**NF2 - Gestió d'usuaris i Dominis en Sistema operatiu servidor propietari**

# 6.1. 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.

**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.**

**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.

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.

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**.

## 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.

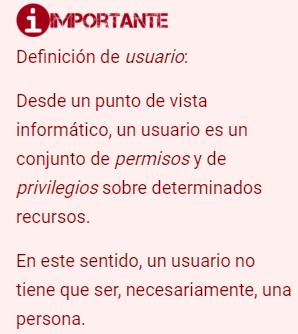
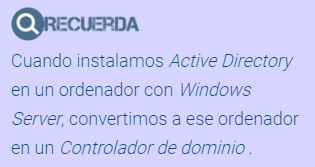
## Objeto

**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.**

En general, los objetos se organizan en tres categorías

* ***Usuarios*:** identificados a través de un nombre (y, casi siempre, una contraseña), que pueden organizarse en grupos, para simplificar la administración.
* ***Recursos*:** que son los diferentes elementos a los que pueden acceder, o no, los usuarios según sus *privilegios*. Por ejemplo, carpetas compartidas, impresoras, etc.
* ***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

**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.

## 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 **administración**.**somebooks.es** e **informatica.somebooks.es** forman parte del mismo árbol, mientras que **sliceoflinux.com** y **somebooks.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

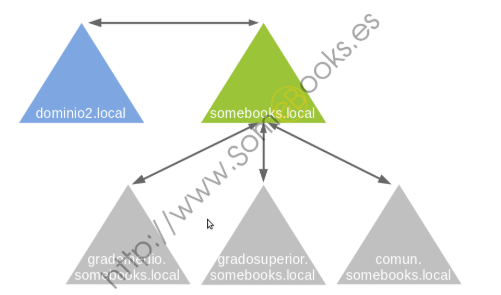
El Bosque es el mayor contenedor lógico dentro de Active Directory, abarcando a todos los dominios dentro de su ámbito.

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.

### **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.

**También suele emplearse una terminología orientada a objetos, donde la palabra Clase se referirá a un determinado tipo de objetos** (con unas propiedades determinadas), **mientras que un objeto determinado recibe el nombre de instancia.** Por ejemplo, podríamos pensar que la clase usuario es una plantilla que definirá a cada uno de los usuarios (que serán instancias de la clase usuario).

# 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).

Como hemos dicho al principio de este capítulo, **cuando disponemos de varios *controladores de dominio* en un mismo dominio, se puede replicar la información contenida en la base de datos a los diferentes *controladores*** a través de la red con el objetivo de **descentralizar diferentes operaciones** (por ejemplo, la autenticación de usuarios) **y agilizar su funcionamiento.**

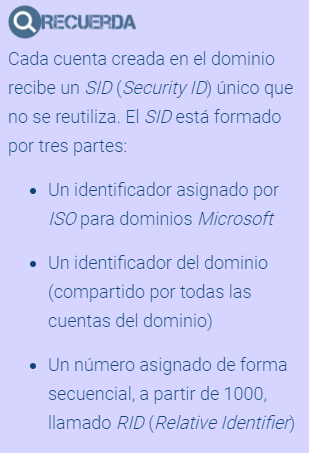
# Maestro de Operaciones

Sin embargo, **existe un conjunto especializado de tareas que deben estar centralizadas en un  *controlador de dominio*  específico** **para evitar inconsistencias**. Este *controlador de dominio* “*especial*” recibe el nombre de *Maestro de Operaciones* o *FSMO* ( de *Flexible Single Master Operations*).

Para entender la situación, vamos a poner un ejemplo:

Supongamos que el *administrador* de un *controlador de dominio* realiza una modificación en el esquema del dominio al mismo tiempo que, un segundo administrador, desde un controlador distinto, realiza una modificación que resulta incompatible con la primera. Como podrás imaginar, cuando se produzca la replicación de la base de datos, estaremos en un aprieto.

Pues bien, para evitar este tipo de situaciones, sólo uno de los controladores del dominio podrá realizar este tipo de cambios.



# 6.3. 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.

* Después convertiremos (promocionaremos) el servidor en un controlador de dominio.

# Instalar el rol Servicios de dominio de Active Directory

Si quieres aprender a instalar paso a paso el rol Servicios de dominio de Active Directory, puedes recurrir a uno de los siguientes artículos, según la versión del sistema operativo con el que estés trabajando:

<http://somebooks.es/instalar-dominio-desde-la-interfaz-grafica-windows-server-2016-parte-1/>

# Promocionar el servidor como controlador de dominio

Una vez que hayas completado la instalación del rol, el siguiente paso consistirá en Promocionar el servidor como controlador de dominio, algo tan sencillo como seguir la explicación paso a paso de uno de los artículos siguientes, según la versión del sistema operativo con el que estés trabajando:

<http://somebooks.es/instalar-dominio-desde-la-interfaz-grafica-windows-server-2016-parte-2/>

# 6.4. Degradar un controlador de dominio desde la interfaz gráfica

Degradar un controlador de dominio es una tarea que no se realiza a menudo. Sin embargo, **en algunas ocasiones, necesitamos que un controlador de dominio deje de actuar como tal. Por ejemplo, cuando pensamos modificar sus características *hardware*, cuando vamos a modificar los servicios que ofrece, o cuando sus funciones van a ser asumidas por un ordenador diferente**.

Pues bien**, igual que sucedió al promocionar un ordenador como controlador de dominio, cuando nos disponemos a degradarlo, también nos enfrentaremos a dos pasos: la degradación propiamente dicha y la desinstalación de los roles implicados.**

Para ver cómo resolverlo en *Windows Server 2016*, puedes recurrir a la explicación, paso a paso, que hicimos en los artículos:

<http://somebooks.es/degradar-controlador-dominio-desde-la-interfaz-grafica-windows-server-2016-parte-1/>

<http://somebooks.es/degradar-controlador-dominio-desde-la-interfaz-grafica-windows-server-2016-parte-2/>

# 6.5. Instalar un dominio básico sin interfaz gráfica

También podemos instalar un controlador de dominio usando la  línea de comandos desde una instalación de Windows sin interfaz gráfico (core)

Para aprender a completar la tarea sólo tienes que seguir alguno de nuestros artículos, en función de la versión del sistema operativo que estés utilizando:

<http://somebooks.es/instalar-dominio-basico-windows-server-2016-sin-interfaz-grafica/>

# 6.6. Degradar un controlador de dominio sin interfaz gráfica

Si lo que tenemos instalado es la versión de Windows Server sin interfaz gráfica y necesitamos degradar un controlador de dominio (o, sencillamente, queremos automatizar la tarea a través de un script), la forma más evidente de hacerlo es recurriendo a PowerShell.

De hecho, ya hemos publicado artículos en [SomeBooks.es](http://somebooks.es/) que te ayudan a solventar esta tarea en función del sistema operativo con el que estés trabajando. Son estos:

<http://somebooks.es/degradar-controlador-dominio-windows-server-2016-desde-la-linea-comandos/>

# 6.7. Herramientas relacionadas con la administración del Directorio Activo

En Windows Server, **existen diferentes herramientas relacionadas con la administración del Directorio Activo.** En este apartado vamos a referirnos las que, probablemente, nos resultarán más útiles.

Todas ellas se encuentran en el menú Herramientas del Administrador del Servidor y son las siguientes:

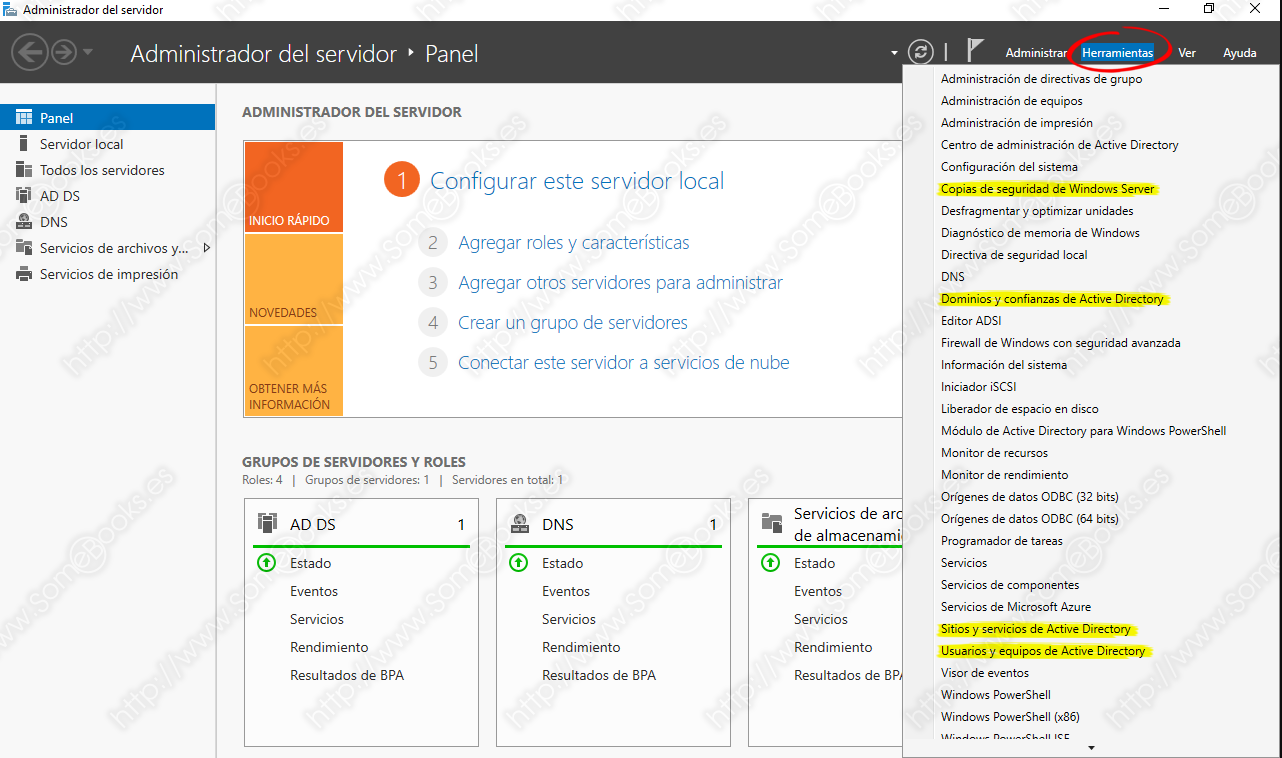
* **Usuarios y equipos de Active Directory.** Con esta herramienta, definiremos el modo en el que se utilizará nuestra infraestructura de red. Como su nombre indica, la utilizaremos para crear y administrar las cuentas de usuario que podrán utilizar los recursos del Directorio y las cuentas para los ordenadores desde los que dichos usuarios podrán establecer su conexión, pero, además, también nos facilitará su organización en grupos y alguna otra característica que estudiaremos más adelante.

**Sitios y servicios de Active directory.** Con esta herramienta podremos diseñar la topología de nuestro Directorio Activo, creando y administrando los sitios que forman la estructura geográfica de la red y estableciendo vínculos entre ellos.

* **Dominios y confianzas de Active Directory.** Esta herramienta nos permitirá aumentar el nivel de funcionalidad del dominio para añadir nuevas características al Directorio Activo o, incluso, establecer relaciones de confianza entre dominios.
* Copias de seguridad de Windows. El establecimiento de una política de copias de seguridad, es una de las operaciones que todo administrador debe tener siempre presente.

Le permitirán dormir tranquilo frente a las posibles situaciones de emergencia que amenacen la red.

En Windows Server disponemos de una extraordinaria herramienta que nos facilita este tipo de trabajos.



# 8.1. Introducción

En este **capítulo nos centraremos en los aspectos del dominio relacionados con los clientes.** **Comenzaremos por detallar cómo unir un cliente**, con un sistema operativo Windows de escritorio, **al dominio que implementamos en el Capítulo anterior.**

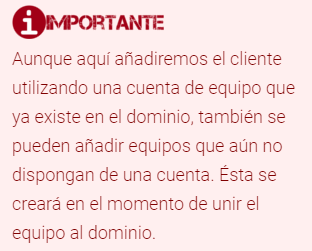
Después **aprenderemos a compartir con los equipos cliente el espacio de almacenamiento del servidor, asignaremos derechos a los usuarios y grupos del sistema y crearemos perfiles móviles y obligatorios para las cuentas de usuario.**

**Por último, aprenderemos a instalar y configurar las herramientas de administración remota que permiten controlar un dominio con *Windows Server* desde equipos cliente. En concreto, instalaremos *Remote Server Administration Tools***(*RSAT*) sobre un sistema *Windows* de escritorio. Una vez que hemos establecido nuestros objetivos, iniciemos la marcha…

# 8.2. Unir un cliente Windows al dominio

Lo primero que tenemos que hacer para utilizar los recursos de un dominio es añadirle los ordenadores que puedan actuar como clientes. En este caso, comenzaremos por un ordenador que está ejecutando Microsoft Windows.

Básicamente, **el proceso consistirá en establecer las características de red, para que coincidan con las necesidades del dominio, ajustar el nombre del equipo cliente, unir el equipo al dominio y, finalmente, iniciar sesión utilizando una cuenta de usuario de las que ya tenemos definidas en el dominio**.



<http://somebooks.es/unir-cliente-windows-8-dominio-windows-server-2012-r2/>

<http://somebooks.es/unir-cliente-windows-10-dominio-windows-server-2016/>

# 8.3. Crear carpetas personales para los usuarios en el servidor

Una de las primeras cosas que podemos hacer para beneficiarnos del dominio es crear un espacio de almacenamiento (una carpeta) en el servidor donde cada usuario pueda almacenar su información particular.

Dentro de la carpeta contenedora, cada usuario dispondrá de una subcarpeta propia que, según la configuración que vamos a hacer aquí, tendrá el mismo nombre que la cuenta de usuario (aunque, si no te gusta esta idea, se podría elegir cualquier otro).

El espacio compartido que consiste en una carpeta en el servidor, en el cliente se verá como una unidad de red.

Para realizar este trabajo,puedes recurrir a los siguientes artículos, según cuál sea tu sistema operativo de trabajo:

<http://somebooks.es/crear-carpetas-personales-los-usuarios-windows-server-2016/>

# 8.4. Crear carpetas compartidas por un grupo de usuarios

Como habrás comprendido por el título de este apartado, **la idea consiste en crear una carpeta en el servidor que funcione como un almacenamiento común para diferentes usuarios.**

Cuando finalicemos, **los usuarios implicados verán el espacio de almacenamiento compartido como una unidad de red. Para conseguirlo, dividiremos el trabajo en las siguientes tareas:**

* Primero **crearemos una carpeta y la compartiremos con todos los miembros del grupo Profesores**, que ya hemos utilizado en otros ejemplos.
* Después **escribiremos un script que monte la carpeta como una unidad de red.**
* Por último, **modificaremos el perfil de los usuarios para que se ejecute el script cada vez que inicien sesión en el dominio** y comprobaremos que todo funciona correctamente.

<http://somebooks.es/crear-carpetas-compartidas-grupo-usuarios-windows-server-2016/>

# 8.5. Asignación de derechos a usuarios y grupos

Un *derecho* le otorga a un usuario la capacidad de llevar a cabo determinadas acciones sobre el sistema.

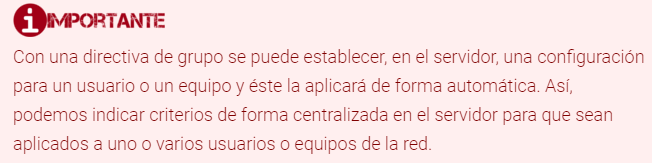
Los derechos se pueden asignar de forma predeterminada a los usuarios cuando se crean, o se pueden asignar con posterioridad. Además, un determinado derecho se puede otorgar de forma particular a un usuario, o se puede otorgar a un grupo para que lo obtengan de forma automática todos sus miembros.

En *Windows Server* se puede distinguir entre *derechos de conexión* (en inglés *logon rights*) y *privilegios*:

* **Los *derechos de conexión*** permiten definir el modo en el que iniciará sesión el usuario en el sistema (por ejemplo, si lo hará en modo local o a través de la red)
* **Los *privilegios*** definen lo que el usuario podrá hacer en el sistema una vez iniciada la sesión (por ejemplo, apagar el sistema o hacer copias de seguridad)

En *Windows Server*, podemos otorgar privilegios a un usuario o a un grupo de dos formas diferentes:

1. **Utilizando los grupos predeterminados** que podemos encontrar dentro del contenedor *Builtin* (Puedes consultar el capítulo anterior para obtener más detalles).
2. **Recurriendo a la herramienta *Administración de Directivas de grupo*** que, además de asignar privilegios individuales a un objeto, permite consultar qué usuarios disponen de un determinado privilegio.



Si queremos que un usuario pertenezca a un grupo predeterminado de Builtin como un operador de Seguridad, seguiremos el siguiente enlace:

<http://somebooks.es/asignar-derechos-usuarios-grupos-del-dominio-windows-server-2016-parte-i/>

Si queremos asignarle privilegios de Administración a un usuario o grupo en el cuál tenemos plena confianza y queremos que inicie sesión en el servidor de forma local para que lo administre, seguiremos el siguiente enlace:

<http://somebooks.es/asignar-derechos-usuarios-grupos-del-dominio-windows-server-2016-parte-ii/>

# 8.6. Perfiles de usuario

El sistema operativo utiliza los perfiles de usuario para contener la configuración del entorno de trabajo de cada usuario en el equipo local. Entre otras cosas, se incluyen las preferencias en cuanto a la configuración del la pantalla, las conexiones de red, la configuración de impresoras, etc.

Esta información se organiza en diferentes archivos que se crean en el momento que el usuario inicia sesión por primera vez. De esta forma, el sistema operativo consigue que varios usuarios puedan utilizar el mismo equipo, de modo que cada uno encuentre, al iniciar la sesión, el mismo entorno que dejó cuando cerró la sesión anterior.

Además, los cambios efectuados por un usuario en la personalización de su entorno no afectará a ningún otro usuario del equipo.

Desde el punto de vista del administrador del dominio, los perfiles de usuario ofrecen la posibilidad de crear perfiles predeterminados que se ajusten a cada tipo de usuario. Incluso pueden crearse perfiles obligatorios que no guarden los cambios efectuados por los usuarios, creando así cuentas con un aspecto y funcionalidad homogénea, que el usuario no puede alterar.

## Tipos de perfiles de usuario

Como se ha podido deducir por lo dicho hasta ahora, existen diferentes tipos de perfiles de usuario que utilizaremos según las necesidades particulares de cada momento. Entre los perfiles de usuario que podemos utilizar, se encuentran los siguientes:

* **Perfil de usuario local:** Se guarda en el disco duro local del equipo cliente, de modo que todas las modificaciones que se realicen serán específicas del ordenador en el que se han establecido.
* **Perfil de usuario móvil:** Los crea el administrador y se almacenan en una carpeta compartida por el servidor. Está asociada a la cuenta del dominio, de modo que estará disponible de forma independiente al ordenador concreto desde el que inicie sesión el usuario. Dado que el perfil se encuentra en el servidor, todos los cambios realizados en éste también se guardan en el servidor.
* **Perfil de usuario obligatorio:** Podríamos decir que son perfiles móviles de sólo lectura, ya que solamente los administradores del dominio pueden realizar cambios en estos perfiles. De esta forma, el administrador podrá definir configuraciones para usuarios o grupos, y éstos no podrán cambiarlos.
* **Perfil de usuario temporal:** Cuando se produce un error que impide cargar un perfil móvil o un perfil obligatorio, se crea un perfil temporal para facilitar el inicio de sesión del usuario. Cuando el usuario acaba su sesión, el perfil temporal se elimina y se pierden todas las modificaciones realizadas por el usuario en su entorno.
* **Perfil de usuario super-obligatorio:** Este tipo de perfiles se incorpora a partir de Windows Server 2008 y su objetivo es similar al de los perfiles obligatorios, con la diferencia de que, si se produce un error que impida cargar el perfil, el usuario no podrá iniciar sesión. En otras palabras, un perfil de usuario super-obligatorio impedirá que se cargue un perfil temporal cuando exista algún motivo que impida la carga del perfil super-obligatorio.

Si queremos crear un perfil móvil para un usuario comercial o Administrativo seguiremos el siguiente enlace:

<http://somebooks.es/crear-perfil-usuario-movil-active-directory-windows-server-2016/>

Si queremos crear un perfil obligatorio porque queremos tener siempre una misma imagen corporativa en el escritorio de los usuarios seguiremos el siguiente enlace:

<http://somebooks.es/crear-perfil-obligatorio-active-directory-windows-server-2016/>

# Capítulo 9: Usuarios, grupos y equipos en Windows Server

## Cuenta de usuario

Una cuenta de usuario es un objeto que posibilita el acceso a los recursos del dominio de dos modos diferentes:

* 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.

## 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:

**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.

## Cuentas de Equipo

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

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.

**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:

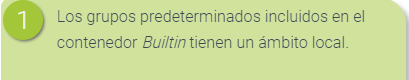
**Grupos de distribución:** Se utilizan en combinación con programas como Microsoft Exchange Server, para crear listas de distribución de correo electrónico. Estos grupos no disponen de características de seguridad, por lo que no pueden aparecer en las listas de control de acceso discrecional (DACL, Discretionary Access Control Lists).

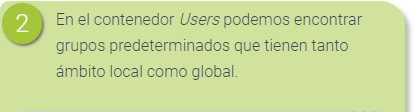
**Grupos de seguridad:** Permiten asignar permisos a las cuentas de usuario, de equipo y grupos sobre los recursos compartidos. Con los grupos de seguridad podemos:

* **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.

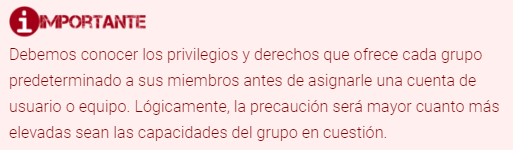
## Grupos integrados

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 Directory. Cuando ejecutemos esta herramienta, encontraremos los grupos predeterminados en dos contenedores:





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.



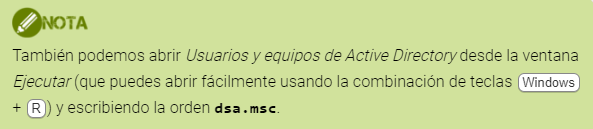
# 9.2. Crear una cuenta de usuario

Si queremos crear una cuenta de usuario ADDS seguiremos el siguiente enlace:

<http://somebooks.es/crear-una-cuenta-usuario-del-dominio-la-interfaz-grafica-windows-server-2016/>

**Se explican todos los detalles**

Recuerda:



# 9.3. 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.

Si has de aplicar alguna de las modificaciones de la lista anterior seguiremos el siguiente enlace:

<http://somebooks.es/operaciones-frecuentes-cuentas-usuario-dominio-windows-server-2016-parte-i/>

# 9.4. Otras operaciones frecuentes con cuentas de usuario

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 (una vez hemos creado la plantilla)
* Eliminar una cuenta de usuario

Si has de aplicar alguna de las modificaciones de la lista anterior seguiremos el siguiente enlace:

<http://somebooks.es/operaciones-frecuentes-cuentas-usuario-dominio-windows-server-2016-parte-ii/>

# 9.5. 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

Si quieres crear una cuenta de equipo o modificar valores de los equipos seguiremos el siguiente enlace:

<http://somebooks.es/capitulo-4-usuarios-grupos-y-equipos-en-windows-server-2012-r2/5/>

# 9.6. Administrar cuentas de grupo

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.

Si quieres realizar cualquier acción anterior de la lista sigue los siguientes enlaces:

<http://somebooks.es/administrar-cuentas-grupo-dominio-windows-server-2016-desde-la-interfaz-grafica-parte-i/>

<http://somebooks.es/administrar-cuentas-grupo-dominio-windows-server-2016-desde-la-interfaz-grafica-parte-ii/>

# 9.7. Operaciones frecuentes con 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.

Si queremos crear una unidad organizativa en la interfaz gráfica de Windows Server 2016 y asignarle contenido sigue el siguiente enlace:

<http://somebooks.es/crear-una-unidad-organizativa-la-interfaz-grafica-windows-server-2016-asignarle-contenido/>

Si queremos eliminar una unidad organizativa sigue el siguiente enlace:

<http://somebooks.es/eliminar-una-unidad-organizativa-la-interfaz-grafica-windows-server-2016/>

# APENDICE I - Administración Avanzada de un servidor Windows Server 2016

## Administrar usuarios del dominio desde la Línea de comandos

Resolver las tareas básicas de administración de usuarios desde la línea de comandos. En particular, nos centraremos en las siguientes situaciones:

* Crear una nueva cuenta de usuario
* Obtener toda la información relacionada con una cuenta de usuario
* Eliminar una cuenta de usuario
* Consultar los usuarios que existen en el dominio

<http://somebooks.es/administrar-usuarios-del-dominio-desde-la-linea-comandos-windows-server-2016-parte-i/>

## Administrar usuarios del dominio desde la Línea de comandos. Parte II

En esta segunda parte aprenderemos a:

* Asignar o cambiar la contraseña de una cuenta de usuario
* Habilitar o deshabilitar una cuenta de usuario existente
* Duplicar una cuenta de usuario existente
* Modificar los datos de una cuenta

<http://somebooks.es/administrar-usuarios-del-dominio-desde-la-linea-comandos-windows-server-2016-parte-ii/>

## Administrar usuarios del dominio desde la Línea de comandos. Parte III

En esta tercera parte aprenderemos a:

* Convertir a un usuario en miembro de un grupo
* Comprobar de qué grupos es miembro un usuario
* Establecer horas de inicio de sesión para una cuenta de usuario

<http://somebooks.es/administrar-usuarios-del-dominio-desde-la-linea-comandos-windows-server-2016-parte-iii/>

## Automatizar la creación de usuarios del dominio en Windows Server 2016 con un archivo csv

<http://somebooks.es/automatizar-la-creacion-usuarios-del-dominio-windows-server-2016-archivo-csv/>

## Exportar los usuarios de un dominio en Windows Server 2016 a un archivo csv

<http://somebooks.es/exportar-los-usuarios-dominio-windows-server-2016-archivo-csv/>

## Administrar cuentas de equipo del dominio desde la línea de comandos de Windows Server 2016

<http://somebooks.es/administrar-cuentas-equipo-del-dominio-desde-la-linea-comandos-windows-server-2016/>

## Administrar cuentas de grupo del dominio desde la línea de comandos de Windows Server 2016

<http://somebooks.es/administrar-cuentas-grupo-del-dominio-desde-la-linea-comandos-windows-server-2016/>

## Administrar unidades organizativas del dominio desde la línea de comandos de Windows Server 2016

<http://somebooks.es/administrar-unidades-organizativas-del-dominio-desde-la-linea-comandos-windows-server-2016/>

**APENDICE 2**

# Crear, editar o eliminar Políticas de Grupo (GPO) en Windows Server 2016

A nivel de Windows Server 2016, contamos con una utilidad integrada al sistema que será muy funcional para **controlar ciertas acciones que pueden ser aplicadas tanto a usuarios como equipos y son las directivas de** [políticas de grupo o GPO](https://www.solvetic.com/tutoriales/article/2416-uso-de-gpos-group-policy-object-en-windows-server/) (Group Policy Object).

Una GPO es básicamente una política que podremos crear y editar, obviamente remover en cualquier momento, mediante la cual se **permite establecer la configuración en los diversos** [**objetos a administrar**](https://www.solvetic.com/tutoriales/article/2655-manual-del-editor-de-gpo-local-en-windows-10/) **como usuarios y equipos.**

Una de las ventajas de las GPO es que **pueden ser implementadas en cualquier tipo de escenario y** [**podremos usarlas**](https://www.solvetic.com/tutoriales/article/4069-restablecer-directivas-grupos-locales-gpo-windows-server-2016-2012/) **para todo el dominio en general o solo para una unidad organizativa, OU, en especial**.

La implementación de una GPO **ha sido diseñada para que sea implementada en redes basadas en los Servicios de dominio de Active Directory (AD DS**) de Windows Server.

Requisitos para usar las políticas de grupo en Windows Server 2016:

1.- Un servidor debe de tener instalado el Active Directori Domain Services

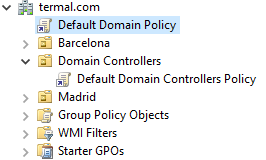
2.- Los equipos clientes deben de estar unidos al dominio y los usuarios que gestionaremos deben de usar las credenciales de dominio

3.- Para editar las políticas de grupo debemos de ser Administradores o Administradores de políticas de grupo

Existen dos tipos de GPO, de dominio y locales, esto implica:

* **La política de grupo basada en el dominio** nos da la posibilidad de **centralizar la administración** de modo que una sola política creada puede afectar a todos los equipos del dominio a la vez.
* **La política de grupo local** requiere que se tenga que **configurar cada máquina** lo cual implica más trabajo administrativo.

Las políticas de grupo en Windows Server 2016 viene con dos políticas por defecto:





Dentro de ella encontramos configuraciones de políticas que se aplican específicamente a los controladores de dominio creados.



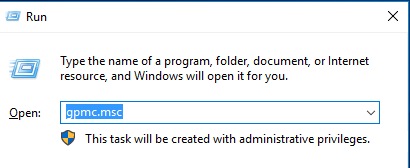
Dentro de ella encontramos configuraciones de políticas que se aplican a todas los equipos y usuarios en el dominio.



**Paso 1:**



Y escribimos:



También podemos acceder desde el Administrador del Servidor / herramientas (tools) y buscar la opción: 

**Paso 2:**

Desplegamos la carpeta dominios (domains) y haremos clic a nuestro dominio con el botón derecho:

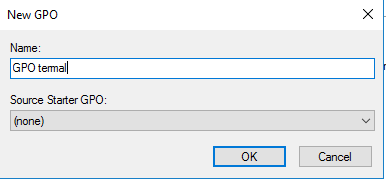


Seleccionamos la primera opción "Crear una GPO en este dominio, y enlazarlo aquí"



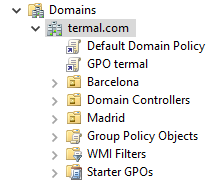
**Paso 3:**

Al seleccionar esta opción será desplegada la siguiente ventana donde asignaremos un nombre a dicha GPO:

****

**Paso 4:**

Al pulsar en el botón “Aceptar” veremos que se ha creado la GPO según nuestro criterio:

****

****

Hasta este punto hemos creado la GPO, pero esta no efectuara ninguna acción ya que no le hemos definido los parámetros requeridos que deben ser aplicados a los usuarios o equipos del dominio o OU indicada.

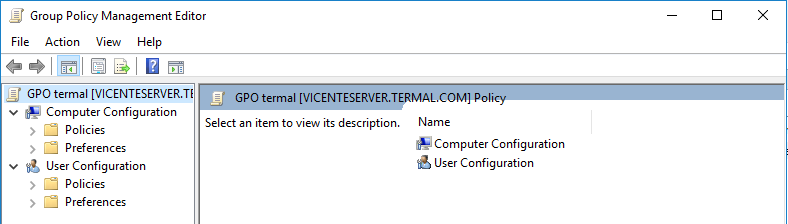
**Paso 1:**

Clic con el botón derecho en la GPO creada anteriormente y Editar



**Paso 2:**

Al hacer clic en editar seremos redireccionados a la siguiente pantalla:



**Paso 3:**

Aquí encontramos dos secciones principales:



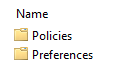
Dentro de configuración de equipo encontramos configuraciones que **se aplican exclusivamente a los equipos, independientemente de qué usuarios inicien sesión en ellos**. Estas suelen ser configuraciones de sistema y seguridad que configuran y controlan el equipo.

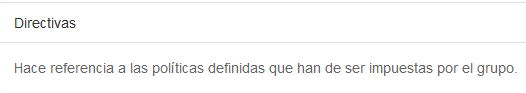


En esta sección encontramos configuraciones que **se aplican a los usuarios**, **independientemente del equipo que sea usado**. Estas configuraciones tienen que ver con la experiencia del usuario.

**Paso 4:**

También encontramos dos elementos en cada una de estas carpetas que son: **Directivas y Preferencias**



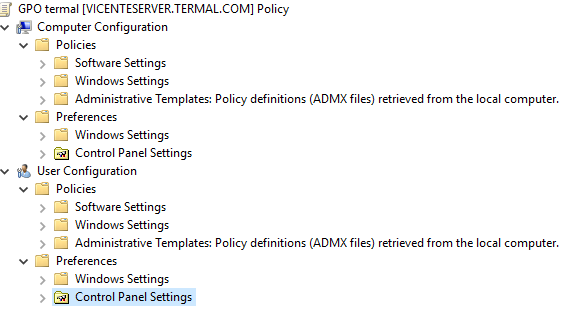




Esta opción incluye configuraciones de preferencias que podemos implementar para cambiar elementos como configuración de registro, archivo, carpeta u otro elemento. Al usar la configuración de preferencias, será posible configurar aplicaciones y funciones de Windows que no sean compatibles con la directiva de grupo.

**Paso 5:**

Dentro de cada carpeta vamos a las diferentes categorias:

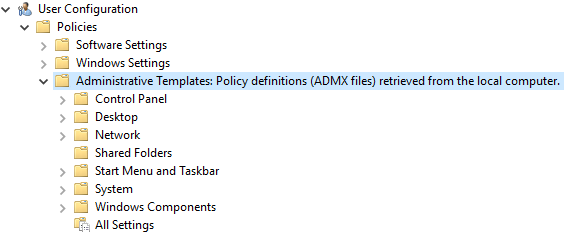


**Paso 6:**

Dentro de cada categoria podemos editar la acción que la GPO usará en el objecto seleccionado.

**Paso 7:**

Por ejemplo, si seguimos el siguiente path llegaremos a Plantillas Administrativas. Dentro encontramos diferentes opciones.



**Paso 8:**

Por ejemplo, si entramos en Componentes de Windows, dentro de esta carpeta buscamos

**Paso 9:**

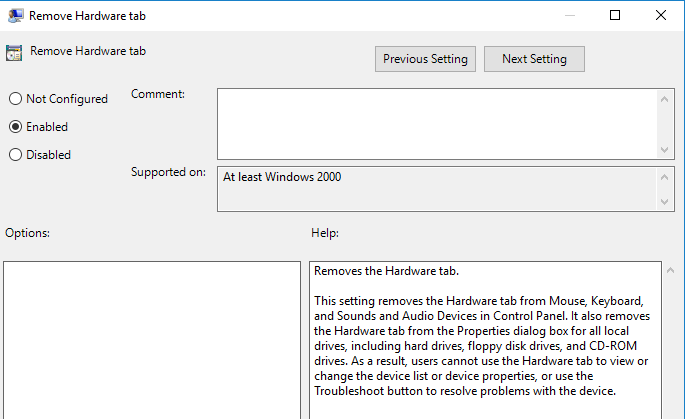
A continuación entre la lista de políticas buscamos la política.



En este caso, usaremos la política llamada “Ocultar la pestaña Hardware”, es decir, cuando accedemos al panel de control vemos allí la opción Hardware:

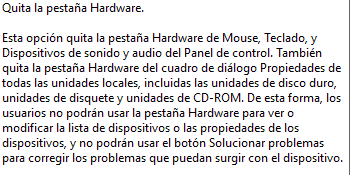


Y lo que haremos es editar esta política para habilitarla:



**Paso 10.-**

Es importante leer lo que supone habilitar esta política de grupo. Y supone eliminar o quitar la pestaá Hardware del Panel de Control. Seguidamente Aplicamos y OK



Paso 11.-

La política ahora queda habilitada

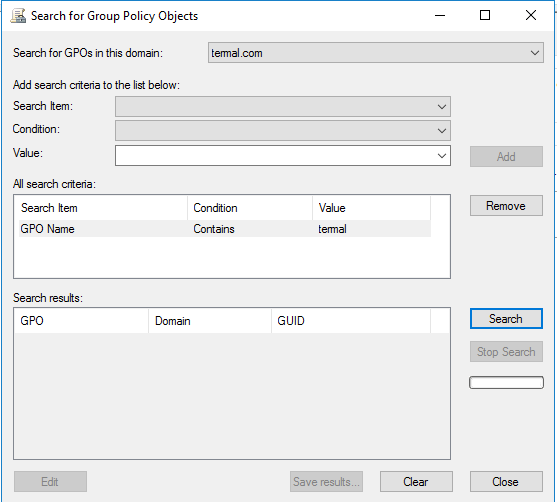




**Paso 1:**

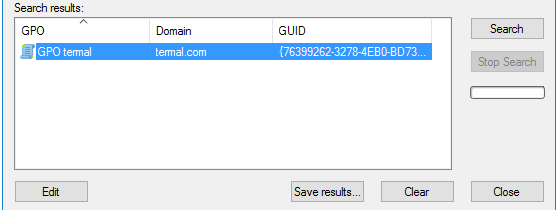
Si clicamos con el botón derecho al dominio podemos realizar una búsqueda de una GPO:

Podemos rellenar un criterio para luego realizar la búsqueda:



**Paso 2:**

Si ahora clicamos en Buscar en resultados de búsqueda nos aparece la GPO creada anteriormente. A partir de aquí nos da la opción de volver a editarla:



<https://www.solvetic.com/tutoriales/article/4910-crear-editar-eliminar-politicas-de-grupo-gpo-windows-server-2016/>