos un nombre para el mismo.

6.- Cuando hayamos escrito el nuevo nombre del equipo, haremos clic en Aceptar.

Antes de cerrarse la ventana, aparece un aviso informándonos de que el nuevo nombre no estará en activo hasta que no reiniciemos el servidor.

7.- Para seguir, hacemos clic en Aceptar.

Por último, cuando salgamos de la ventana de *Propiedades del sistema*, aparecerá un nuevo aviso dándonos la oportunidad de reiniciar el sistema en ese preciso instante o aplazar esta operación para más adelante.

8.- Sea cual sea la opción elegida, haremos clic en el botón correspondiente.

D.- Habilitar las actualizaciones automáticas en Windows Server 2012 R2.

Como sabes, un servidor que se encuentra en explotación debe mantenerse lo más actualizado posible por dos cuestiones: Rendimiento y seguridad. Por ese motivo, hoy vamos a explicarte cómo habilitar las actualizaciones de forma sencilla. Veamos cómo lograrlo:

1.- En la ventana Administrador del servidor, hacemos clic sobre el enlace Servidor local.

Una vez dentro de la categoría *Servidor local*, vemos que tenemos acceso a muchas de las características del equipo (como el *Nombre del equipo*, o la *Zona horaria*, que ya hemos aprendido a modificar de otro modo).

En la columna derecha, tenemos una entrada titulada *Windows Update*, cuyo estado se muestra en un enlace con el texto *No configurado*.

2.- Hacemos clic sobre dicho enlace.

Al hacerlo, aparecerá una ventana titulada *Windows Update*. En ella, observamos el icono típico de aviso de *Windows* para avisarnos de que el valor de configuración no es el más adecuado.

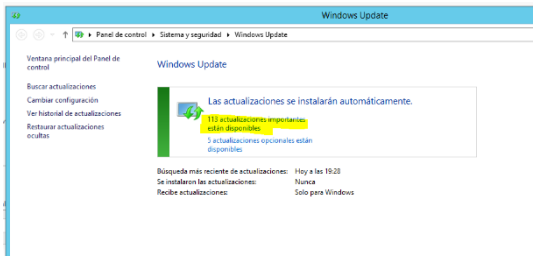
3.- Para resolverlo, hacemos clic sobre el botón Activar actualizaciones automáticas.

Windows comenzará de forma inmediata a buscar actualizaciones a través de Internet, que aún no hayan sido aplicadas a nuestro sistema.

4.- Nos limitamos a esperar un tiempo que dependerá del número de actualizaciones que tengamos pendientes.

Cuando concluye la búsqueda, la ventana muestra el número de actualizaciones que hay pendientes de instalar y el aviso de que se instalarán de forma automática, lo que significa que ya tenemos el sistema activado.

5.- Para obtener el detalle de las actualizaciones obtenidas y decidir cuáles se instalarán, hacemos clic sobre el enlace.



Si lo hacemos, obtendremos una ventana como la siguiente, donde aparecen todas las actualizaciones seleccionadas. Junto a cada una de ellas encontraremos su tamaño y, cuando seleccionemos una, obtendremos a la derecha una explicación detallada de su objetivo.

6.- Si quisiéramos instalarlas todas en este momento, bastaría con hacer clic sobre el botón Instalar.

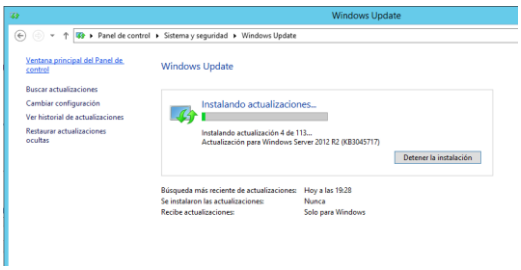
También podemos desmarcar la casilla de la parte superior (que las desmarca todas) y marcar sólo aquellas en las que estemos interesados. A modo de ejemplo, nosotros hemos dejado marcadas sólo las cuatro primeras.

7.- … Y para instalarlas, hacemos clic sobre el botón Instalar.

Si lo hacemos, se cierra la ventana y comienza la descarga e instalación de las actualizaciones que hayamos indicado. Podemos esperar hasta que termine el proceso…

8.- … o hacer clic sobre el botón Detener descarga y dejarlo para otro momento.

Si decidimos esperar a que termine el proceso anterior, es muy probable que al final el sistema nos pida reiniciar el ordenador para que se complete la instalación de las actualizaciones.



Dado que se trata de un servidor, y que puede que cuando se descarguen e instalen las actualizaciones, ni siquiera estemos delante, *Windows Server 2012 R2* tiene un mecanismo que le permite reiniciarse de forma automática si no lo hacemos nosotros (aunque nos esperará durante todo un día).

9.- Si decidimos reiniciar el servidor en este momento, bastará con hacer clic sobre el botón Reiniciar ahora.

Aunque el proceso que sigue es un poco monótono, lo incluiré completo, para que sepas lo que verás en tu sistema.

Lo primero será que el fondo de la pantalla se pone en color azul y nos muestra un aviso para que no apaguemos el servidor antes de terminar la actualización.

10.- Nos limitamos a esperar, mientras los puntos de la izquierda realizan su incansable movimiento.

Cuando termine, nos aparece un aviso indicando que el servicio que se encarga de la instalación de los componentes de *Windows* se está cerrando.

11.- … aunque nosotros seguiremos esperando

Después, el sistema nos indica que está trabajando con las actualizaciones y nos recuerda que no debemos apagar el equipo.

12.- … así es que, como no nos queda otra, seguimos esperando.

Por fin, cuando haya terminado todo el proceso, el sistema comienza su reinicio.

13.- Aparece la palabra Reiniciando durante unos instantes y, después, se reinicia el equipo.

Durante el arranque, puede que aún se necesiten unos instantes más para concluir la instalación de las actualizaciones, pero pronto veremos que se está iniciando el Administrador de sesión local.

14.- … aunque nosotros seguiremos esperando.

Como es habitual, después de autenticarnos, se abrirá la ventana del *Administrador del servidor*.

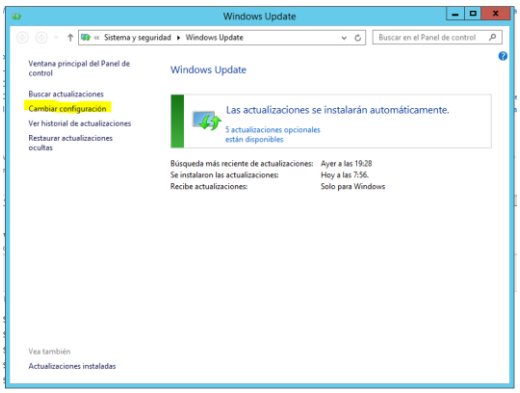
15.- Para terminar la configuración, volvemos a hacer clic sobre la categoría *Servidor local*.

Como antes, volvemos a hacer clic sobre el enlace que hay junto a la entrada *Windows Update*.

16.- … aunque ahora el texto será Instalar actualizaciones automáticamente mediante Windows Update.

De nuevo, aparecerá la ventana *Windows Update*.

17.- Para ajustar el comportamiento de la herramienta, hacemos clic sobre el enlace *Cambiar configuración*.



En la ventana que aparece, podemos controlar el momento en el que se aplican las actualizaciones (teniendo en cuenta que en muchos casos será preciso reiniciar el sistema).

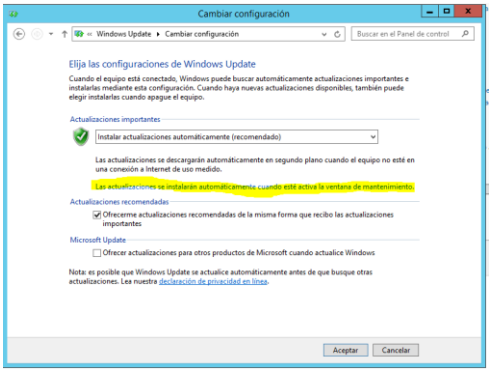
Uno de los aspectos más cruciales de esta ventana es que podremos indicar cómo se debe comportar el sistema con las actualizaciones importantes. Las opciones disponibles son estas:

- Instalar actualizaciones automáticamente (recomendado)
- Descargar actualizaciones, pero permitirme elegir si deseo instalarlas
- Buscar actualizaciones, pero permitirme elegir si deseo descargarlas e instalarlas
- No buscar actualizaciones (no recomendado)

Como puedes ver, las opciones van de más seguras a menos seguras. Por este motivo, nosotros dejaremos activa la opción predeterminada: *Instalar actualizaciones automáticamente (recomendado)*.

Bajo las opciones anteriores disponemos de un enlace con el texto *Las actualizaciones se instalarán automáticamente cuando esté activa la ventana de mantenimiento*, que nos llevará a una ventana donde podremos cambiar el momento en el que se realizan las tareas de mantenimiento.

18.-Hacemos clic sobre el enlace.

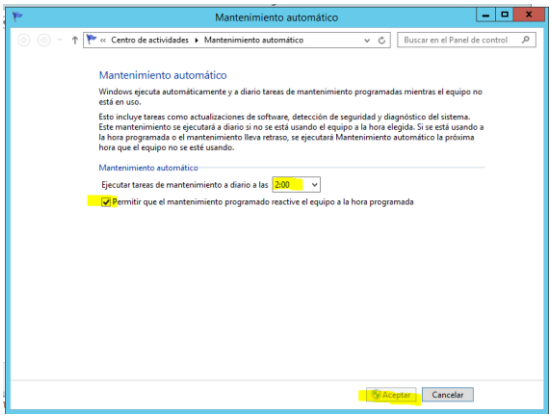


No debemos olvidar que las operaciones de mantenimiento incluyen procesos de actualización, comprobaciones de seguridad y otros diagnósticos del sistema. Estas tareas se ejecutan cuando el equipo no está en uso. Si, llegado el momento de realizar este tipo de operaciones, el sistema está en uso, se aguardará hasta un momento en el que se encuentre inactivo.

Como se puede entender, si elegimos bien la hora, podremos estar bastante seguros de que las operaciones de mantenimiento se realizan cuando nosotros hemos estimado.

También podremos indicar que, cuando el sistema se encuentre suspendido, las operaciones de mantenimiento puedan activarlo.

19.-Una vez establecidos los valores adecuados, hacemos clic sobre el botón *Aceptar*.



convertir un servidor Windows Server 2012 R2 en controlador de dominio

En lo relativo a la instalación del dominio, *Windows Server 2012 R2* sigue la misma estructura que las versiones anteriores:

- Primero deberemos instalar el rol *Servicios de dominio de Active Directory*.
- A continuación, convertiremos (promocionaremos) el servidor en un controlador de dominio.

Esto es lógico, ya que son muchos los roles que puede desempeñar un servidor *Windows Server 2012 R2* en una red, y no tendría sentido que todos ellos estuviesen instalados de forma predeterminada. Será el administrador del sistema quien decida la función que deba realizar el servidor. Y el primer paso siempre será instalarla.

Por otro lado, la tarea de convertir un equipo con *Windows Server 2012 R2*, en un *controlador de dominio de Active Directory*, aunque no es complicada, sí es un poco larga .

Instalar el rol Servicios de dominio de Active Directory

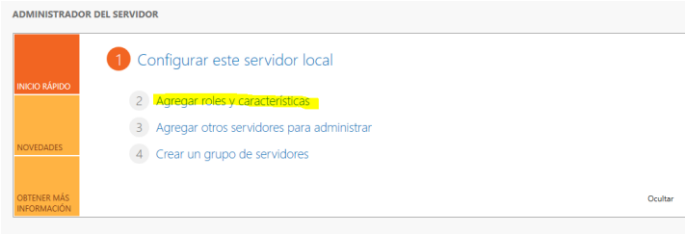
La instalación de roles y características de *Windows Server 2012 R2*, se realiza desde la herramienta *Administrador del servidor*.

Lo normal es que se abra automáticamente al iniciar sesión con la cuenta de *Administrador*, pero si la has cerrado, puedes encontrarla, fácilmente, haciendo clic sobre el botón *Inicio*. Después, sólo tendrás que hacer clic sobre el icono que representa a la herramienta.

La cuestión es que para iniciar la instalación de un dominio en nuestro servidor, necesitamos partir de esta ventana.

Para comenzar, haremos clic sobre el enlace *Agregar roles y características* de la página principal de la ventana.

1.- Si no estamos en la página principal, también podemos recurrir al menú *Administrar*, que contiene una opción con el mismo título.



Puede que el servidor no pueda atendernos de forma inmediata porque se encuentre recopilando datos. Si esto es así, además de una ventana de aviso, observaremos que los cuadros de estado de la parte inferior se han puesto de color rojo.

2.- Sólo tenemos que hacer clic sobre el botón *Aceptar* y esperar unos instantes.

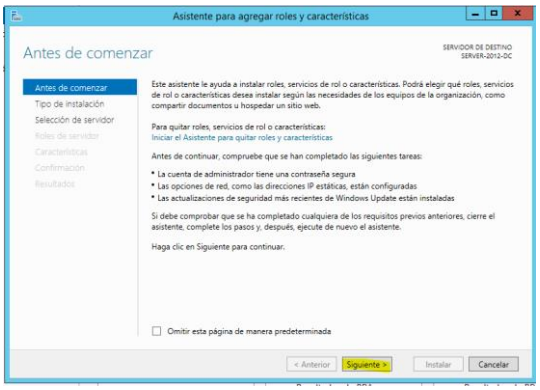
Poco después, observaremos que al menos se habrá puesto de color verde el cuadro de la izquierda.

3.- En ese momento volveremos a hacer clic sobre el enlace *Agregar roles y características*.

En ese momento se iniciará el *Asistente para agregar roles y características*. Este asistente no es específico de *Active Directory*, sino que nos puede guiar a través de la instalación de otras funciones tan diversas como DNS, Internet Information Server (IIS), fax, etc.

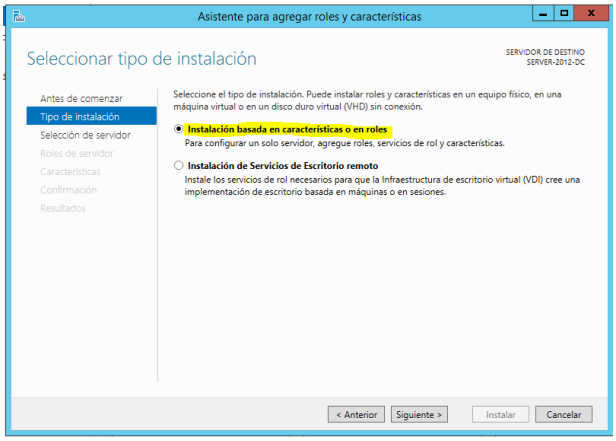
Es importante seguir las recomendaciones del propio asistente en cuanto a asegurarnos de que la contraseña de la cuenta de *Administrador* es segura, que la configuración de red es correcta, que disponemos de direcciones IP estáticas y que hemos instalado las últimas actualizaciones de seguridad en el sistema operativo.

4.- Una vez que todo sea correcto, hacemos clic en el botón Siguiente.



Como vemos en la siguiente imagen, ahora tenemos la posibilidad de instalar los servicios de escritorio remoto de forma independiente. Sin embargo, de momento sólo nos centraremos en la instalación de roles y características, de forma similar a como lo hacíamos con Windows Server 2008.

5.- Elegimos *Instalación basada en características o en roles* y hacemos clic sobre el botón *Siguiente*.



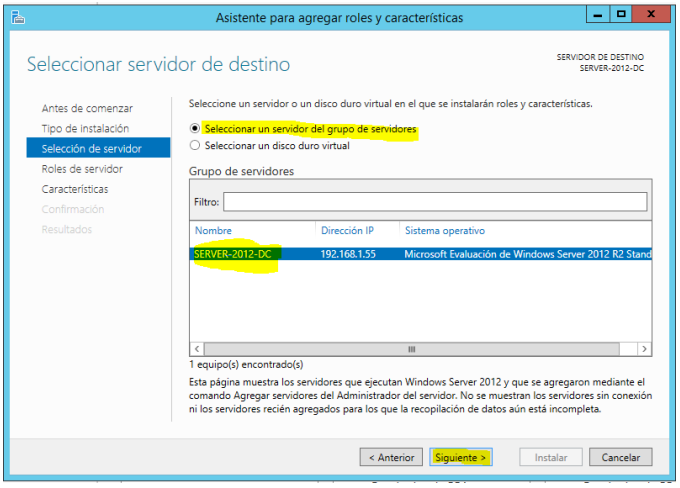
Una característica muy interesante que se ha añadido al Administrador del Servidor de Windows Server 2012 es la posibilidad de usar el Asistente para Agregar roles y características para instalarlas en el disco duro virtual (*VHD*) sin que éste tenga que estar unido a una máquina virtual (o que lo esté, pero que la máquina virtual esté apagada). Esto facilita los cambios en una instalación virtual a la vez que reduce el esfuerzo administrativo.

Si necesitamos cubrir esta tarea, en el siguiente paso elegiremos la opción *Seleccionar un disco duro virtual*.

Sin embargo, en nuestro caso, necesitamos instalar el rol del *Directorio Activo* en el sistema con el que estamos trabajando, por lo que la opción elegida será *Seleccionar un servidor del grupo de servidores*. De esta forma, obtendremos una lista con los servidores de nuestra red local que ejecutan *Windows Server 2012*. Lógicamente, sólo se muestran los servidores que estén funcionando y se haya completado su recopilación de datos.

En nuestro caso, sólo aparece el servidor en el que estamos trabajando.

6.- Hacemos clic sobre su entrada y, a continuación, sobre el botón Siguiente.



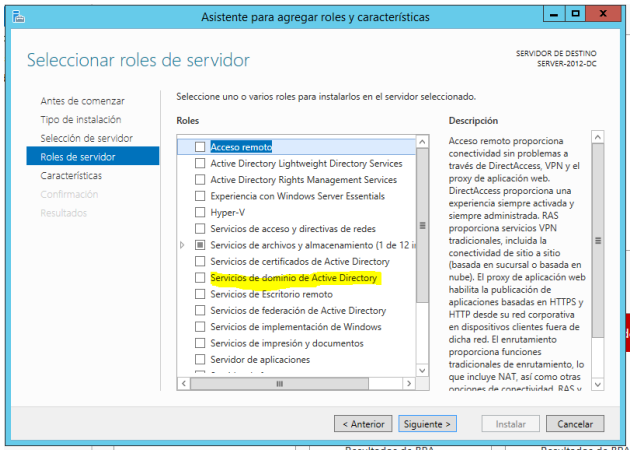
En la siguiente etapa, tendremos que elegir el servicio o servicios que queremos instalar.

Debemos tener en cuenta que, para que *Active Directory* funcione

correctamente, es preciso tener instalado un *Servidor DNS*. Sin embargo, aquí lo dejaremos sin seleccionar para comprobar que, más adelante, el asistente lo habrá seleccionado de forma predeterminada.

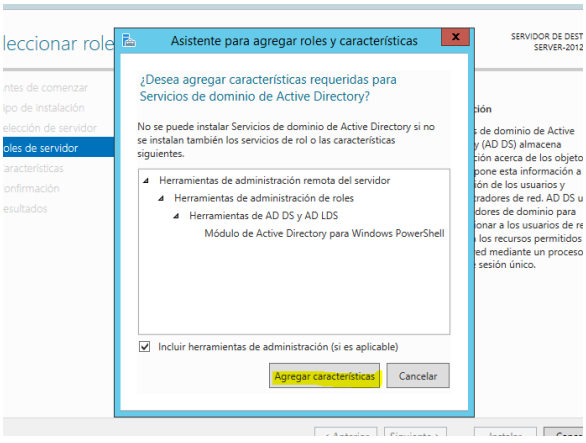
Observa que, a la derecha de la lista, en el cuadro *Descripción*, aparece una breve explicación del rol sobre el que nos encontremos en ese momento.

7.- Activamos la entrada *Servicios de dominio de Active Directory*.



Al hacerlo, el asistente nos muestra un aviso indicando que los servicios elegidos dependen de otros roles y características que necesitaremos instalar también de forma complementaria.

8.- Nos limitamos a hacer clic sobre el botón *Agregar características*.

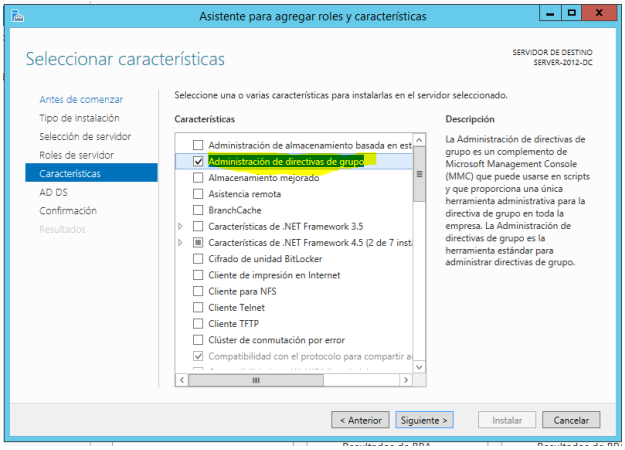


Al hacerlo, comprobamos que la línea *Servicios de dominio de Active Directory* ya aparece seleccionada.

9.- Para continuar, hacemos clic sobre el botón *Siguiente*.

Después de seleccionar los roles, el asistente nos ofrece la posibilidad de instalar características. En nuestro caso, aprovecharemos para instalar *Administración de directivas de grupo*, de forma que centralicemos en una sola herramienta las directivas de grupo de toda la instalación.

10.- Una vez elegida la característica, hacemos clic sobre el botón *Siguiente*.



Podemos definir el concepto de *rol* como un servicio que el equipo ofrece a los clientes de la red. Por el contrario, una *característica* es una función que usa el servidor para llevar a cabo su propia labor.

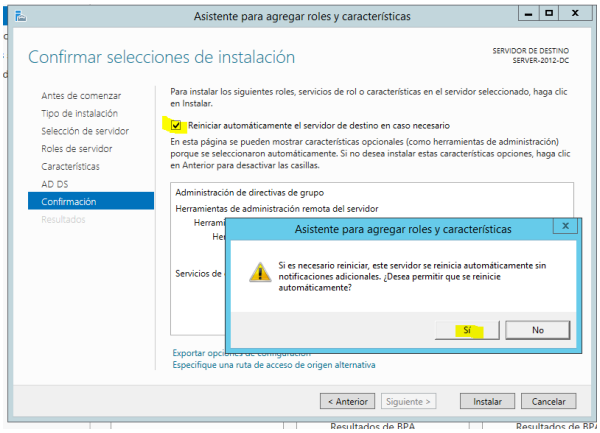
Después de esto, aparece una pantalla informativa que debemos leer atentamente. Quizás uno de los aspectos más interesantes de esta ventana es la recomendación de instalar al menos dos controladores de dominio para un determinado dominio, con el fin de aumentar la disponibilidad de la infraestructura de red.

También nos recuerda la necesidad de disponer de un *servidor DNS* y nos informa de que se instalará el servicio de *espacio de nombres* y los de *replicación*, que son necesarios para el servicio de directorio.

11.- Cuando estemos seguros de haber entendido toda la información, haremos clic en el botón *Siguiente*.

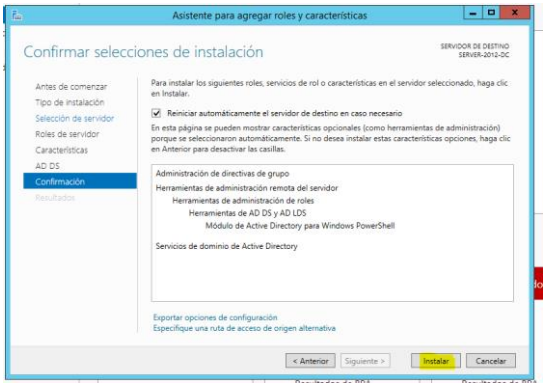
Antes de proceder con la instalación, tenemos la oportunidad de marcar la opción *Reiniciar automáticamente el servidor de destino en caso necesario*. Al hacerlo aparece un cuadro de diálogo que nos advierte de que al marcar la opción, pueden producirse reinicios sin notificaciones previas.

12.- En nuestro caso, haremos clic sobre el botón *Sí*.



Por último, en la pantalla que resumen de la instalación, podemos comprobar los distintos roles y características que van a instalarse. Como es habitual, si observamos algún error, podemos usar el botón *Anterior* para retroceder hasta el paso adecuado y realizar las modificaciones.

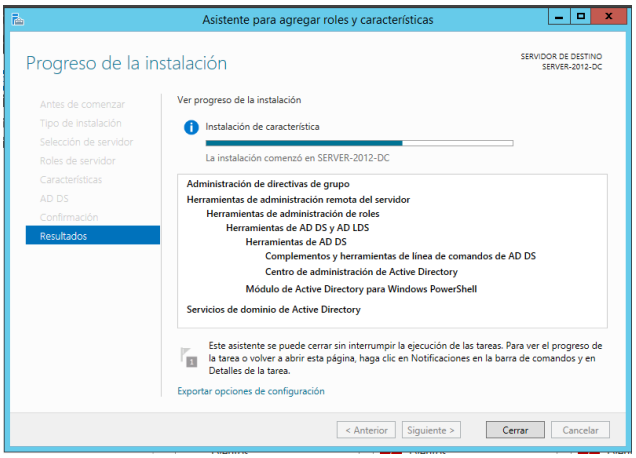
13.- Sin embargo, si todo es correcto, haremos clic sobre el botón *Instalar*.



A partir de aquí, en la parte superior de la ventana podremos ver una barra de progreso que nos mantiene informados del avance de la instalación.

Observa que ya puedes cerrar el asistente y el proceso de instalación no se interrumpirá. Si lo haces, podrás consultar el avance de la tarea o abrir la ventana del asistente usando el icono  que aparece en la parte superior del *Administrador del servidor*.

14.- En nuestro caso, nos limitamos a esperar.



Cuando termine la instalación, aparecerá un enlace con el texto *Promover este servidor a controlador de dominio*.

15.- Bastará con hacer clic sobre el enlace para iniciar el paso siguiente…

Instalar un dominio desde la interfaz gráfica de Windows Server 2012 R2 (parte 2).

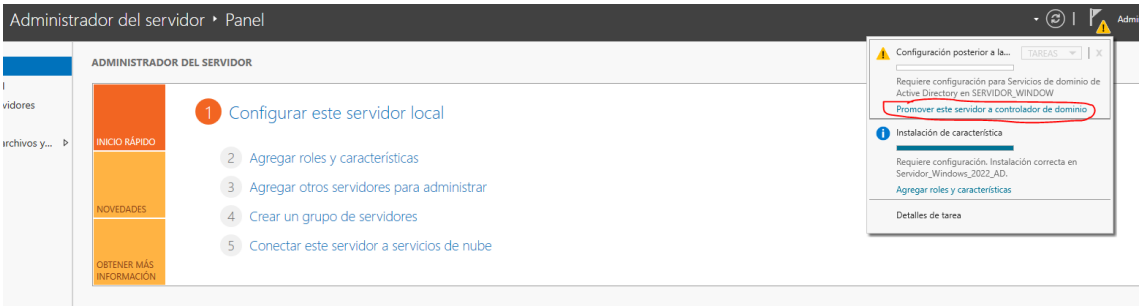
El objetivo final consistirá en disponer de un controlador de dominio para administrar los recursos de nuestra infraestructura de red. Como recordarás, en la primera parte habíamos instalado el rol *Servicios de dominio de Active*

Directory. Ahora es el momento de convertir (*promocionar*) el servidor para convertirlo en un controlador de dominio.

Como vimos al final de la primera parte, después de realizar la instalación del rol *Servicios de dominio de Active Directory*, bastaría con hacer clic sobre el enlace *Promover este servidor a controlador de dominio* de la última pantalla del asistente. Así iniciaríamos la promoción.

No obstante, si hubiésemos cerrado la ventana, también podremos hacer uso del icono que aparece en la parte superior del *Administrador del servidor*.

1.- En cualquier caso, hacemos clic en el enlace Promover este servidor a controlador de dominio.



Al hacerlo, se abrirá la ventana del *Asistente para configuración de Servicios de dominio de Active Directory*. En la primera pantalla, deberemos indicar el tipo de operación que queremos implementar:

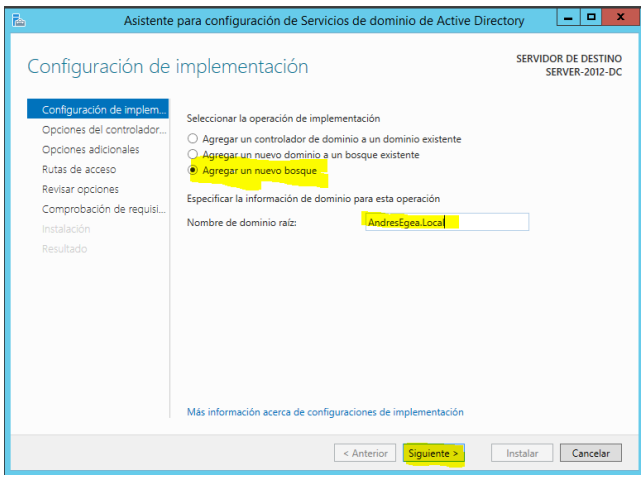
D. Agregar un controlador de dominio a un dominio existente.

E. Agregar un nuevo dominio a un bosque existente.

F. Agregar un nuevo bosque.

Lógicamente, como en este caso estamos partiendo de una situación en la que no disponemos de infraestructura previa, la opción que deberemos elegir es la última. Cuando lo hagamos, en la parte inferior se nos solicitará el dominio raíz para el nuevo bosque. Si disponemos de un dominio registrado en Internet, aquí incluiremos el nombre de dicho dominio (p. ej. **`AndreEgea.es`**). Sin embargo, de momento supondremos que no es así y terminaremos nuestro dominio en *.local* (p. ej. **`AndresEgea.local`**).

2.- Cuando hayamos escrito el nombre, hacemos clic en *Siguiente*.



Microsoft recomienda que todos los controladores de dominio sean también *servidores DNS* para asegurar que *Active Directory* esté siempre disponible.

En el siguiente paso (*Opciones del controlador*) indicamos el nivel de funcionalidad del controlador. Si no tenemos en la red controladores de dominio que ejecuten versiones más antiguas de *Windows Server*, deberemos elegir *Windows Server 2012 R2* (que será el valor predeterminado).

Lógicamente, también podemos elegir un nivel de funcionalidad con *Windows Server 2008* o (*2008 R2*) si pensamos añadir este tipo de controladores más adelante.

Como cabe esperar, cuanto más antiguo sea el nivel de funcionalidad que elijamos, más limitadas se verán las prestaciones de nuestro árbol de dominios.

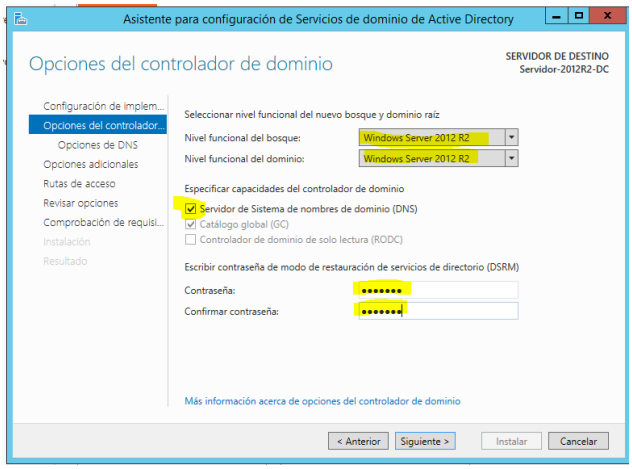
Bajo el epígrafe Especificar capacidades del controlador de dominio, indicaremos que el equipo también actuará como Servidor de Nombres de Dominio (DNS). Además, aparecen dos opciones más: Catálogo global (GC) y Controlador de dominio de solo lectura (RODC).

El primero aparecerá seleccionado de forma obligatoria porque todo dominio debe tener un catálogo global y estamos instalando el único controlador que hay ahora mismo en la red.

Del mismo modo, dado que el servidor actual es único, no puede ser de sólo lectura.

Por último, antes de cambiar de página, deberemos escribir la contraseña del *modo de restauración de servicios de directorio* (*DSRM*). Como es habitual, se escribe por duplicado para evitar errores tipográficos.

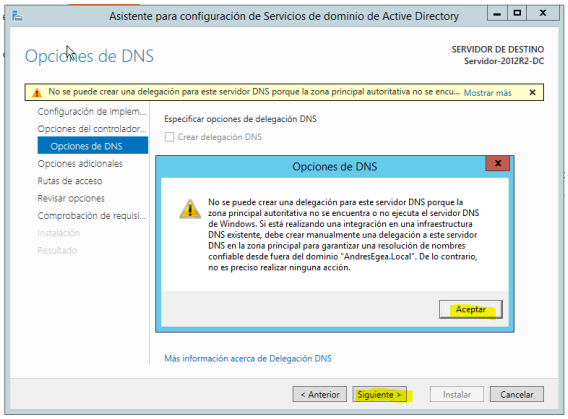
3.- Finalmente, hacemos clic sobre el botón *Siguiente*.



En el siguiente paso, *Opciones de DNS*, si dispusiésemos una infraestructura DNS anterior a la instalación del dominio, deberíamos especificar si deseamos crear en dicha infraestructura una delegación para el servidor DNS que vamos a instalar ahora.

Sin embargo, como no se encuentra un *Servidor DNS* principal, *Windows Server* nos muestra una ventana de aviso y nos informa de que, en caso de que sea necesaria, habrá que hacer dicha delegación a mano.

4.- … Como no es el caso, basta con hacer clic sobre el botón *Aceptar* de la ventana de aviso y después clic sobre el botón *Siguiente* de la ventana principal del asistente.

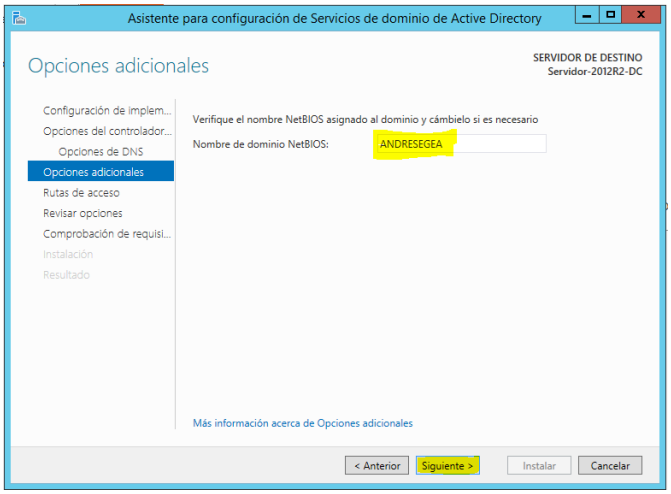


El nombre *NetBIOS* puede tener hasta 15 caracteres formado por letras (mayúsculas o minúsculas), dígitos o guiones ('-'), aunque no puede ser enteramente numérico.

A continuación, en el paso *Opciones adicionales*, el asistente sugiere un nombre *NetBIOS* para el dominio raíz del bosque. Lógicamente, podemos aceptar el nombre que nos propone o indicar cualquier otro.

En nuestro caso, el nombre sugerido nos parece bien, por lo que lo dejamos tal cual.

5.- Para seguir, hacemos clic sobre el botón *Siguiente*.



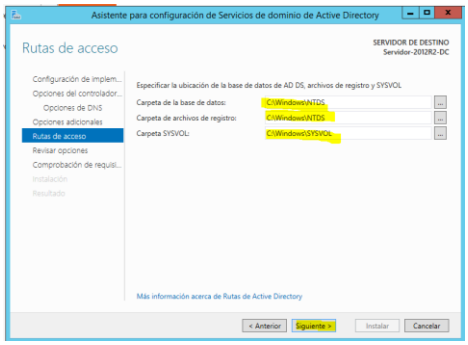
Los *archivos de registro* también suelen llamarse *archivos log*.

Después de esto, en el apartado *Rutas de acceso*, el asistente nos pregunta dónde queremos almacenar los archivos de trabajo de *Active Directory* (la base de datos, los archivos de registro y la carpeta SYSVOL).

Puede ser una opción interesante que los archivos de registro y la base de datos se almacenen en volúmenes separados. De esta forma mejorará el rendimiento (ya que se podrá acceder a ambos archivos de forma simultánea) y las posibilidades de recuperación de los datos si se producen problemas.

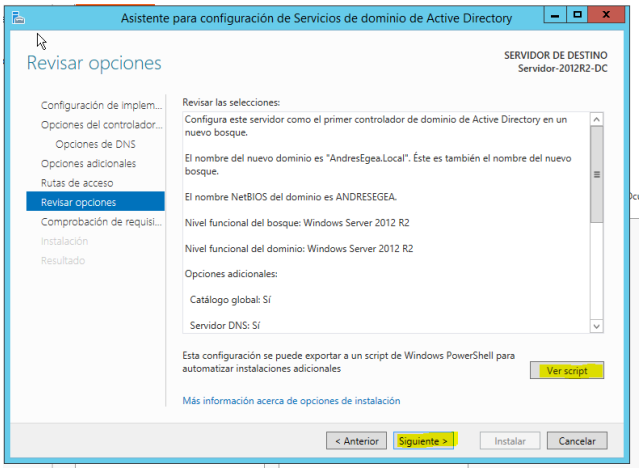
A pesar de todo, en la ventana aparece de forma predeterminada una ubicación de la unidad C. El motivo es muy sencillo: no tenemos otra.

6.- Por lo tanto, nos limitamos a hacer clic en *Siguiente*.

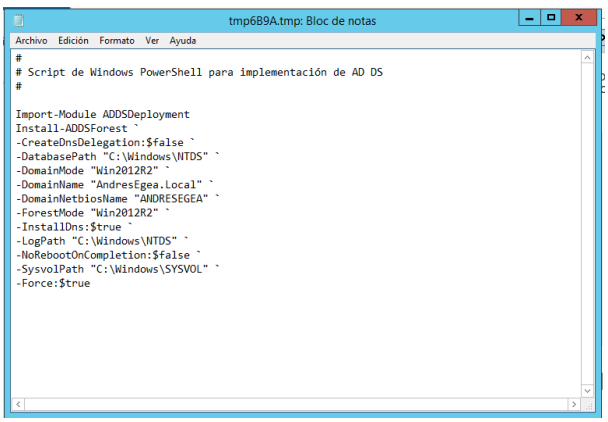


En el apartado *Revisar opciones*, como cabe esperar, el asistente muestra un resumen del proceso de instalación. Debemos revisarlo para asegurarnos de que no hemos cometido errores en los pasos anteriores. Como es habitual, disponemos del botón *Anterior* para resolver cualquier error que podamos observar.

7.- Si todo es correcto, basta con hacer clic sobre el botón *Siguiente*.



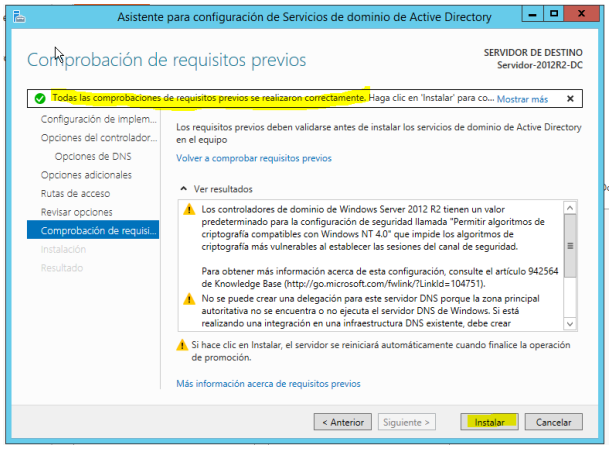
NOTA: También disponemos del botón *Ver script*, que nos permite obtener un script de *PowerShell* para automatizar una instalación como esta sin tener que volver a introducir de nuevo todos los datos.



Por último, en el apartado *Comprobación de requisitos*, se verifica que el sistema cumple todas las condiciones para convertirse en un controlador de dominio.

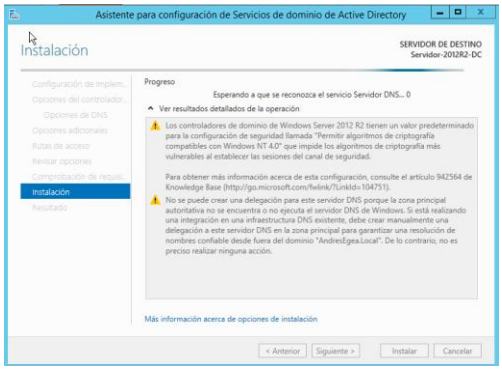
Como puedes ver en la imagen siguiente, pueden aparecer algunos avisos, como el que nos informa de que no puede crearse una delegación para el servidor DNS que estamos a punto de instalar (ya comentamos esta circunstancia más arriba). También pueden aparecer errores que impidan la instalación del controlador de dominio. En estos casos, no podremos continuar hasta que no los resolvamos.

8.- Como en nuestro sistema no han aparecido errores, podemos hacer clic sobre el botón *Instalar* para completar la operación.



Durante el proceso de instalación seguirán apareciendo mensajes informativos que deberemos tener en cuenta para una futura configuración del servidor.

9.- Nos limitamos a esperar unos instantes.



Cuando termine la instalación, el servidor se reiniciará automáticamente.

10.- Cuando aparezca el mensaje, hacemos clic sobre el botón *Cerrar*.

Al hacerlo, se inicia el proceso de reinicio

11.- Sólo tenemos que esperar a que se complete.

El proceso puede durar más de lo normal, porque se está completando la configuración del sistema.

12.- Cuando acabe, obtendremos la pantalla de bienvenida. Pulsamos las teclas *Ctrl* + *Alt* + *Supr* para autenticarnos.

Cuando finalmente se nos solicite la contraseña de la cuenta *Administrador*, veremos que ahora la cuenta aparece precedida del nombre *NetBios* del dominio (en este caso, *ANDRESEGEA*). Esta es la primera constatación de que todo ha sido correcto.

13.- Nos limitamos a escribir la misma contraseña que utilizábamos hasta ahora.

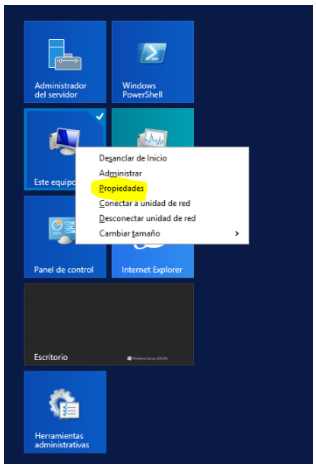
La primera vez que iniciemos sesión con la cuenta *Administrador*, también observaremos que tarda bastante más tiempo del normal. El motivo, de nuevo, es que el rol que tiene esta cuenta dentro del sistema también ha cambiado y dichos cambios se aplicarán en este momento.

Para finalizar, podremos asegurarnos de que todo el proceso ha sido correcto, observando la pantalla de propiedades del equipo. Una de las formas más sencilla de conseguirlo es desde el menú *Metro*.

14.- Hacemos clic sobre el menú *Inicio*.

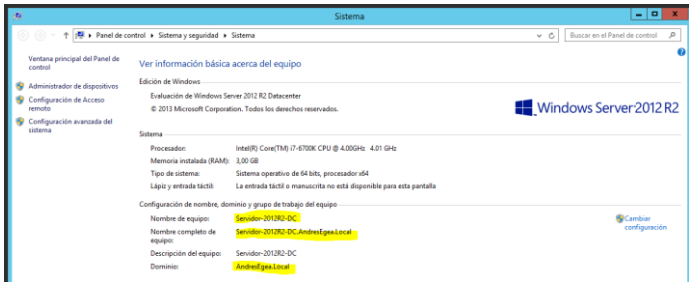
De forma inmediata, la pantalla cambiará para mostrarnos el contenido del menú *Metro*.

15.- Hacemos clic, con el botón derecho del ratón sobre el icono Este Equipo.



Cuando se muestre la ventana Sistema, podremos comprobar que los valores de los campos Nombre completo del equipo y Dominio son correctos.

16.- Después de hacer la comprobación, podemos cerrar la ventana para seguir trabajando.



6.3.- Administración del directorio activo

6.3.1.- Herramientas Administrativas

La mayor parte de las tareas administrativas en el Directorio Activo se realiza con alguna de estas herramientas:

- **Usuarios y Equipos de Active Directory.** Permite realizar las tareas diarias con usuarios, grupos, equipos, impresoras, carpetas compartidas, etc.
- **Sitios y Servicios de Active Directory.** Permite administrar la replicación y temas relacionados con la topología de la red.
- **Dominios y Confianzas.** Permite realizar las relaciones de confianza y los niveles funcionales del dominio y del bosque.

6.3.2 Conceptos básicos

Uno de los elementos fundamentales en la administración de una red, es el control de los usuarios, grupos y equipos. Por ello, debemos aprender cómo crearlos, modificarlos, organizarlos y, si llega el caso, eliminarlos. Además, deberemos asignar privilegios para cada uno de ellos, de modo que podamos establecer en qué medida y en qué condiciones podrán beneficiarse de los recursos de la red. Este objetivo lo cubriremos, en parte durante el presente capítulo, pero seguiremos completándolo en el siguiente.

Cuenta de usuario

Las cuentas de usuario también suelen identificarse como **entidades de seguridad**.

Como ya comentábamos en el capítulo anterior, una de las primeras ideas que deben quedar claras cuando hablamos de cuentas de usuario es que no siempre representan a personas concretas, sino que también pueden ser utilizadas como mecanismos de acceso para determinados servicios o aplicaciones de la máquina local o, incluso, de un equipo remoto. En definitiva, una cuenta de usuario es un objeto que posibilita el acceso a los recursos del dominio de dos modos diferentes:

Por razones de seguridad, debes evitar que varios usuarios utilicen la misma cuenta para iniciar sesión en el dominio.

- Permite **autenticar la identidad** de un usuario, porque sólo podrán iniciar una sesión aquellos usuarios que dispongan de una cuenta en el sistema asociada a una determinada contraseña.
- Permite **autorizar**, **o denegar**, el acceso a los recursos del dominio, porque, una vez que el usuario haya iniciado su sesión sólo tendrá acceso a los recursos para los que haya recibido los permisos correspondientes.

Cada cuenta de usuario dispone de un identificador de seguridad (*SID*, *Security IDentifier*) que es único en el dominio.

Cuentas integradas

Cuando se crea el dominio, se crean también dos nuevas cuentas: *Administrador* e *Invitado*. Posteriormente, cuando es necesario, se crea también la cuenta *Asistente de ayuda*. Estas son las denominadas *cuentas integradas* y disponen de una serie de derechos y permisos predefinidos:

Desde el punto de vista de la seguridad, puede ser interesante cambiar el nombre de la cuenta *Administrador*.

- **Administrador**: Tiene control total sobre el dominio y no se podrá eliminar ni retirar del grupo *Administradores* (aunque sí podemos cambiarle el nombre o deshabilitarla).
- **Invitado**: Está deshabilitada de forma predeterminada y, aunque no se recomienda, puede habilitarse, por ejemplo, para permitir el acceso a los usuarios que aún no tienen cuenta en el sistema o que la tienen deshabilitada. De forma predeterminada no requiere contraseña, aunque esta característica, como cualquier otra, puede ser modificada por el administrador.
- **Asistente de ayuda**: se utiliza para iniciar sesiones de *Asistencia remota* y tiene acceso limitado al equipo. Se crea automáticamente cuando se solicita una sesión de asistencia remota y se elimina cuando dejan de existir solicitudes de asistencia pendientes de satisfacer.

Por último, es importante tener en cuenta que, aunque la cuenta *Administrador* esté deshabilitada, podrá seguir usándose para acceder al controlador de dominio en *modo seguro*.

Cuenta de equipo

Los sistemas de escritorio *Windows* que sean anteriores a *XP* no pueden disponer de cuentas de equipo. El motivo es que estos sistemas carecen de características de seguridad avanzadas.

Como ocurría con las cuentas de usuario, una cuenta de equipo sirve para autenticar a los diferentes equipos que se conectan al dominio, permitiendo o denegando su acceso a los diferentes recursos del dominio. Del mismo modo que con las cuentas de usuario, las cuentas de equipo deben ser únicas en el dominio. Aunque una cuenta de equipo se puede crear de forma manual (como veremos más adelante), también se puede crear en el momento en el que el equipo se une al dominio.

Cuenta de grupo

Cuando una cuenta de usuario o de equipo está incluida en un grupo se dice que es *miembro del grupo*.

Un grupo es un conjunto de objetos del dominio que pueden administrarse como un todo. Puede estar formado por cuentas de usuario, cuentas de equipo, contactos y otros grupos. Podemos utilizar los grupos para simplificar algunas tareas, como:

- *Simplificar la administración*: Podemos asignar permisos al grupo y éstos afectarán a todos sus miembros.
- *Delegar la administración*: Podemos utilizar la directiva de grupo para asignar derechos de usuario una sola vez y, más tarde, agregar los usuarios a los que queramos delegar esos derechos.
- *Crear listas de distribución de correo electrónico*: Sólo se utilizan con los grupos de distribución que comentaremos más abajo.

El *Directorio Activo* proporciona un conjunto de grupos predefinidos que pueden utilizarse tanto para facilitar el control de acceso a los recursos como para delegar determinados roles administrativos. Por ejemplo, el grupo *Operadores de copia de seguridad* permite a sus miembros realizar copias de seguridad de todos los controladores de dominio, en el dominio al que pertenecen.

Ámbito de los grupos

El ámbito de un grupo establece su alcance, es decir, en qué partes de la red puede utilizarse, y el tipo de cuentas que pueden formar parte de él. En ese sentido, pueden pertenecer a una de las siguientes categorías:

- Ámbito local: Entre sus miembros pueden encontrarse uno o varios de los siguientes tipos de objetos:
  - Cuentas de usuario o equipo.
  - Otros grupos de ámbito local.
  - Grupos de ámbito global.
  - Grupos de ámbito universal.

Las cuentas o grupos contenidos tendrán necesidades de acceso similares dentro del propio dominio. Por ejemplo, los que necesiten acceder a una determinada impresora.

Los grupos de *ámbito global* son perfectos para contener objetos que se modifique con frecuencia, debido a que, como no se replican fuera del dominio, no generan tráfico en la red para la actualización del catálogo global.

- Ámbito global: Sólo pueden incluir otros grupos y cuentas que pertenezcan al

dominio en el que esté definido el propio grupo. Los miembros de este tipo de grupos pueden tener permisos sobre los recursos de cualquier dominio dentro del bosque. Sin embargo, estos grupos no se replican fuera de su propio dominio, de modo que, la asignación de derechos y permisos que alberguen, no serán válidas en otros dominios del bosque.

- Ámbito universal: Entre sus miembros pueden encontrarse cuentas o grupos de cualquier dominio del bosque, a los que se les pueden asignar permisos sobre los recursos de cualquier dominio del bosque.

Tipos de grupos

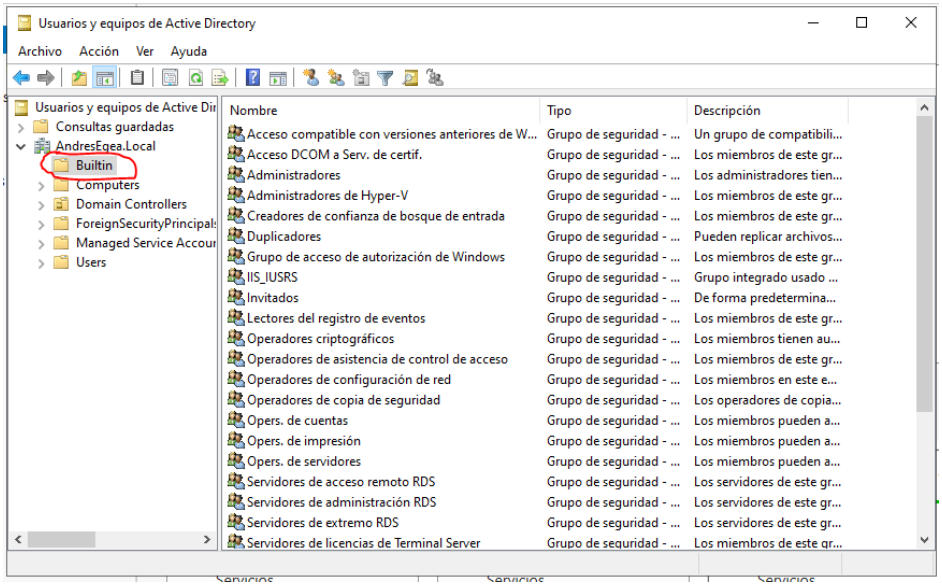
Existen dos tipos de grupos en *Active Directory*:

- Grupos de distribución: Se utilizan en combinación con programas como *Microsoft Exchange Server*, para crear listas de distribución de correo electrónico. Estos grupos no disponen de características de seguridad, por lo que no pueden aparecer en las listas de control de acceso discrecional (*DACL*, *Discretionary Access Control Lists*).
- Grupos de seguridad: Permiten asignar permisos a las cuentas de usuario, de equipo y grupos sobre los recursos compartidos. Con los grupos de seguridad podemos:
    - Asignar derechos de usuario a los grupos de seguridad del Directorio Activo. De esta forma, podemos establecer qué acciones pueden llevar a cabo sus miembros dentro del dominio (o del bosque). Como veremos después, durante la instalación del Directorio Activo, se crean grupos de seguridad predeterminados que facilitan al administrador la delegación de ciertos aspectos de la administración (como, por ejemplo, las copias de seguridad) en otros usuarios del sistema.
    - Asignar permisos para recursos a los grupos de seguridad. Lo que nos permite definir quién accede a cada recurso y bajo qué condiciones (control total, sólo lectura, etc.) También se establecen permisos de forma predeterminada sobre diferentes objetos del dominio para ofrecer distintos niveles de acceso.

Grupos integrados

Como hemos mencionado antes, durante la instalación del Directorio Activo se crean una serie de grupos que podremos utilizar para simplificar la asignación de derechos y permisos a otras cuentas o grupos. Como veremos más abajo, los grupos se administran con el complemento Usuarios y equipos de Active Director*y*. Cuando ejecutemos esta herramienta, encontraremos los grupos predeterminados en dos contenedores:

1.- Los grupos predeterminados incluidos en el contenedor *Builtin* tienen un ámbito local. Puedes ver un pequeño resumen de todos ellos en la siguiente tabla:



- **Operadores de cuentas**: Sus miembros pueden crear, modificar y eliminar cuentas de usuarios, grupos y equipos que se encuentran en los contenedores Usuarios o Equipos y en las unidades organizativas del dominio, excepto la unidad organizativa Controladores de dominio. Los miembros de este grupo no tienen permiso para modificar los grupos Administradores o Administradores del dominio ni las cuentas de los miembros de dichos grupos. Los miembros de este grupo pueden iniciar la sesión de forma local en los controladores del dominio y apagarlos. Como este grupo tiene una autoridad considerable en el dominio, hay que ser prudente al agregarle usuarios.

- **Creadores de confianza de bosque de entrada (sólo aparece en el dominio raíz del bosque):** Sus miembros pueden crear confianzas de bosque de entrada unidireccionales en el dominio raíz del bosque. Por ejemplo, los miembros de este grupo que residen en el Bosque A pueden crear una confianza de bosque de entrada unidireccional desde el Bosque B. Esta confianza de bosque de entrada unidireccional permite a los usuarios del Bosque A tener acceso a recursos ubicados en el Bosque B. Los miembros de este grupo disponen del permiso Crear confianza de bosque de entrada en el dominio raíz del bosque. Este grupo no tiene ningún miembro predeterminado.

- **Acceso compatible con versiones anteriores a Windows 2000**: Sus miembros tienen acceso de lectura en todos los usuarios y grupos del dominio. Este grupo se proporciona para garantizar la compatibilidad con versiones anteriores en los equipos con Windows NT 4.0 y anteriores. De forma predeterminada, la identidad especial Todos es miembro de este grupo.

- **Operadores de servidores**: En los controladores de dominio, los miembros de este grupo pueden iniciar sesiones interactivas, crear y eliminar recursos compartidos, iniciar y detener varios servicios, hacer copias de seguridad y restaurar archivos, formatear el disco duro y apagar el equipo. Este grupo no tiene ningún miembro predeterminado. Dado que este grupo tiene mucha importancia para los controladores de dominio, agrega los usuarios con precaución.

- **Administradores:** Los miembros de este grupo controlan por completo todos los controladores del dominio. De forma predeterminada, los grupos Administradores del dominio y Administradores de organización son miembros del grupo Administradores. La cuenta Administrador es miembro de este grupo de forma predeterminada.

- **Operadores de copia de seguridad**: Sus miembros pueden realizar copias de seguridad y restaurar todos los archivos en los controladores del dominio, independientemente de sus permisos individuales en esos archivos. Los Operadores de copia de seguridad también pueden iniciar la sesión en los controladores de dominio y apagarlos. Este grupo no tiene ningún miembro predeterminado.
- **Invitados**: De forma predeterminada, el grupo Invitados del dominio es un miembro de este grupo. La cuenta Invitado (que está deshabilitada de forma predeterminada) también es un miembro predeterminado de este grupo.

- **Operadores de configuración de red**: Sus miembros pueden modificar la configuración TCP/IP, así como renovar y liberar las direcciones TCP/IP en los controladores del dominio. Este grupo no tiene ningún miembro predeterminado.

- **Usuarios del monitor de sistema**: Sus miembros pueden supervisar los contadores de rendimiento en los controladores del dominio, tanto de forma local como desde clientes remotos, sin ser miembros de los grupos Administradores o Usuarios del registro de rendimiento.

- **Usuarios del registro del rendimiento**: Sus miembros pueden administrar los contadores de rendimiento, los registros y las alertas de los controladores del dominio, tanto de forma local como desde clientes remotos, sin ser miembros del grupo Administradores.

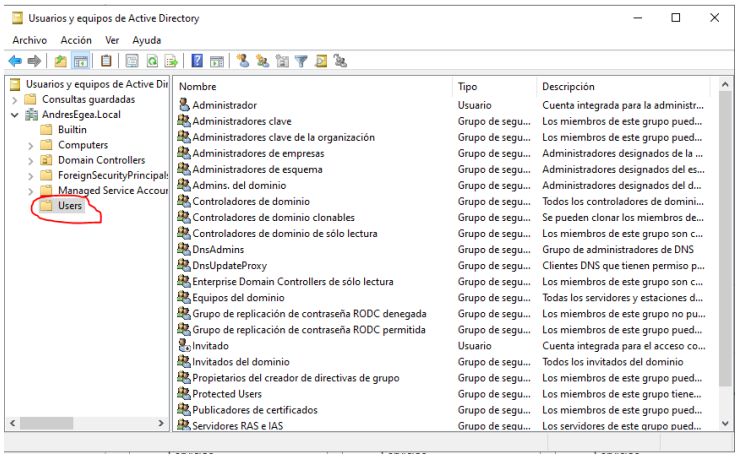
- **Operadores de impresión**: Los miembros de este grupo pueden administrar, crear, compartir y eliminar impresoras que están conectadas a los controladores del dominio. También pueden administrar objetos de impresora de Active Directory en el dominio. Los miembros de este grupo pueden iniciar la sesión de forma local en los controladores del dominio y apagarlos. Este grupo no tiene ningún miembro predeterminado. Puesto que los miembros de este grupo pueden cargar y descargar controladores de dispositivos en todos los controladores del dominio, agregale usuarios con precaución.

- **Usuarios de escritorio remoto**: Los miembros de este grupo pueden iniciar la sesión en los controladores del dominio de forma remota. Este grupo no tiene ningún miembro predeterminado.

- **Replicador**: Este grupo admite funciones de replicación de directorio y el Servicio de replicación de archivos lo utiliza en los controladores del dominio. Este grupo no tiene ningún miembro predeterminado. No agregues usuarios a este grupo.

- **Usuarios**: Los miembros de este grupo pueden realizar las tareas más habituales, como ejecutar aplicaciones, utilizar impresoras locales y de red, así como bloquear el servidor. De forma predeterminada, el grupo Usuarios del dominio, Usuarios autenticados e Interactivo son miembros de este grupo. Por tanto, todas las cuentas de usuario que se crean en el dominio son miembros de este grupo.

2.- En el contenedor *Users* podemos encontrar grupos predeterminados que tienen tanto ámbito local como global.



También en este caso tienes una tabla con un resumen de sus grupos:

- **Publicadores de certificados**: Los miembros de este grupo tienen permitida la publicación de certificados para usuarios y equipos. Este grupo no tiene ningún miembro predeterminado.

- **DnsAdmins (instalado con DNS):** Los miembros de este grupo tienen acceso administrativo al Servidor DNS. Este grupo no tiene ningún miembro predeterminado.

- **DnsUpdateProxy (instalado con DNS):** Los miembros de este grupo son clientes DNS que pueden realizar actualizaciones dinámicas en lugar de otros clientes, como los servidores DHCP. Este grupo no tiene ningún miembro predeterminado.

- **Administradores de dominio**: Los miembros de este grupo controlan el dominio por completo. De forma predeterminada, este grupo pasa a ser

miembro del grupo Administradores en todos los controladores, estaciones de trabajo y servidores miembro del dominio en el momento en que se une al dominio. De forma predeterminada, la cuenta Administrador es miembro de este grupo. Puesto que el grupo controla el dominio por completo, agrega usuarios con precaución.

- **Equipos del dominio**: Este grupo contiene todas las estaciones de trabajo y los servidores unidos al dominio. De forma predeterminada, todas las cuentas de equipo creadas pasan a ser miembros de este grupo automáticamente.

- **Controladores de dominio**: Este grupo contiene todos los controladores del dominio.

- **Invitados del dominio**: Este grupo contiene todos los invitados del dominio.

- **Usuarios del dominio**: Este grupo contiene todos los usuarios del dominio. De forma predeterminada, todas las cuentas de usuario creadas en el dominio pasan a ser miembros de este grupo automáticamente. Este grupo se puede utilizar para representar todos los usuarios del dominio. Por ejemplo, si desea que todos los usuarios del dominio tengan acceso a una impresora, puede asignar permisos para la impresora a este grupo (o puede agregar el grupo Usuarios del dominio en un grupo local del servidor de impresoras que disponga de los permisos para utilizarla).

- **Administradores de organización (sólo aparece en el dominio raíz del bosque)**: Los miembros de este grupo controlan por completo todos los dominios del bosque. De forma predeterminada, este grupo es un miembro del grupo Administradores en todos los controladores de dominio del bosque. De forma predeterminada, la cuenta Administrador es miembro de este grupo.

- **Propietarios del creador de directiva de grupo:** Los miembros de este grupo pueden modificar la Directiva de grupo en el dominio. De forma predeterminada, la cuenta Administrador es miembro de este grupo. Como este grupo tiene una autoridad considerable en el dominio, sea prudente al agregar usuarios.

- **IIS_WPG (instalado con IIS)**: El grupo IIS_WPG es el grupo de procesos de trabajo de los Servicios de Internet Information Server (IIS) 6.0. El funcionamiento de IIS 6.0 incluye procesos de trabajo para espacios de nombres específicos. Este grupo no tiene ningún miembro predeterminado.

- **Servidores RAS e IAS**: Los servidores de este grupo tienen permitido el acceso a las propiedades de acceso remoto de los usuarios.

- **Administradores de esquema (sólo aparece en el dominio raíz del bosque)**: Los miembros de este grupo pueden modificar el esquema de Active Directory. De forma predeterminada, la cuenta Administrador es miembro de este grupo.

Tanto los grupos del contenedor *Builtin* como los del contenedor *Users* pueden cambiarse libremente de contenedor, siempre que se mantengan dentro del mismo dominio. Los grupos ubicados en estos contenedores se pueden mover a otros grupos o unidades organizativas (OU) del dominio, pero no se pueden mover a otros dominios.

Debemos conocer los privilegios y derechos que ofrece cada grupo predeterminado a sus miembros antes de asignarle una cuenta de usuario o equipo. Lógicamente, la precaución será mayor cuanto más elevadas sean las capacidades del grupo en cuestión.

6.3.3. Administrar cuenta de usuario

Una vez que hemos explicado qué son y para qué sirven las cuentas de usuario de un *Dominio*, el siguiente paso será aprender a crearlas.

En este apartado y en los siguientes, veremos cómo acceder a la herramienta *Usuarios y equipos de Active Directory* desde el menú *Herramientas* del *Administrador del Servidor*.

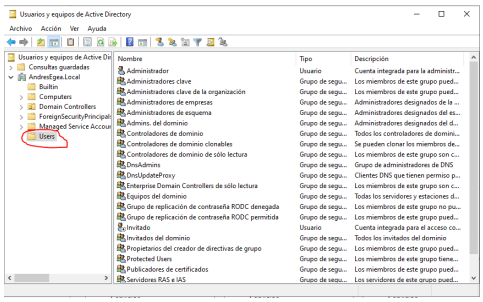
Una vez que nos encontremos en la herramienta *Usuarios y equipos de Active Directory*, es muy sencillo crear una nueva cuenta.

También podemos abrir *Usuarios y equipos de Active Directory* haciendo clic, con el botón derecho del ratón, sobre el botón *Inicio* y eligiendo *Ejecutar*. Después, en la ventana *Ejecutar* escribimos la orden `dsa.msc`.

Vemos que se abre la ventana *Usuarios y equipos de Active Directory*. En ella disponemos de un panel a la izquierda donde podemos ver nuestro dominio (*AndresEgea.local*) y, dentro, los diferentes contenedores de los que disponemos. Entre ellos, se encuentran *Builtin* y *Users*, los contenedores que describimos antes.

Si tuviésemos acceso a más de un dominio, los demás también aparecerían en el panel izquierdo. Ya veremos esto en temas posteriores.

1.- De momento, la cuenta que crearemos se ubicará dentro del contenedor *Users*.

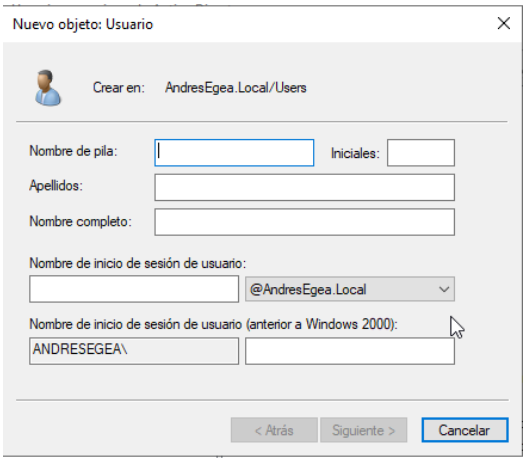


Sólo tenemos que hacer clic con el botón derecho del ratón sobre Users.

2.- En el menú de contexto que aparece, elegimos *Nuevo* y, a continuación, *Usuario*.

3.- Veremos que aparece la ventana *Nuevo objeto – Usuario*, que es el asistente de creación de usuarios.

En el primer paso, tendremos que rellenar los datos del usuario:
Su *Nombre*, *Apellidos* e *Iniciales*. Con ellos se formará el campo *Nombre completo* (aunque, si no te gusta el resultado, puedes editarlo).



A continuación, escribiremos el *Nombre de inicio de sesión de usuario* que, en realidad, se compone de dos partes: el nombre propiamente dicho y el sufijo, que lo elegimos de una lista desplegable. Si disponemos de varios dominios en la red, en la lista aparecerá una entrada por cada uno de ellos.

Por último, el campo *Nombre de inicio de sesión de usuario (anterior a Windows 2000)* tiene como objeto permitir que se conecten al dominio clientes que ejecuten Windows 95, Windows 98 o Windows NT.

4.- Cuando hayamos concluido, haremos clic sobre *Siguiente*.

A continuación, tendremos que escribir una contraseña para el usuario, que deberá cumplir con los requerimientos de seguridad del sistema operativo. Es decir, que deberá tener, de forma predeterminada, un mínimo de seis caracteres de larga y contener caracteres de, al menos, tres de los cuatro conjuntos siguientes:

- Mayúsculas del alfabeto inglés.
- Minúsculas del alfabeto inglés.
- Dígitos decimales (del 0 al 9).
- Caracteres no alfanuméricos.

Además, en la parte inferior de la ventana disponemos de cuatro opciones:

- **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**: Si

lo marcamos (opción por defecto), obligaremos al usuario a cambiar la contraseña que estamos escribiendo la próxima vez que inicie sesión en el dominio. De esta forma, el usuario estará seguro de que nadie más conoce su contraseña.

- **El usuario no puede cambiar la contraseña**: Al contrario que la anterior, esta opción impide que el usuario pueda cambiar su contraseña en ningún momento. Esta opción puede resultar interesante para que el administrador mantenga el control total sobre alguna cuenta temporal o de invitado.
- **La contraseña nunca expira:** hace que la contraseña no expire en el plazo que establezca el sistema operativo. *Microsoft* recomienda que las cuentas de servicio tengan esta opción habilitada y usen contraseñas seguras
- **La cuenta está deshabilitada:** Mientras esta opción esté habilitada, el usuario no podrá iniciar sesión en el sistema.

5.- Cuando hayamos completado los datos necesarios en este paso, haremos clic sobre el botón *Siguiente*.

Como es habitual en todas las herramientas de configuración de *Windows Server 2022*, el asistente nos muestra un resumen de los datos introducidos antes de crear la cuenta de manera efectiva.

6.- Si todo es correcto, haremos clic sobre el botón *Finalizar*. De lo contrario, utilizaremos el botón *Atrás*.

En estos momentos, si la contraseña que hemos elegido no cumpliera las condiciones de complejidad predeterminadas que hemos comentado más arriba, aparecería un mensaje de aviso y tendríamos que volver atrás para resolver el problema.

No obstante, si todo es correcto, la ventana *Nuevo objeto – Usuario* se cerrará y volveremos a ver la ventana *Usuarios y equipos de Active Directory*.

7.- Ahora ya podremos encontrar entre los usuarios la cuenta que acabamos de crear.

Recuerda que, cuando creamos una cuenta de usuario nueva, se le asigna un Identificador de Seguridad (SID) que es único en el sistema. De esta forma, aunque eliminemos una cuenta y volvamos a crear otra con el mismo nombre, ésta será diferente, porque su SID también lo es, lo que significa que no coincidirán ni sus certificados de seguridad, ni sus permisos ni su pertenencia a determinados grupos.

Modificar valores de las cuentas de usuario

Una vez que hemos creado una cuenta de usuario, podemos volver a la herramienta *Usuarios y equipos de Active Directory*, en cualquier momento, para ajustar sus propiedades. Como antes, usaremos el menú *Herramientas* del *Administrador del Servidor*.

En su interior, haremos clic sobre *Usuarios y equipos de Active Directory* .

Una vez abierta la ventana, podemos aplicar, por ejemplo, las siguientes modificaciones:

- Modificar valores generales de las cuentas.
- Establecer horas de inicio de sesión.
- Limitar los equipos desde los que un usuario puede iniciar sesión.
- Averiguar de qué grupos es miembro un usuario.

Otras operaciones frecuentes con cuentas de usuario

En el apartado anterior, hemos visto algunas de las operaciones fundamentales para modificar la configuración de las cuentas que hayamos creado con anterioridad. Sin embargo, existen algunas más que nos pueden resultar de gran utilidad en algunos momentos. En particular, me refiero a operaciones como …

- Recuperar contraseñas
- Deshabilitar una cuenta de usuario
- Hacer que un usuario sea miembro de un grupo
- Copiar cuentas de usuario
- Eliminar una cuenta de usuario

6.3.4 Administrar cuentas de equipo

Muchas de las operaciones que podemos hacer sobre las cuentas de equipo son idénticas a las que hemos visto más arriba con las cuentas de usuario. Por este motivo, en este apartado nos centraremos en algunas de las operaciones fundamentales:

- Crear una cuenta de equipo
- Modificar valores en las cuentas de los equipos

CREAR UNA CUENTA DE EQUIPO

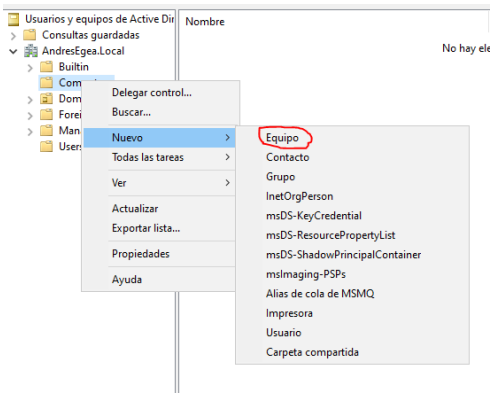
Para crear una cuenta de equipo, debemos volver a la herramienta *Usuarios y equipos de Active Directory*, desde el menú *Herramientas* del *Administrador del Servidor*.

Como hicimos con las cuentas de usuario, cuando se abra la ventana *Usuarios y equipos de Active Directory*, buscaremos en el panel de la izquierda el contenedor que nos interese. En este caso, utilizaremos el contenedor *Computers*.

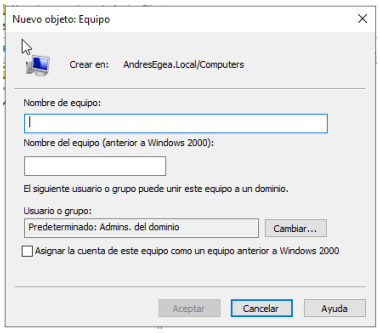
Suele ser una buena idea mantener a las cuentas de equipo en una Unidad Organizativa separada de las cuentas de usuario. Así, simplificaremos la aplicación de *Políticas de grupo* cuando sea preciso.

Después haremos clic con el botón derecho del ratón sobre el contenedor.

1.- En el menú de contexto que aparece, elegiremos *Nuevo > Equipo*



Veremos que aparece la ventana *Nuevo objeto: Equipo*



En ella, rellenaremos el nombre que queremos que tenga la cuenta de equipo que estamos creando (*Nombre de equipo*).

Además, de forma automática, se irá completando el campo *Nombre del equipo (anterior a Windows 2000)* con los primeros 15 caracteres que escribamos en el campo de arriba. Además, las minúsculas se convertirán en mayúsculas.

También podremos elegir el usuario o grupo que podrá unir a este equipo al dominio, aunque, de forma predeterminada sólo lo podrán hacer los administradores.

Si el cliente que utilizará esta cuenta de equipo ejecuta *Windows 95*, *Windows 98* o *Windows NT*, deberemos marcar la opción *Asignar la cuenta de este equipo como un equipo anterior a Windows 2000*.

3.- Cuando hayamos concluido, haremos clic sobre el botón *Aceptar*.

La ventana *Nuevo objeto: Equipo* se cerrará y volveremos a ver la ventana *Usuarios y equipos de Active Directory*.

4.- Ahora ya podremos encontrar la nueva cuenta entre los objetos del contenedor Computers.

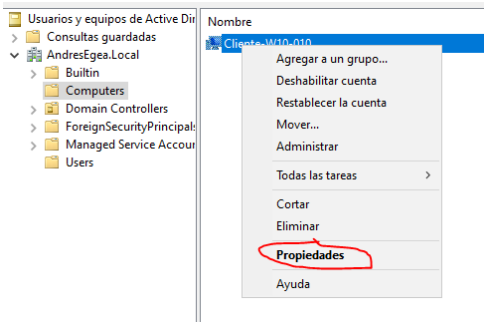
MODIFICAR VALORES EN LAS CUENTAS DE LOS EQUIPOS

Igual que ocurría con las cuentas de usuario, podemos volver a la herramienta *Usuarios y equipos de Active Directory* en cualquier momento para ajustar las propiedades de las cuentas de equipos.

Como antes, usaremos el menú *Herramientas* del *Administrador del Servidor* y, después, *Usuarios y equipos de Active Directory* .

Una vez abierta la ventana, hacemos clic con el botón derecho del ratón sobre el equipo que queremos modificar.

1.- En el menú de contexto que aparece elegimos Propiedades.



Aparece la ventana titulada *Propiedades:*, seguido del nombre de la cuenta elegida. Aquí disponemos de multitud de características diferentes de la cuenta, organizadas en 7 solapas distintas. No obstante, en este capítulo no profundizaremos más en ellas.

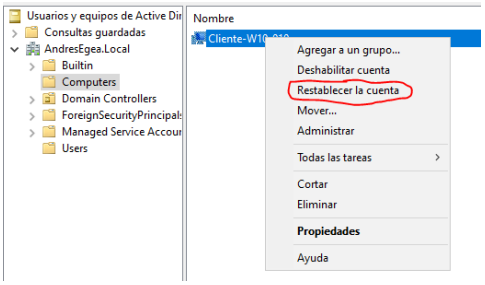
2.- Nos limitamos a cerrar la ventana.

RESTABLECER CUENTAS DE EQUIPO

En ocasiones, tratamos de iniciar sesión en el dominio desde un equipo cliente y recibimos un error de conexión aún después de asegurarnos de que los datos que hemos introducido son correctos.

Esto puede ocurrir porque se ha desincronizado la contraseña que introducimos con la almacenada en la *Autoridad de Seguridad Local* (*LSA*, *Local Security Authority*). Para resolverlo, volveremos a abrir la herramienta *Usuarios y equipos de Active Directory*, buscaremos la cuenta de equipo que está ocasionando los problemas y haremos clic sobre ella con el botón derecho del ratón.

1.- En el menú de contexto que aparece, hacemos clic sobre Restablecer la cuenta.



Aparecerá un cuadro de diálogo que nos pregunta si estamos seguros de reiniciar la cuenta.

2.- Sólo queda hacer clic en el botón *Sí*.

Cuando concluya la operación, aparecerá un nuevo mensaje indicando que la cuenta se ha restablecido correctamente.

3.- Hacemos clic en *Aceptar*.

6.3.5. Administrar cuentas de grupo

Ya hemos comentado al principio del capítulo que los grupos nos permiten administrar objetos del dominio de forma conjunta. Un grupo puede estar formado por cuentas de usuario, de equipo, contactos o, incluso, otros grupos.

Las acciones más frecuentes que podemos llevar a cabo con cuentas de grupo son:

- Crearlas.
- Modificar sus valores.
- Añadir miembros a un grupo.
- Eliminar miembros de un grupo.
- Convertir a un grupo en miembro de otro grupo.
- Conseguir que un grupo deje de ser miembro de otro.
- Eliminar grupos.

CREAR UNA CUENTA DE GRUPO

Si lo que queremos es crear un nuevo grupo, deberemos volver a la herramienta *Usuarios y equipos de Active Directory*.

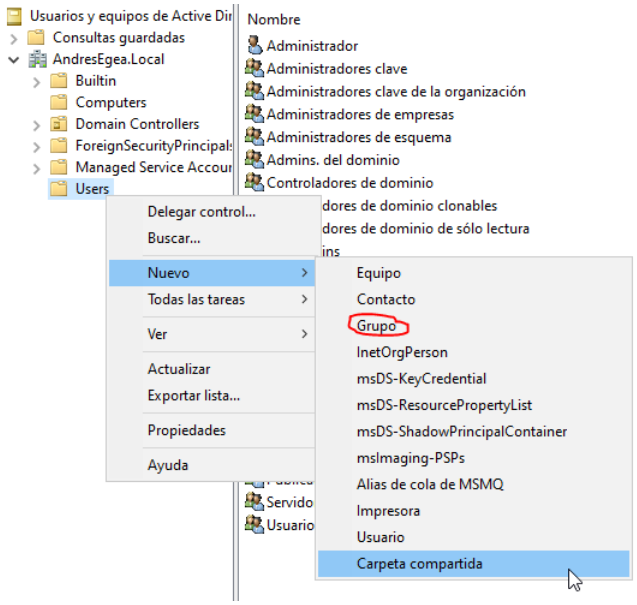
Recuerda que hemos aprendido a llegar hasta ella de tres modos diferentes:

- Desde el menú *Herramientas* del *Administrador del Servidor*.
- Ejecutando la orden **`dsa.msc`** desde la ventana *Ejecutar* (que puedes abrir fácilmente usando la combinación de teclas `Windows` + `R`).

Como en ocasiones anteriores, cuando se abra la ventana *Usuarios y equipos de Active Directory*, buscaremos en el panel de la izquierda el contenedor en el que queramos guardar el nuevo grupo. En este caso, volveremos a usar el contenedor *Users*, que ya utilizamos para las cuentas de usuario

Después haremos clic con el botón derecho del ratón sobre el contenedor.

1.- En el menú de contexto que aparece, elegiremos *Nuevo > Grupo*.



2.- Veremos que aparece la ventana *Nuevo objeto: Grupo*.

En ella, rellenaremos el nombre que queremos darle a la cuenta de grupo que estamos creando (*Nombre de grupo*).

Por defecto, el nombre que escribamos se utilizará para completar el campo *Nombre de grupo (anterior a Windows 2000)*, aunque, en este caso no se aplican las restricciones de 15 caracteres y letras mayúsculas.

3.- Cuando hayamos concluido, haremos clic sobre el botón Aceptar.

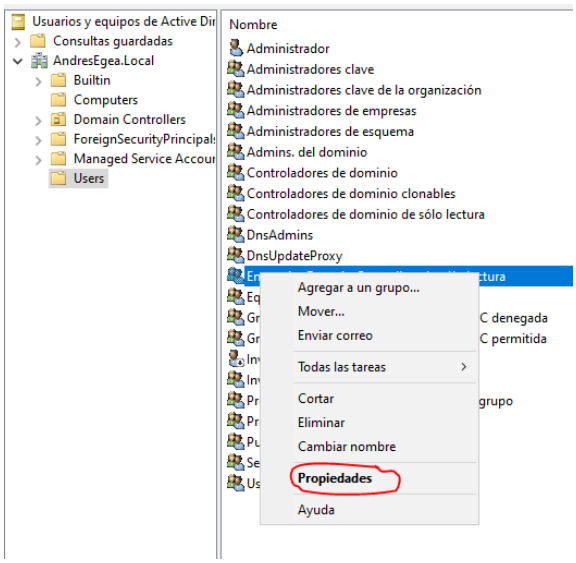
La ventana *Nuevo objeto: Grupo* se cerrará y volveremos a ver la ventana *Usuarios y equipos de Active Directory*.

MODIFICAR VALORES EN LAS CUENTAS DE LOS GRUPOS

Como en ocasiones anteriores, podemos volver a la herramienta *Usuarios y equipos de Active Directory* siempre que necesitemos ajustar las propiedades de las cuentas de grupos.

Cuando se abra la ventana, haremos clic con el botón derecho del ratón sobre el grupo que queremos modificar.

1.- En el menú de contexto que aparece elegimos *Propiedades*.

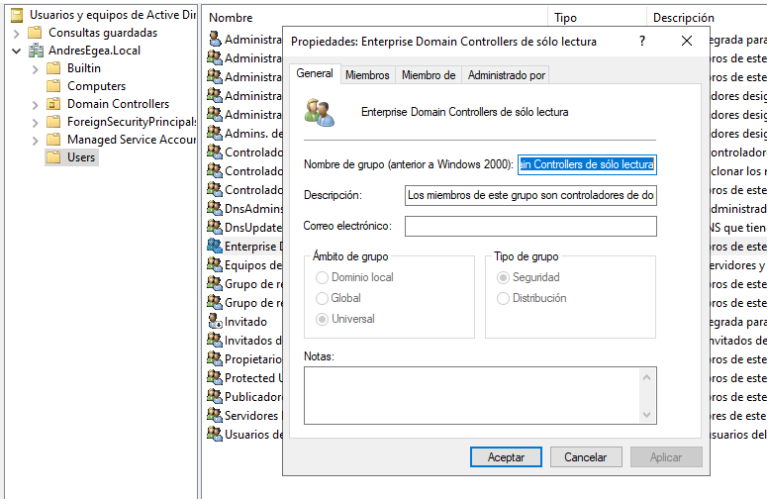


Aparece la ventana titulada *Propiedades:*, seguido del nombre de la cuenta elegida. Aquí disponemos de multitud de características de la cuenta, organizadas en 4 solapas diferentes.

Como puedes ver, en la solapa *General*, además de poder cambiar el *Nombre de grupo (anterior a Windows 2000)*, la *Descripción* y el *Correo electrónico* donde se recibirán incidencias relacionadas con el grupo, también podemos modificar el *Ámbito del grupo* y el *Tipo de grupo*.

Ya hemos visto al principio de este capítulo el significado de los conceptos *Ámbito de grupo* y *Tipo de grupo*.

2.- Después de ajustar los valores a nuestras necesidades, haremos clic sobre *Aceptar* o elegiremos otra solapa para seguir trabajando.



Desde la solapa *Miembros*, elegiremos los usuarios, equipos o grupos que son miembros del grupo que estamos editando. Para verlo en detalle, dedicaremos más adelante un apartado completo a este aspecto.

3.- Como antes, cuando hayamos terminado, podremos elegir una solapa diferente o hacer clic en Aceptar para cerrar la ventana.

Utilizaremos la solapa *Miembro de*, para hacer que este grupo sea, a su vez, miembro de un grupo distinto. Como en el caso anterior, estudiaremos este aspecto con más detalle en un apartado más adelante.

4.- De nuevo, si hemos terminado, haremos clic en el botón Aceptar. De lo contrario, elegiremos la siguiente solapa.

La solapa *Administrado por*, nos permite delegar la administración de este grupo en otro usuario diferente.

5.- Cuando terminemos, haremos clic en el botón *Aceptar*.

6.3.6. Administrar Unidades Organizativas

Como recordarás, las *Unidades Organizativa*s (en inglés, *Organizational Units* o, simplemente, *OUs*) son contenedores del *Directorio Activo* que pueden incluir *usuarios*, *equipos*, *grupos* y otras *unidades organizativas*.

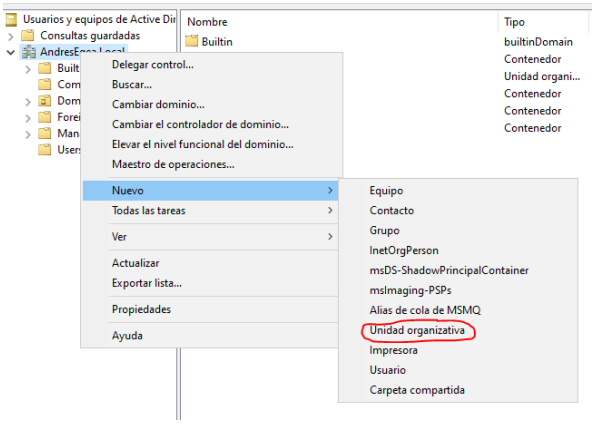
A una *Unidad Organizativa* le podemos otorgar valores de configuración de directiva de grupo o podemos delegar sobre ella una parte de la autoridad administrativa. De esta forma, un usuario puede tener autoridad para administrar una determinada unidad organizativa y no tenerla para el resto.

En definitiva, esto significa que podemos definir contenedores que representen la organización lógica de nuestra red.

CREAR UNA NUEVA UNIDAD ORGANIZATIVA

Lo primero es aprender a crear una *Unidad Organizativa*, aunque, a estas alturas del capítulo, no creo que esta operación suponga una dificultad.

Como de costumbre, comenzamos por abrir la herramienta Usuarios y equipos de Active Directory.



A continuación, ponemos el puntero del ratón sobre el nombre del dominio y hacemos clic con el botón derecho.

1.- En el menú de contexto que aparece, elegimos *Nuevo* y a continuación, *Unidad organizativa*.

Si lo que queremos es crear la *Unidad Organizativa* dentro de otra que ya existe, en lugar de hacer clic con el botón derecho del ratón sobre el nombre del dominio, lo haremos sobre dicha *Unidad Organizativa*.

A continuación, escribimos el nombre que queramos, en este ejemplo, *Usuarios y grupos predeterminados*. También podemos dejar marcada la opción *Proteger contenedor contra eliminación accidental*. De esta forma, el sistema impedirá que eliminemos la *Unidad Organizativa* por error.

2.- Finalmente, hacemos clic en Aceptar.

Al hacerlo, volvemos a la ventana *Usuarios y equipos de Active Directory*…

3.- Y veremos que ya aparece creada la *Unidad Organizativa*.

De paso, hemos repetido el proceso para crear otra más unidad organizativa más, llamada *Usuarios y grupos propios*, que usaremos en el siguiente apartado.

DESPLAZAR OBJETOS DE UNA UBICACIÓN A OTRA

En ocasiones, para conseguir que nuestro dominio refleje la estructura organizativa que hemos diseñado, necesitamos cambiar la ubicación de algunos de los objetos. Por ejemplo, en el apartado anterior hemos creado dos *Unidades Organizativas* nuevas. En una de ellas ubicaremos a todos los usuarios y grupos que vienen de forma predeterminada en el sistema y en la otra los que creemos nosotros.

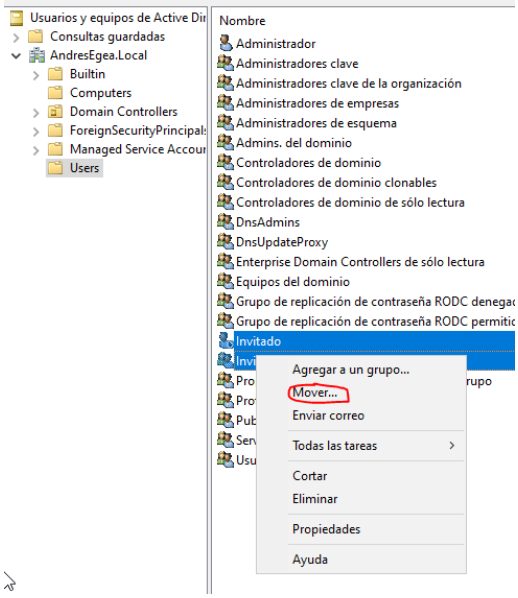
Puedes utilizar las teclas Mayúsculas (*Shift*) y Control (*Ctrl*) combinadas con el clic del ratón para realizar selecciones múltiples.

Por supuesto, esto no es más que un ejemplo. Lo importante es comprender que podemos utilizar esta técnica para establecer la organización lógica que más nos convenga.

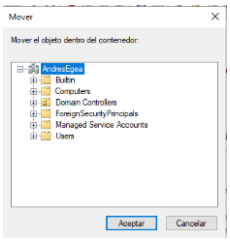
El objetivo de este apartado es trasladar los usuarios y grupos que hemos ido creando en los últimos artículos dentro de la *Unidad Organizativa Usuarios y grupos propios*, que tenemos del apartado anterior.

Como en ocasiones anteriores, comenzamos por abrir la herramienta *Usuarios y equipos de Active Directory*. A partir de aquí, seleccionaremos los diferentes elementos que vamos a desplazar y haremos clic con el botón derecho del ratón sobre cualquiera de ellos.

1.- En el menú de contexto que aparece, elegimos la opción Mover…



Aparecerá la ventana *Mover*, que contiene todos los posibles lugares a los que podemos trasladar los objetos seleccionados. Recuerda que en *Windows Server 2012 R2*, podemos tener unas *Unidades Organizativas* dentro de otras. Para encontrarlas, puede ser necesario desplegar la rama correspondiente usando el botón '+' que hay junto a algunos de los contenedores.



2.- Cuando encontremos el contenedor de destino, sólo tenemos que hacer clic sobre él y, a continuación, sobre el botón Aceptar.

Por último, en la ventana *Usuarios y equipos de Active Directory*, podemos hacer clic sobre la *Unidad Organizativa Usuarios y grupos propios*.

3… y comprobamos que ahora contiene los objetos desplazados.

ELIMINAR UNA UNIDAD ORGANIZATIVA

Ponemos el puntero del ratón sobre el nombre de la Unidad Organizativa que queremos eliminar y hacemos clic con el botón derecho del ratón.

1.- En el menú de contexto que aparece, elegimos *Eliminar*.

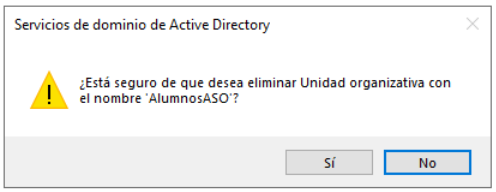
Aparecerá un cuadro de diálogo donde debemos confirmar la eliminación.

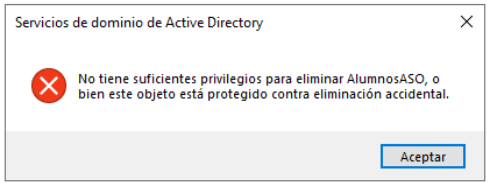
2.-Para seguir, hacemos clic sobre el botón Sí.

Si todo va bien, la *Unidad organizativa* desaparecerá del árbol del panel izquierdo.

Sin embargo, también puede que tengamos un ligero contratiempo si, al crearla, elegimos la opción *Proteger contenedor contra eliminación accidental*. En ese caso, aparecerá un aviso como el de la ventana siguiente.

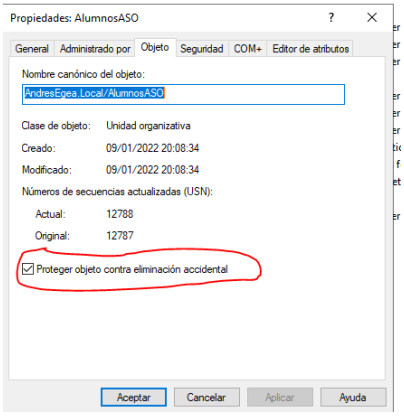
3.- Hacemos clic en el botón Aceptar para cerrar la ventana.





En estos casos, deberemos habilitar las características avanzadas de *Usuarios y equipos de Active Directory*, lo que nos permitirá tener un mayor control sobre todos los objetos que administramos con esta herramienta.

4.- Hacemos clic sobre el menú *Ver* y, a continuación, sobre la opción *Características avanzadas*.



Después de esto, hacemos clic son el botón derecho del ratón sobre el nombre de la Unidad Organizativa.

5.- En el menú de contexto que aparece, elegimos *Propiedades*.

Se abrirá una ventana titulada *Propiedades:*, seguido del nombre de la *Unidad Organizativa*. En ella, haremos clic sobre la solapa *Objeto* y quitaremos la selección de la opción *Proteger objeto contra eliminación accidental*.

6.- A continuación, haremos clic sobre el botón *Aceptar*.

A continuación, repetiremos los pasos 1 y 2 para eliminar la Unidad Organizativa. No debemos olvidar deshabilitar las *Características avanzadas* después de terminar.

7.-Al terminar, la *Unidad Organizativa* habrá desaparecido.

No debemos olvidar deshabilitar las *Características avanzadas* después de terminar.

Una última situación en la que podemos encontrarnos es que la *Unidad Organizativa* que pretendemos eliminar no esté vacía. En estos casos, aparecerá una ventana de aviso como la que ves en la imagen siguiente. En ella, podremos hacer clic sobre el botón *No* para anular la eliminación de la *Unidad Organizativa* o podremos hacer clic en *Sí* y eliminar todos los objetos que contenga.

Si la Unidad Organizativa contiene a su vez otras Unidades Organizativas, tendremos que elegir *Usar el control de servidor Eliminar subárbol* para conseguir eliminarlo todo.

8.- Confirmamos, o no, la eliminación de la Unidad Organizativa.

6.4.- Administración de directivas de grupo.

En cualquier sistema Windows existen unas directivas de grupo que el administrador puede editar según su criterio para personalizar el comportamiento del equipo. Para facilitar la administración del sistema, las políticas de grupo se han integrado dentro de la administración del Directorio Activo como una utilidad de configuración centralizada en dominios Windows Server.

A continuación primero se van a ver las características más importantes de las directivas de seguridad y posteriormente aprenderá a administrar las directivas locales del sistema y las directivas de grupo del directorio activo.

Def. Directivas de grupo. Permiten establecer la configuración del sistema en un equipo o para un determinado usuario.

6.4.1. Directivas de seguridad

Las directivas de grupo se definen mediante objetos del Directorio Activo denominados Objetos de directiva de grupo (Group Policy Objects – GPO) . Un GPO es un objeto que contiene una o varias directivas de grupo que se aplican a la configuración de uno o más usuarios o equipos. Por ejemplo, puede crear un GPO que configure el fondo de escritorio y conecte una unidad de red a un recurso compartido. Un GPO es un objeto que puede aplicarse tanto a usuarios y equipos Windows (desde Windows XP a Windows 2008R2).

Tipos

Para crear una configuración específica para un grupo de usuarios o equipos es necesario configurar una GPO. Existen dos tipos de GPO dependiendo de su ámbito:

Los tipos de directivas son:

- **GPO locales.** Se utilizan principalmente para los equipos que no forman parte de un directorio activo y como su nombre indica, la GPO se aplica únicamente al equipo local.

- **GPO no locales.** Las GPO no locales se crean en el Directorio Activo y se vinculan a un sitio, dominio, unidad organizativa (UO), usuarios o equipos. De esta forma es posible establecer directivas que afecten a toda la empresa, a un departamento, grupo de usuarios, etc.

De forma predeterminada, al configurar el servicio de Directorio activo crean dos GPO no locales:

- Directiva predeterminada de dominio. Se vincula al dominio y afecta a todos los usuarios y equipos del dominio.
- Directiva predeterminada de controladores de dominio. Esta directiva se vincula únicamente a los controladores del dominio.

Puesto que es posible que se produzcan conflictos en una misma política que se encuentra definida en distintos GPO, es necesario que exista un orden de aplicación concreto y conocido de forma que conozca que política afecta a cada usuario o equipo sin ambigüedades. El orden de aplicación de las GPO es el siguiente:

- Se aplica la GPO local del equipo
- Se aplica las GPO vinculadas al sitio
- Se aplica las GPOs vinculadas al dominio
- Se aplica las GPO vinculadas a unidades organizativas de primer nivel, posteriormente de segundo nivel …etc.

Configuración

Las directivas de seguridad se clasifican en dos grandes grupos:

- **La configuración del equipo** agrupa todas las políticas o parámetros de configuración que pueden establecerse a nivel de equipo. Las GPO que afectan a un equipo se aplican cada vez que se reinicia el equipo.
- **La configuración de usuario** agrupa todas las políticas o parámetros de configuración que pueden establecerse a nivel de usuario. Las GPO que afectan a un usuario se aplican cada vez que el usuario inicia sesión en cualquier equipo del dominio.

Internamente, cada subcategoría se divide en:

- **Directivas**
  - **Configuración de software.** Permite la instalación automática de software.
  - **Configuraciones de Windows,** incluyendo entre otros aspectos configuración de seguridad y ejecución de scripts.
  - **Plantillas administrativas** que incluyen aquellas políticas basadas en la configuración de los elementos más importantes del equipo (componentes de Windows, impresoras, panel de control, red y sistema).
- **Preferencias**
  - **Configuración de Windows.** Incluye opciones de configuración como la creación de variables de entorno, creación de accesos directos, unidades de red, etc.

- **Configuración del panel de control.** Incluye opciones de configuración como, por ejemplo, la instalación de dispositivos e impresoras, usuarios y grupos locales, opciones de energía, tareas programadas, servicios, etc.

Aplicación

Como ha visto anteriormente, la configuración de las directivas de seguridad se aplican de dos formas diferentes:

- Para la configuración de equipo se aplica al arrancarlo y posteriormente cada 90 a 120 minutos.
- Para la configuración de usuario se aplica al iniciar sesión el usuario y cada 90-120 minutos.

Nota :

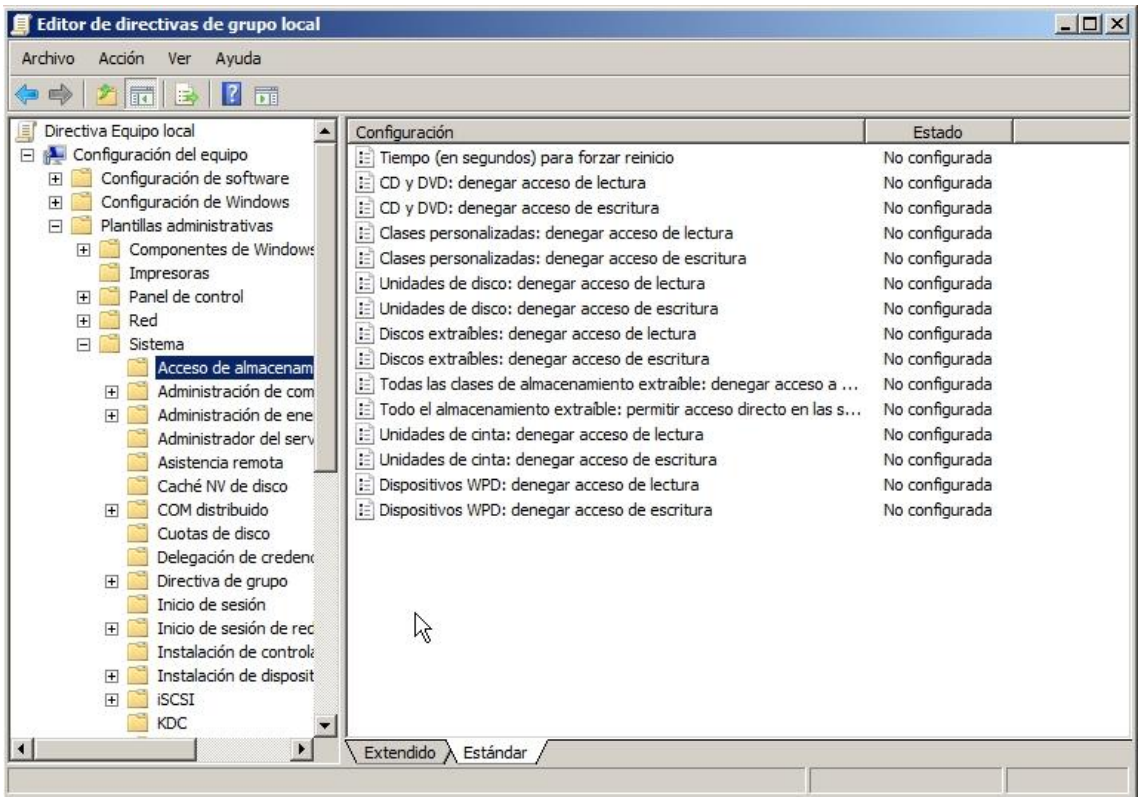
Puede forzar la aplicación o refresco de las directivas de grupo utilizando el comando gpupdate.

6.4.2.- Directivas de grupo local

Las directivas de grupo son conjuntos de opciones de configuración de usuario y equipo que especifican cómo funcionan los programas, los recursos de red, sistema operativo, etc.

Las directivas de grupos se pueden configurar para equipos, sitios, dominios o unidades organizativas. Por ejemplo, mediante las directivas de grupo, puede determinar los programas que se encuentran disponibles para los usuarios, los programas que aparecen en el escritorio, opciones de menú de inicio, configuración del sistema, etc.

Para configurar las directivas de grupo locales hay que ejecutar el comando: gpedit.msc



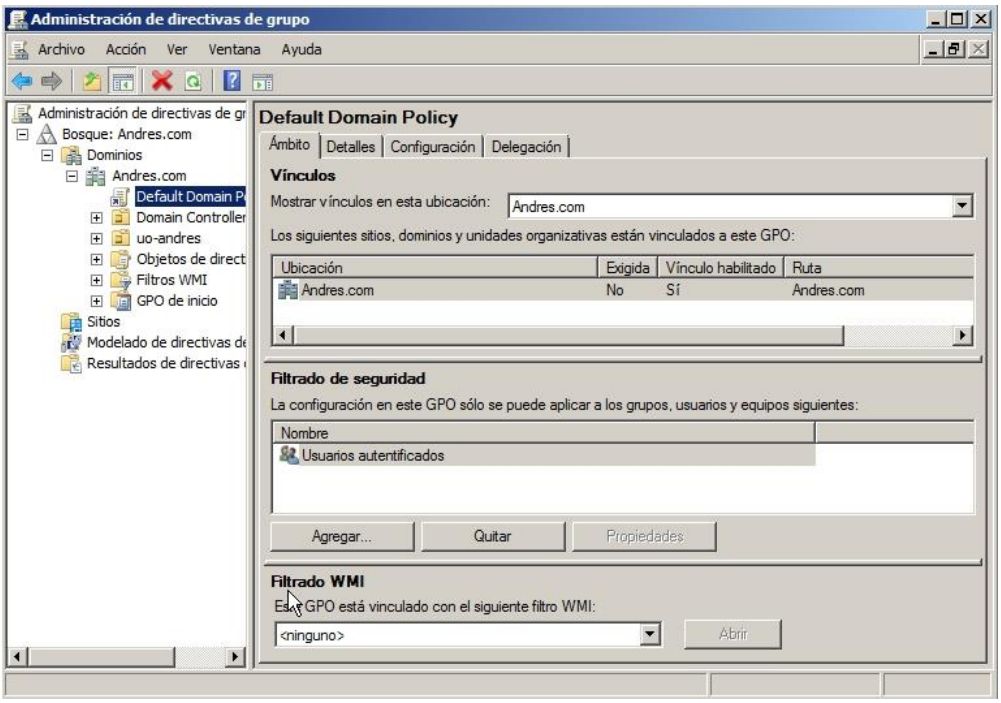
6.4.3.- Administración de directivas de grupo

Para administrar las directivas de grupo de los equipos o usuarios del Directorio Activo ejecute la herramienta administrativa Administración de directivas de grupo.

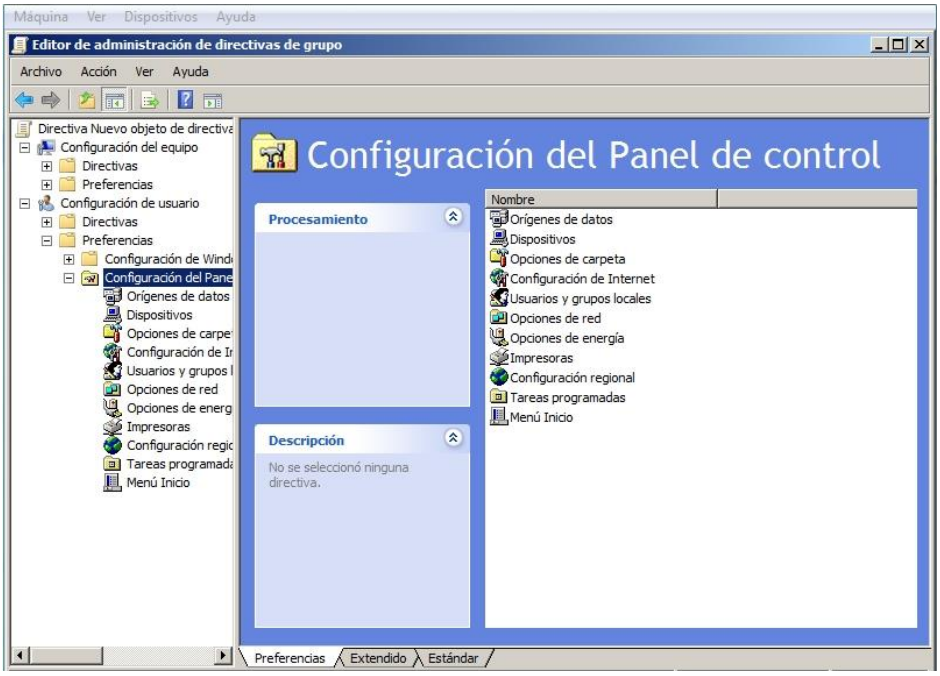
Al ejecutar la herramienta en el menú de la izquierda puede ver que en el dominio tiene la directiva general del dominio (Default Domain Policy) ', la directiva específica para los controladores del dominio ('Default Domain Controllers Policy que se encuentra dentro de la carpeta Domain Controllers) , y las carpetas Clientes y GPO de inicio. Además, en la estructura del dominio puede encontrar o crear las diferentes unidades organizativas que le permiten definir la estructura de la empresa.

Para crear y personalizar la GPO asociada a una unidad organizativa (p.ej., para aplicarla a un grupo de equipos o clientes) debe realizar los siguientes pasos:

- Seleccione la unidad organizativa.
- Pulse el botón derecho y seleccione una de las siguientes opciones:
  - Crear un GPO en este dominio y vincularlo aquí.
  - Vincular un GPO existente.
- Dependiendo de la opción seleccionada indique el nombre de la nueva directiva o seleccione la directiva que desea vincular.
- Automáticamente aparece la GPO creada. Por ejemplo, en la figura 7-11 se muestra la GPO equipos oficina dentro de la unidad organizativa Oficina.



- Una vez que se ha creado o vinculado la directiva de grupo, seleccione la directiva y pulse Editar para personalizar la GPO.
- Ya se ha creado la nueva directiva de grupo. Seleccione la nueva directiva, pulse el botón derecho y seleccione Editar para poder personalizar la GPO



- Nota: Recuerde que se aplican las directivas de grupo al reiniciar el equipo (si es configuración de equipo), al iniciar sesión un determinado usuario (si es configuración de usuario), de forma automática cada 90 minutos o al ejecutar el comando gpudate.