

UD05 - Xestión de recursos nunha rede baixo SSOO Windows

Índice

1. Xestión do servizo de directorio.....	3
1.1 Introducción.....	3
1.2 Actividade.....	3
1.2.1 Administración centralizada y administración descentralizada.....	3
Administración centralizada.....	3
Administración descentralizada.....	4
Vantaxes e desvantaxes de empregar unha administración centralizada.....	4
Vantaxes.....	4
Desvantaxes.....	4
Dominio.....	4
1.2.2 Windows Server e Active directory.....	5
Active Directory.....	6
1.2.3 Instalación de Active directory.....	7
Nome do equipo.....	7
Configuración de rede.....	7
Instalación do rol servizos de dominio de AD.....	9
Promoción do servidor a controlador de dominio.....	17
Dominio activado.....	24
Ferramenta de usuarios e equipos de Active directory.....	26
1.2.4 Unidades organizativas.....	27
Creación de unidades organizativas.....	28
Creación de unidades organizativas mediante comandos.....	36
Nomenclatura LDAP.....	36
Comando csvde.....	38
Comando ldifde.....	40
Atributos dos obxectos de AD.....	44
Buscar obxectos no Active directory.....	48
Familia de comandos ds.....	50
Dsadd.....	51
Dsmod.....	52
Dsquery.....	53
Dsget.....	54
Dsrm.....	55
1.2.5 Usuarios e contas de usuarios.....	56
Creación de contas de usuario.....	56
Horas de conexión permitidas a un usuario.....	65
Equipos permitidos para realizar unha conexión.....	66
Desbloqueo dunha conta de usuario.....	68
Habilitación e deshabilitación dunha conta de usuario.....	68
Familia de comandos ds.....	69
Dsadd.....	69
Dsmod, dsquery, dsget e dsrm.....	70
1.2.6 Engadir equipos ao dominio.....	71
Engadir estacións de traballo Windows ao dominio.....	71

Autenticación no dominio.....	74
Estación de traballo vista desde o servidor.....	76
1.2.7 Grupos.....	77
Creación de grupos.....	78
Pertenza dun usuario a varios grupos.....	82
Pertenza dun grupo a outro grupo.....	83
Familia de comandos ds.....	84
Dsadd.....	84
Dsmod, dsquery, dsget e dsrm.....	85
1.2.8 Carpetas persoais.....	85
Creación de carpetas persoais.....	86
Familia de comandos ds.....	92
1.2.9 Carpetas compartidas no dominio.....	92
Creación de carpetas compartidas no dominio.....	93
Acceso aos recursos compartidos mediante unidades de rede.....	97
Familia de comandos ds.....	99
1.2.10 Directiva de grupos.....	100
Creación dun GPO.....	100
Aplicación das directivas de grupo.....	105
Habilitar e deshabilitar GPOs.....	106
Aplicación de varios GPOs sobre un mesmo obxecto.....	107
Herdanza de GPOs.....	108
Anulación da herdanza.....	109
Exigir cumprimento dun GPO.....	110
Advertencias sobre as directivas de grupo.....	110
1.2.11 Estruturas de dominios.....	111

1. Xestión do servizo de directorio

1.1 Introducción

Na actividade que nos ocupa aprenderase a xestionar o servizo de directorio dun sistema operativo, tanto desde o punto de vista da súa instalación como desde o punto de vista da súa xestión. Ao longo desta actividade aprenderemos a facer emprego das características do servizo de directorio empregadas máis habitualmente.

1.2 Actividade

1.2.1 Administración centralizada y administración descentralizada

Nunha rede informática na cal hai funcionando varios equipos, a administración do acceso dos usuarios ao sistema informático e a xestión dos recursos existentes, pódese realizar de dous modos:

- Administración centralizada
- Administración descentralizada.

Administración centralizada

Cando falamos de unha administración centralizada, estamos referíndonos a unha maneira de traballar na cal a administración do sistema está centralizada nun único equipo da rede o como moito nun número limitado deles. Este punto de centralización da administración almacena e permite xestionar a información necesaria para que os usuarios poidan acceder aos equipos que compoñen o sistema informático, así como a información referente aos permisos de acceso sobre os diferentes recursos existentes no sistema informático.

A grandes trazos, un sistema informático en rede con administración centralizada define un sistema informático en rede, no cal hai un número indefinido de equipos de traballo e ademais hai un equipo único o un número limitado deles cuxa función é a de xestionar e administrar o sistema informático. Un sistema informático en rede con administración centralizada está compostos por tódolos equipos do sistema informático, podendo diferenciar entre eles tres tipos de equipos:

- Servidores. Algúns deles teñen como finalidade xestionar e administrar o sistema informático (denomínanse controladores de dominio), mentres que outros simplemente proporcionan algún servizo adicional aos equipos do sistema informático da rede (p.e. un servidor de páxinas web). En xeral os servidores soen ser equipos moi potentes desde un punto de vista hardware.
- Estacións de traballo ou clientes. Son os equipos que empregan los usuarios para conectarse ao sistema informático para traballar e poder acceder aos recursos que hai compartidos nel. A súa potencia é moito menor que a dos servidores desde un punto de vista hardware.

- Outros recursos hardware. Dentro desta categoría inclúese calquera outro tipo de elemento hardware conectado ao sistema informático que poida ser empregado polos usuarios do mesmo, p.e. Impresoras, escáneres, ...

Administración descentralizada

Cando falamos dunha administración descentralizada, estamos referíndonos a unha maneira de traballar na cal non hai un punto central para a administración do sistema informático, senón que cada equipo xestiona o acceso dos usuarios e os permisos de acceso sobre os seus recursos.

Unha administración descentralizada é fácil de xestionar e económica cando o número de equipos a xestionar nunha rede é reducido, pero a pouco que medre o número destes, a xestión do sistema informático vólvese complexa e o seu custo medra enormemente.

Vantaxes e desvantaxes de empregar unha administración centralizada

Vantaxes

- A administración do sistema informático límitase a un único punto.
- Os usuarios poden conectarse desde calquera equipo do sistema informático (desde o que teñan permiso) empregando as mesmas credenciais.
- Alta escalabilidade, xa que a tarefa de engadir equipos ao sistema informático é relativamente sinxela.
- Fácil mantemento, xa que ao estar distribuídas as funcións e responsabilidades entre diferentes servidores, é posible substituír, reparar, actualizar, ou incluso mover un servidor, mentres que os seus clientes non se verán afectados polos cambios (unicamente non poderán acceder ao servidor mentres é mantido, pero unha vez finalizado o mantemento o cliente poderá volver a facer uso do servidor sen ningún problema).

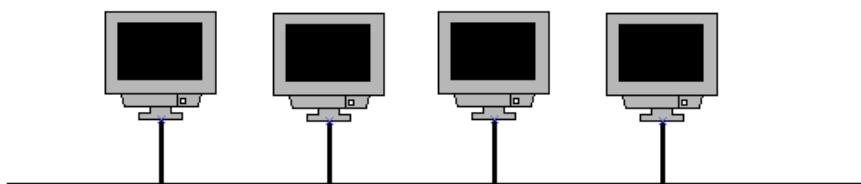
Desvantaxes

- Cando un servidor está caído, as peticións dos clientes non poden ser satisfeitas. Ademais no caso de que o servidor caído sexa o controlador de dominio, o sistema informático podería quedar inhabilitado (é por elo que se recomenda que ao montar un sistema informático con administración centralizada existan ao menos dous controladores de dominio. Un é o controlador principal de dominio e é o servidor empregado habitualmente para a administración do sistema informático. O outro é o controlador secundario de dominio. Funciona en espello co principal e unicamente entra a funcionar no caso de que caia o controlador principal de dominio).
- O custo dos servidores é elevado.

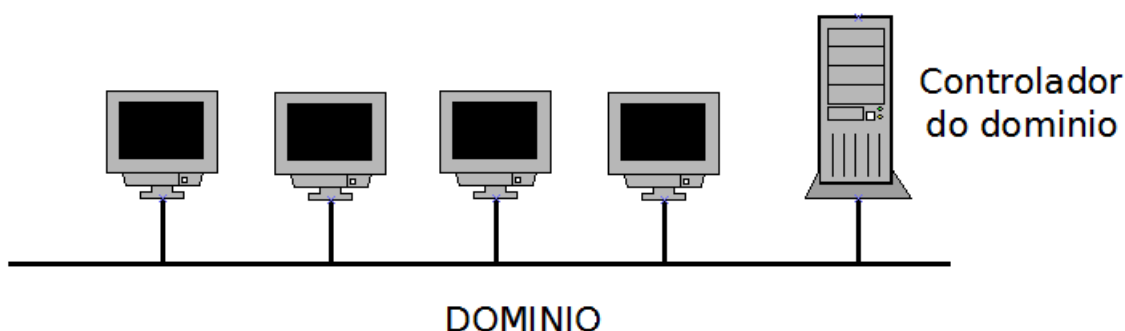
Dominio

Cando a administración e xestión dun sistema informático é levada a cabo dun modo centralizado, estamos falando da administración e xestión dun dominio.

Supoñamos que temos un sistema informático composto por varios equipos conectados entre si mediante unha rede:



Inicialmente cada equipo informático, a pesar de estar conectado en red con los demás equipos, es una isla desde un punto de vista administrativo. Cada equipo gestiona que usuarios pueden acceder a él y que recursos pueden ser accedidos. La administración es una administración descentralizada. Con el fin de simplificar este funcionamiento desde un punto de vista administrativo, vamos a modificar la administración para convertirla en una administración centralizada. Para ello creamos un dominio. Un dominio es una estructura compuesta por los diferentes equipos informáticos conectados a la red con la peculiaridad de que uno de ellos, llamado controlador de dominio, tiene instalado un software de gestión de directorio que se encarga de almacenar toda la información necesaria para poder gestionar el acceso de los usuarios al dominio, así como la información necesaria para gestionar el acceso de los usuarios a los recursos del dominio:



Cuando un usuario quiere identificarse en el dominio, puede hacerlo desde cualquier equipo, ya que la base de datos que almacena los usuarios que pueden acceder al dominio se encuentra almacenada en el controlador de dominio. Una vez que un usuario se identifica correctamente ante el controlador de dominio, este le asigna unas credenciales, las cuales permitirán o no al usuario acceder a los diferentes recursos del dominio.

El controlador de dominio centraliza la información necesaria para la administración y gestión de los usuarios del dominio y de los recursos del mismo. Como ya dijéramos con anterioridad, la administración simplifícase enormemente ya que ahora únicamente hay un punto de administración.

1.2.2 Windows Server e Active directory

Los sistemas operativos en red suelen ofrecer las herramientas necesarias para crear y gestionar estructuras de dominio. A lo largo de esta documentación vamos a montar y administrar dominios empleando un sistema operativo de Microsoft. Dentro de los sistemas operativos de Microsoft, es la familia de los sistemas Windows Server la que nos permite crear y gestionar dominios. En concreto, el producto que emplearemos para crear el controlador de dominio

vai ser Windows Server 2012 R2 versión Standard. Nas estacións de traballo que conectemos ao dominio empregaremos o sistema operativo Windows 8.1.

Active Directory

Para administrar un dominio facendo uso dalgún sistema operativo da familia Microsoft Windows Server empregaremos o software Active directory (directorio activo). Active directory (AD) é a denominación que da Microsoft á súa implementación do servizo de directorio.

En xeral, un servizo de directorio é un software empregado para almacenar e xestionar a información dos usuarios e dos recursos dunha rede informática, permitíndonos mediante a xestión da información que almacena administrar dun modo centralizado o sistema informático, tanto desde un punto de vista de acceso dos usuarios ao sistema, como desde un punto de vista de xestión dos diferentes recursos existentes no sistema informático.

AD apoíase en varios protocolos para funcionar, sendo os máis importantes LDAP, DNS, DHCP e Kerberos:

- **LDAP:** Lightweight directory access protocol (protocolo lixeiro de acceso a directorios). LDAP basicamente implementa unha base de datos centralizada que se emprega para almacenar información referente aos diferentes obxectos que compoñen o sistema informático (usuarios, grupos, equipos, ...). A vantaxe de utilizar unha base de datos centralizada é evidentemente que á hora de administrar o sistema, a información necesaria para elo está situada nun único punto en lugar de estar distribuída entre os diferentes sistemas que compoñen o sistema informático.
- **DNS:** Domain name system (sistema de nomes de dominio). A labor do sistema DNS é a de traducir as direccións IP das máquinas do sistema informático a nomes de dominio, os cales empregan unha nomenclatura máis amigable. LDAP necesita de DNS para funcionar axeitadamente xa que o seu funcionamento á hora de xestionar os equipos informáticos do sistema non se basea nas súas direccións IP, senón que o fai baseándose nos seus nomes de dominio os cales son xestionados polo protocolo DNS.
- **DHCP:** Dynamic Host Configuration Protocol (protocolo de configuración dinámica de host). Mediante este protocolo libérase ao administrador de configurar manualmente os parámetros de configuración de rede para cada un dos equipos do sistema informático, xa que dita tarefa realízase desde un único punto centralizado (servidor DHCP) e de xeito automático. Cando un equipo do sistema informático precisa configurar os seus parámetros de rede os solicita ao servidor DHCP, sendo este o que lle indica que parámetros de configuración de rede debe empregar.
- **Kerberos:** ao traballar con AD é preciso que a autenticación dos usuarios sexa realizada dun modo seguro. Para elo emprégase Kerberos. Kerberos é un protocolo de autenticación en redes de ordenadores que permite a xestión de credenciais dun modo seguro.

AD inclúe:

- Un conxunto de regras, o esquema, que define as clases de obxectos e atributos incluídos no directorio, as restricións e os límites das instancias destes obxectos e o formato dos seus nomes.

- Un catálogo global que contén información sobre todos os obxectos do directorio. Isto permite aos usuarios e administradores buscar información de directorio independentemente do dominio do directorio que conteña realmente os datos.
- Un mecanismo de consulta e índice, de modo que os usuarios ou as aplicacións de rede poidan publicar e atopar os obxectos e as súas propiedades, para permitir a explotación dos datos de dita base de datos para administrar o sistema informático
- Un servizo de replicación que distribúe os datos de directorio a través dunha rede. Todos os controladores de dominio dun dominio participan na replicación e conteñen unha copia completa de toda a información de directorio do seu dominio. Calquera cambio nos datos do directorio replícase en todos os controladores de dominio do dominio.

1.2.3 Instalación de Active directory

A instalación do AD será levada a cabo sobre un Windows Server 2012 R2 Standard acabado de instalar e sen ningunha característica adicional (o sistema operativo estará virtualizado mediante VirtualBox). O obxectivo é instalar o servizo de dominio de AD nunha máquina Windows Server e convertela no controlador principal dun dominio chamado empresa.local. Dito dominio será o empregado por unha organización para administrar os seus recursos informáticos.

Nome do equipo

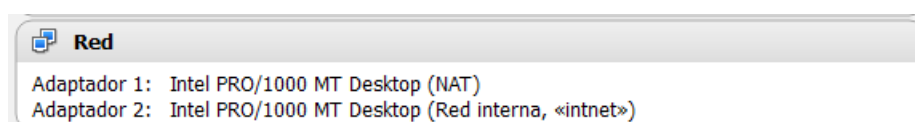
O primeiro que faremos será cambiar o nome do equipo co fin de que teña un nome que o identifique facilmente e que sexa máis fácil de lembrar que o nome asinado por defecto durante a instalación do sistema operativo. Non explicaremos como realizar este proceso pois xa se indicou nunha unidade didáctica anterior. O novo nome que daremos ao equipo será SERVIDOR.

Configuración de rede

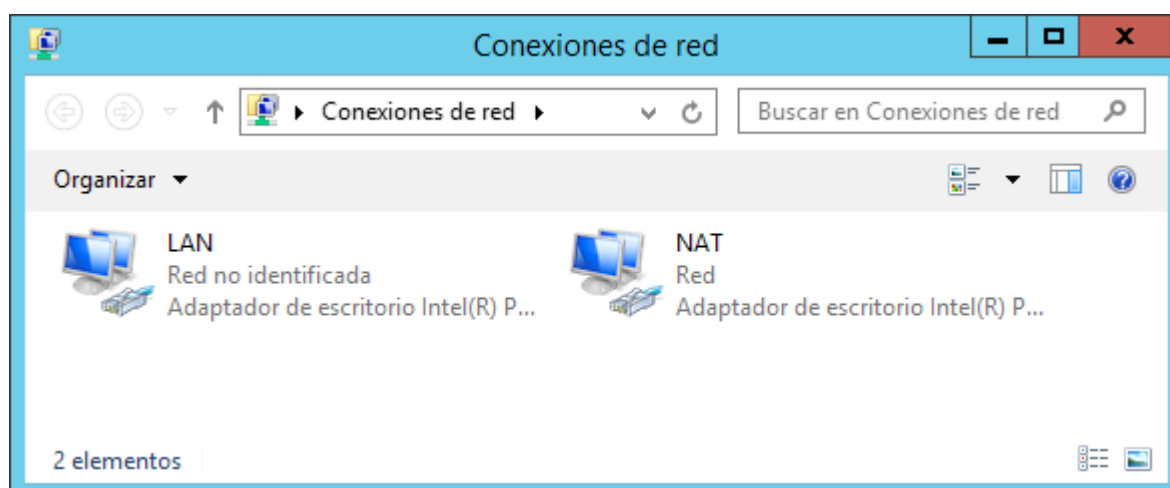
Imos configurar a máquina virtual sobre a que corre o Windows Server 2012 R2 Standard con dúas tarxetas de rede. Unha será configurada en rede interna e a outra en NAT (poderíanse empregar outras configuracións de rede, pero nesta ocasión imos empregar esta):

- A tarxeta configurada en rede interna será empregada para conectar os diferentes equipos da LAN (equipos do dominio).
- A tarxeta configurada en NAT será empregada para poder saír a internet a través da máquina anfitrión do sistema virtual.

As direccións dos equipos da rede interna serán do tipo 192.168.20.0/24. Calquera equipo que funcione como controlador de dominio debe ter establecida unha dirección ip estática. A dirección ip do equipo SERVIDOR para a interface que se conecta á LAN vai ser a 192.168.20.1.



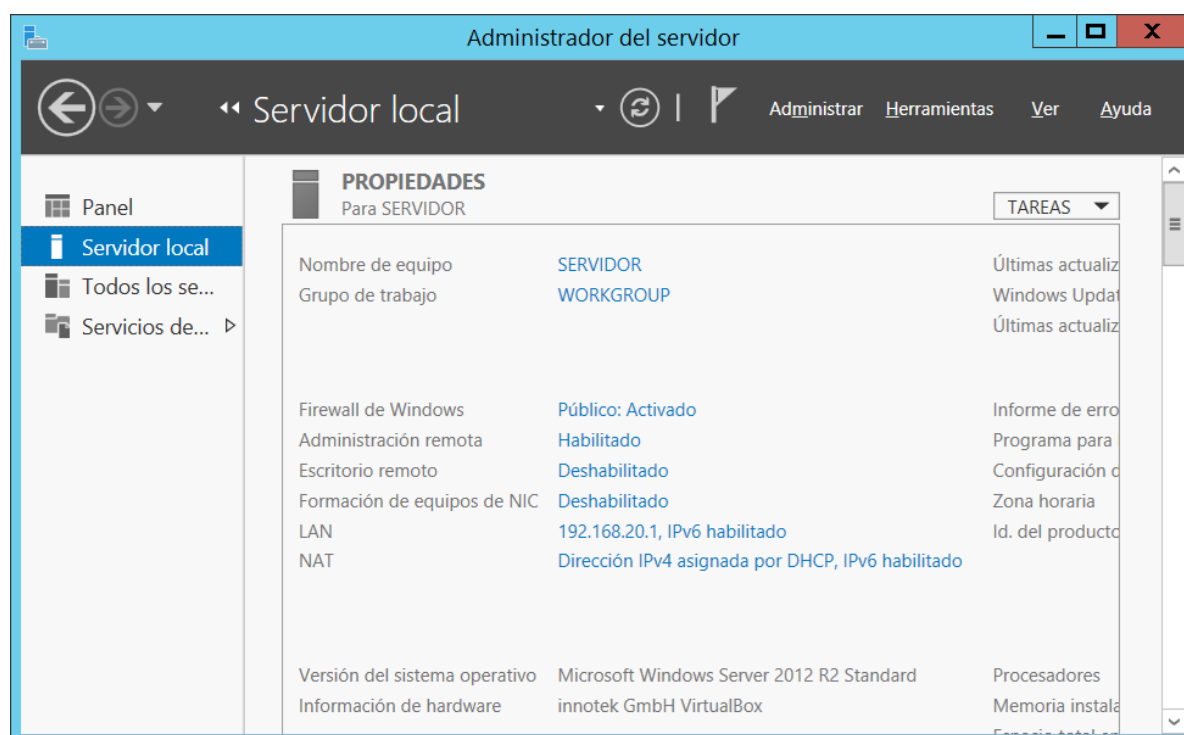
Na seguinte imaxe podemos ver as conexións de rede definidas para o Windows Server 2012 R2 Standard:



Modificouse o nome dos adaptadores de rede para que sexa máis fácil xestionalos.

- O adaptador NAT está ligado ao adaptador 1 da máquina virtual.
- O adaptador LAN está ligado ao adaptador 2 da máquina virtual.

Se abrimos o administrador do servidor e accedemos ás características do servidor local podemos comprobar que o nome do equipo e os interfaces de rede están establecidos correctamente:

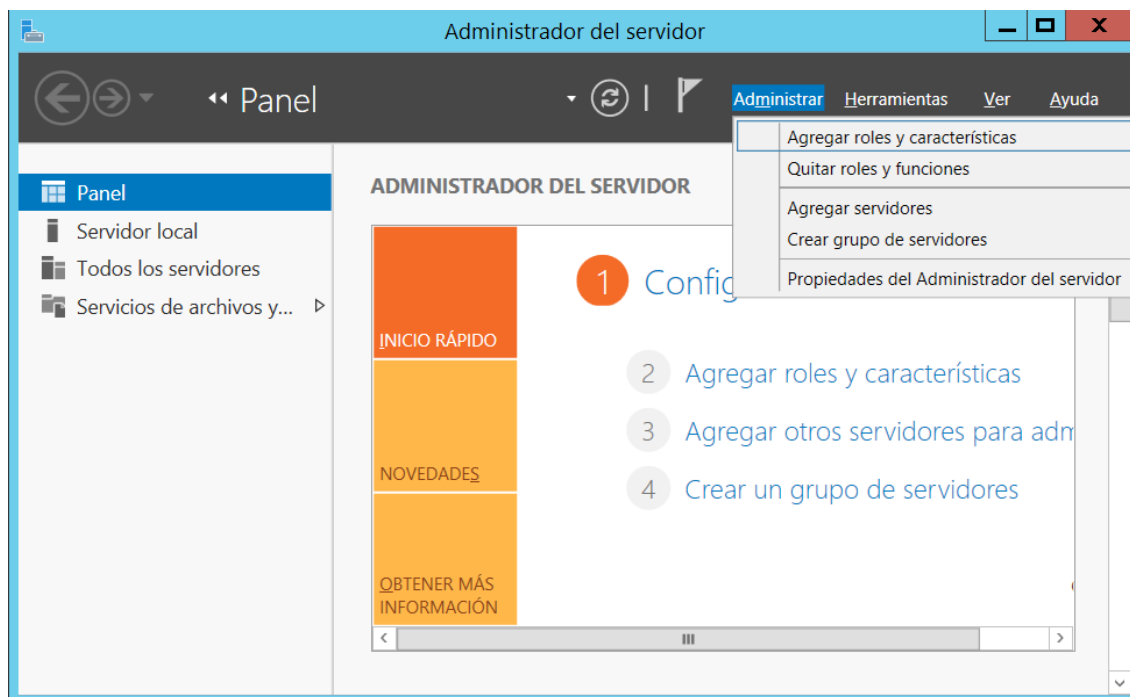


Unha vez realizados estes pasos previos imos comezar coa instalación do servizo de dominio de AD.

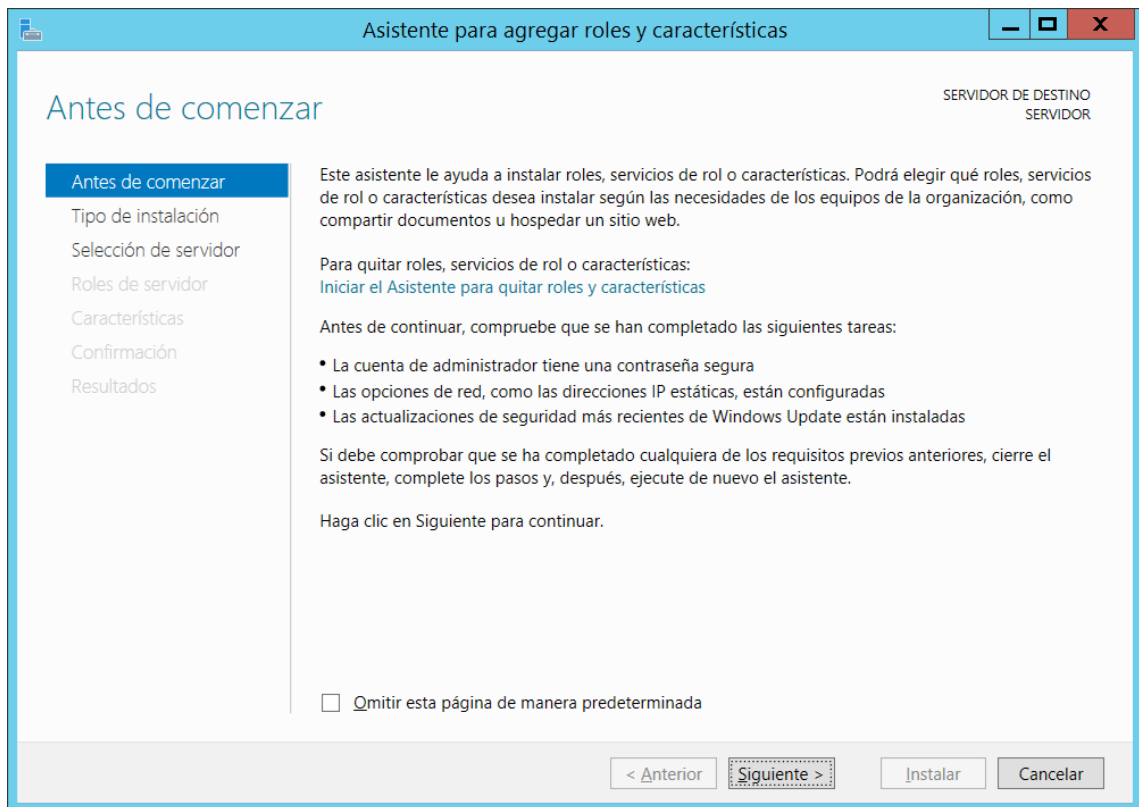
Instalación do rol servizos de dominio de AD

Para instalar o servizo de dominio do AD nun equipo debemos de instalar nel o rol servizos de dominio de AD. Un rol é a terminoloxía que emprega Microsoft para referirse a un conxunto de programas que unha vez que se instalan e configuran correctamente, permiten a un equipo realizar unha función específica para varios usuarios ou para outros equipos dunha rede. En versións anteriores a Windows Server 2008 un rol acostumaba denominarse coa palabra servizo.

O primeiro que debemos facer é indicar ao sistema que queremos instalar un rol. Para facer isto, accedemos á pantalla de administración do servidor e prememos sobre administrar / Agregar roles y características:



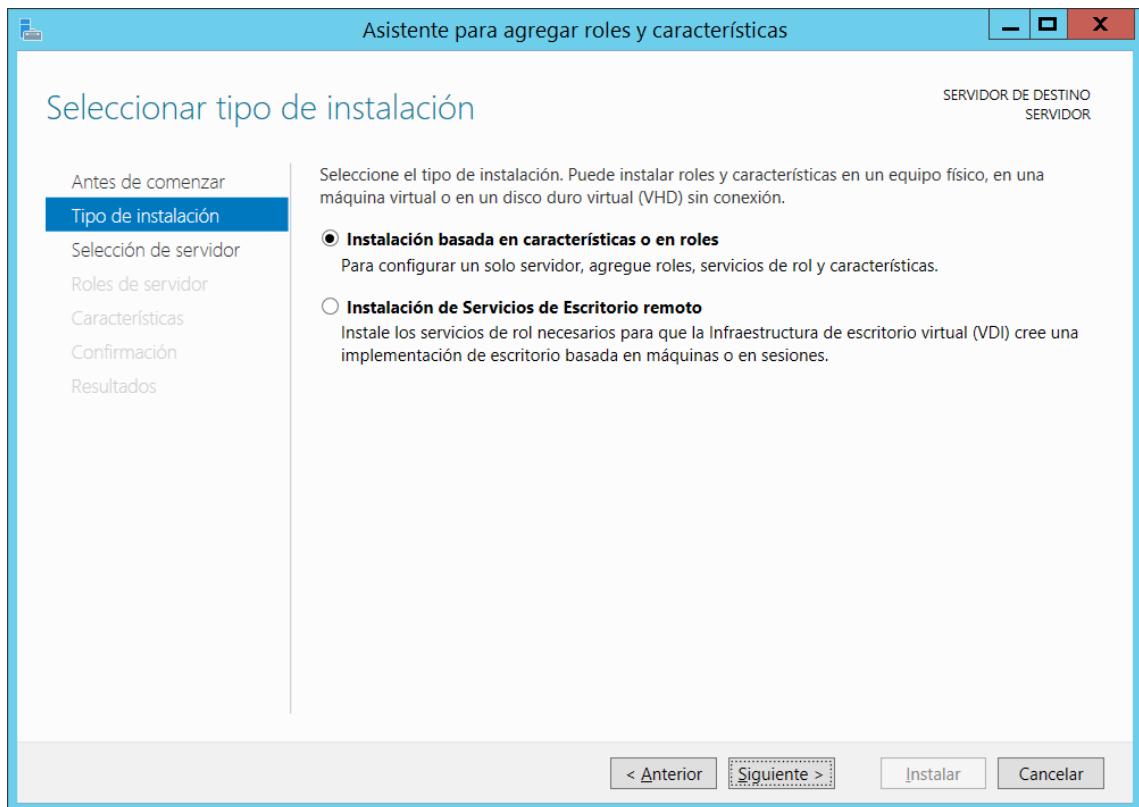
Ao facelo abrirásenos a seguinte xanela:



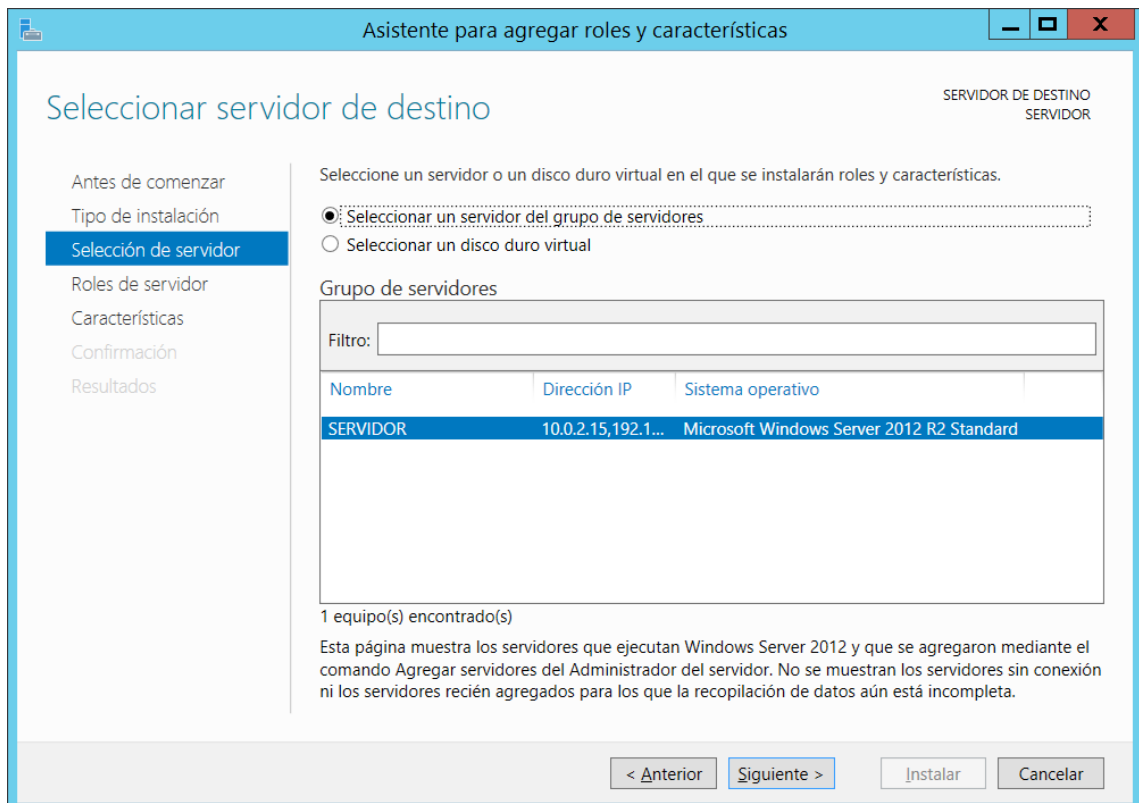
Esta xanela é o inicio do asistente que se utiliza para instalar roles e características en Windows Server 2012. Fixémonos que nos indica que comprobemos unha serie de puntos:

- Que o administrador ten un contrasinal establecido e que é seguro.
- Que a rede está correctamente configurada.
- Que o sistema está actualizado.

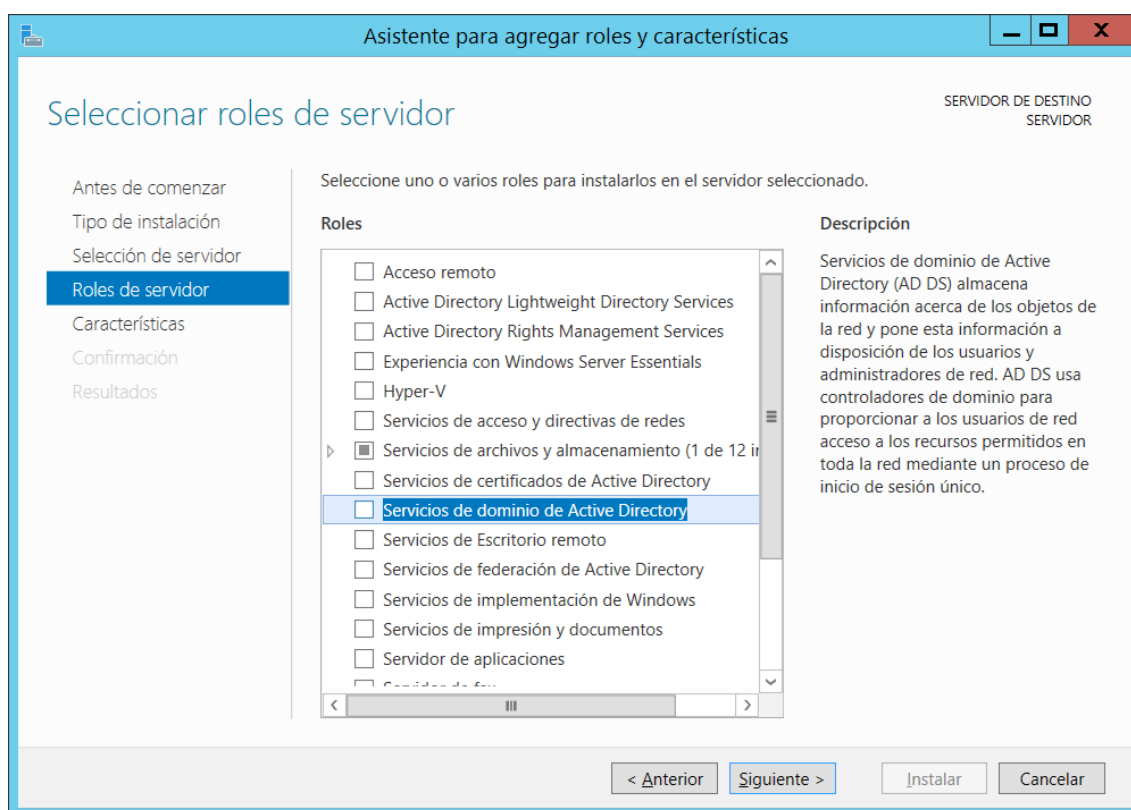
Respecto aos dous primeiros requisitos, podemos afirmar que se cumpren. Respecto ao terceiro, o seu cumprimento dependerá do estado inicial da instalación do sistema operativo. No caso de ter que actualizar o sistema, dita actualización será feita do mesmo modo que xa vimos nunha unidade didáctica previa para outros produtos da familia Microsoft. Unha vez que estamos seguros de que o sistema está listo prememos sobre o botón Siguiente. Abrirásenos a seguinte xanela:



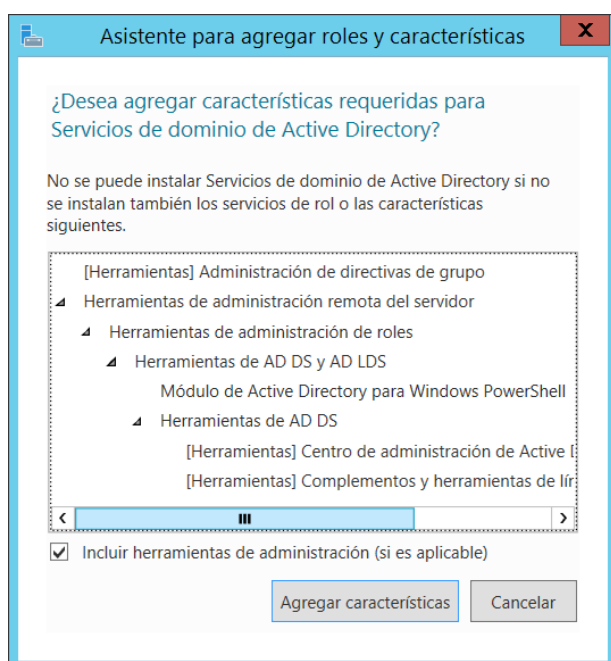
Seleccionaremos a primeira opción, instalacion basada en características o roles e prememos sobre o botón Siguiente. Abrirásenos a seguinte xanela:



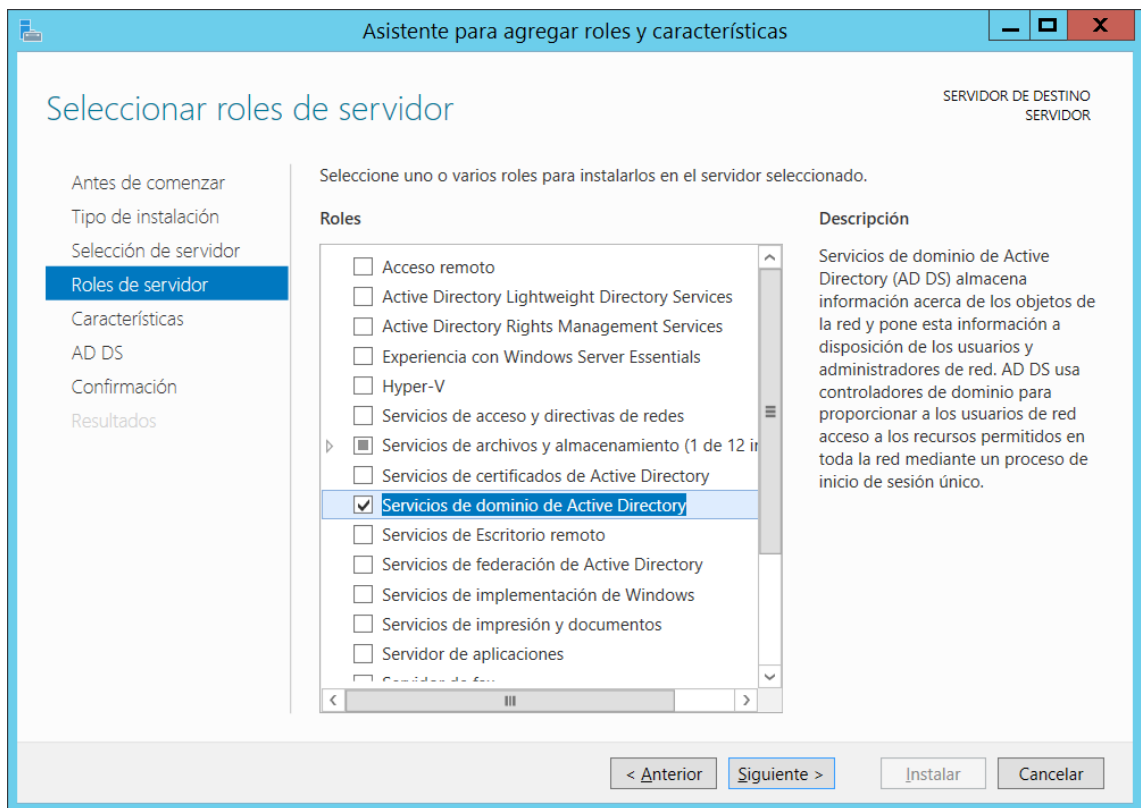
Mediante esta xanela seleccionaremos onde queremos instalar o rol, neste caso na máquina **SERVIDOR**. Prememos sobre o botón **Siguiente**. Abrirásenos a seguinte xanela:



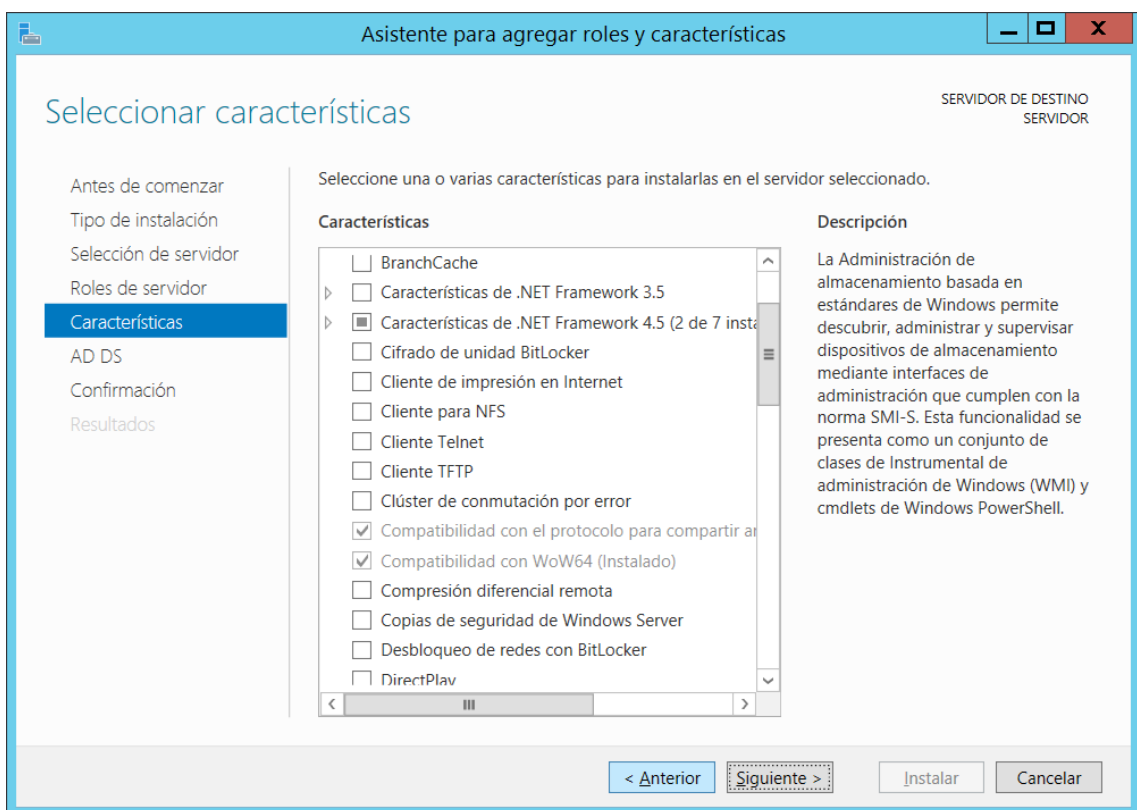
Nesta xanela seleccionaremos o rol que queremos instalar, neste caso seleccionamos o rol **servicios de dominio de Active Directory**. Ao seleccionar este rol amosarásenos unha xanela que nos indica que roles e características adicionais é preciso instalar no sistema para poder utilizar o rol de **servicios de dominio de Active Directory**:



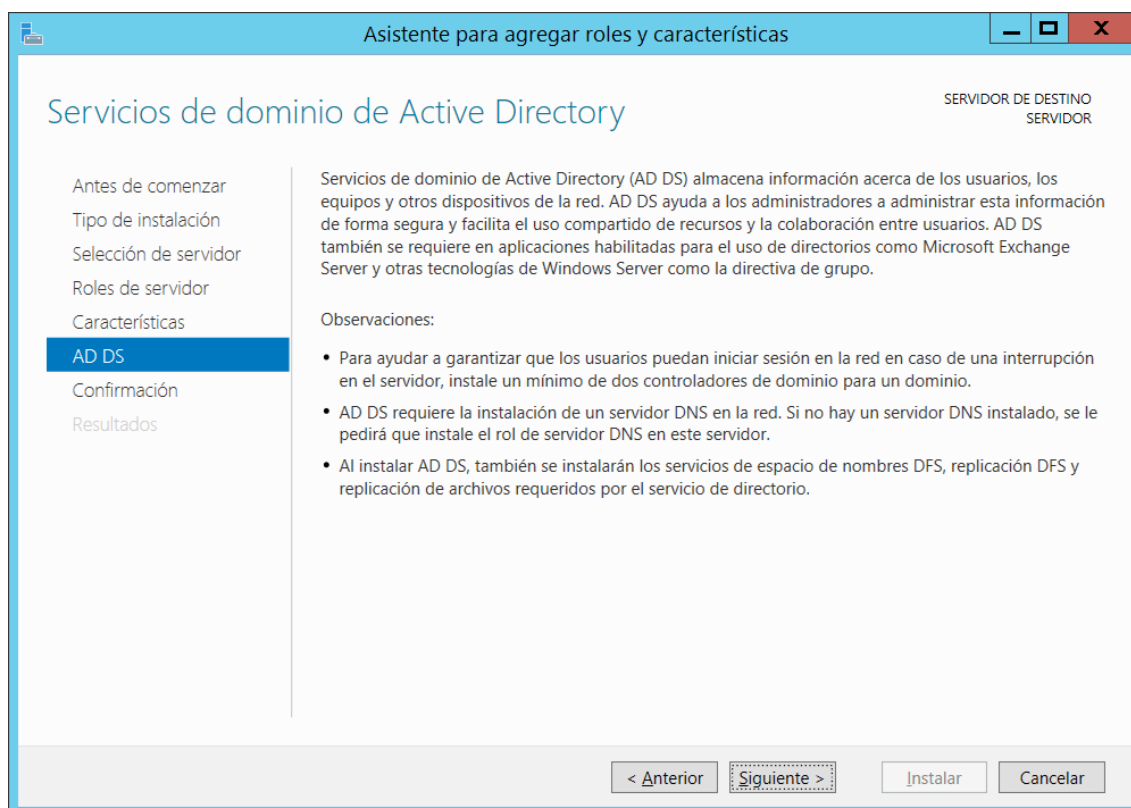
Se estamos de acordo premeremos sobre o botón agregar características e volveremos a esta xanela:



Agora xa temos realmente seleccionado para instalar o rol servicios de dominio de Active Directory. Prememos no botón siguiente e o asistente pasará a amosar un resumen das características que van ser instaladas:



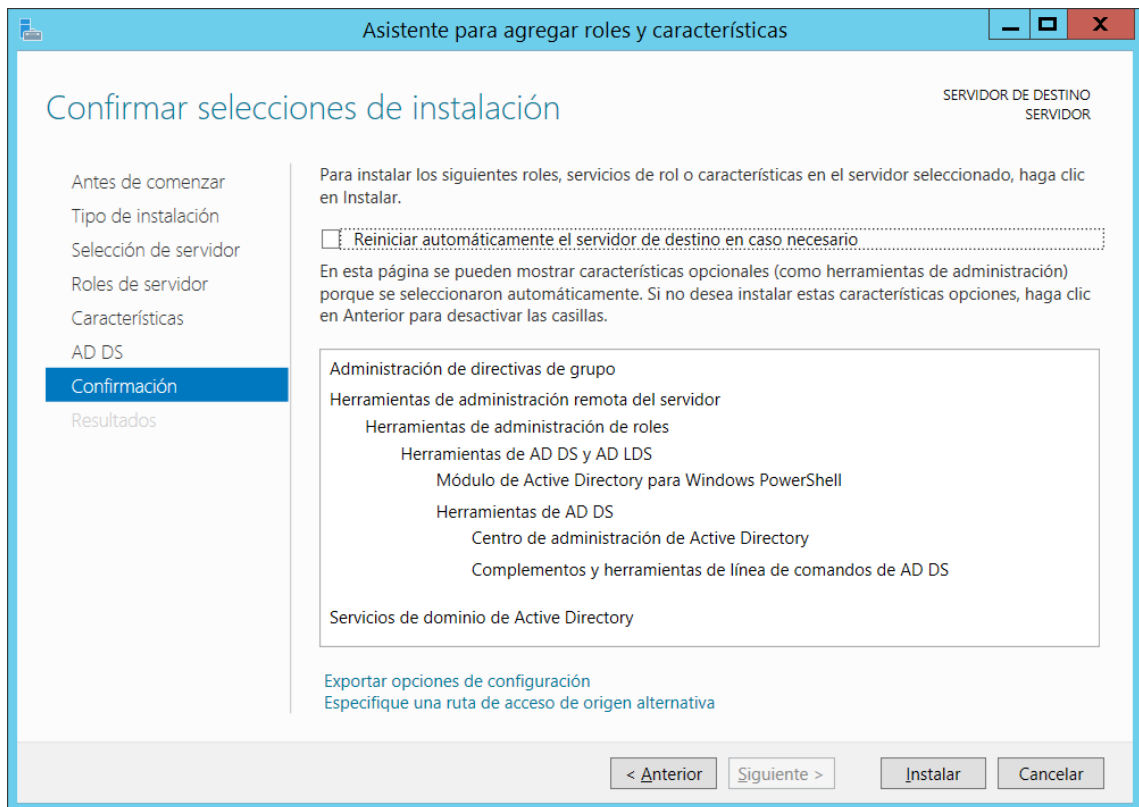
Característica é a terminoloxía que emprega Microsoft para referirse a programas que, aínda que non forman parte directamente dos roles, poden complementar ou aumentar a súa funcionalidade ou mellorar a funcionalidade do servidor independentemente dos roles que estean instalados. Prememos sobre o botón seguinte co cal amosarásenos a seguinte xanela do asistente:



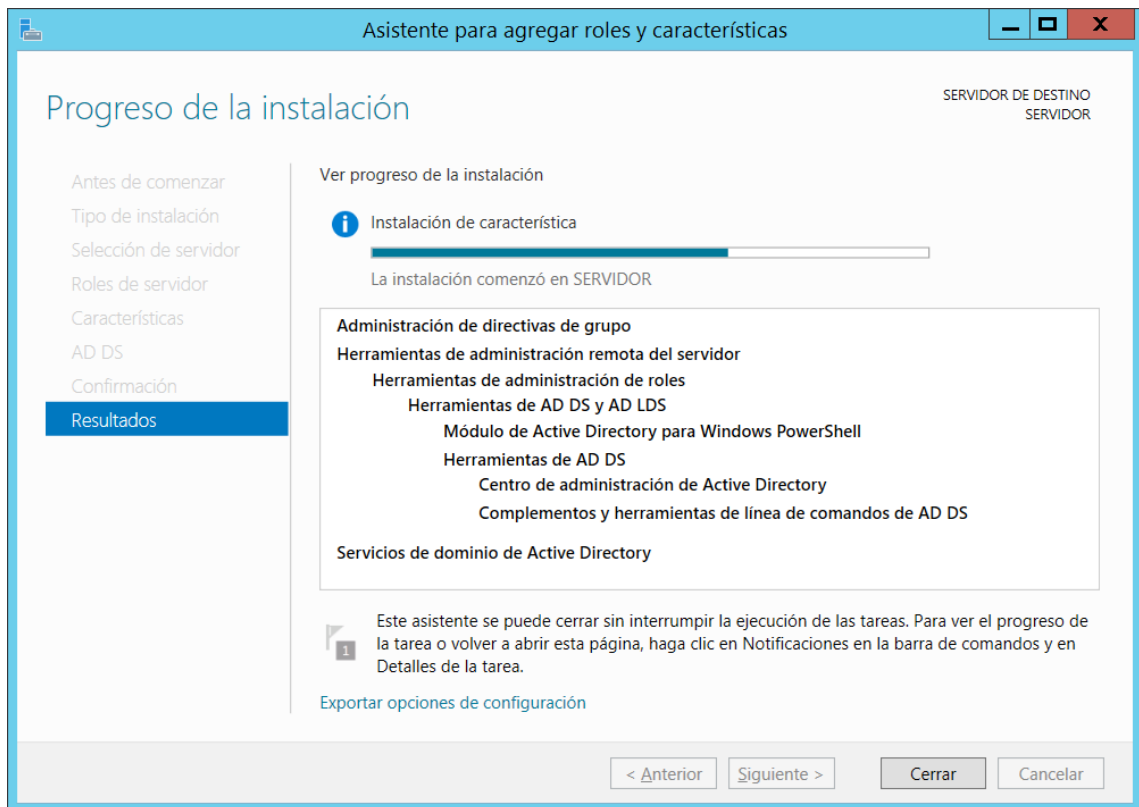
Nesta xanela:

- Amósase información sobre cal é a utilidade de AD.
- Recoméndase a instalación dun segundo controlador de dominio (de modo que se cae o controlador de dominio principal entre a funcionar e segundo e o dominio siga funcionando).
- E o máis importante, infórmase de que AD necesita dun servidor de DNS para poder funcionar. Temos dúas opcións: ou ben utilizar un servidor DNS xa existente ou ben deixar que durante o proceso de instalación de AD sexa instalado o servizo de DNS na propia máquina que vai funcionar como controlador de dominio. Neste caso faremos isto último.
- Ademais infórmase de que serán instalados unha serie de servizos adicionais necesarios para o correcto funcionamento de AD.

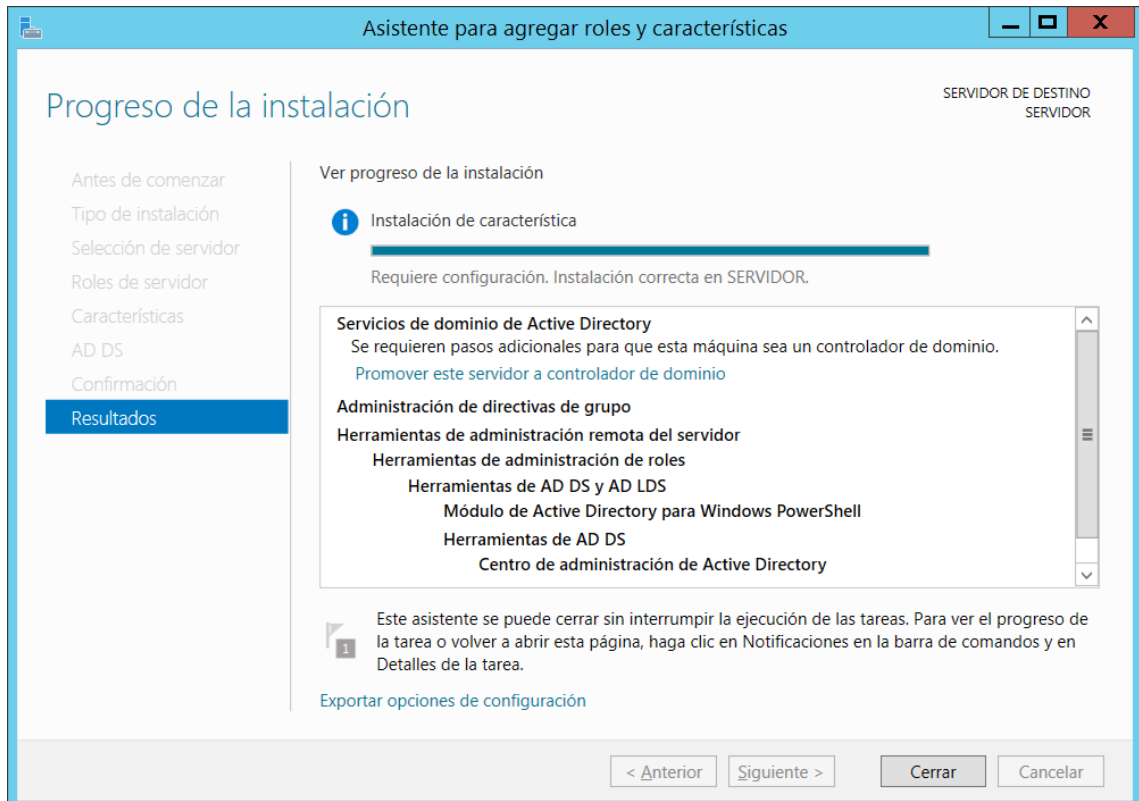
Prememos sobre o botón seguinte. Amosarase a xanela de confirmación de instalación do rol:



Nesta xanela amósase un resumo de todo o que se vai instalar e ademais danos a opción de que o sistema sexa reiniciado automaticamente cando sexa necesario durante o proceso de instalación do rol. Unha vez comprobado que todo é correcto pasamos ao proceso de instalación. Para elo prememos sobre o botón instalar de modo que se comezará a instalar o rol. Ao longo da instalación amosarase a seguinte xanela:

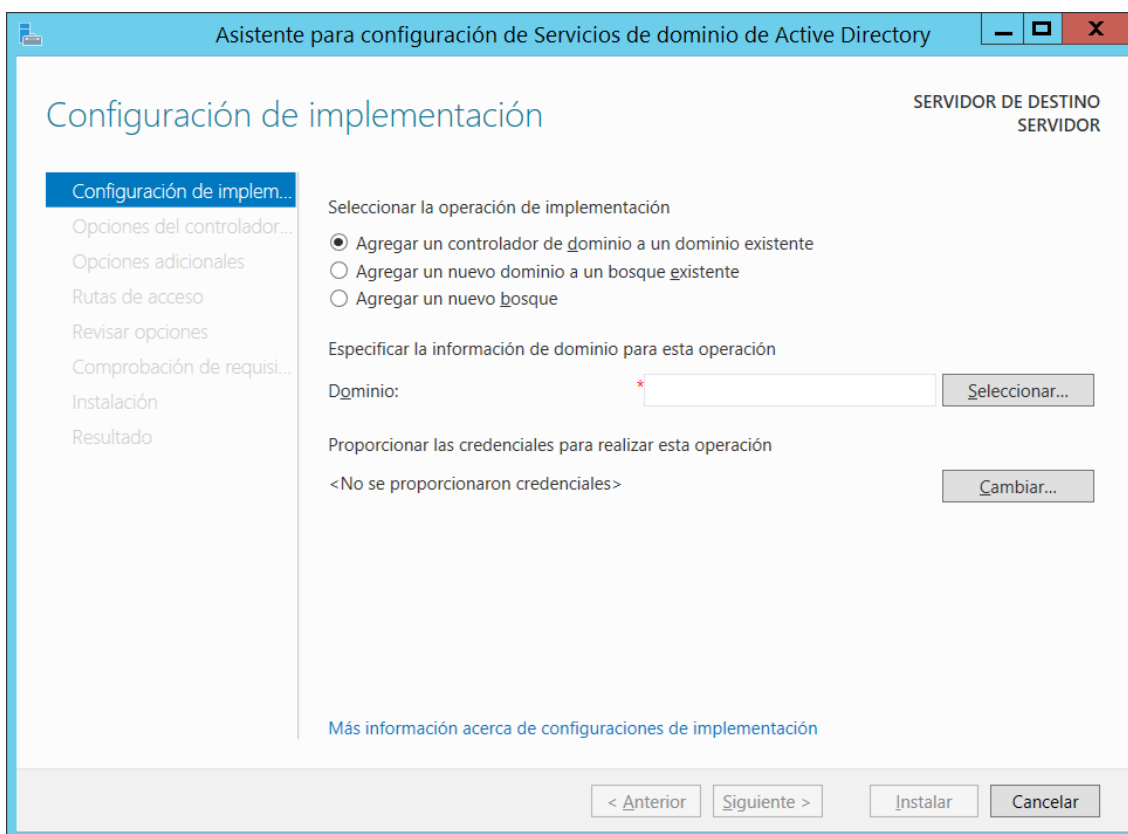


Esta xanela conten unha barra de progreso que nos indica en todo momento o progreso da instalación. Unha vez que a instalación finaliza amosarase a seguinte xanela:



Promoción do servidor a controlador de dominio

Neste momento o rol servizos de dominio de Active Directory está instalado, pero a máquina aínda non é un controlador de dominio. O servizo está instalado pero non está activado. Se queremos converter a máquina en controlador de dominio deberemos indicalo de modo que se active o servizo de AD. Para elo premeremos sobre o enlace que pon Promover este servidor a controlador de dominio. Opcionalmente poderíamos premer sobre o botón cerrar e realizar a promoción da máquina a controlador de dominio noutro momento. Neste caso imos facelo agora. Para elo prememos sobre o enlace Promover este servidor a controlador de dominio. Ao facelo amosarase a seguinte xanela:



Nesta xanela indicamos que estrutura de dominio imos a configurar (nun apartado posterior deste material falaremos respecto as diferentes estruturas de dominio existentes). O asistente ofrécenos tres opcións:

- Agregar el controlador de dominio a un dominio ya existente.
- Agregar un nuevo dominio a un bosque ya existente
- Agregar un nuevo bosque

No caso que estamos desenvolvendo eliximos a opción Agregar a un nuevo bosque xa que imos a crear un dominio novo e a máquina SERVIDOR vai ser o seu controlador de dominio. Ao seleccionar esta opción, indicaremos o nome que lle imos dar ao dominio. Neste caso imos crear un dominio chamado empresa.local:

Asistente para configuración de Servicios de dominio de Active Directory

Configuración de implementación

SERVIDOR DE DESTINO
SERVIDOR

Configuración de implem...

Opciones del controlador...

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisi...

Instalación

Resultado

Seleccionar la operación de implementación

☐ Agregar un controlador de dominio a un dominio existente

☐ Agregar un nuevo dominio a un bosque existente

☒ Agregar un nuevo bosque

Especificar la información de dominio para esta operación

Nombre de dominio raíz: empresa.local

Más información acerca de configuraciones de implementación

< Anterior

Siguiente >

Instalar

Cancelar

Prememos sobre o botón siguiente. Amósase a seguinte xanela:

Asistente para configuración de Servicios de dominio de Active Directory

Opciones del controlador de dominio

SERVIDOR DE DESTINO
SERVIDOR

Configuración de implem...

Opciones del controlador...

Opciones de DNS

Opciones adicionales

Rutas de acceso

Revisar opciones

Comprobación de requisi...

Instalación

Resultado

Seleccionar nivel funcional del nuevo bosque y dominio raíz

Nivel funcional del bosque: Windows Server 2012 R2

Nivel funcional del dominio: Windows Server 2012 R2

Especificar capacidades del controlador de dominio

☒ Servidor de Sistema de nombres de dominio (DNS)

☒ Catálogo global (GC)

☐ Controlador de dominio de solo lectura (RODC)

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

Contraseña: *

Confirmar contraseña: *

Más información acerca de opciones del controlador de dominio

< Anterior

Siguiente >

Instalar

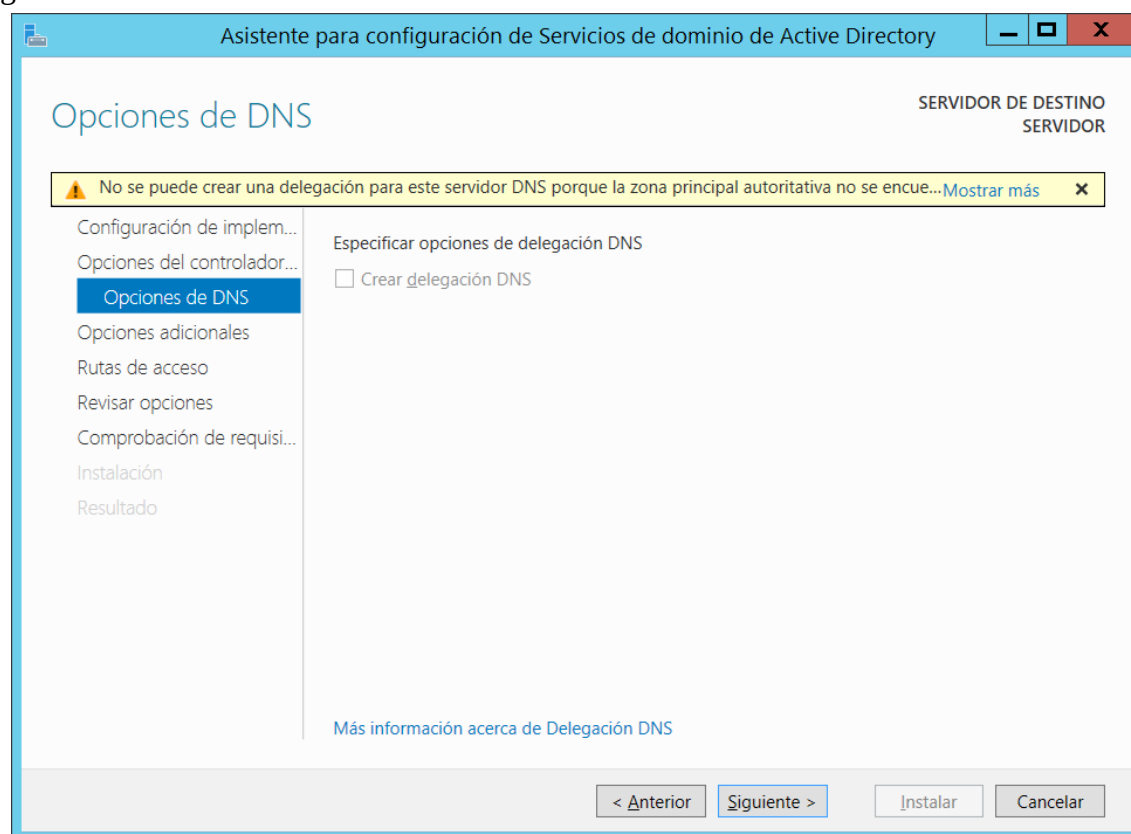
Cancelar

Mediante esta xanela configuramos as opcións principais do controlador de dominio. Mediante o despregable nivel funcional del bosque (como xa comentamos anteriormente, nun apartado posterior deste material falaremos respecto as diferentes estruturas de dominio existentes. Unicamente comentar que un bosque é unha destas estruturas. Podemos ver a un bosque como a suma de varios dominios) condicionamos os valores do despregable nivel funcional del dominio. Mediante o despregable nivel funcional del dominio indicamos os sistemas operativos admitidos nos controladores de dominio do bosque que imos crear. P.e, se seleccionamos como nivel funcional do bosque Windows Server 2012 R2, estamos indicando que no bosque os controladores de dominio deben ser Windows Server 2012 R2 y polo tanto no despregable nivel funcional del dominio unicamente poderemos elixir a opción Windows Server 2012 R2. Sen embargo, se en nivel funcional del bosque seleccionamos Windows Server 2008 R2, no despregable nivel funcional del dominio imos ter tres opcións: Windows Server 2008 R2, Windows Server 2012 e Windows Server 2012 R2, é dicir, Windows Server 2008 R2 e os produtos superiores. É importante elixir correctamente que sistemas operativos imos permitir instalar nos controladores de dominio do bosque xa que non tódolos sistemas operativos teñen as mesmas funcionalidades. Neste caso unicamente imos deixar instalar sistemas operativos de tipo Windows Server R2.

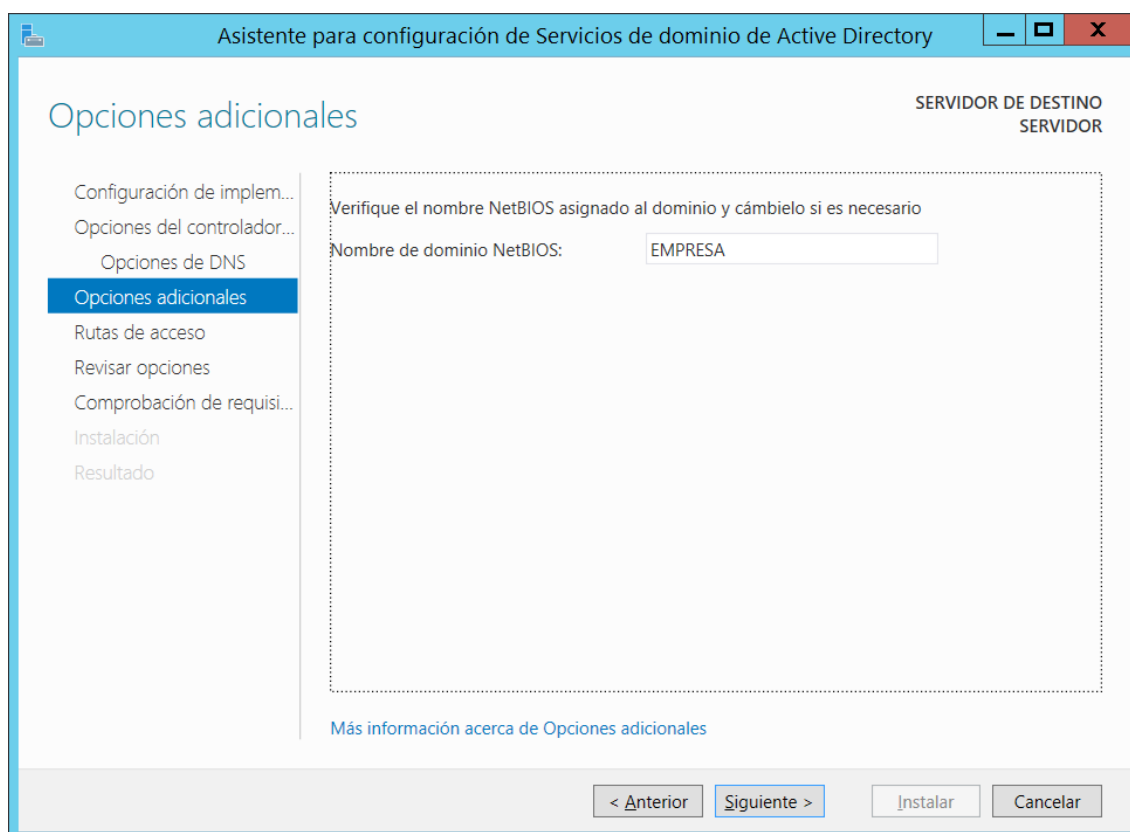
Mediante a activación da casilla de verificación Servidor de sistema de nombres de dominio (DNS) estamos indicando que o controlador de dominio tamén funcionará como servidor de DNS.

Por ultimo debemos escribir o contrasinal de modo de restauración de servizos de directorio. Este contrasinal emprégase para poder realizar unha conexión contra o controlador de dominio cando o AD falla.

Unha vez indicados tódolos campos prememos sobre o botón seguinte. Amósase a seguinte xanela:



Esta xanela emprégase para configurar opcións do DNS, pero como aínda non se creou o servidor de DNS, vains dar un erro que pódese ignorar. Prememos sobre seguinte. Abrirásenos a seguinte xanela:



Nesta xanela amósase cal é o nome NETBIOS (xa vimos nunha unidade didáctica previa que era NETBIOS) do dominio e opcionalmente permítenos modificalo. Prememos sobre o botón Siguiete. Amosase a seguinte xanela:

Asistente para configuración de Servicios de dominio de Active Directory

Rutas de acceso

SERVIDOR DE DESTINO
SERVIDOR

Configuración de implem...
Opciones del controlador...
Opciones de DNS
Opciones adicionales
Rutas de acceso
Revisar opciones
Comprobación de requisi...
Instalación
Resultado

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

Carpeta de la base de datos: C:\Windows\NTDS

Carpeta de archivos de registro: C:\Windows\NTDS

Carpeta SYSVOL: C:\Windows\SYSVOL

Más información acerca de Rutas de Active Directory

< Anterior Siguiente > Instalar Cancelar

Mediante esta xanela amósase onde vai ser almacenada a diferente información xestionada polo controlador de dominio. No caso de que queiramos que se garde noutra localización poderemos indicalo. Prememos sobre o botón seguinte e amosarase a seguinte xanela:

Asistente para configuración de Servicios de dominio de Active Directory

Revisar opciones

SERVIDOR DE DESTINO
SERVIDOR

Configuración de implem...
Opciones del controlador...
Opciones de DNS
Opciones adicionales
Rutas de acceso
Revisar opciones
Comprobación de requisi...
Instalación
Resultado

Revisar las selecciones:

Configura este servidor como el primer controlador de dominio de Active Directory en un nuevo bosque.

El nombre del nuevo dominio es "empresa.local". Éste es también el nombre del nuevo bosque.

El nombre NetBIOS del dominio es EMPRESA.

Nivel funcional del bosque: Windows Server 2012 R2

Nivel funcional del dominio: Windows Server 2012 R2

Opciones adicionales:

Catálogo global: Sí

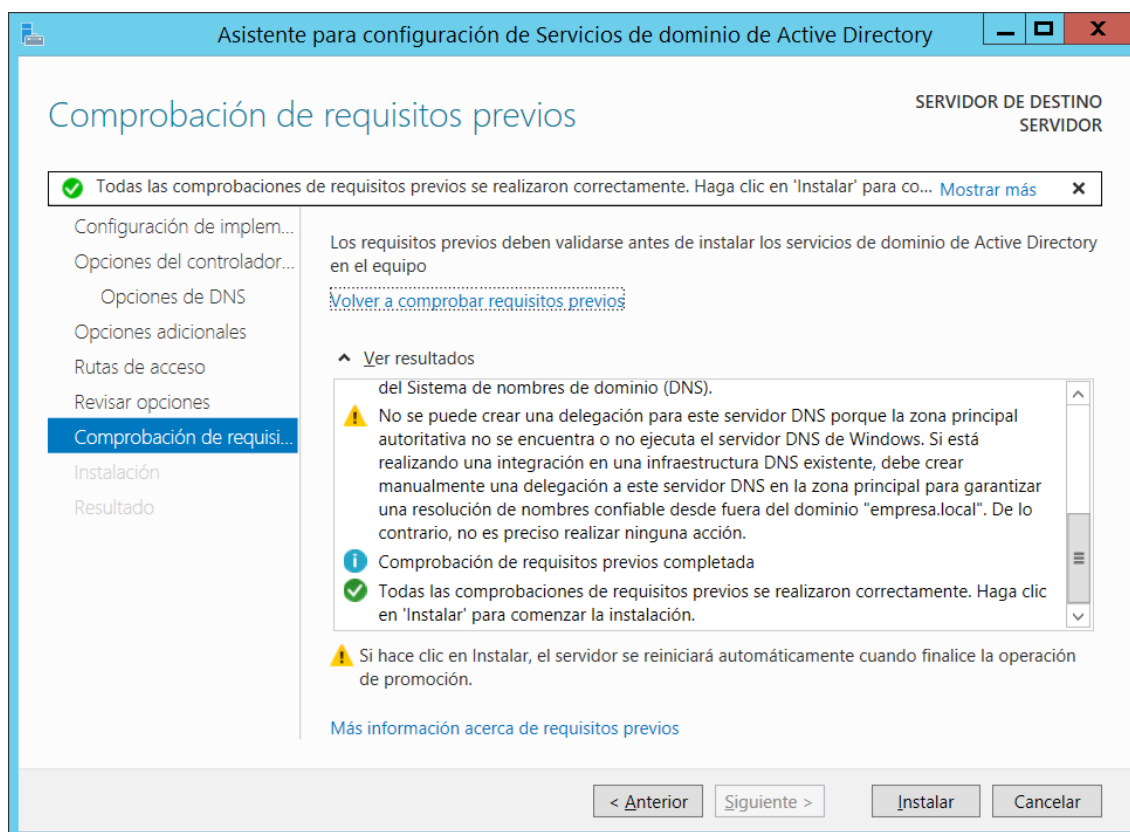
Servidor DNS: Sí

Esta configuración se puede exportar a un script de Windows PowerShell para automatizar instalaciones adicionales

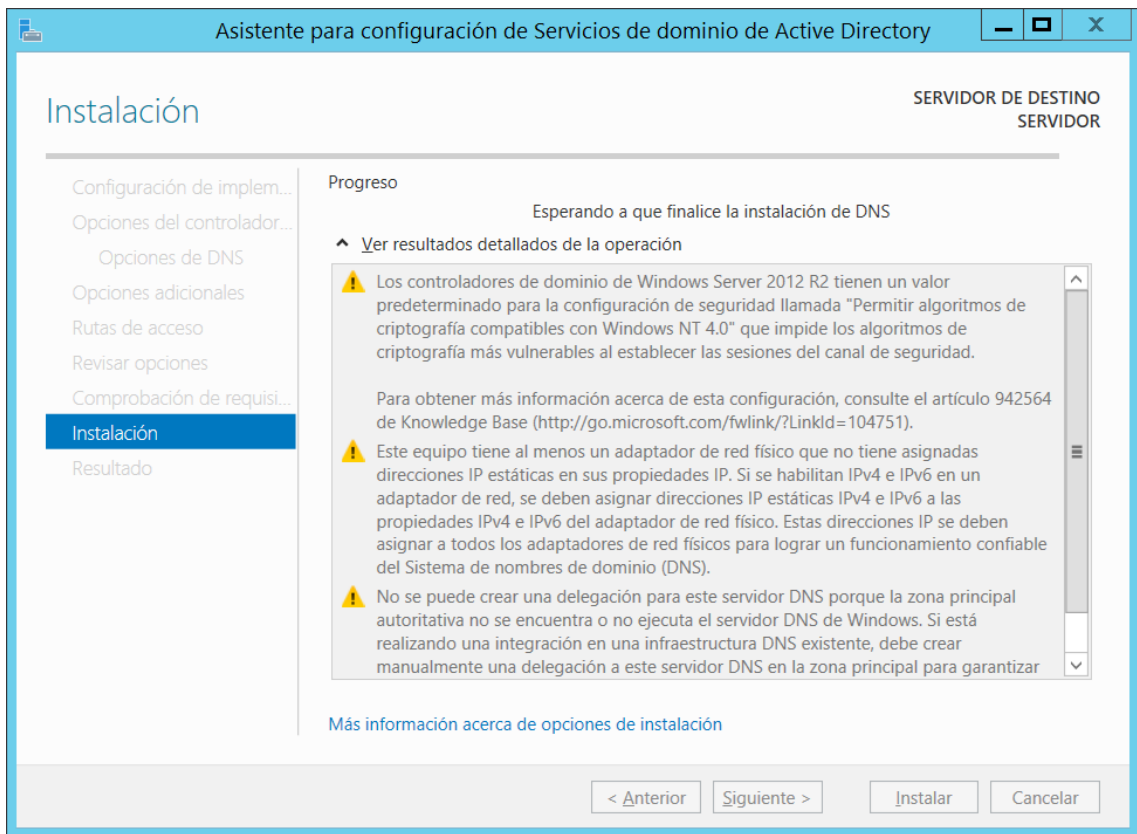
Más información acerca de opciones de instalación

< Anterior Siguiente > Instalar Cancelar

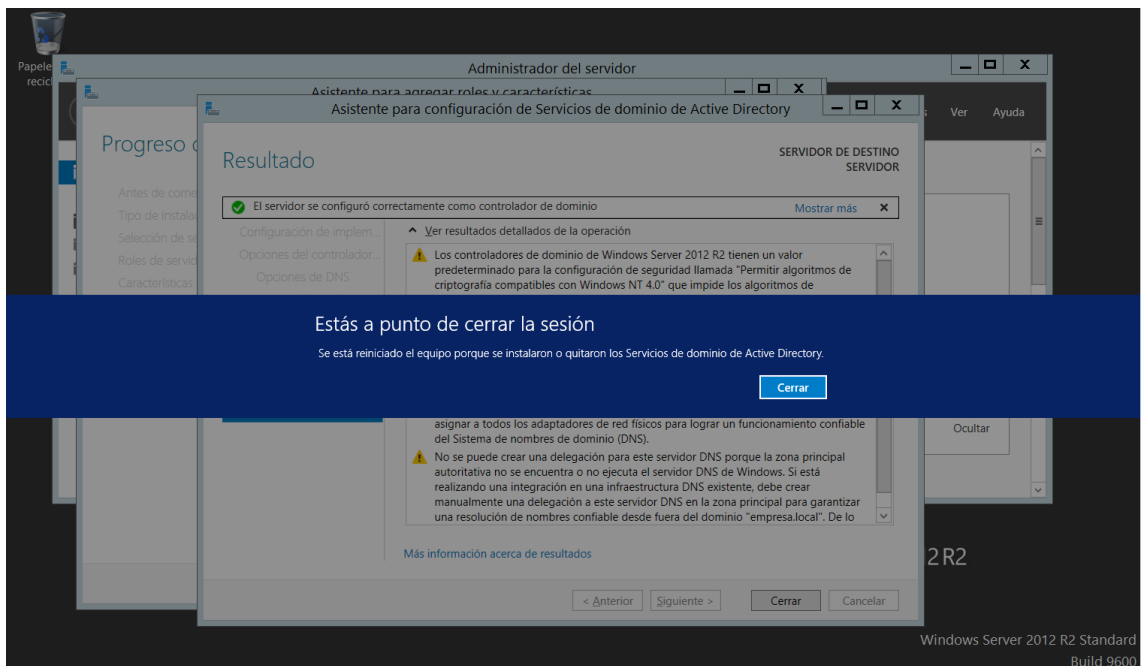
Esta xanela amosa un resumo de tódalas opcións seleccionadas, de modo que deberemos comprobar que todo é correcto antes de que se leve a cabo o proceso de activación do servizo de dominio de AD coa configuración indicada. Cando esteamos seguros de que a configuración é a que queremos premeremos sobre o botón seguinte. Amonosarase a seguinte xanela:



Antes de activarse o servizo de dominio de AD, o sistema operativo realiza unha comprobación para determinar se é posible activalo ou se existe algunha circunstancia que o impide. Se o servizo de dominio de AD pode ser activado se indicará nesta xanela e o único que deberemos facer é premer sobre o botón instalar para proceder á súa activación. Durante o proceso de activación informarase ao usuario das diferentes tarefas que se están a realizar:

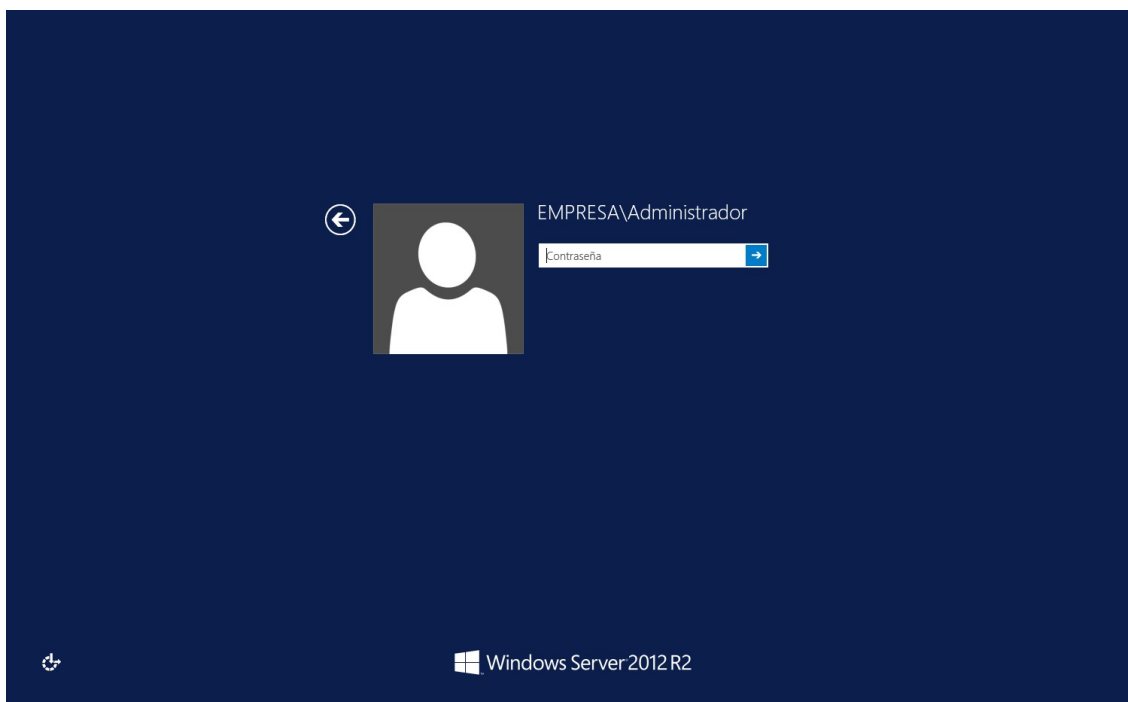


Unha vez que remata o proceso de activación do servizo de dominio de AD o sistema operativo amosa a seguinte xanela:



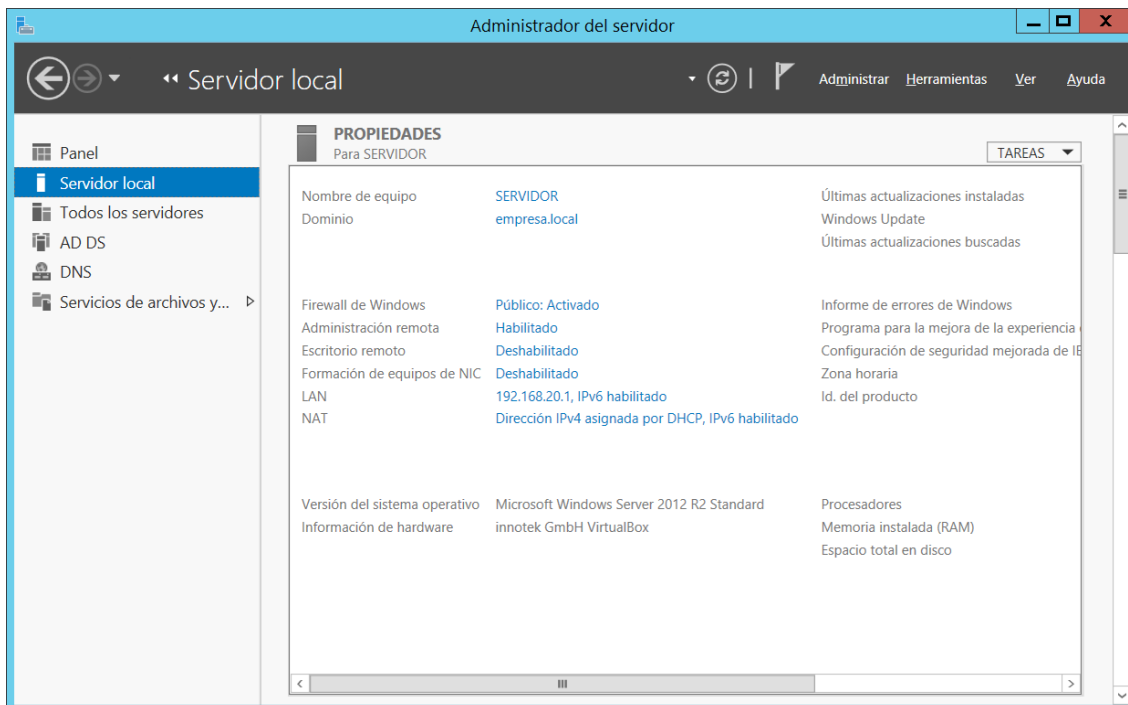
Dominio activado

Finalmente o sistema operativo reinicia o equipo. Ao iniciar de novo o sistema xa é un controlador de dominio. O primeiro indicio de isto é a propia xanela de identificación de entrada no sistema:

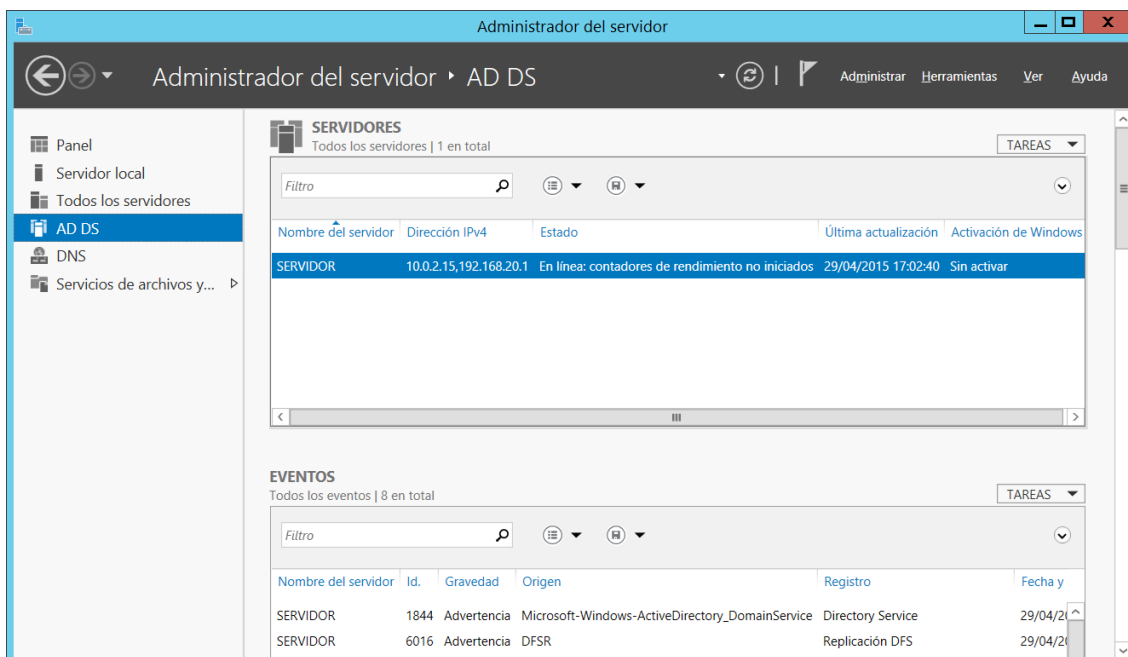


Como pódese observar na imaxe anterior, estásenos a solicitar o contrasinal para o usuario Administrador do dominio EMPRESA (EMPRESA/Administrador). Se entramos no sistema utilizando este usuario, o estaremos facendo cun usuario do dominio EMPRESA. Se quixeramos entrar cun usuario local da máquina e non cun usuario do dominio deberíamos premer na frecha que aparece na imaxe anterior, seleccionar Otro usuario na nova xanela que se abre e indicar como nome de usuario SERVIDOR/NombreUsuarioLocal. P.e.: SERVIDOR/Administrador. Deste modo o que estaremos a facer é autenticarnos contra a base de datos de usuarios locais da máquina SERVIDOR en lugar de facelo contra a base de datos do AD.

Nesta ocasión identificarémonos contra a base de datos do AD, é dicir, identificarémonos no sistema empregando o usuario EMPRESA/Administrador. Unha vez que entremos imos acceder ás propiedades do servidor local desde a xanela de administración do servidor. Amosarase a seguinte xanela:



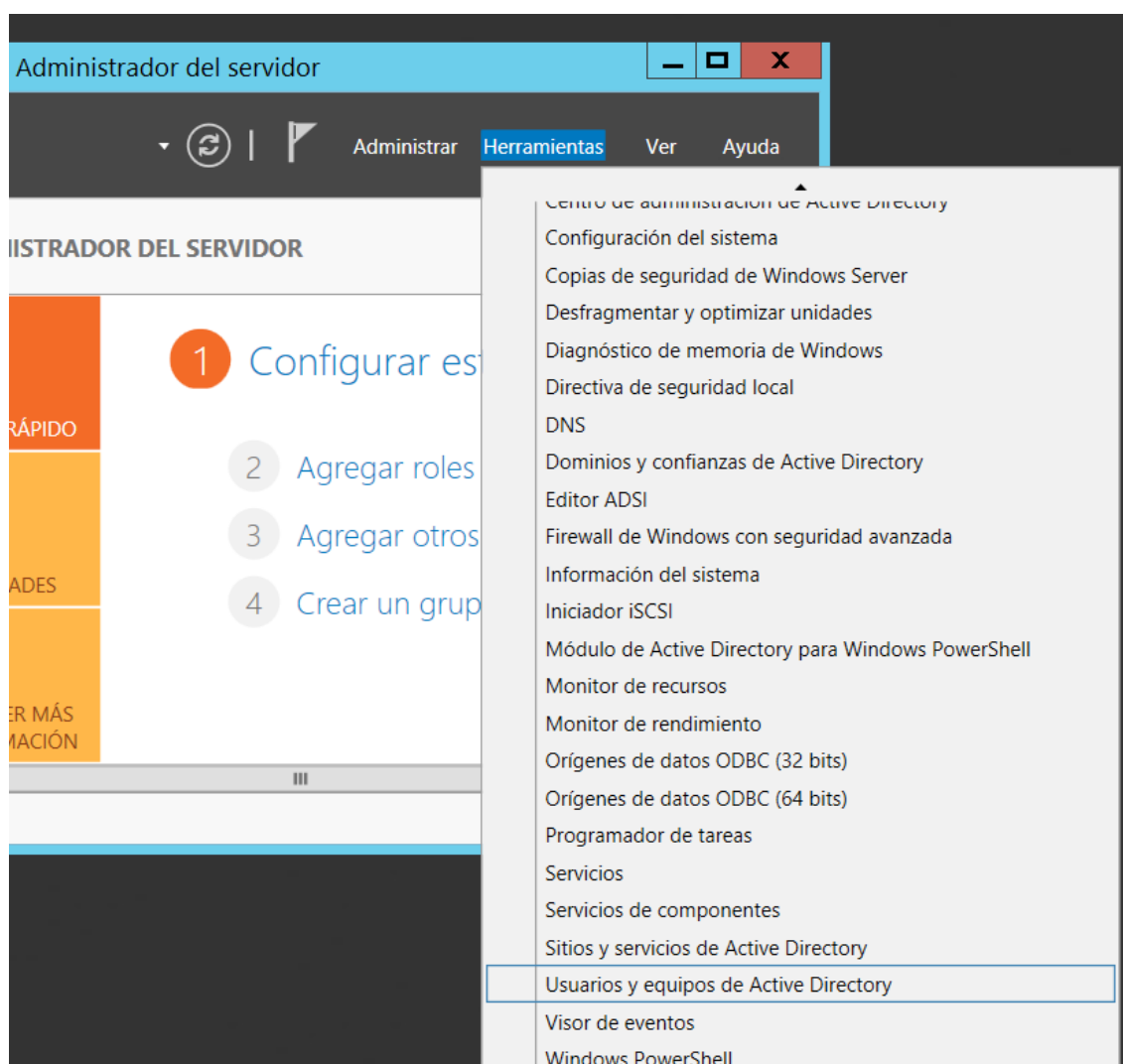
Como pódese observar na imaxe previa, o equipo SERVIDOR está no dominio empresa.local. Ademais, no administrador do servidor vemos que engadíronse novos elementos no menú da esquerda. Estes novos elementos son AD DS e DNS. AD DS empregarémosto para recoller información sobre os controladores de dominio, mentres que mediante DNS poderemos acceder á información referente ao servidor de DNS. Se prememos sobre AD DS amósase información dos controladores de dominio. Neste caso unicamente aparécenos un equipo, o equipo SERVIDOR, xa que é o único controlador de dominio existente:



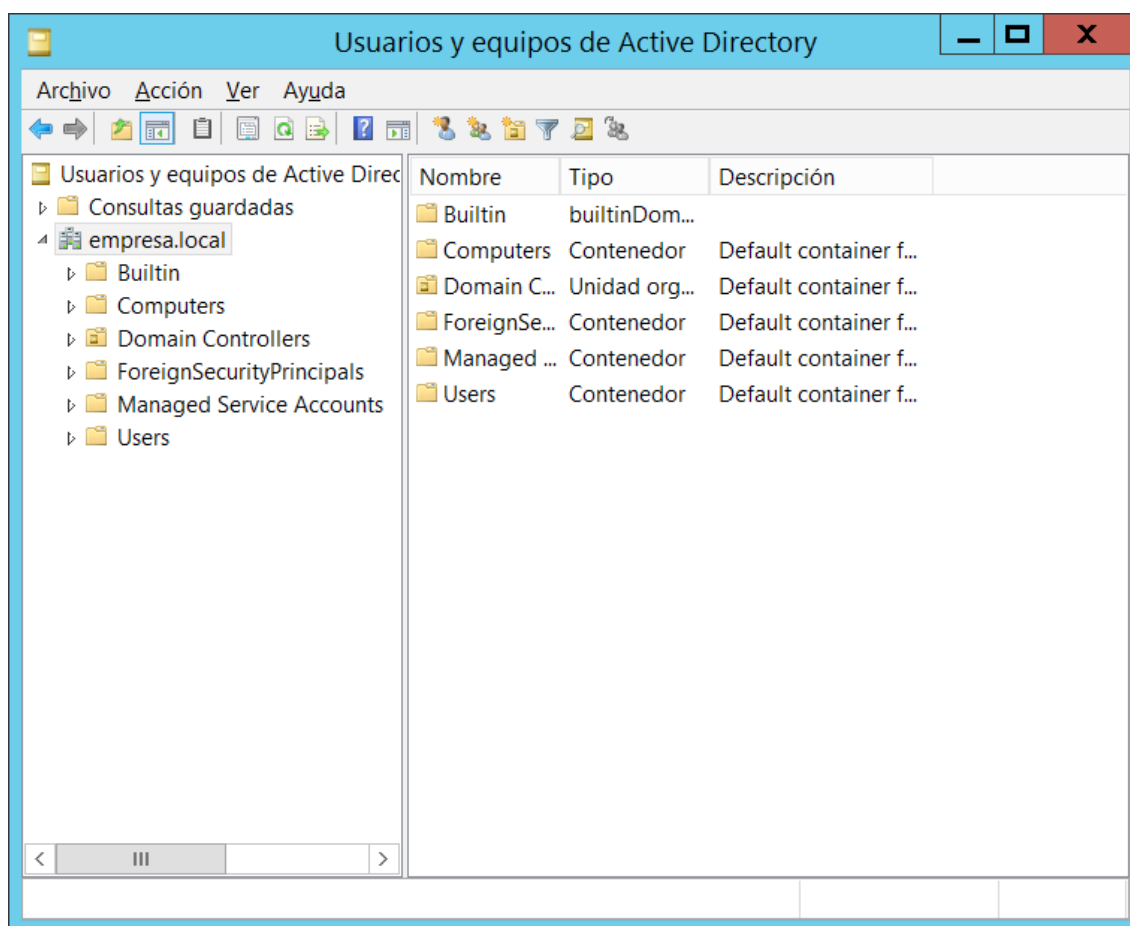
Una vez que temos funcionando o controlador de dominio estamos en disposición de administralo co fin de xestionar os recursos informáticos da nosa organización.

Ferramenta de usuarios e equipos de Active directory

Unha vez que temos instalado o servizo de directorio activo nunha máquina e promovémola a controlador de dominio é necesario configurar os diferentes obxectos que van formar parte do dominio. Ditos obxectos principalmente son as unidades organizativas, os usuarios, os grupos e os equipos. Co fin de xestionar estes obxectos do AD temos diferentes ferramentas. Merece mención especial pola súa facilidade de emprego unha ferramenta denominada usuarios e equipos de active directory. Podemos acceder a esta ferramenta de múltiples formas, p.e: abrimos o administrador do servidor, prememos en herramientas e por último seleccionamos a opción de menú usuarios y equipos de active directory:



O aspecto da ferramenta é o seguinte:



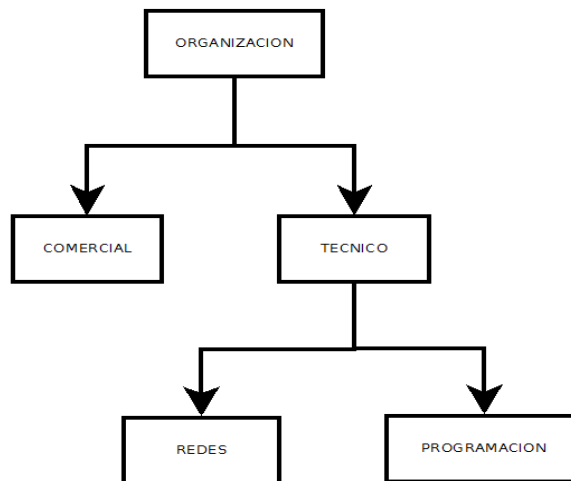
Como pódese observar na imaxe amosase o nome do dominio administrado polo controlador de dominio instalado no equipo (aínda que sería posible empregar esta ferramenta para conectarse a outro dominio e administralo). Dentro do dominio podemos observar a existencia dunha estrutura de carpetas que se emprega para organizar os diferentes obxectos existentes no dominio. Esta estrutura pode ser modificada para axustala ás necesidades de calquera dominio.

A ferramenta de usuarios e equipos de active directory amósanos os contidos da base de datos de AD e ademais proporcionáanos os procedementos necesarios para modificar dita base de datos de modo que a poidamos axustar ás nosas necesidades.

1.2.4 Unidades organizativas

Unha vez que temos instalado e activado un dominio o seguinte paso é crear as unidades organizativas (UO). As UOs son contedores nos cales podemos colocar usuarios, grupos, equipos e outras UOs. As UOs permítenos plasmar nunha estrutura lóxica a estrutura física dunha organización.

Imaxinemos p.e. que queremos administrar unha organización mediante unha estrutura de dominio e a estrutura física de dita organización está composta por dous departamentos: o departamento técnico e o departamento comercial. Ademais, á súa vez o departamento técnico divídese no subdepartamento de programación e no subdepartamento de redes:



Traducir o esquema anterior a un esquema lóxico sería tan sinxelo como crear as seguintes UOs dentro do dominio:

- UO COMERCIAL
- UO TECNICO

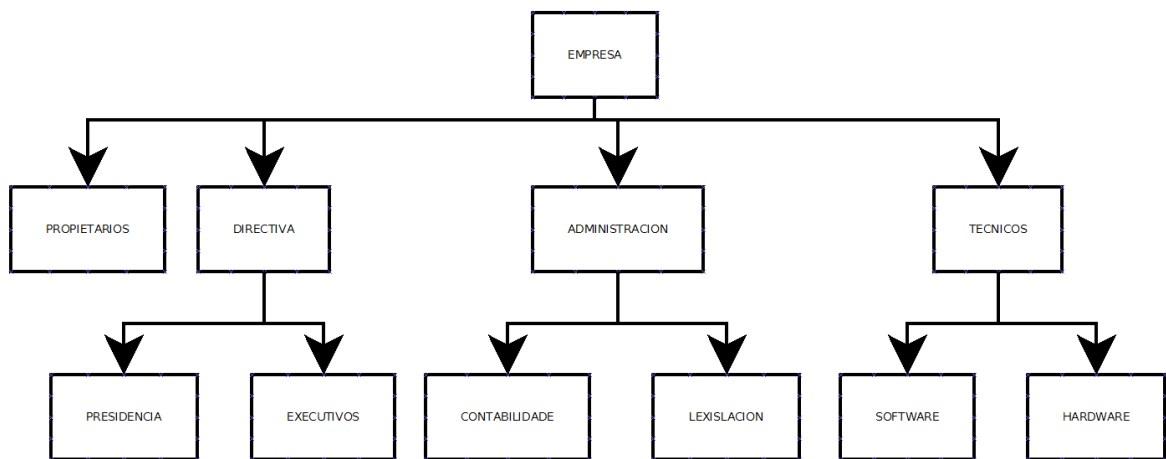
e dentro da UO TECNICO crearíamos dúas unidades organizativas máis que serían:

- UO REDES
- UO PROGRAMACION

Como pódese observar as UOs, ao igual que os departamentos dunha empresa organízanse nunha estrutura xerárquica en forma de árbore. Pero, ¿que nos aporta unha UO?. Partindo do exemplo que acabamos de expoñer, na empresa ademais de existir departamentos haberá traballadores que traballarán para os diferentes departamentos. Cada un destes traballadores necesitará un usuario para poder conectarse ao dominio da empresa a través do sistema informático. Os usuarios creados categorizaranse empregando as UOs, de modo que p.e, todos aqueles usuarios dos traballadores que pertencen ao departamento comercial serán asignados á UO COMERCIAL. Evidentemente a utilidade final das UOs non é simplemente a de clasificar aos usuarios. A utilidade final é a de poder aplicar directivas aos diferentes elementos que conforman unha UO. As directivas serán vistas en profundidade máis adiante. A súa finalidade é permitir fixar restricións de funcionamento sobre o modo de operar no dominio, p.e. imaxinemos que queremos que os usuarios que pertencen á UO COMERCIAL non poidan acceder ao panel de control en aqueles equipos desde os que se poden conectar. Sin entrar en detalles, o que faríamos sería crear unha directiva que indique que a aqueles usuarios aos que se lles aplique no poderán acceder ao panel de control. A continuación aplicaríamos esta directiva sobre a UO COMERCIAL. A aplicación da directiva á UO COMERCIAL dará lugar a que tódolos usuarios que pertencen a ela non poderán acceder ao panel de control.

Creación de unidades organizativas

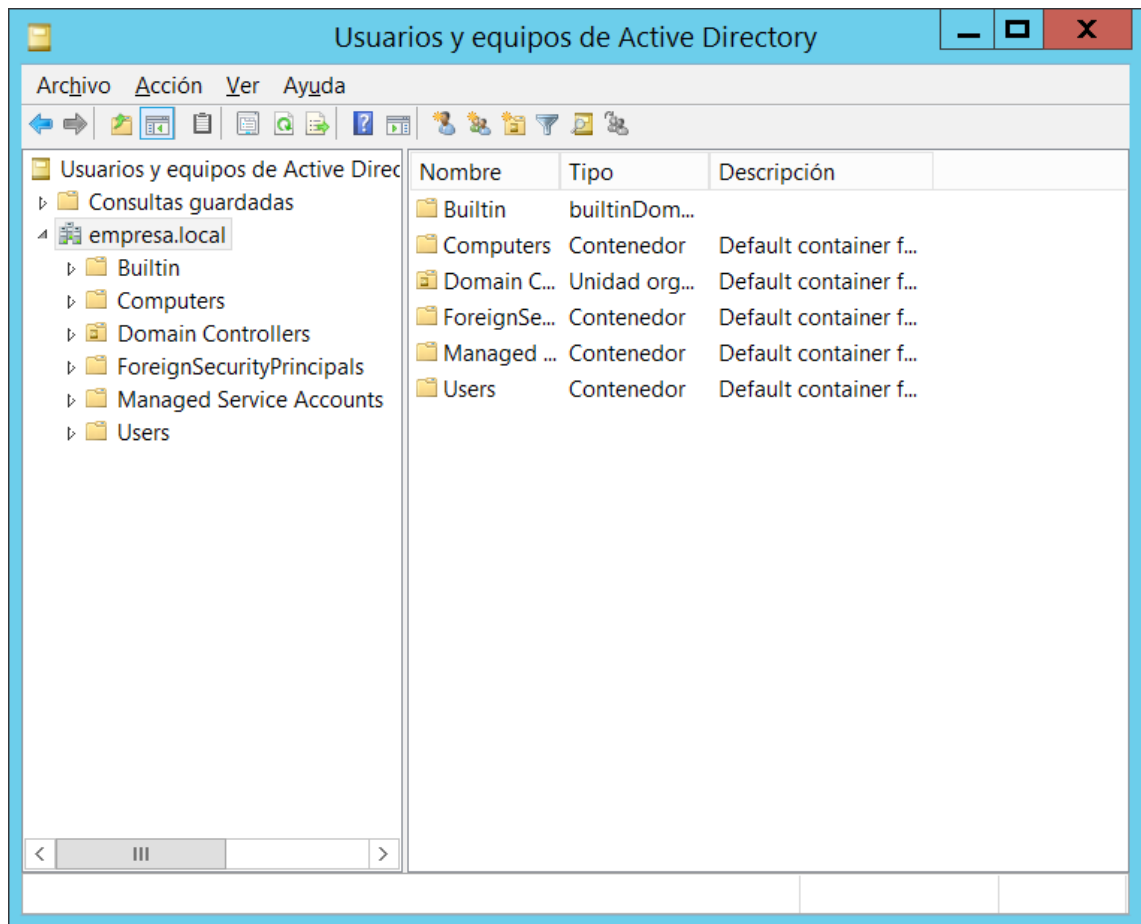
Partindo do dominio empresa.local creado con anterioridade para una empresa xenérica, imos crear as UOs que definen a estrutura lóxica de dita empresa no dominio. A estrutura física real da empresa que queremos definir mediante o uso de UOs é a seguinte:



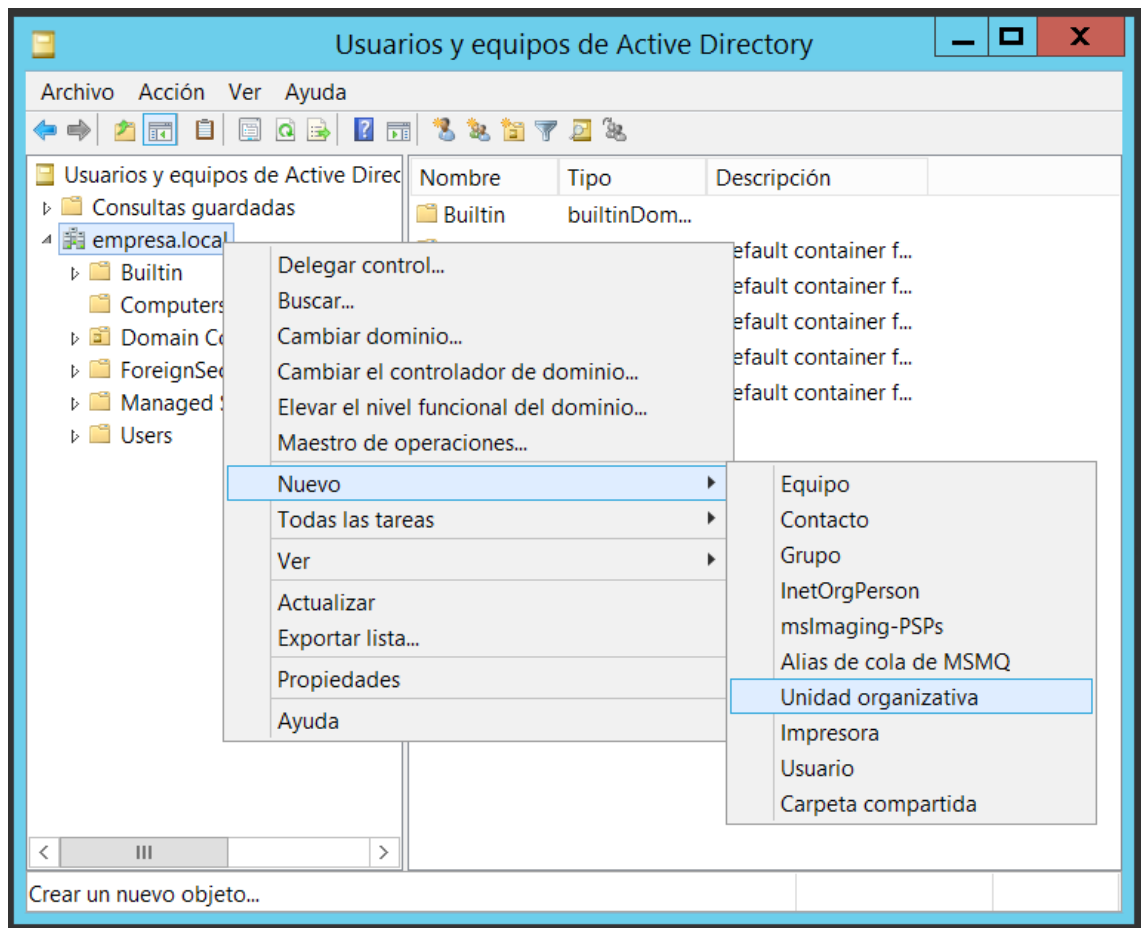
A empresa está dividida en catro grandes bloques. Imos ver cada un deles:

- Propietarios: dentro deste bloque englóbanse as persoas propietarias da empresa.
- Directiva: dentro deste bloque englóbanse as persoas que dirixen o funcionamento da empresa. Á súa vez divídese en dous bloques:
 - Presidencia: persoa que dirixe a empresa. É a persoa responsable da empresa. Toma as decisións finais para o funcionamento da empresa.
 - Executivos: dentro deste bloque englóbanse as persoas que se encargan de asesorar á presidencia.
- Administración: dentro deste bloque englóbanse as persoas que se encargan da administración da empresa. Á súa vez divídese en dous bloques:
 - Contabilidade: persoal que se encarga de xestionar a contabilidade da empresa.
 - Lexislación: persoal que se encarga de adecuar o funcionamento da empresa ao marco legal existente en cada momento.
- Técnicos: dentro deste bloque englóbanse as persoas que se encargan de actividades técnicas dentro da empresa. Á súa vez divídese en dous bloques:
 - Software: engloba ao persoal que xestiona o software da empresa.
 - Hardware: engloba ao persoal que xestiona o hardware da empresa.

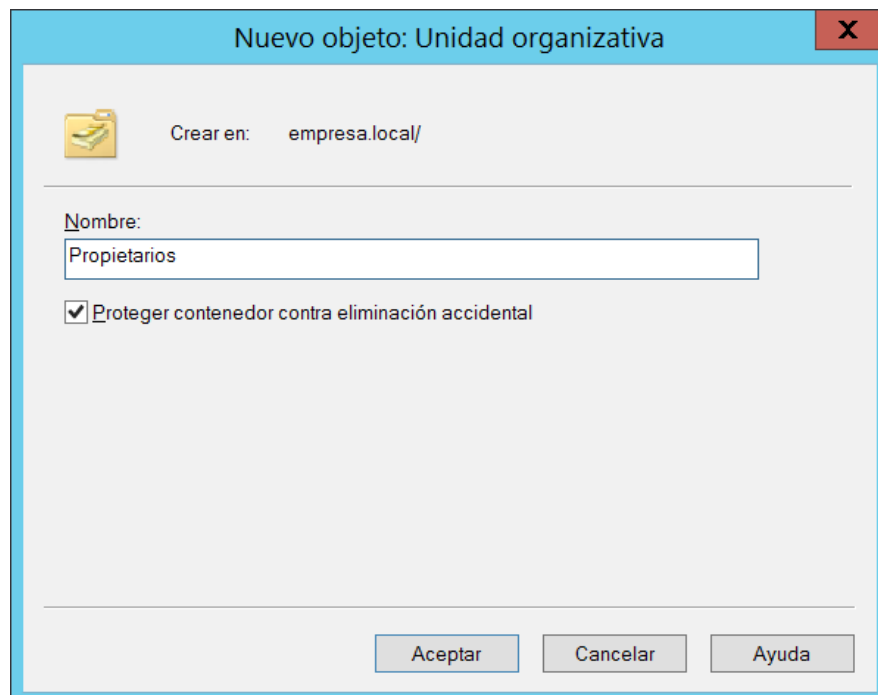
Unha vez definida a estrutura física da empresa imos plasmalo nunha estrutura lóxica mediante o emprego de UOs. Para xestionar as UOs utilizaremos a ferramenta usuarios e equipos de AD. Abrimos a ferramenta. Amosarase a seguinte pantalla:



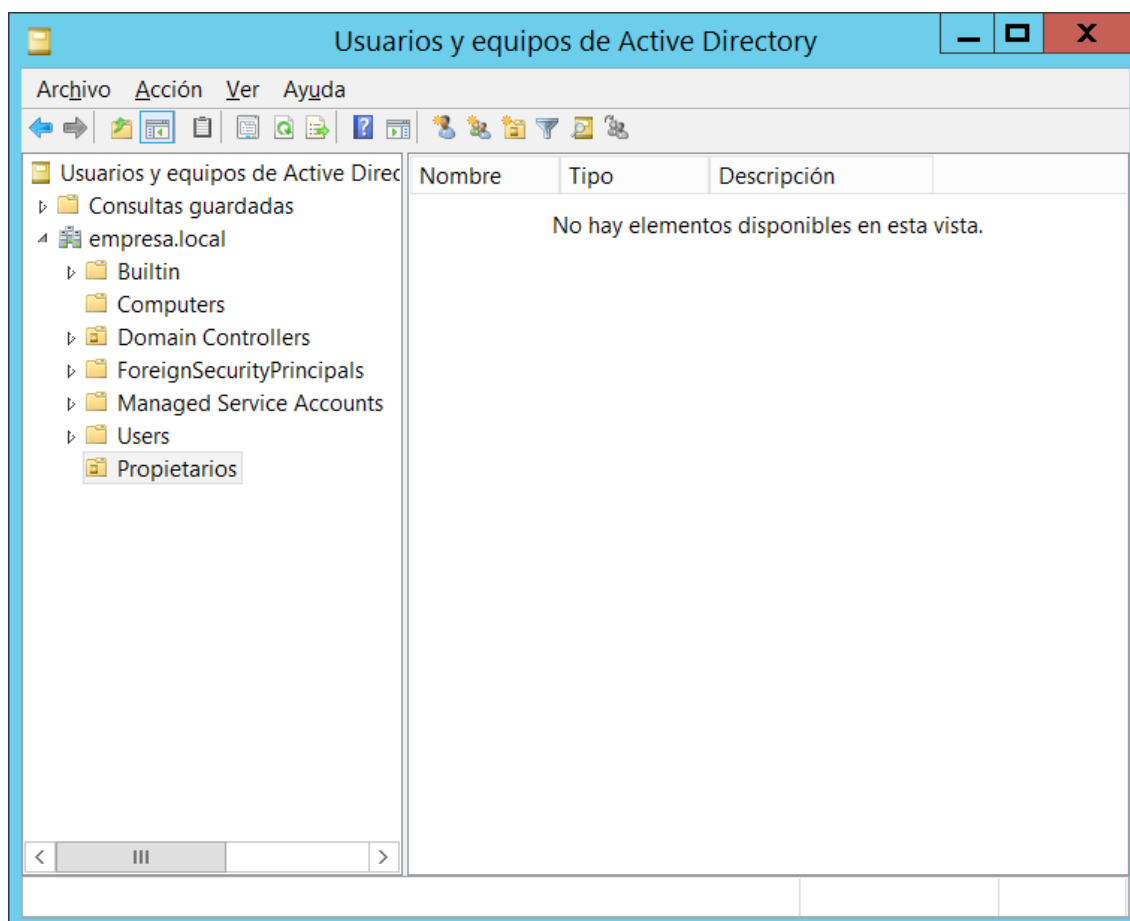
A continuación imos crear a primeira UO. Neste caso será Propietarios. Para elo prememos co botón dereito sobre o nome do dominio. Despregarase un menú contextual. Nel eliximos a opción nuevo de modo que se despregará un submenú. Neste submenú elixiremos a opción unidad organizativa:



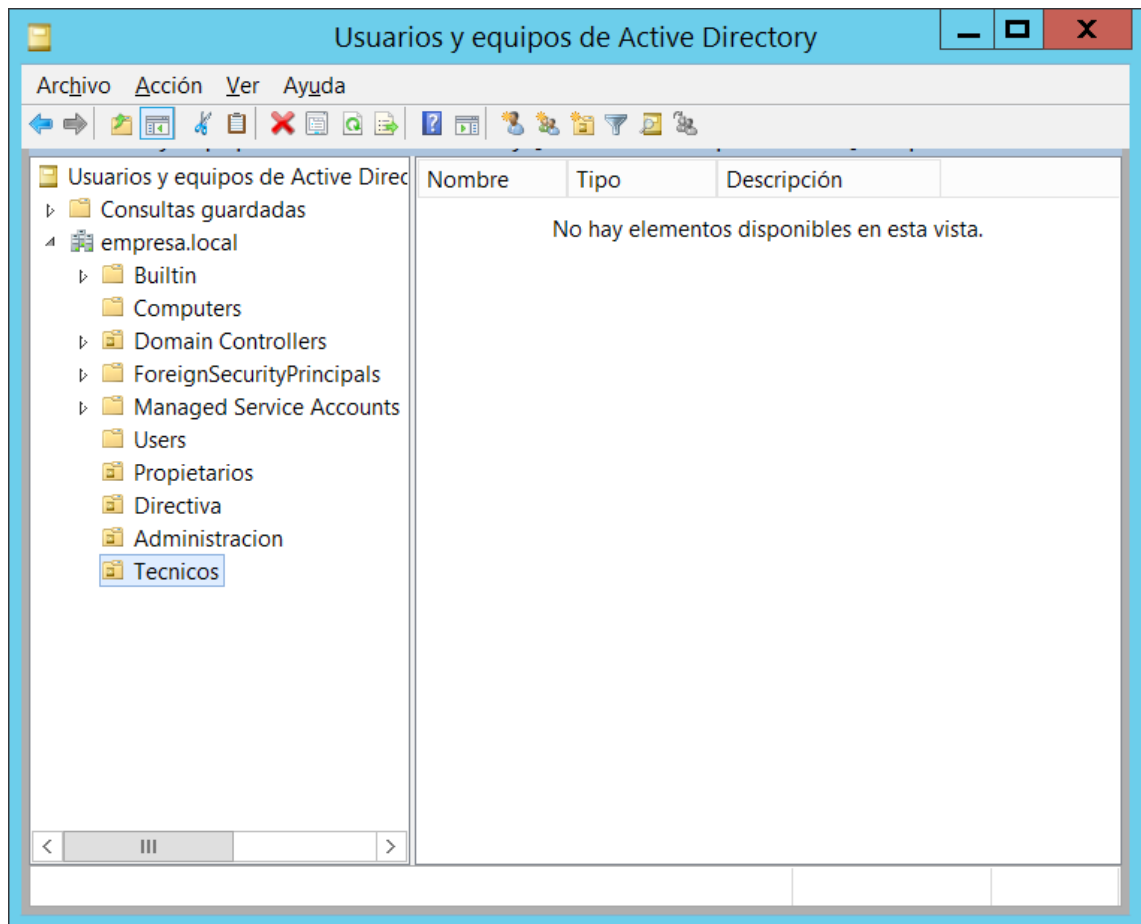
Ao seleccionar a opción unidade organizativa abrírase unha pantalla na cal indicaremos o nome da UO que queremos crear:



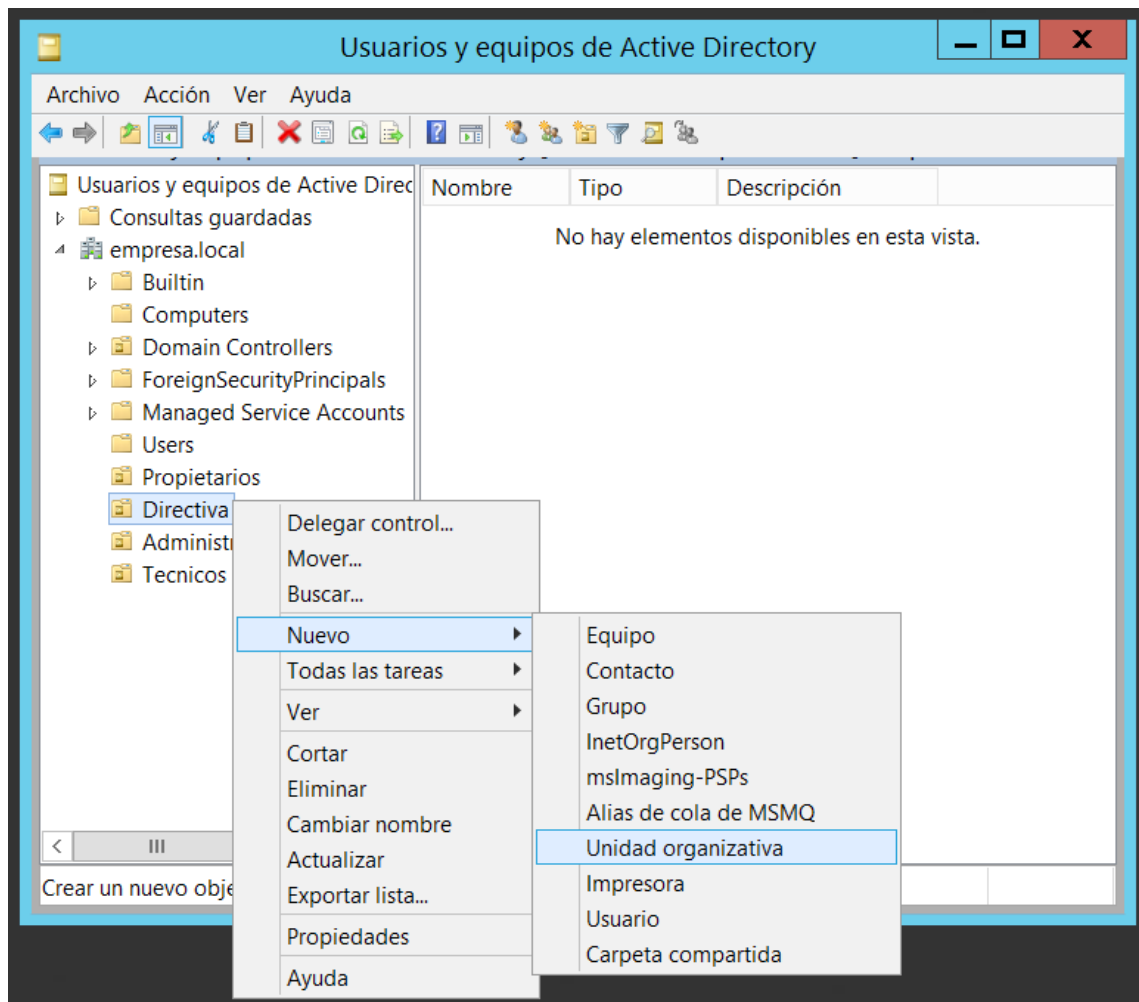
Prememos sobre o botón aceptar e a UO será creada:



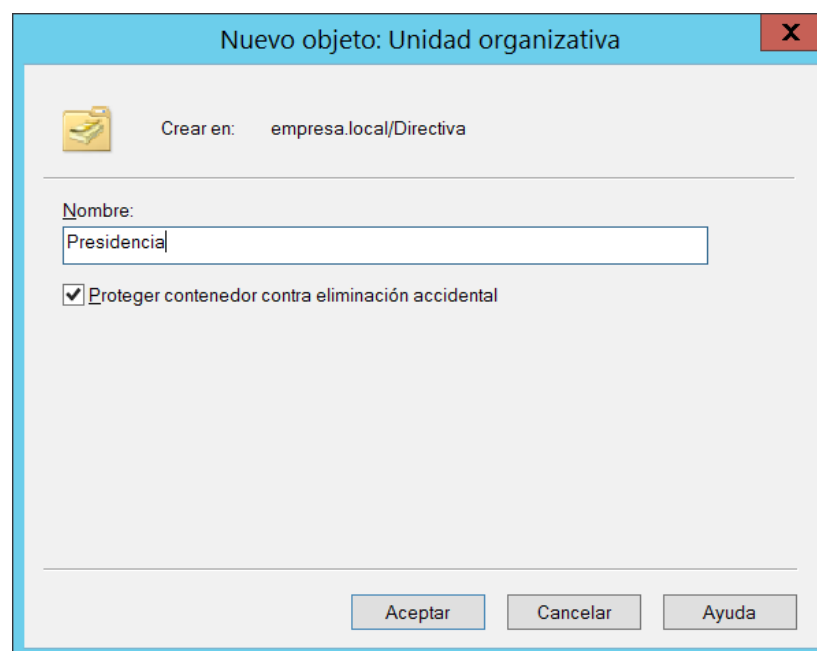
Repetiremos os pasos anteriores para as UOs Directiva, Administracion e Tecnicos, sendo o resultado o seguinte:



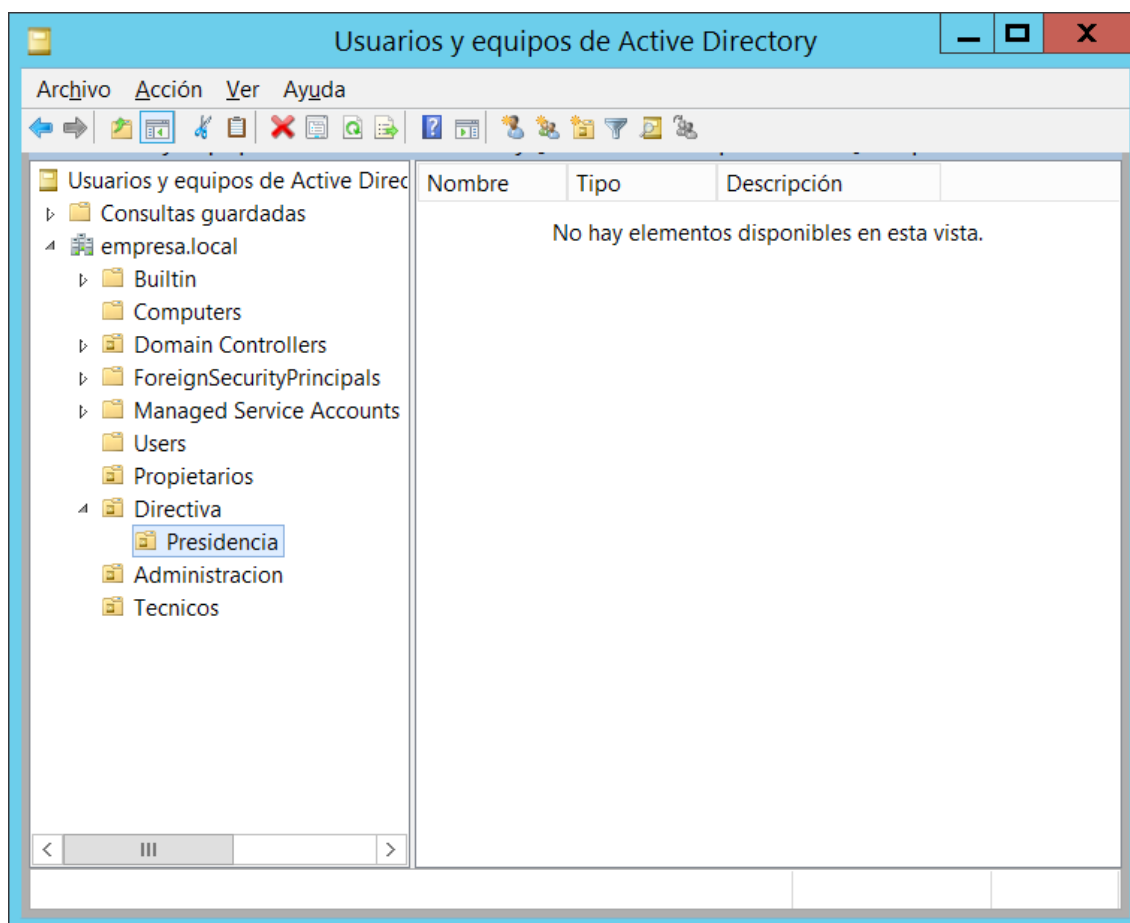
Acabamos de traducir o primeiro nivel da estrutura física da organización a unha estrutura lóxica. A continuación imos ver como creamos no AD as UOs que representan aos niveis inferiores da organización. Vexámolo coa UO Presidencia. A UO Presidencia colga da UO Directiva. Para crear esta UO faremos o seguinte: prememos co botón dereito sobre a UO Directiva. Despregarase un menú contextual. Nel eliximos a opción nuevo, de modo que se despregará un submenú. Neste submenú elixiremos a opción unidad organizativa:



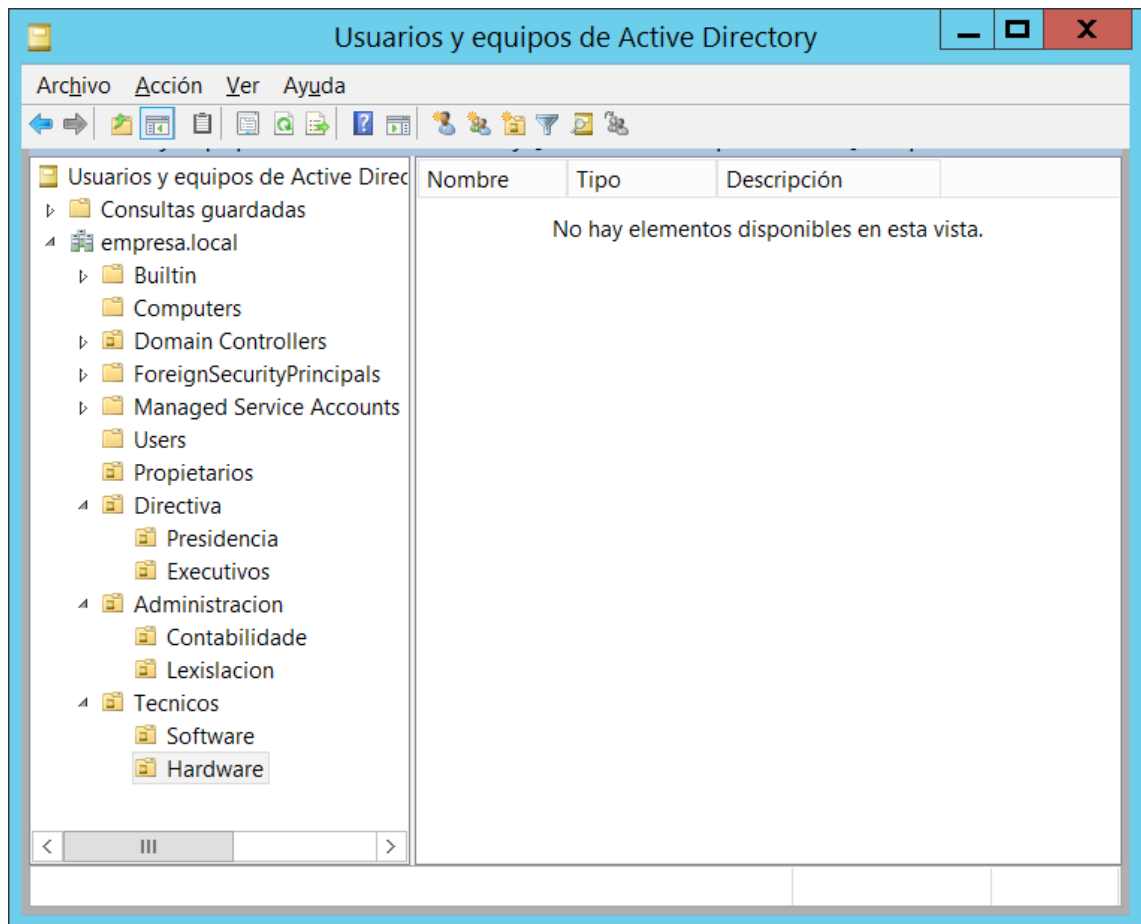
e repetimos o proceso descrito anteriormente para definir o nome da nova UO que imos crear:



Unha vez creada a UO Presidencia este será o aspecto dos obxectos creados no dominio:



Como pódese observar na imaxe, a UO Presidencia colga da UO Directiva tal e como ocorre na estrutura física que representa á empresa. Repetiremos o proceso tantas veces como sexa necesario co fin de crear o resto de UOs que compoñen o dominio. Unha vez que finalicemos este será o resultado:



Agora si que podemos dicir que o AD contén unha representación lóxica da estrutura física da organización. As UOs que acabamos de crear poden ser renomeadas, modificadas ou movidas a outras UOs de ser preciso. Ademais podemos engadir máis UOs en calquera momento para adaptar a estrutura lóxica do dominio aos posibles cambios que se poden dar ao longo do tempo sobre a estrutura física da empresa. É dicir, AD é un elemento flexible e dinámico que pode ser modificado en calquera momento co fin de adecuar a súa estrutura á da empresa.

Creación de unidades organizativas mediante comandos

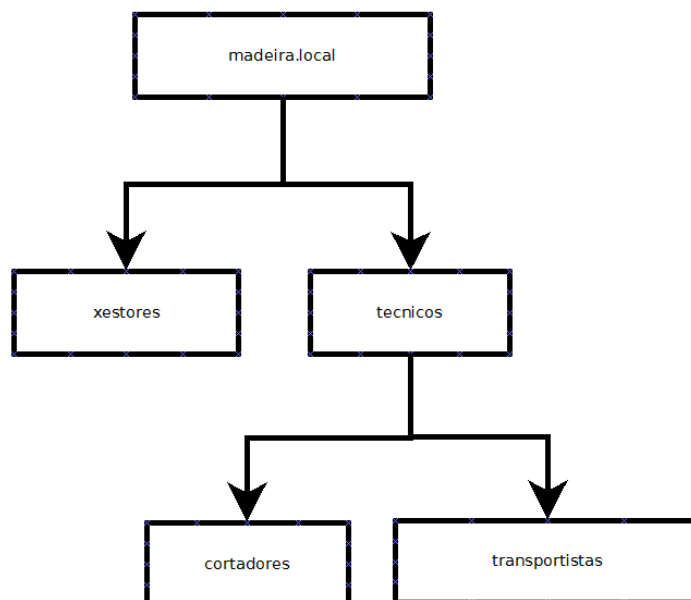
Nomenclatura LDAP

Tal como indicouse con anterioridade, Windows Server fai uso de varios protocolos para funcionar. Un de eles é o protocolo LDAP. En realidade LDAP é unha implementación lixeira doutro protocolo chamado DAP (directory access protocol). Á súa vez DAP está incluído dentro dunha serie de estándares chamado X.500 que se utilizaba para servizos de directorio. Debido a esta ligazón histórica, Windows Server utiliza unha nomenclatura similar á de X.500 para xestionar a localización dos diferentes obxectos existentes dentro da base de datos de AD. Cada un dos elementos existentes na base de datos de AD pode ser identificado dun modo unívoco utilizando para elo unha nomenclatura herdada dos estándares X.500.

- DN: Distinguished Name.
- RDN: Relative Distinguished Name.

- DC: Domain Component.
- OU: Organizational Unit.
- CN: Common Name.

Facendo uso desta nomenclatura é posible xestionar a base de datos de AD. A continuación imos ver a través dun exemplo para comprendelo como identificar no AD aos obxectos de tipo UO dun dominio. Supoñamos que temos o dominio madeira.local coas seguintes UO:



O identificador da UO xestores sería o seguinte: ou=xestores, dc=madeira, dc=local. A este identificador chámase distinguish name (DN). Polo tanto o DN de xestores é ou=xestores, dc=madeira, dc=local.

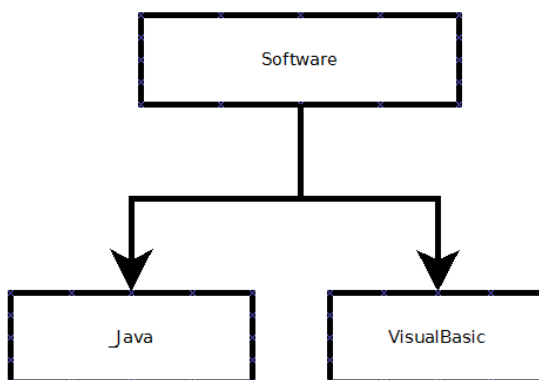
¿Porque isto é así?. O primeiro que temos que indicar é o significado de dc e ou. A cadea dc fai referencia a domain controller e a cadea ou a organizational unit name. Agora a solución xa é máis evidente. Para o caso da UO xestores, vemos na árbore do dominio que colga directamente do controlador de dominio madeiras.local. Para construír o DN dunha UO unicamente temos que percorrer a árbore do dominio desde a UO da cal queremos calcular o seu DN ata a raíz da árbore. Para cada elemento que atopemos que sexa unha UO engadiremos ao DN a cadea ou=nombre_UO. Cando atopemos o nome do dominio, para cada un das compoñentes do seu FQDN engadiremos ao DN a cadea dc=componente_FQDN. Seguindo estas regras imos ver os DN das catro UO anteriores:

UO	DN
xestores	ou=xestores,dc=madeira,dc=local
tecnicos	ou=tecnicos,dc=madeira,dc=local
cortadores	ou=cortadores,ou=tecnicos,dc=madeira,dc=local
transportistas	ou=transportistas,ou=tecnicos,dc=madeira,dc=local

Comando csvde

Facendo uso da nomenclatura empregada para lidiar directamente coa base de datos do AD, imos crear UOs directamente desde a consola de comandos.

Partindo das UOs xa creadas sobre o dominio empresa.local imos engadir un par de UOs máis ás xa existentes. Colgando da UO existente chamada Software imos colgar dous UOs. Unha chamarase Java e a outra VisualBasic:



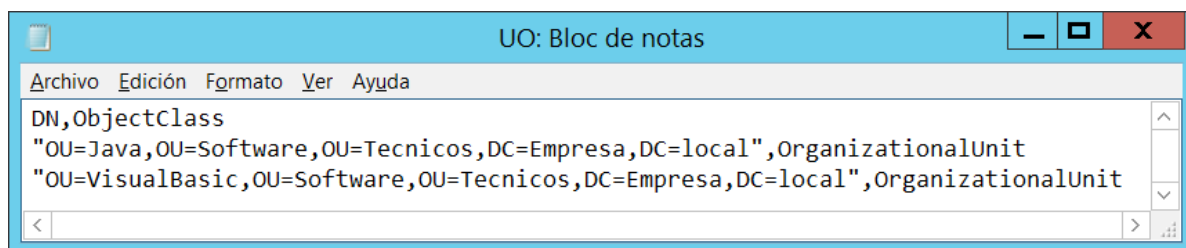
O primeiro imos calcular os DN das UOs que queremos engadir ao AD:

UO	DN
Java	ou=Java,ou=Software,ou=Tecnicos,dc=empresa,dc=local
VisualBasic	ou=VisualBasic,ou=Software,ou=Tecnicos,dc=empresa,dc=local

Para realizar el alta das UOs no AD a través da consola de comandos, podemos empregar a orde csvde. O comando scvde sérvenos para importar e para exportar datos do AD. Neste caso queremos introducir datos no AD, é dicir, queremos importar datos ao AD. Para facer isto crearemos un arquivo en formato CSV que conterá a información referente ás UOs que queremos crear e o importaremos ao AD utilizando a seguinte orde: csvde -i -f ficheroCSV.

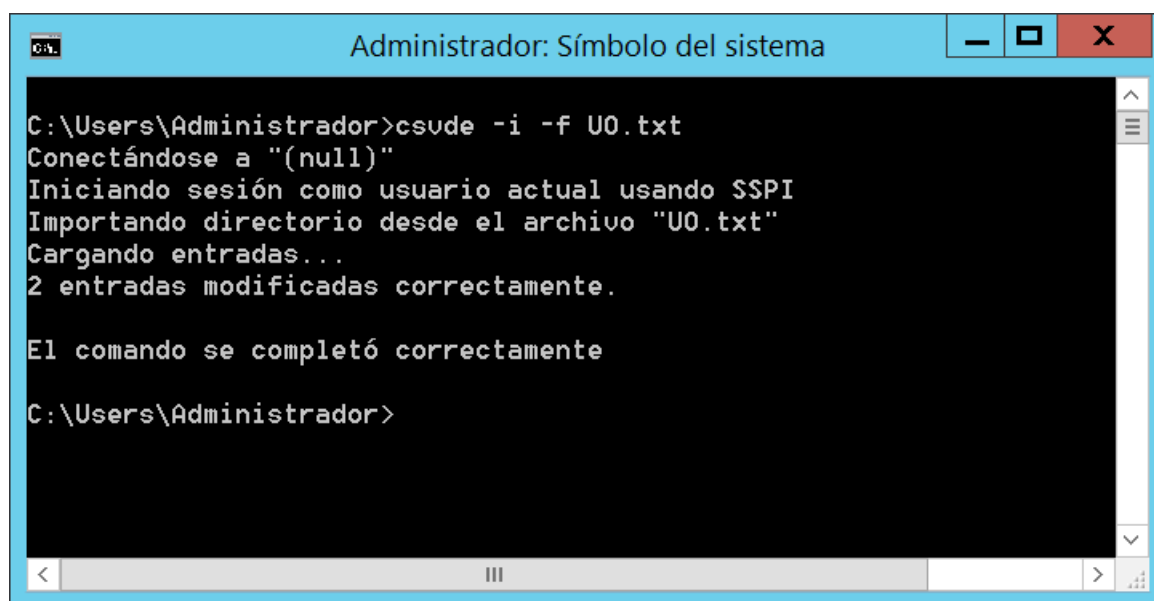
- O parámetro -i indica que imos importar datos ao AD (se non o empregamos exportaríamos os datos do AD).
- O parámetro -f ficheroCSV indica onde está almacenada a información que queremos importar ao AD.

Neste caso o arquivo CSV ímolo chamar UO.txt e este será o seu contido:



Na primeira liña do arquivo indicamos o formato da información que imos pasar ao AD. Estamos indicando que cada unha das liñas do arquivo CSV ten no seu primeiro campo un DN e no seu segundo campo o tipo de obxecto que se quere crear co DN indicado no

primeiro campo. Da segunda liña en diante envíanse os DNs e os tipos de obxectos que se queren crear, neste caso obxectos de tipo `OrganizationalUnit`. Unha vez xerado o arquivo CSV unicamente hai que executalo. Para elo desde unha consola de comandos lanzamos o comando indicado anteriormente:

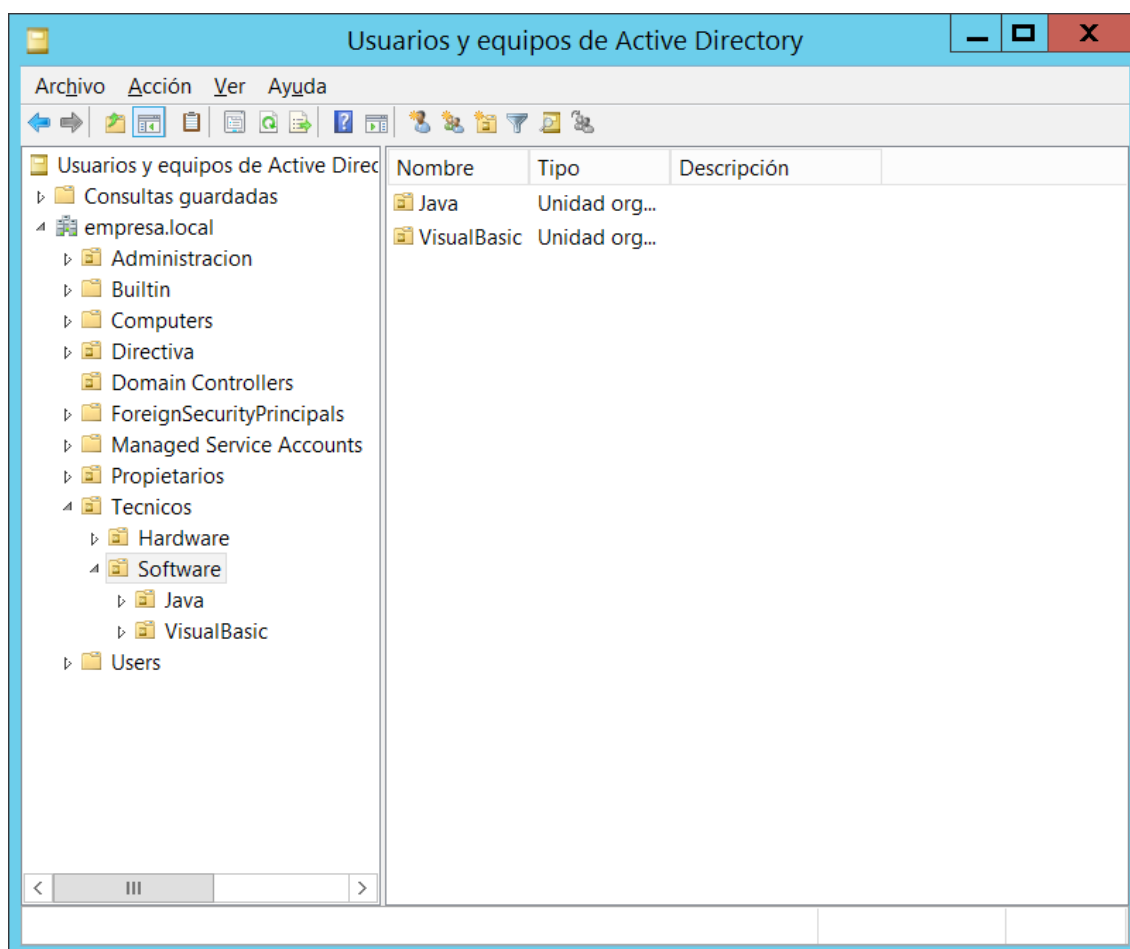


```
C:\Users\Administrador>csude -i -f U0.txt
Conectándose a "(null)"
Iniciando sesión como usuario actual usando SSPI
Importando directorio desde el archivo "U0.txt"
Cargando entradas...
2 entradas modificadas correctamente.

El comando se completó correctamente

C:\Users\Administrador>
```

Como pódese ver na imaxe anterior o resultado da execución do comando é correcta xa que nos indica dúas entradas modificadas correctamente. Para comprobar que realmente a execución foi correcta podemos abrir a ferramenta de usuarios e equipos de AD e ver que realmente as UOs foron creadas:

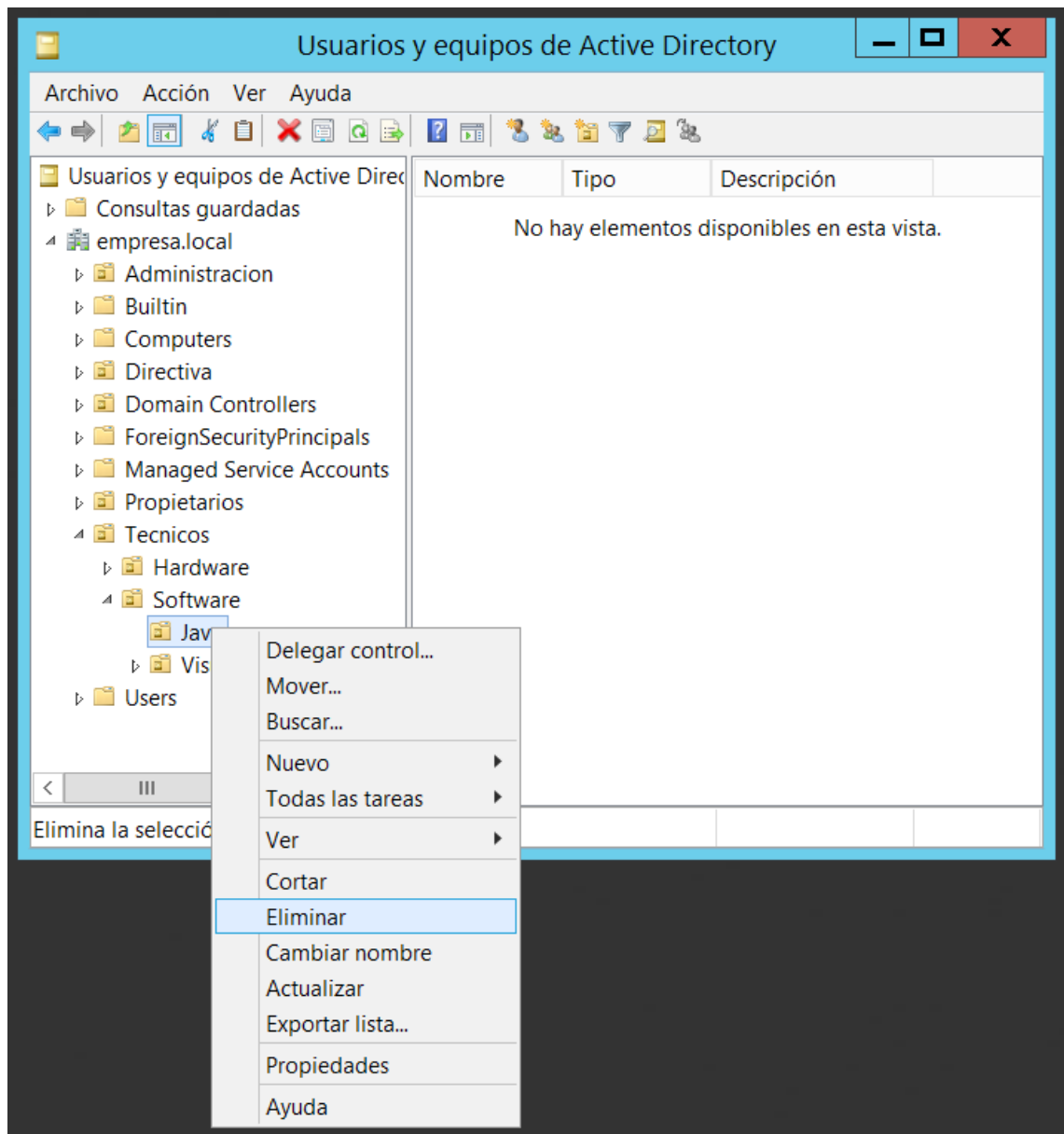


Como pódese observar na imaxe as UOs foron creadas e están situadas onde deben estar. O problema de CSVDE é que unicamente permite importar novos obxectos ao AD ou exportar os xa existentes, pero non permite a súa modificación.

Comando Ldifde

O comando ldifde ao igual que scvde sérvenos para importar e para exportar datos do AD, pero coa vantaxe de que tamén nos permite modificar os datos existentes no AD. Outra vantaxe de xestionar o AD mediante ldifde é que o formato dos arquivos de comandos utilizados por ldifde para xestionar o AD é similar ao utilizado na xestión de dominios por outros sistemas operativos.

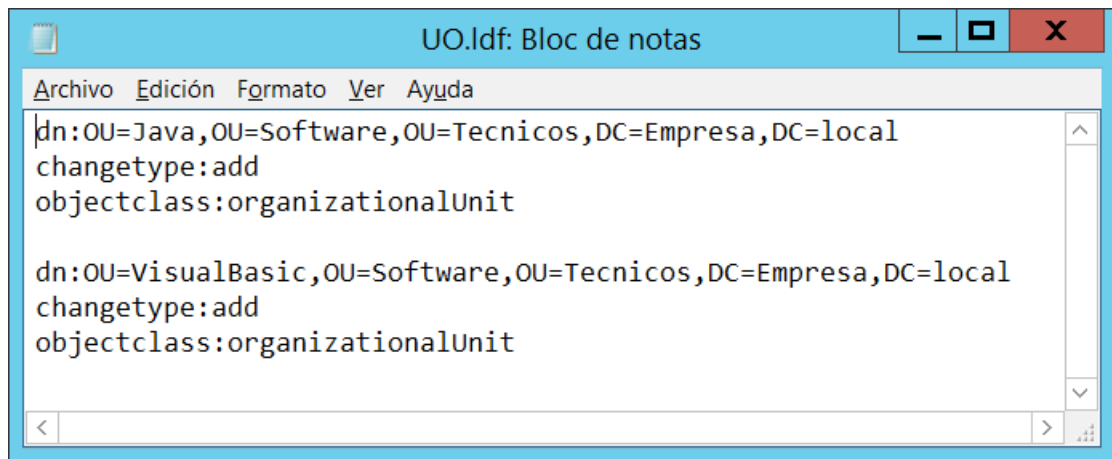
Imos eliminar as dous UOs que acabamos de crear e ímolas volver crear utilizando o comando ldifde. A eliminación das UOs java e visualBasic a realizaremos utilizando a ferramenta de usuarios e equipos de AD. Para elo prememos co botón dereito sobre a UO que queremos eliminar e do menú contextual que se desprega seleccionamos a opción eliminar:



O sistema pediranos confirmación para eliminar a UO. Unha vez eliminadas as UO java e visualBasic imos volver crealas utilizando o comando ldifde. Neste caso queremos introducir datos no AD, é dicir, queremos importar datos ao AD. Para facer isto crearemos un arquivo que conterá a información referente ás UOs que queremos crear e importarémolo ao AD utilizando a seguinte orde: `ldifde -i -f ficheroInfoUO.ldf`

- -i indica que imos importar datos ao AD
- -f ficheroInfoUO.ldf indica onde está almacenada a información que queremos importar ao AD. A súa extensión acostuma ser ldf.

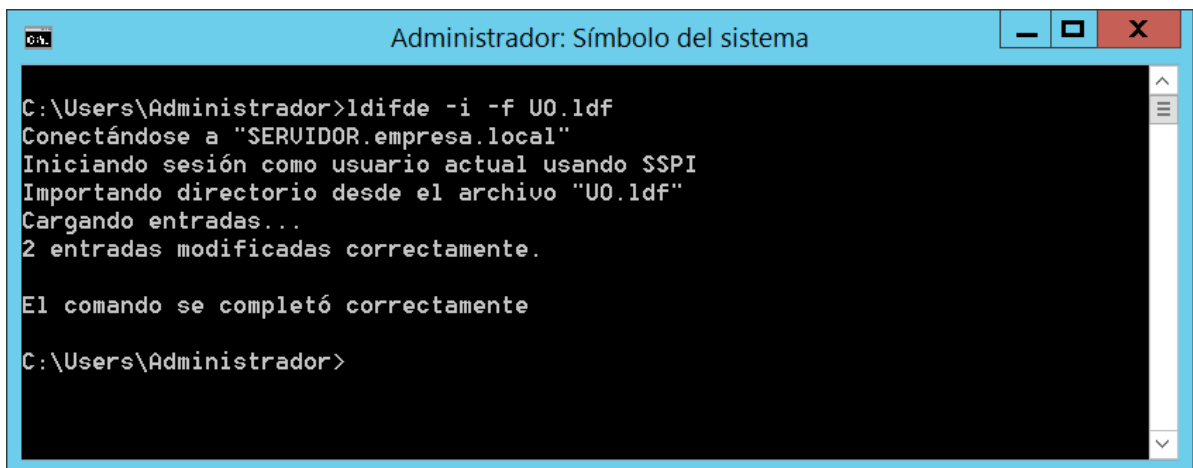
Neste caso ao ldf ímolo chamar UO.ldf e este será o seu contido:



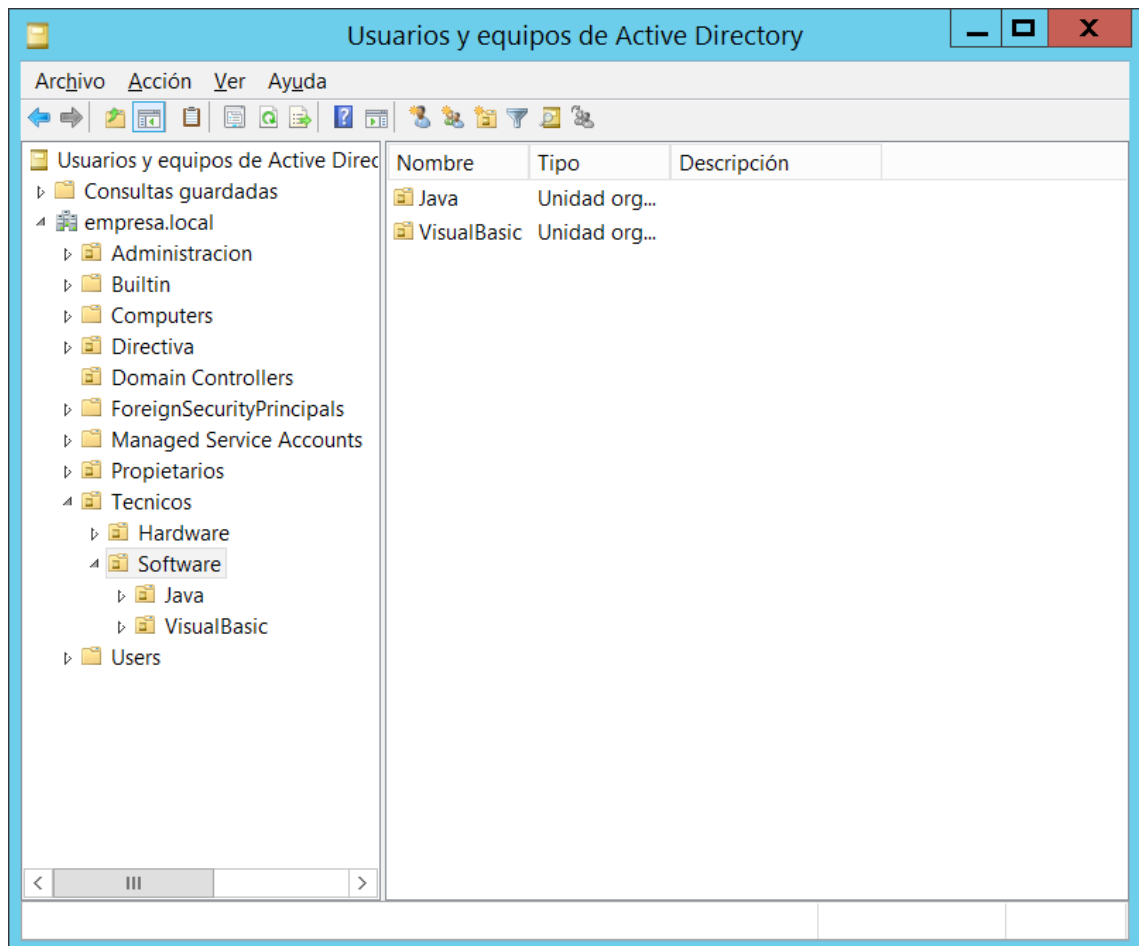
Para cada unha das UO que queremos engadir no AD creamos 3 liñas:

- A primeira liña contén o DN da UO que queremos engadir.
- Na segunda liña indicamos a operación que queremos realizar, neste caso engadir (add)
- Na terceira liña indicamos o tipo de obxecto que queremos engadir, neste caso unha UO (organizationalUnit).

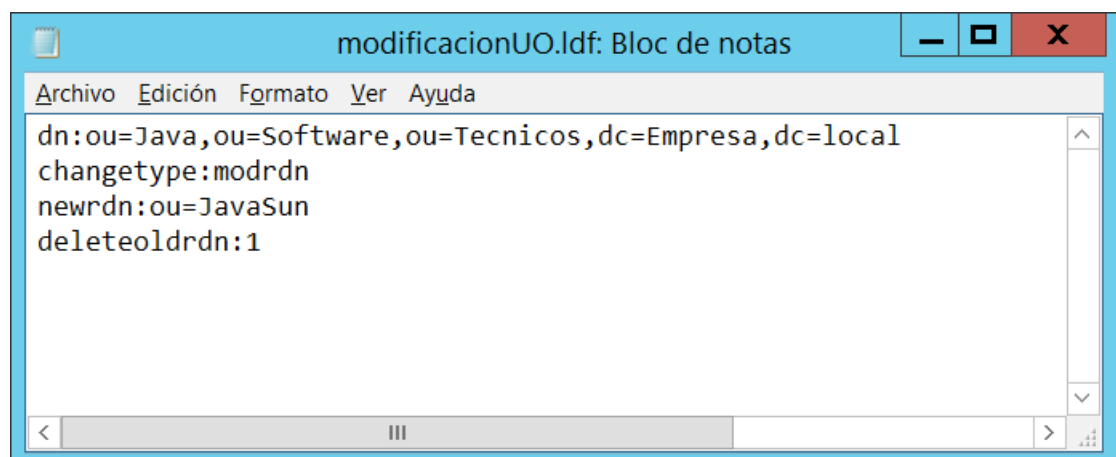
Unha vez xerado o arquivo ldf unicamente hai que executalo. Para elo desde unha consola de comandos lanzamos o comando indicado anteriormente:



Como pódese ver na imaxe anterior o resultado da execución do comando é correcta xa que nos indica dúas entradas modificadas correctamente. Para comprobar que realmente a execución foi correcta podemos abrir a ferramenta de usuarios e equipos de AD e ver que realmente as UOs foron creadas:

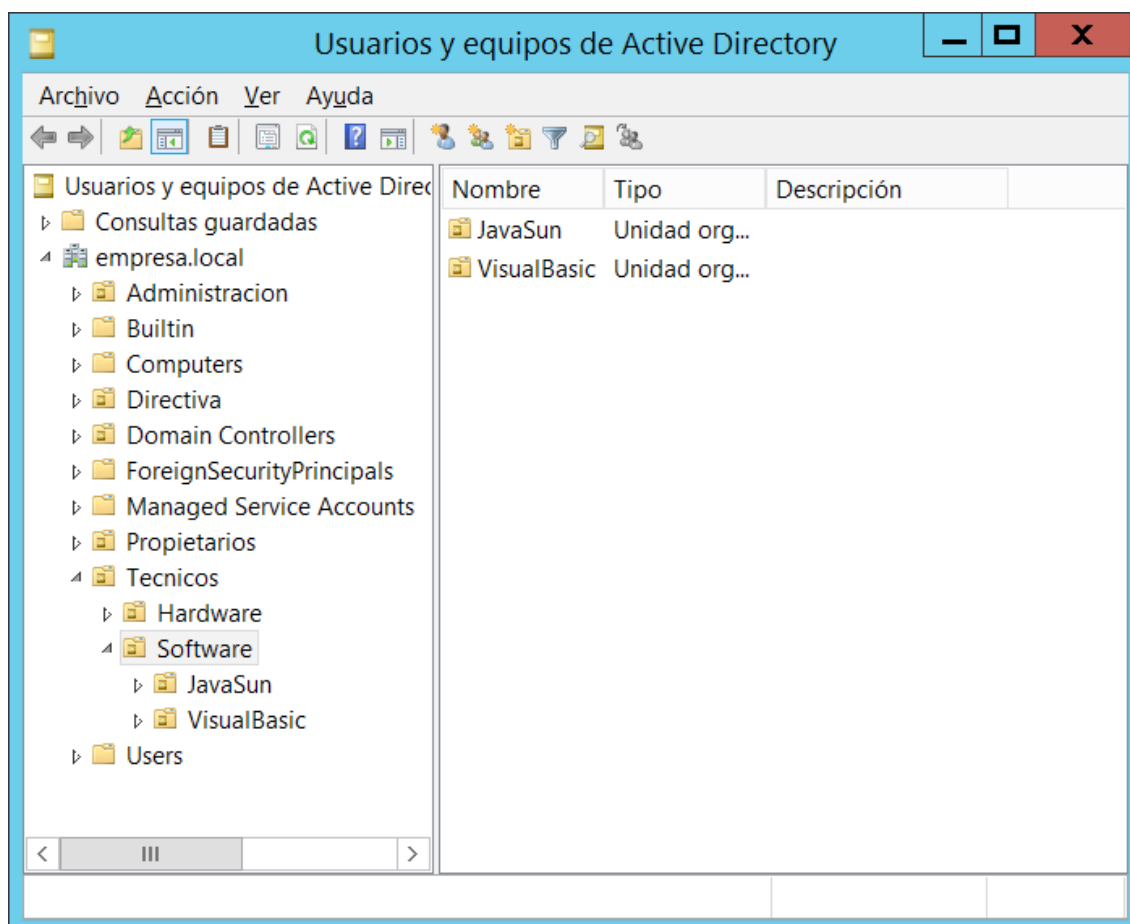


Como pódese observar na imaxe as UOs foron creadas e están situadas onde deben estar. Ata este punto vemos que non hai diferenza coa execución do comando `csvde`, pero como indicamos anteriormente, con `csvde` non podemos modificar os obxectos almacenados no AD, mentres que con `ldifde` si é posible facelo. Imos modificar o nome da UO java para que se pase a chamar JavaSun. Creamos o arquivo `ldf` coas ordenes para modificar o nome da UO:



Primeiro indicamos o obxecto que queremos modificar indicando o seu DN. A continuación indicamos a operación, que neste caso será `modrdn` (modificar o RDN. RDN é o relative

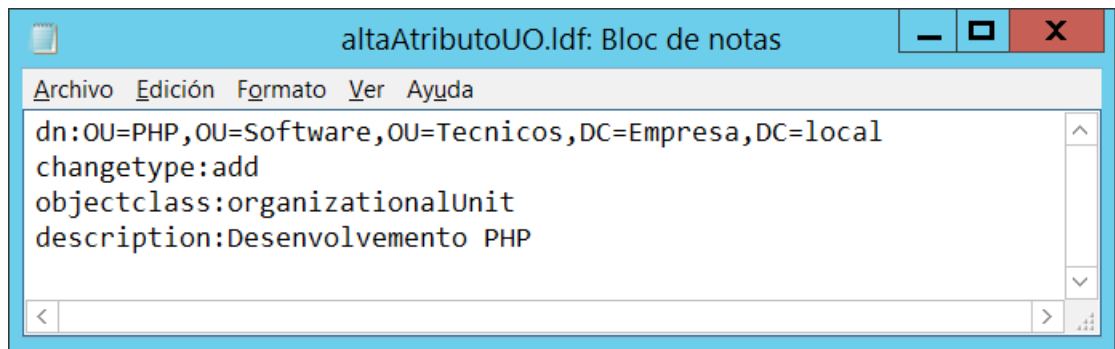
DN, é dicir, o elemento máis á esquerda do DN, neste caso ou=Java). A continuación mediante newrdn indicamos o valor do novo rdn e por último deleteolrdn:1. Se oldrdn vale 1 elimínase do AD o RDN vello. Se vale 0 créase o novo RDN pero mantense tamén o vello RDN. Se executamos o comando ldifde -i -f modificacionUO.ldf, este é o resultado na ferramenta de usuarios e equipos de AD:



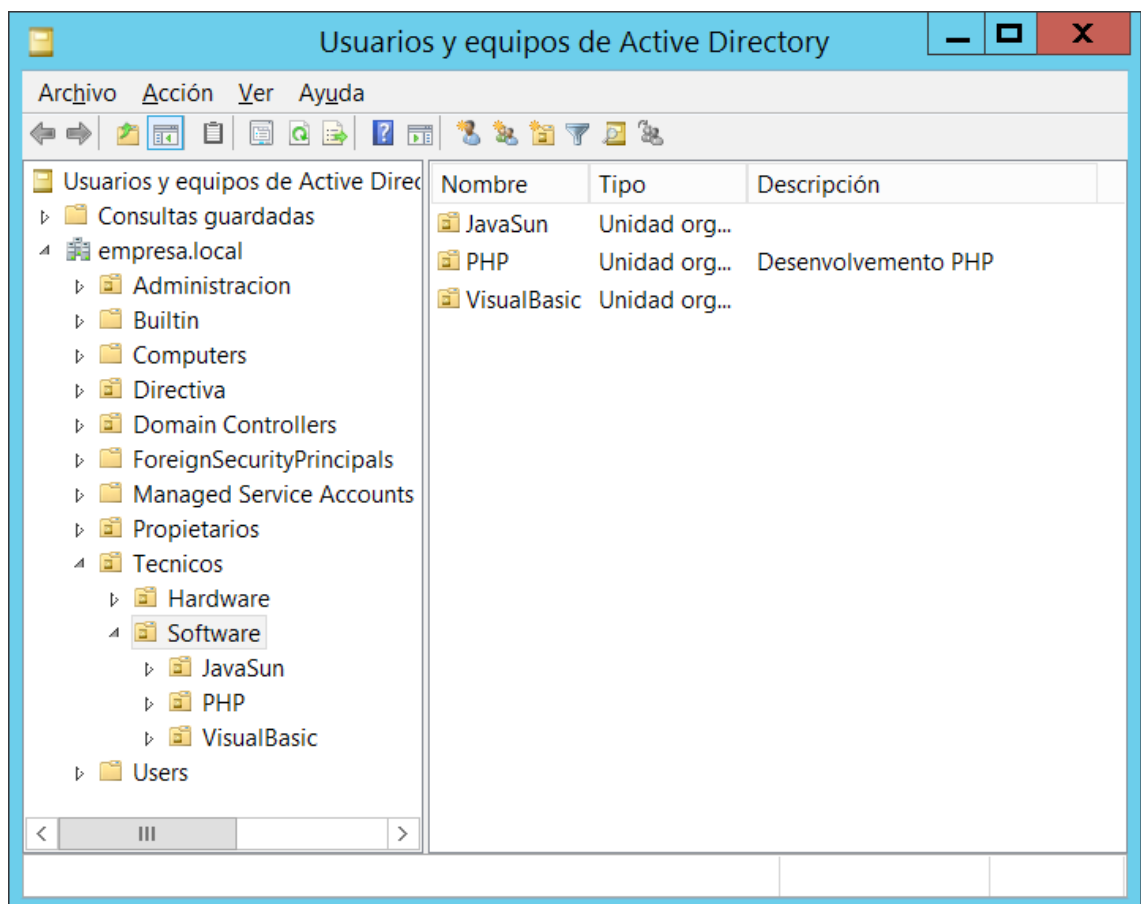
Atributos dos obxectos de AD

Tódolos obxectos que damos de alta no AD ademais do DN tamén teñen asociados unha serie de atributos que poden ser xestionados a través do comando ldifde. P.e., unha UO ten un atributo chamado description no cal podemos almacenar unha cadea de texto que conterá unha descrición asociada á UO. Na imaxe anterior pódese observar que para as dúas UOs creadas amósanse tres datos: nome, tipo e descrición. A columna descrición neste caso está baleira, pero a súa información podería ser xestionada facendo uso do atributo description da UO.

Co fin de aprender a xestionar os atributos dos obxectos do AD mediante ldifde imos crear unha nova UO chamada PHP que vai conter o atributo description. O arquivo ldif empregado será o seguinte:

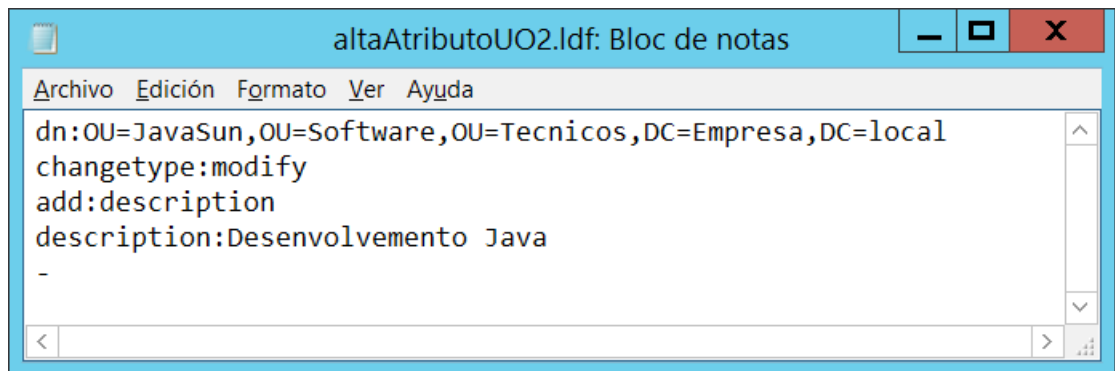


Como pódese observar, a sintaxe é similar á dun alta dunha UO, pero ademais engadimos a liña `description:Desenvolvimento PHP` na cal indicamos o atributo que queremos dar de alta no obxecto que imos crear así como o seu valor. O resultado de executar esta consulta mediante `ldifde` é o seguinte:

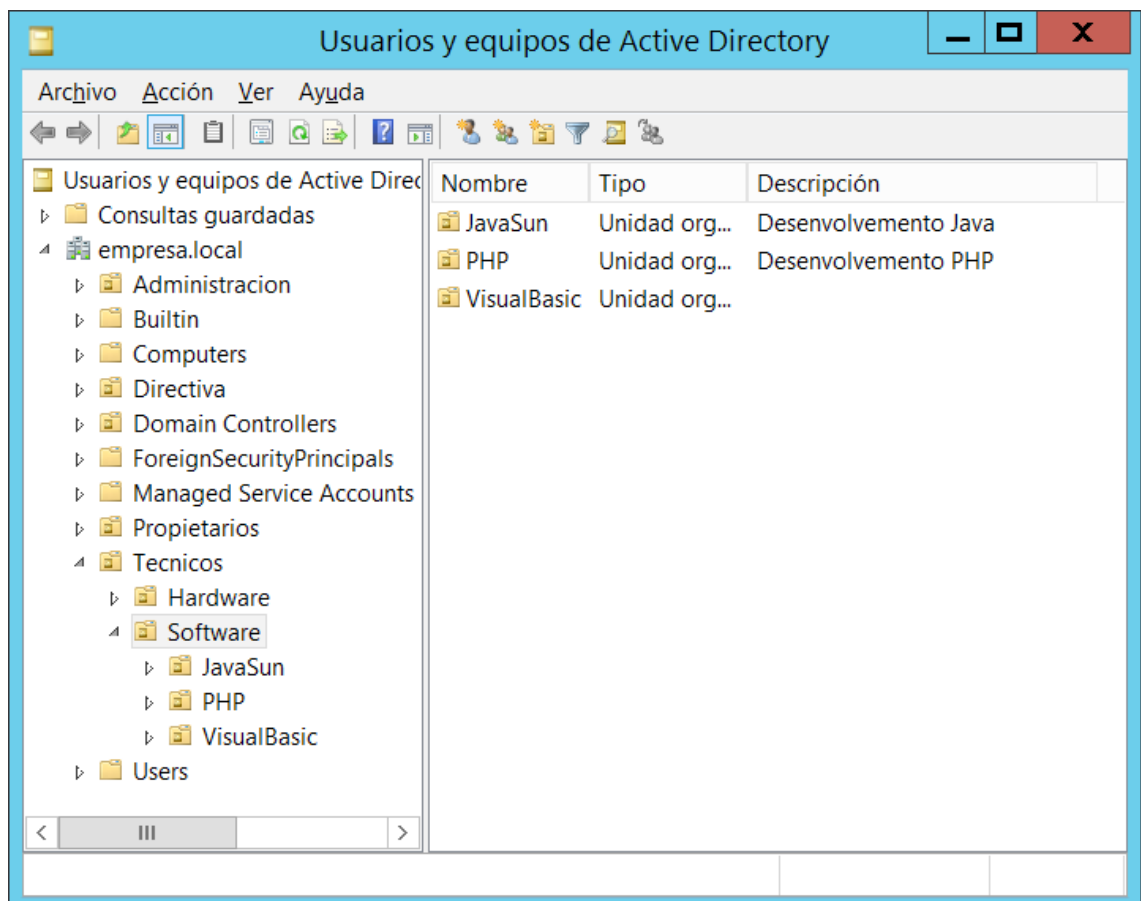


Agora podemos observar na ferramenta de usuarios e equipos de AD que a columna descrición asociada á UO PHP ten o valor que indicamos mediante o uso do atributo `description`.

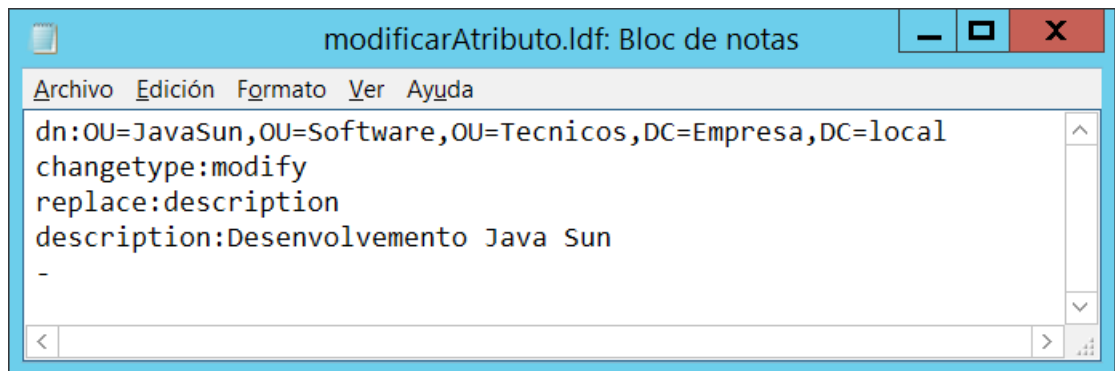
Mediante `ldifde` tamén é posible dar de alta un atributo sobre un obxecto xa creado no AD con anterioridade. P.e., imos dar de alta o atributo `description` para o obxecto `JavaSun`. Para elo utilizamos o seguinte arquivo `ldf`:



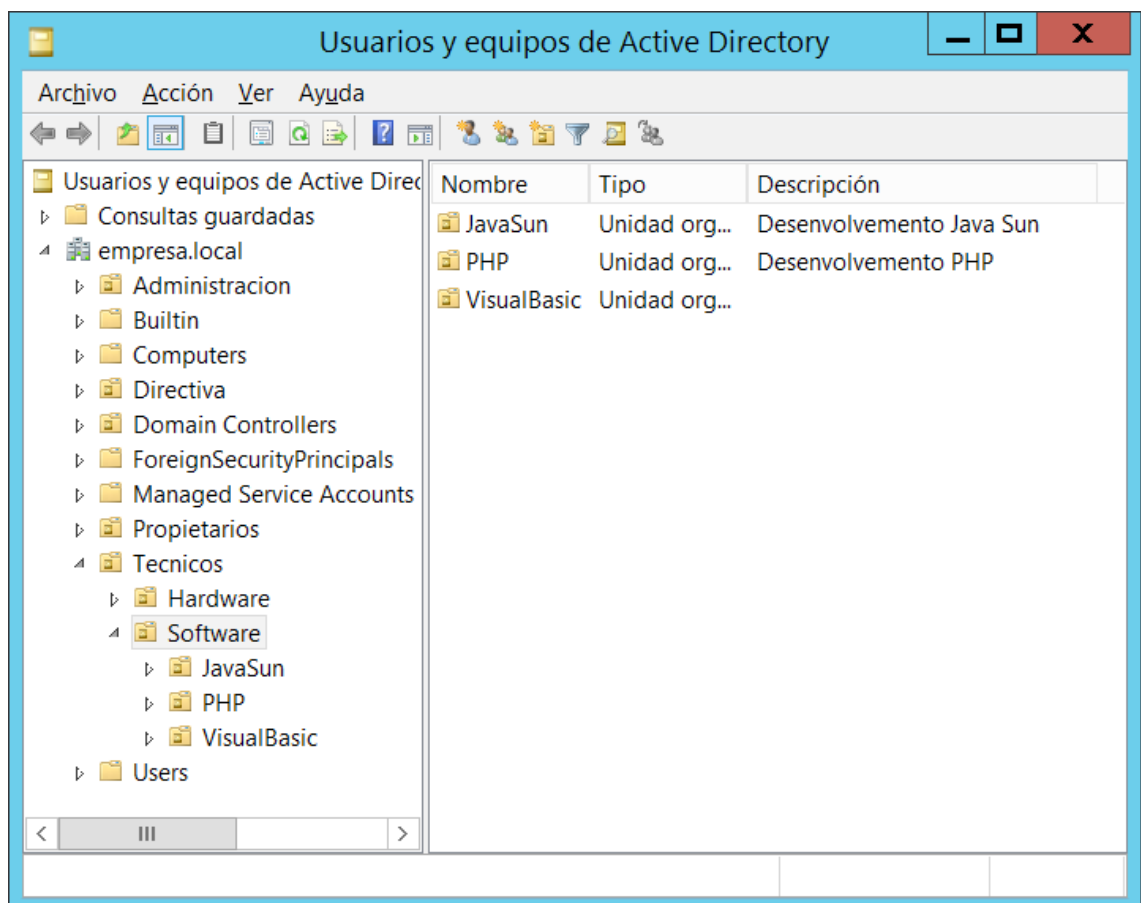
Mediante changetype:modify indicamos que imos realizar a modificación do obxecto indicado mediante o seu dn. Con add:description indicamos que imos engadir no obxecto un atributo chamado description. Por ultimo dámoslle valor ao atributo mediante description:Desenvolvimento Java. O carácter – emprégase para separar esta consulta da seguinte. Neste caso non hai unha seguinte consulta despois desta, pero se non escribimos o carácter - ldifde xera un erro de sintaxe. Unha vez executada a consulta mediante ldifde, podemos ver o seu resultado na ferramenta de usuarios e equipos de AD:



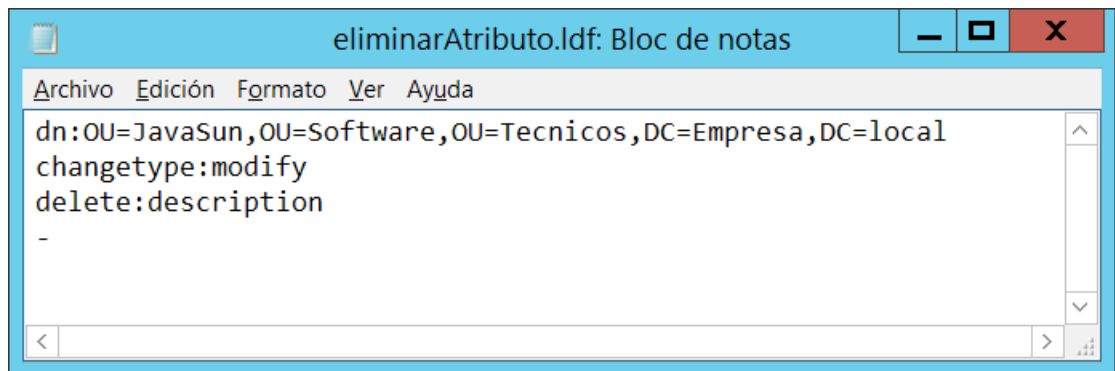
A continuación imos modificar o valor dun atributo dun obxecto do AD. Neste caso modificaremos o valor da descrición da UO JavaSun. O arquivo ldif empregado para realizar a operación é o seguinte:



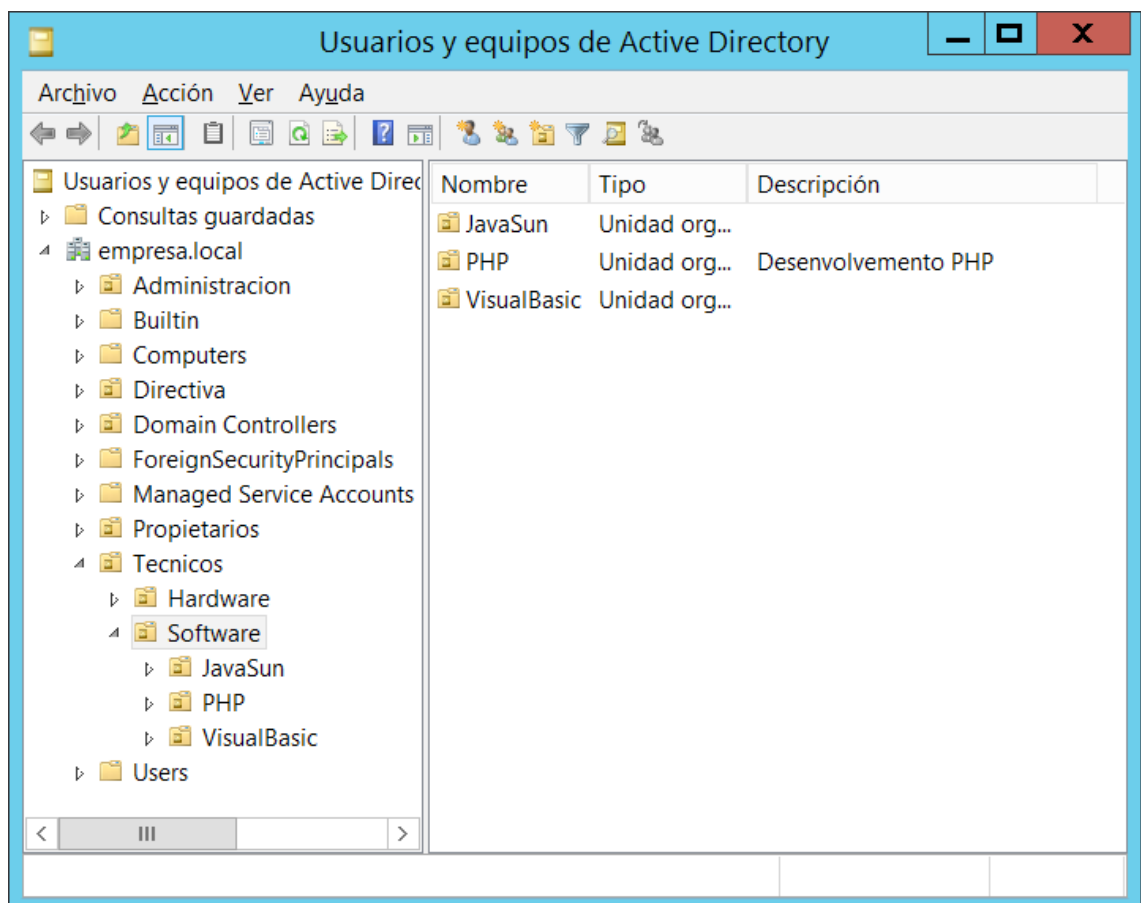
A sintaxe do arquivo ldf empregado é similar á do exemplo anterior, pero neste caso en lugar de empregar add:description, empregamos replace:description para indicar que a operación a realizar sobre o obxecto dn é unha operación de modificación do atributo description. O resultado da execución do arquivo ldf empregando ldifde é o seguinte:



Para finalizar coa xestión de atributos dos obxectos do AD imos ver como eliminar un atributo dun obxecto do AD. Para elo eliminaremos o atributo description do obxecto JavaSun. O arquivo ldf empregado para realizar a operación é o seguinte:



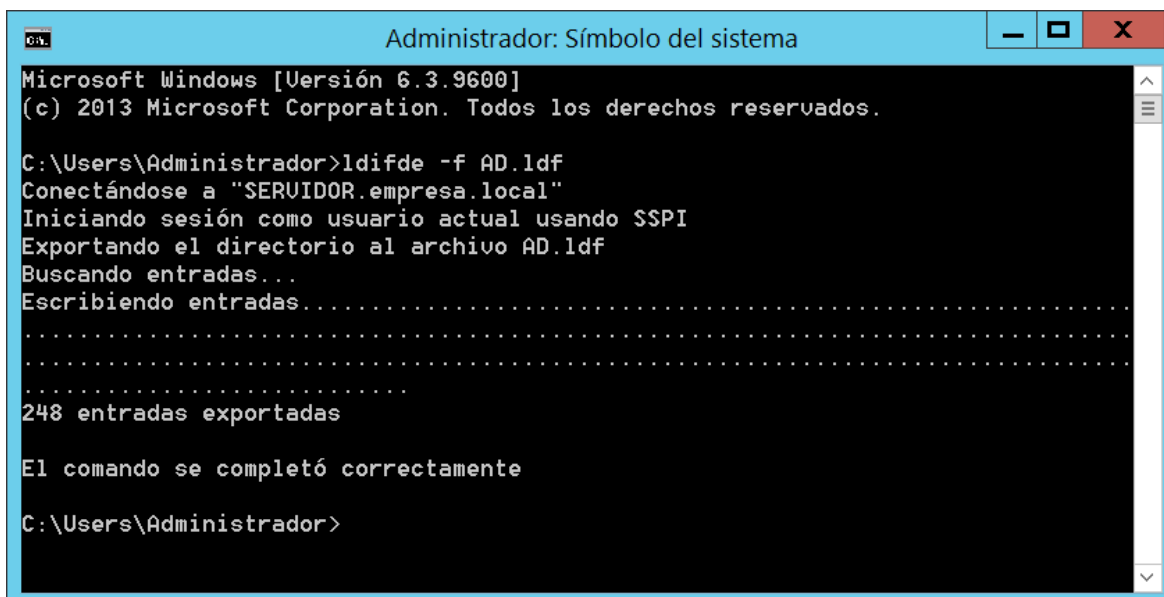
A sintaxe do arquivo ldf empregado é parecida á do exemplo anterior, pero neste caso en lugar de utilizar replace:description utilizamos delete:description para indicar que a operación a realizar sobre o obxecto dn é unha operación de eliminación do atributo description. O resultado da execución do arquivo ldf empregando ldifde é o seguinte:



Buscar obxectos no Active directory

O comando ldifde non so se utiliza para crear e modificar os obxectos do AD. Tamén pode ser utilizado para recuperar a información existente no AD.

Se desexamos recuperar tódolos obxectos do AD utilizaremos o seguinte comando: ldifde -f arquivoDestino.ldf. Deste modo almacenaranse tódolos obxectos do AD no ficheiro arquivoDestino.ldf:



```
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

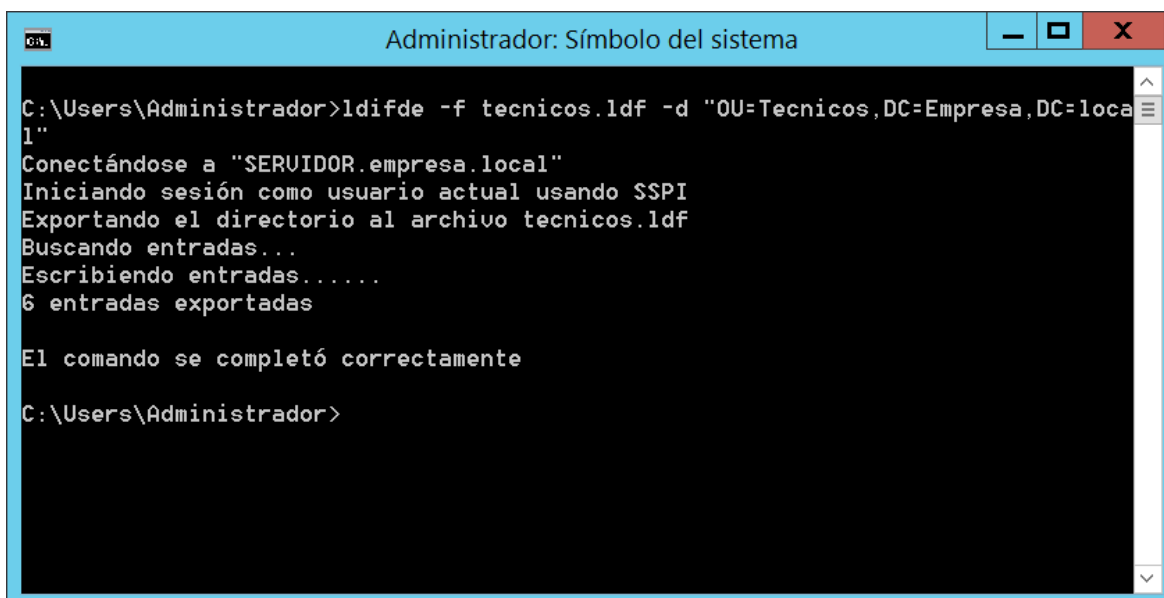
C:\Users\Administrador>ldifde -f AD.ldf
Conectándose a "SERVIDOR.empresa.local"
Iniciando sesión como usuario actual usando SSPI
Exportando el directorio al archivo AD.ldf
Buscando entradas...
Escribiendo entradas.....
.....
248 entradas exportadas

El comando se completó correctamente

C:\Users\Administrador>
```

Na imaxe anterior almacénase a información de tódolos obxectos do AD nun ficheiro chamado AD.ldf. É importante facer notar a saída do comando: 248 entradas importadas. O AD non so almacena os obxectos que nos lle indicamos, senón que almacena bastantes máis, neste caso 248. En xeral cando recuperamos información do AD o facemos porque queremos recuperar información dun obxecto ou dun grupo de obxectos. Nestes casos non é unha boa idea recuperar tódolos obxectos do AD xa que despois teremos que mergullar dentro do arquivo xerado para buscar a información que necesitamos. Nestes casos é mellor filtrar a información que queremos recuperar.

O comando ldifde pode ser executado coa opción -d DN. Deste modo vains devolver unicamente o obxecto cuxo dn coincida co pasado mediante DN e tódolos que estean contidos nel. Vexamos un exemplo:



```
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.

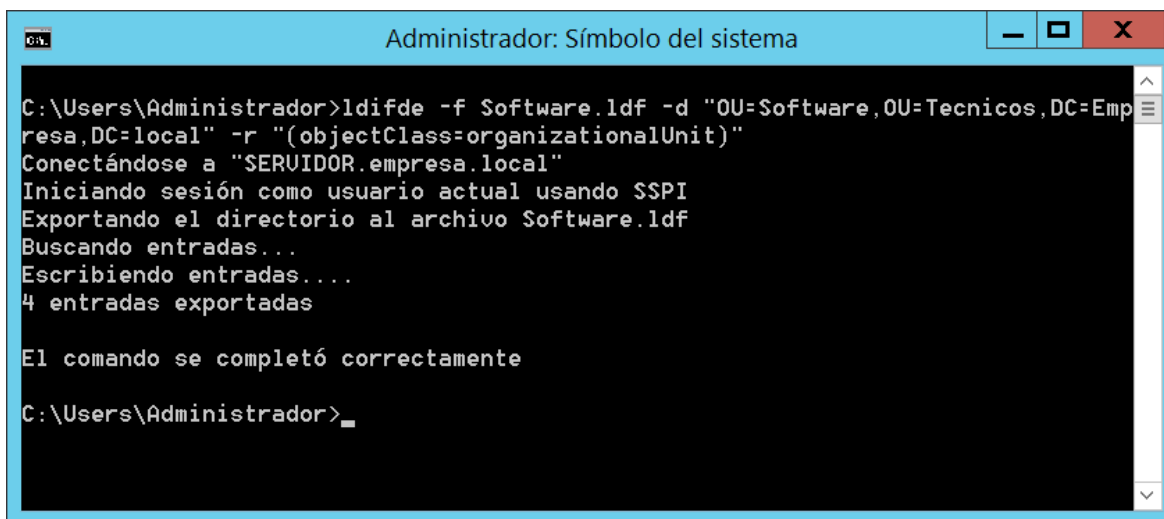
C:\Users\Administrador>ldifde -f tecnicos.ldf -d "OU=Tecnicos,DC=Empresa,DC=local"
Conectándose a "SERVIDOR.empresa.local"
Iniciando sesión como usuario actual usando SSPI
Exportando el directorio al archivo tecnicos.ldf
Buscando entradas...
Escribiendo entradas.....
6 entradas exportadas

El comando se completó correctamente

C:\Users\Administrador>
```

O comando da imaxe solicita mediante o seu dn a UO Tecnicos. Como pódese ver, devolve seis entradas xa que da UO solicitada colgan cinco UO máis.

Se quixeramos refinar aínda máis a busca, poderíamos indicarlle ao comando `ldifde` que nos devolva unicamente obxectos dunha clase (UO, usuarios, equipos, ...). Para elo utilizamos o parámetro `-r FILTRO`. En `FILTRO` indicaremos o tipo de obxectos que queremos recuperar. Vexamos un exemplo:



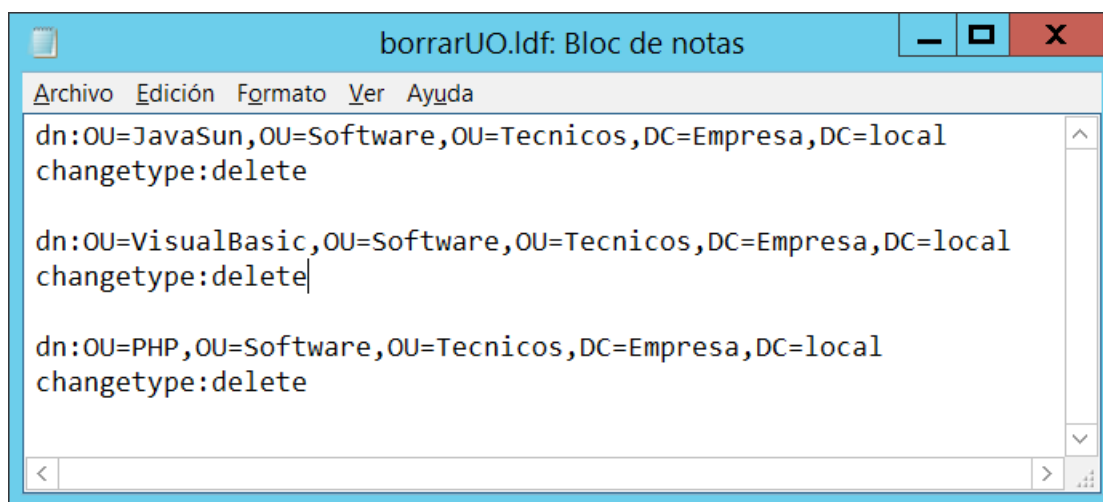
```
C:\Users\Administrador>ldifde -f Software.ldf -d "OU=Software,OU=Tecnicos,DC=Emp
resa,DC=local" -r "(objectClass=organizationalUnit)"
Conectándose a "SERVIDOR.empresa.local"
Iniciando sesión como usuario actual usando SSPI
Exportando el directorio al archivo Software.ldf
Buscando entradas...
Escribiendo entradas....
4 entradas exportadas

El comando se completó correctamente

C:\Users\Administrador>
```

Neste caso estamos indicando a `ldifde` mediante `-r "(objectClass=organizationalUnit)"` que unicamente debe devolver UOs. Evidentemente neste caso da igual utilizar `-r` ou non facelo xa que unicamente hai UOs dentro da UO `Software`, pero no caso de que dentro da UO `JavaSun` tamén houbera usuarios `ldifde` non nos devolvería a información destes senón que se limitaría a amosar a información das UOs.

Para finalizar imos eliminar as UO `JavaSun`, `PHP` e `VisualBasic` do AD. Para elo utilizaremos a seguinte sintaxe nun arquivo `ldf`:



```
dn:OU=JavaSun,OU=Software,OU=Tecnicos,DC=Empresa,DC=local
changetype:delete

dn:OU=VisualBasic,OU=Software,OU=Tecnicos,DC=Empresa,DC=local
changetype:delete

dn:OU=PHP,OU=Software,OU=Tecnicos,DC=Empresa,DC=local
changetype:delete
```

Mediante `changetype:delete` eliminamos do AD o DN indicado.

Familia de comandos `ds`

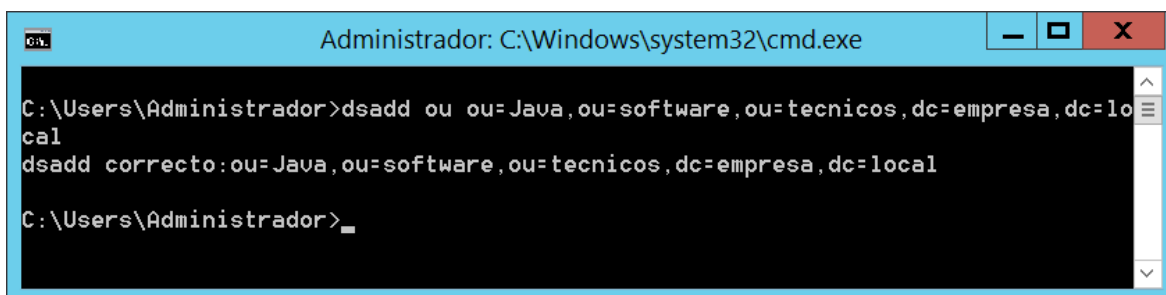
Ademais dos comandos `ldifde` e `csvde`, tamén é posible xestionar os obxectos do AD facendo uso da familia de comandos de consola `ds`.

Dsadd

Este comando emprégase para engadir obxectos ao AD. A súa sintaxe xeral é a seguinte: dsadd obxecto_a_engadir DN_do_obxecto_a_engadir [opcións]

Imos ver como engadir unha UO ao AD facendo uso do comando dsadd. Para engadir UOs o comando dsadd ten a seguinte sintaxe (respecto ás opcións, unicamente imos ver as máis empregadas. No caso de querer conocer máis pódese utilizar o comando dsadd ou /?): dsadd ou DN_da_UO_a_engadir [-desc descrición]. A opción -desc é opcional. No caso de empregala, a utilizaremos para indicar a descrición asociada á UO.

Co fin de probar o comando dsadd ou imos crear dous UOs dentro da UO Software. A primeira vaise chamar Java e a segunda PHP. Ademais a UO PHP terá unha descrición asociada. Este é o comando empregado para crear a UO Java:

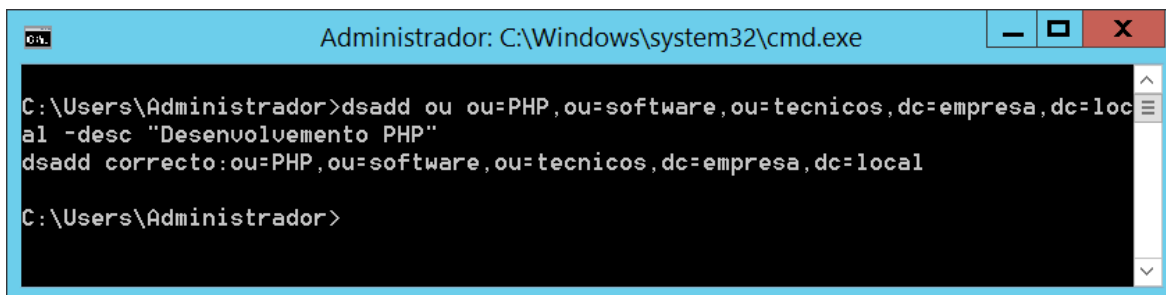


```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsadd ou ou=Java,ou=software,ou=tecnicos,dc=empresa,dc=local
dsadd correcto:ou=Java,ou=software,ou=tecnicos,dc=empresa,dc=local

C:\Users\Administrador>
```

Para crear a UO PHP que ademais ten unha descrición empregamos o seguinte comando:

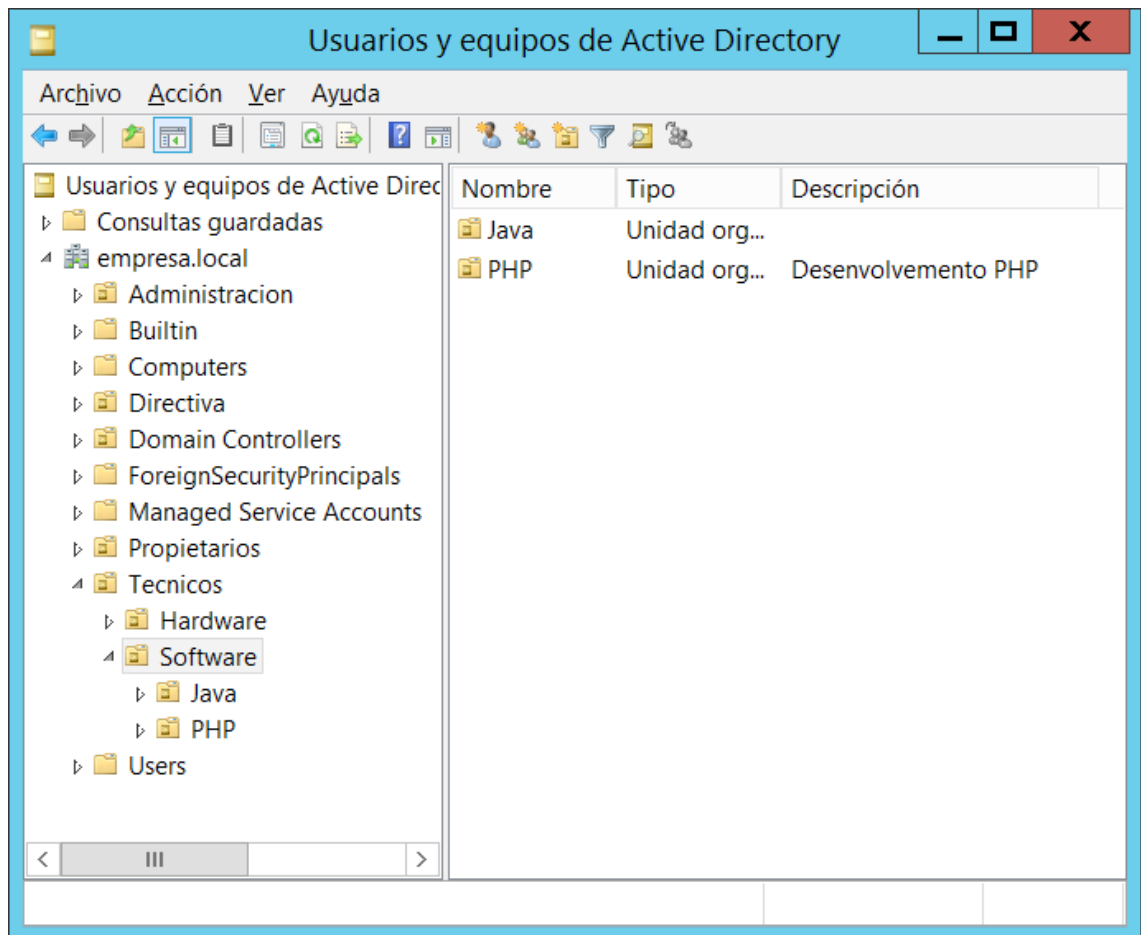


```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsadd ou ou=PHP,ou=software,ou=tecnicos,dc=empresa,dc=local -desc "Desenvolvimento PHP"
dsadd correcto:ou=PHP,ou=software,ou=tecnicos,dc=empresa,dc=local

C:\Users\Administrador>
```

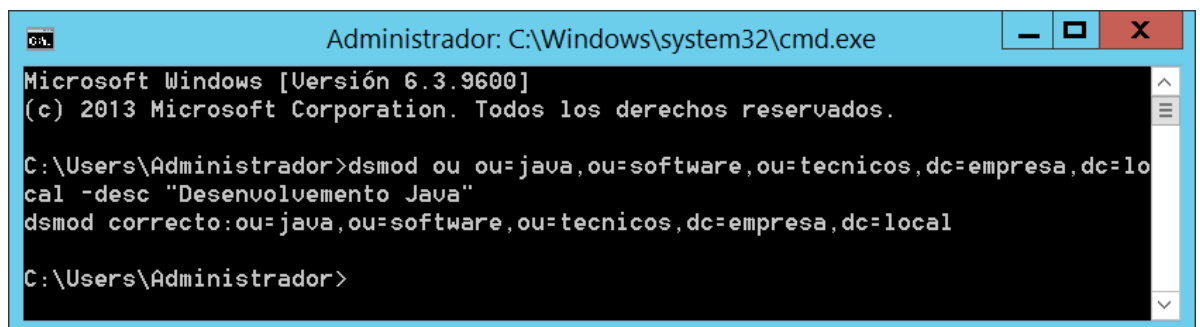
É destacable que como a descrición asociada á UO contén espazos, é necesario entrecomiñala. De non facelo incorreremos nun erro de sintaxe. A continuación amósase na ferramenta de usuarios e equipos do AD o resultado da execución dos comandos anteriores:



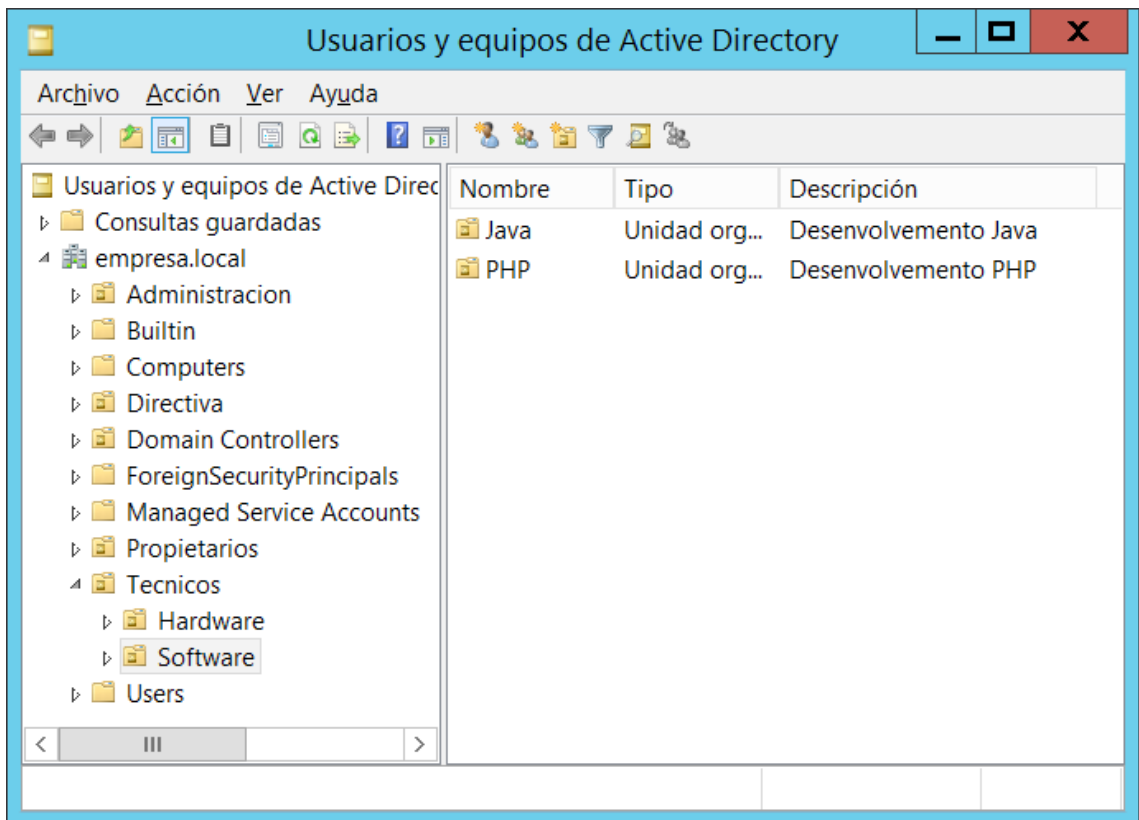
Dsmod

Este comando emprégase para modificar os atributos dos obxectos do AD. A súa sintaxe xeral é a seguinte: `dsmod obxecto_a_modificar_atributos DN_do_obxecto [opcións]`

Imos ver como modificar os atributos dunha UO existente no AD facendo uso do comando `dsmod`. Empregaremos a seguinte sintaxe (axuda completa do comando con `dsmod` ou `/?`): `dsmod ou DN_da_UO_a_modificar_atributos [-desc descrición]`. A opción `-desc` é opcional. No caso de empregala, farémolo para indicar que queremos modificar a descrición asociada á UO. Co fin de probar o comando `dsadd` ou imos modificar a descrición da UO Java:



A continuación amósase na ferramenta de usuarios e equipos do AD o resultado da execución dos comandos anteriores:



Dsquery

Este comando emprégase para buscar obxectos no AD a partir dun criterio de busca. A súa sintaxe é a seguinte: `dsquery tipo_obxecto_a_buscar [opcións_de_busca]`

Imos ver como buscar UOs no AD facendo uso do comando `dsquery`. Empregaremos a seguinte sintaxe (axuda completa do comando con `dsquery` ou `/?`): `dsquery ou [DN_das_UO_a_buscar] [-desc descrición] [-name nome_UO]`. A opción `DN_das_UO_a_buscar` é opcional. No caso de empregala amosaranos tódalas UOs que se atopen a partir do DN indicado. A opción `-desc` é opcional. No caso de empregala, amosaranos tódalas UOs cuxa descrición coincida coa indicada. A opción `-name` é opcional. No caso de empregala, amosaranos tódalas UOs cuxo nome coincida co indicado. Vexamos algún exemplo:

```

Administrador: C:\Windows\system32\cmd.exe

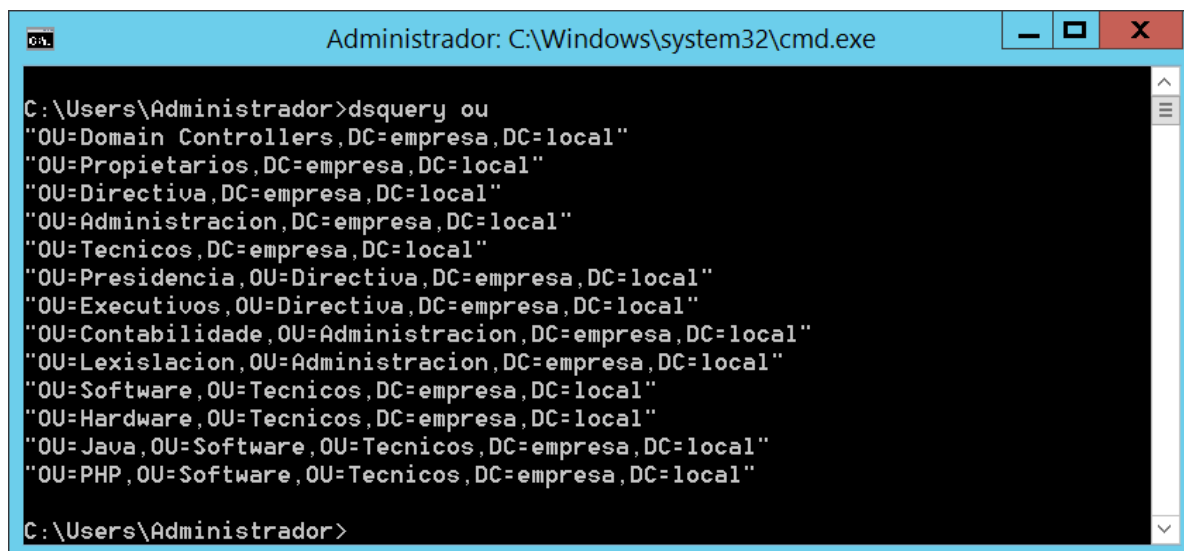
C:\Users\Administrador>dsquery ou ou=tecnicos,dc=empresa,dc=local
"OU=Tecnicos,DC=empresa,DC=local"
"OU=Software,OU=Tecnicos,DC=empresa,DC=local"
"OU=Java,OU=Software,OU=Tecnicos,DC=empresa,DC=local"
"OU=PHP,OU=Software,OU=Tecnicos,DC=empresa,DC=local"
"OU=Hardware,OU=Tecnicos,DC=empresa,DC=local"

C:\Users\Administrador>dsquery ou -name java
"OU=Java,OU=Software,OU=Tecnicos,DC=empresa,DC=local"

C:\Users\Administrador>

```

Se empregamos o comando `dsquery ou`, este vai nos devolver todas as UOs do AD:

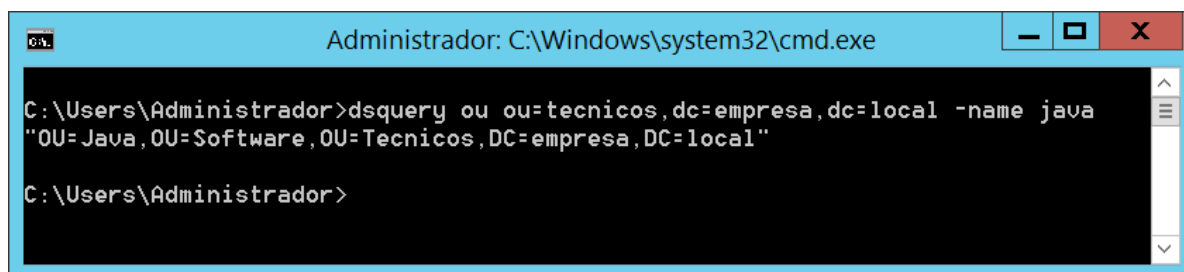


```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsquery ou
"OU=Domain Controllers,DC=empresa,DC=local"
"OU=Propietarios,DC=empresa,DC=local"
"OU=Directiva,DC=empresa,DC=local"
"OU=Administracion,DC=empresa,DC=local"
"OU=Tecnicos,DC=empresa,DC=local"
"OU=Presidencia,OU=Directiva,DC=empresa,DC=local"
"OU=Executivos,OU=Directiva,DC=empresa,DC=local"
"OU=Contabilidad,OU=Administracion,DC=empresa,DC=local"
"OU=Legislacion,OU=Administracion,DC=empresa,DC=local"
"OU=Software,OU=Tecnicos,DC=empresa,DC=local"
"OU=Hardware,OU=Tecnicos,DC=empresa,DC=local"
"OU=Java,OU=Software,OU=Tecnicos,DC=empresa,DC=local"
"OU=PHP,OU=Software,OU=Tecnicos,DC=empresa,DC=local"

C:\Users\Administrador>
```

No caso de empregar varias opcións á vez, farase un `and` entre os diferentes patróns de busca indicados:

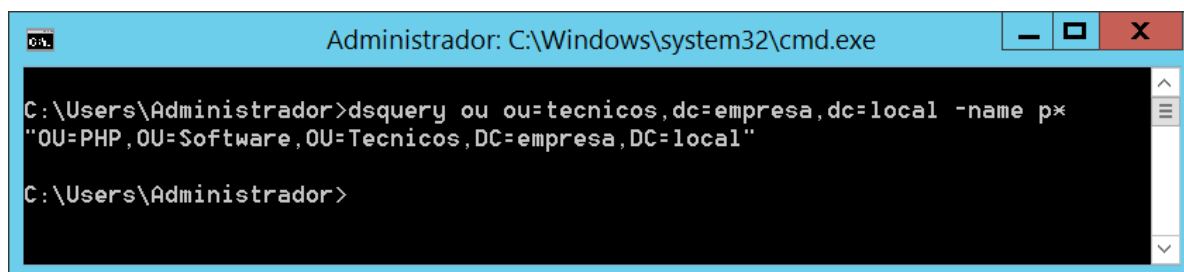


```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsquery ou ou=tecnicos,dc=empresa,dc=local -name java
"OU=Java,OU=Software,OU=Tecnicos,DC=empresa,DC=local"

C:\Users\Administrador>
```

É posible empregar comodíns:



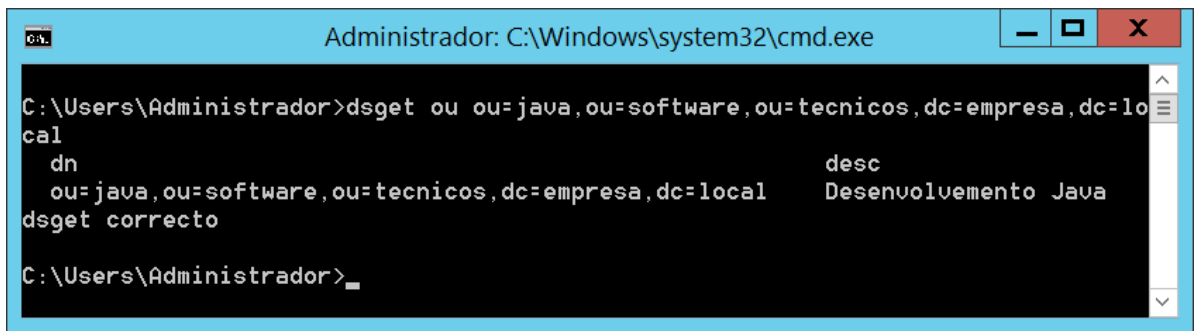
```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsquery ou ou=tecnicos,dc=empresa,dc=local -name p*
"OU=PHP,OU=Software,OU=Tecnicos,DC=empresa,DC=local"

C:\Users\Administrador>
```

Dsget

Este comando emprégase para amosar as propiedades dunha UO do AD. A súa sintaxe é a seguinte: `dsget ou DN_do_obxecto_a_detallar [opcións]`. No caso de non empregar opcións, amosarase toda a información coñecida sobre a UO indicada. Respecto ás opcións, unicamente imos facer referencia á opción `-desc`. A opción `desc` é opcional. No caso de empregala unicamente amosarase a descrición da UO. Co fin de probar o comando `dsget ou`, imos amosar as propiedades da UO Java:

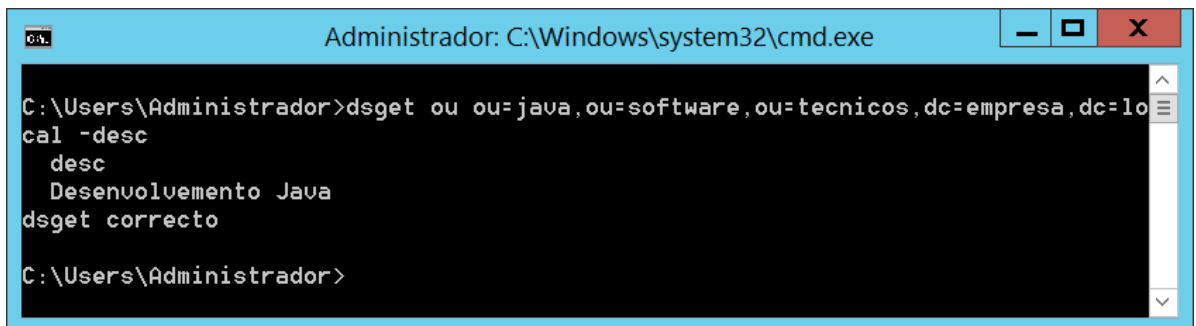


```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsget ou ou=java,ou=software,ou=tecnicos,dc=empresa,dc=local
dn
ou=java,ou=software,ou=tecnicos,dc=empresa,dc=local      desc
Desenvolvimento Java
dsget correcto

C:\Users\Administrador>
```

Como pódese observar na imaxe anterior, amósase toda a información referente ao obxecto do AD indicado. Non obstante, se empregáramos o seguinte comando:



```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsget ou ou=java,ou=software,ou=tecnicos,dc=empresa,dc=local -desc
desc
Desenvolvimento Java
dsget correcto

C:\Users\Administrador>
```

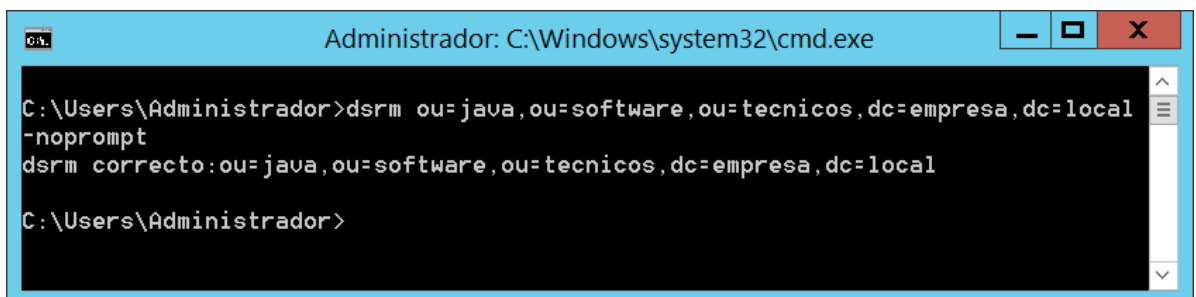
Neste caso unicamente amósase a descrición do obxecto do AD indicado.

Dsrm

Este comando emprégase para eliminar obxectos do AD (non é un comando específico para traballar sobre UOs, senón que pode ser empregado para eliminar outros tipos de obxectos do AD). A súa sintaxe é a seguinte: `dsrm DN_do_obxecto_a_eliminar [opcións]`. Entre as opcións empregadas máis habitualmente, temos as seguintes:

- `-noprompt`. Se empregamos esta opción o sistema non pedirá confirmación á hora de eliminar o obxecto indicado.
- `-subtree`. Se empregamos esta opción, non so eliminaremos o obxecto indicado mediante o comando `dsrm`, senón que tamén eliminaremos os obxectos contidos nel se os houbera. Adicionalmente podemos acompañar esta opción coa opción `-exclude`. De facelo, eliminaremos os obxectos contidos no obxecto indicado mediante o comando `dsrm`, pero non eliminaremos o propio obxecto indicado mediante o comando `dsrm`.

Vexamos de seguido o comando necesario para eliminar a UO Java:



```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsrm ou=java,ou=software,ou=tecnicos,dc=empresa,dc=local -noprompt
dsrm correcto: ou=java,ou=software,ou=tecnicos,dc=empresa,dc=local

C:\Users\Administrador>
```

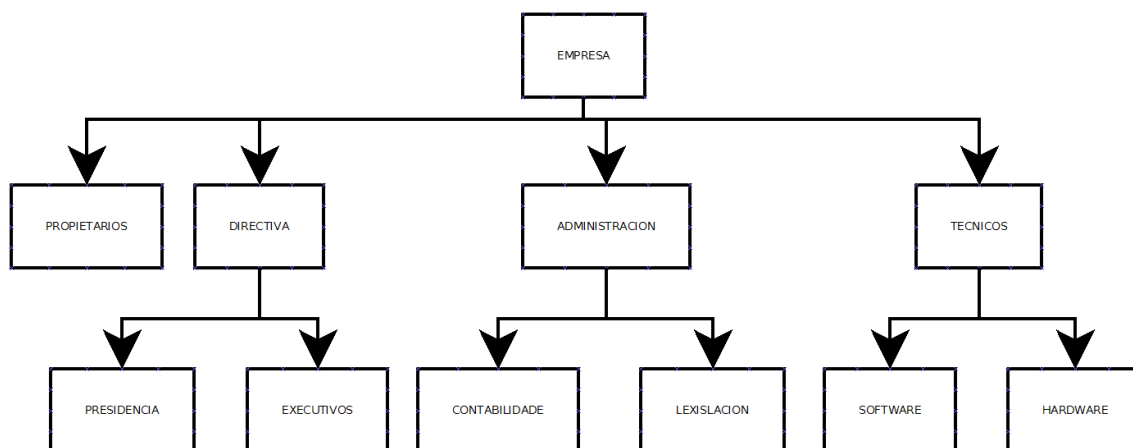
1.2.5 Usuarios e contas de usuarios

Para que o persoal da organización poida acceder ao sistema informático será necesario que o administrador cree un usuario para cada un deles. Un usuario se define mediante unha conta de usuario. Unha conta de usuario será empregada por unha persoa da organización para identificarse e poder acceder ao sistema informático e aos recursos compartidos no mesmo. Unha conta de usuario está composta por un nome de usuario ou login e un contrasinal. Un usuario pode identificarse e acceder ao sistema informático en calquera momento e desde calquera equipo que forme parte do dominio, aínda que este acceso xeral pode ser restrinxido polo administrador do dominio co fin de cumprir cos requisitos impostos na organización (p.e: o usuario so pode conectarse desde os equipos dunha determinada sala ou a certas horas do día). A conta de usuario utilizada para conectarse a un dominio tamén vai determinar a que recursos do mesmo pode acceder o usuario.

É tarefa do administrador dar de alta as contas de usuario do dominio. Habitualmente emprégase a ferramenta usuarios e equipos de AD, aínda que no caso de querer realizar un alta masiva de usuarios pódese facer mediante un script que faga uso dos comandos de consola utilizados para a creación de usuarios.

Creación de contas de usuario

Partindo das UOs creadas para o dominio empresa.local imos crear as contas de usuario para o persoal que traballa nos diferentes departamentos da organización. Lembremos que a estrutura física da organización era a seguinte:



De seguido imos indicar os nomes e os apelidos de cada unha das persoas que gardan algunha relación coa organización e que deben ter acceso aos recursos informáticos do dominio da mesma. Esta información, categorizada por departamentos, é a seguinte:

Departamento	Nome e apelidos
PROPIETARIOS	Ana Frago Bouzon
PROPIETARIOS	Maria Carnero Leira
PRESIDENCIA	Adrian Rego Vilar
EXECUTIVOS	Iria Suarez Platas
EXECUTIVOS	Iago Mendez Vazquez

CONTABILIDADE	Hector Rouco Diaz
CONTABILIDADE	Juan Ferreiro Verez
LEXISLACION	Lorena Pico Garcia
SOFTWARE	Sergio Brandariz Fuentes
SOFTWARE	Saul Lopez Lopez
SOFTWARE	Eva Romero Rivera
HARDWARE	Victor Anca Brage

Con anterioridade creamos unha serie de UOs para reflectir a estrutura física da organización sobre a estrutura lóxica do dominio. Agora facendo uso das UOs creadas con anterioridade imos categorizar os usuarios de xeito que ao dar de alta as contas de usuario cada unha delas será creada dentro da UO que fai referencia ao departamento físico ao que pertence a persoa para a cal imos dar de alta a conta de usuario.

Os nomes das contas de usuario deben de ter un nome único no dominio. Non poderán existir dúas contas de usuario co mesmo login. O login identifica dun modo unívoco a un usuario do dominio. A continuación amósase o login que imos asignar a cada usuario do dominio así como a UO na cal imos crear a súa conta de usuario:

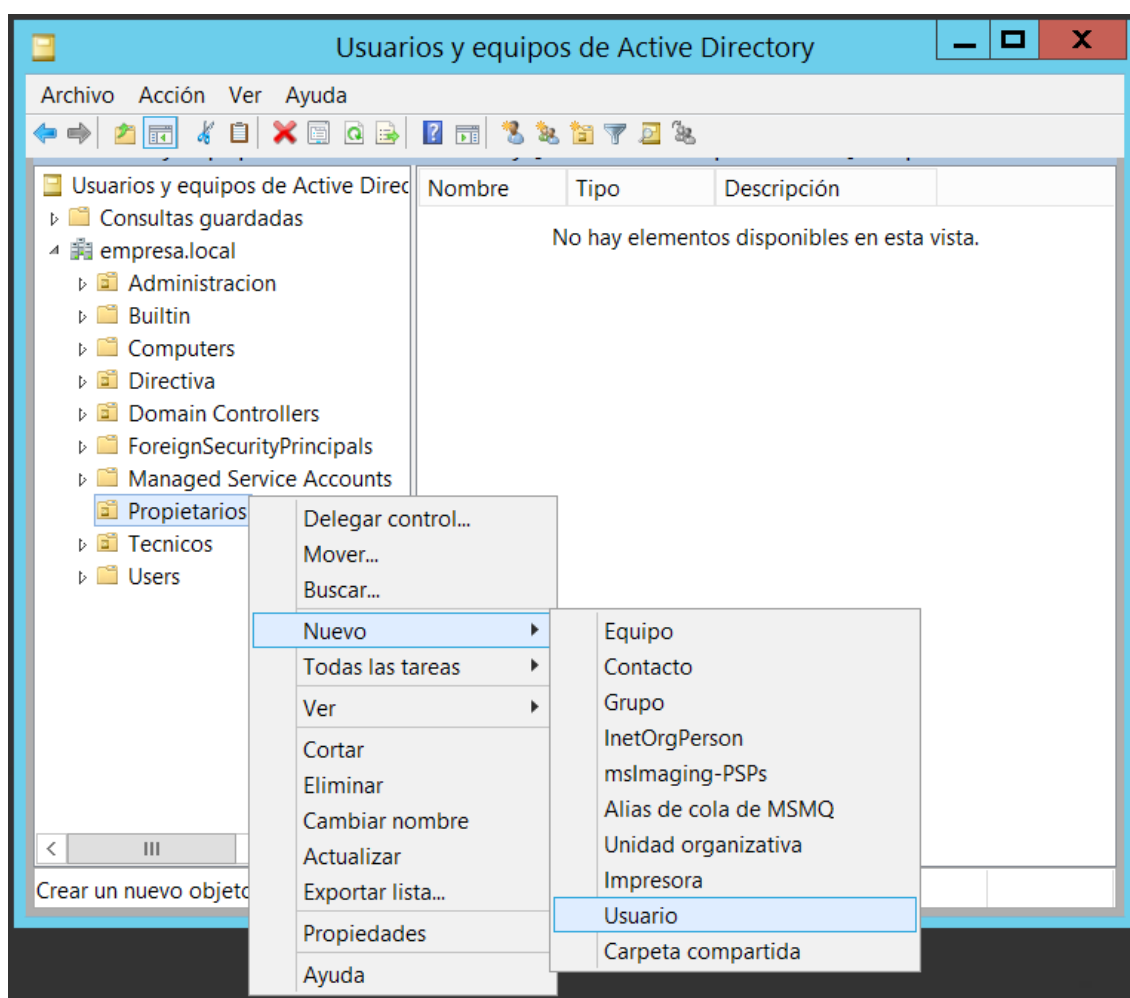
Nome e apelidos	Login	UO
Ana Fraga Bouzon	anafb	Propietarios
Maria Carnero Leira	mariac	Propietarios
Adrian Rego Vilar	adrianrv	Presidencia
Iria Suarez Platas	iriasp	Executivos
Iago Mendez Vazquez	iagomv	Executivos
Hector Rouco Diaz	hectorrd	Contabilidade
Juan Ferreiro Verez	juanfv	Contabilidade
Lorena Pico Garcia	lorenapg	Lexislacion
Sergio Brandariz Fuentes	sergiobf	Software
Saul Lopez Lopez	sauill	Software
Eva Romero Rivera	evarr	Software
Victor Anca Brage	victorab	Hardware

O criterio á hora de establecer os logins é unha cuestión que debe decidir o administrador do dominio. Neste caso decidiuse que os nomes das contas de usuario van estar compostas polo primeiro nome do usuario seguido das iniciais dos seus dos apelidos. Pode darse o caso de que por coincidencias de nomes e iniciais dos apelidos algún login repítase. Neste ultimo caso será labor do administrador o solucionar o problema.

Como pódese observar na táboa anterior, estamos asignando a cada usuario á UO que representa ao departamento físico ao que pertence o usuario. Isto permitiranos máis adiante o refinamento da administración do dominio en función da actividade desenvolvida dentro da organización por cada traballador.

Unha vez decidido cales son os logins das contas de usuario que imos crear, procedemos a elo. Vexamos o proceso para a primeira usuaria da lista, Ana Fraga Bouzon. Empregando a ferramenta de usuarios e equipos de AD, prememos co botón dereito sobre a UO á que

pertence o usuario que queremos dar de alta. Do menú contextual que se abre seleccionamos a opción nuevo e do novo menú contextual que se abre seleccionamos a opción usuario:



Amosarase a seguinte pantalla:

Nuevo objeto: Usuario

Crear en: empresa.local/Propietarios

Nombre de pila: Iniciales:

Apellidos:

Nombre completo:

Nombre de inicio de sesión de usuario: @empresa.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

< Atrás Siguiente > Cancelar

Mediante esta pantalla indicaremos o nome da conta de usuario e opcionalmente outra información de identificación do usuario:

Nuevo objeto: Usuario

Crear en: empresa.local/Propietarios

Nombre de pila: Iniciales:

Apellidos:

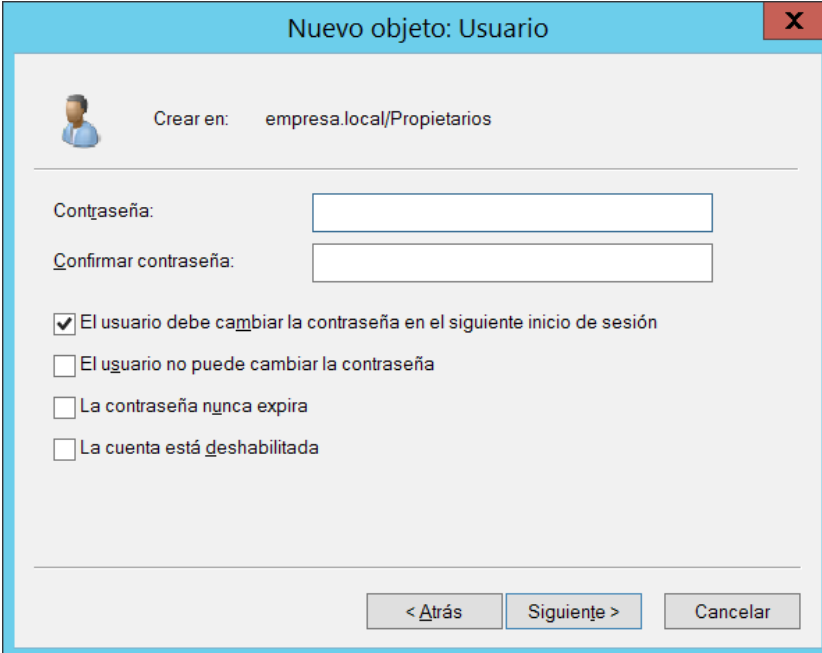
Nombre completo:

Nombre de inicio de sesión de usuario: @empresa.local

Nombre de inicio de sesión de usuario (anterior a Windows 2000):

< Atrás Siguiente > Cancelar

O login de usuario para acceder ao dominio será o indicado na caixa de texto nombre de inicio de sesión de usuario. Prememos sobre o botón siguiente y amosarase la siguiente pantalla:



Nuevo objeto: Usuario

Crear en: empresa.local/Propietarios

Contraseña:

Confirmar contraseña:

☒ El usuario debe cambiar la contraseña en el siguiente inicio de sesión

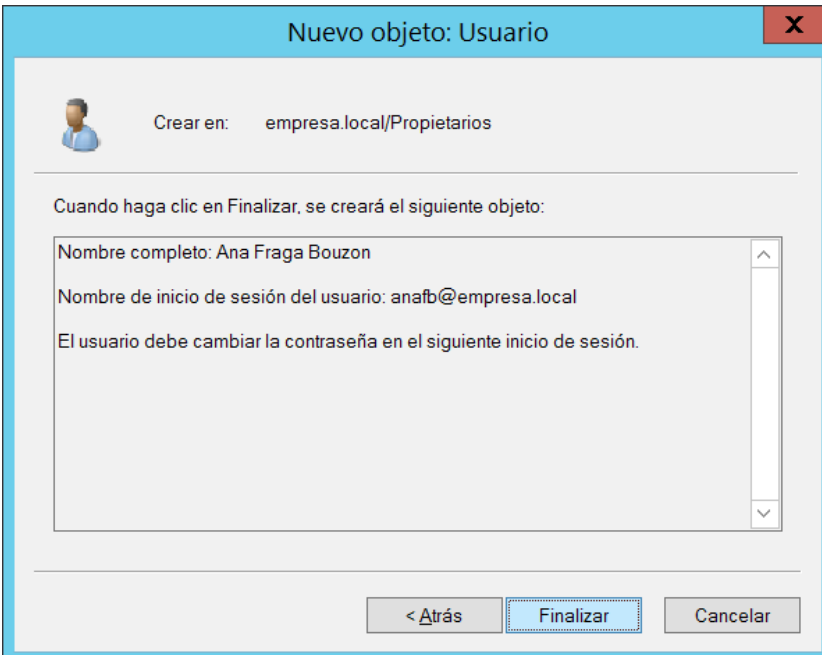
☐ El usuario no puede cambiar la contraseña

☐ La contraseña nunca expira

☐ La cuenta está deshabilitada

< Atrás Siguiente > Cancelar

Mediante esta pantalla establecerase a información relativa á creación e xestión do contrasinal do usuario. O contrasinal introducido debe de cumprir cos requisitos de complexidade establecidos nas directivas de seguridade do sistema. Respecto aos campos asociados as casillas de verificación pouco hai que dicir xa que son suficientemente descriptivos. Quizás pódese comentar sobre o último campo (la conta esta deshabilitada) que no caso de marcalo, a pesar de que creamos a conta de usuario, dita conta non poderá ser utilizada ata que o administrador non a habilite (unha conta pode ser habilitada ou deshabilitada polo administrador en calquera momento). Unha vez introducido un contrasinal que cumpra cos requisitos de complexidade, prememos sobre o botón seguinte. Amosarase unha pantalla que resume as características da conta de usuario que vai ser creada:



Nuevo objeto: Usuario

Crear en: empresa.local/Propietarios

Cuando haga clic en Finalizar, se creará el siguiente objeto:

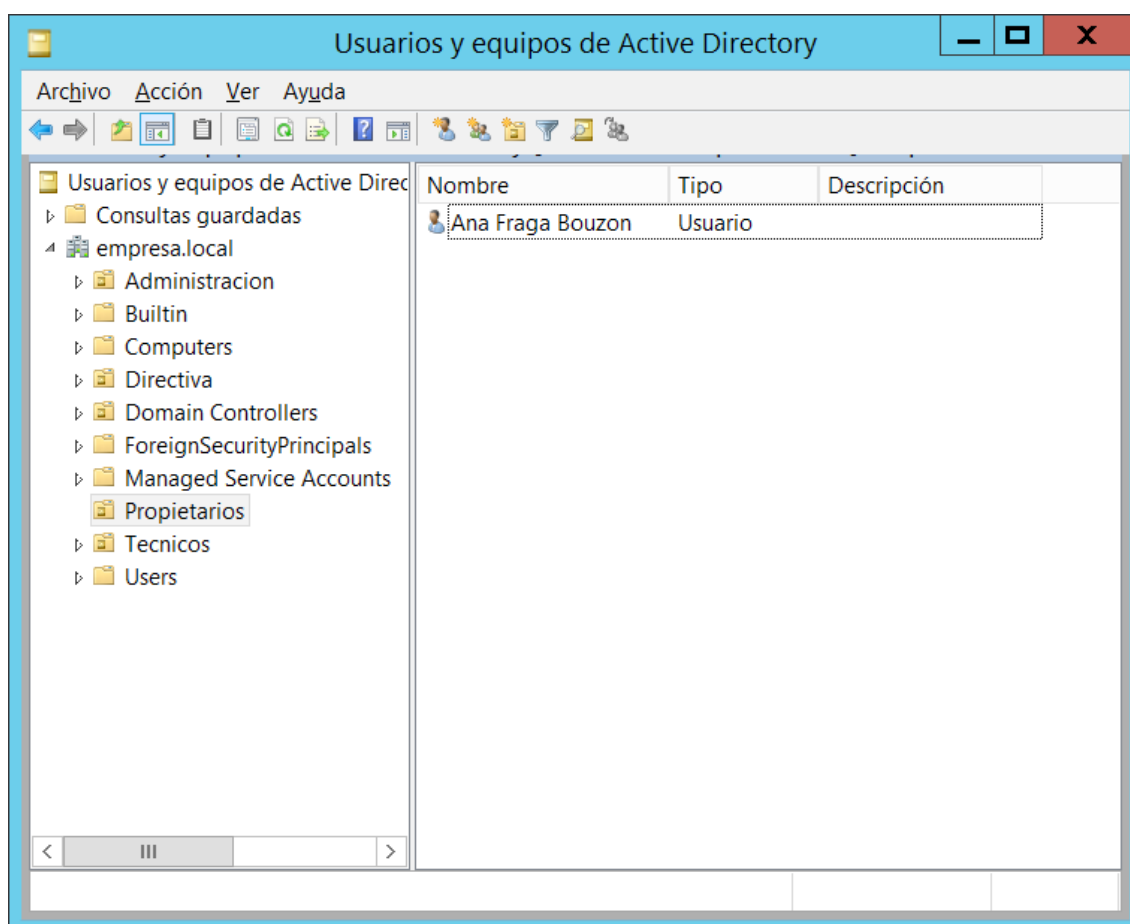
Nombre completo: Ana Fraga Bouzon

Nombre de inicio de sesión del usuario: anafb@empresa.local

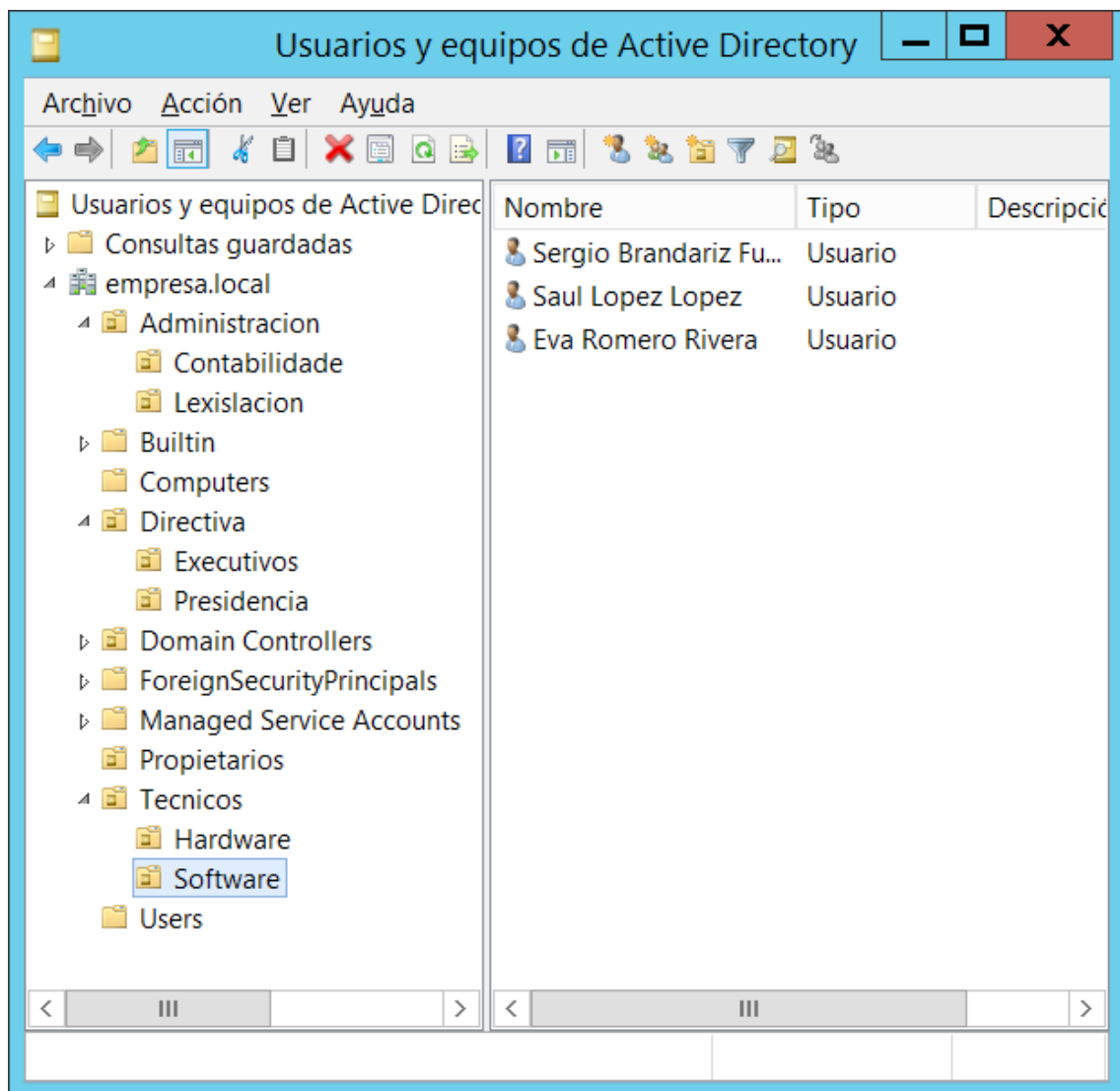
El usuario debe cambiar la contraseña en el siguiente inicio de sesión.

< Atrás Finalizar Cancelar

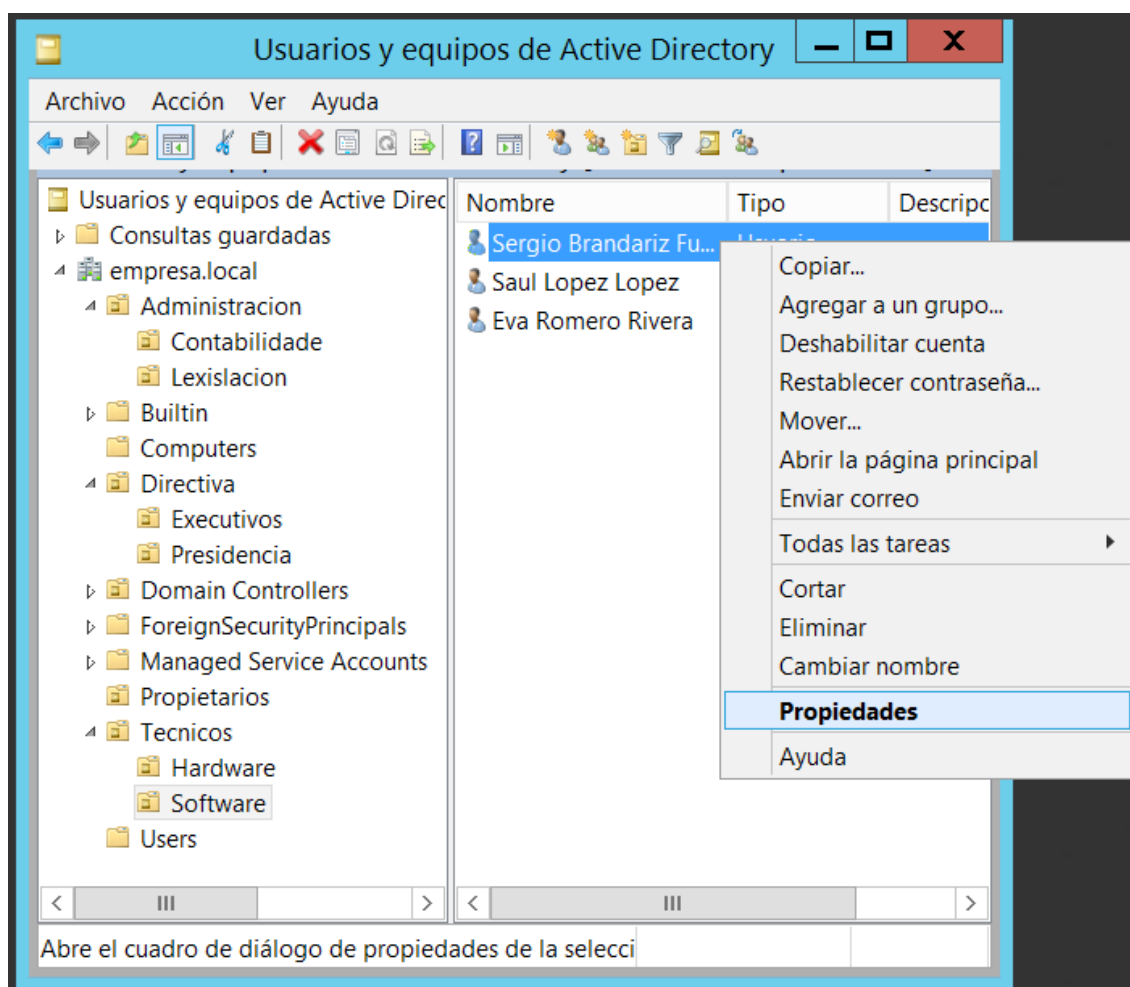
Se todo é correcto prememos sobre o botón finalizar. Crearase a conta de usuario e estará situada na UO indicada:



Procedemos a repetir o proceso para o resto de contas de usuario tendo en conta a UO na que creamos cada conta de usuario. Unha vez realizado o proceso teremos dadas de alta tódalas contas de usuario que necesitamos para que poida acceder o persoal da organización ao dominio.




Unha vez creada unha conta podemos visualizar e/ou modificar as súas propiedades. Para elo, premeremos co botón dereito sobre a conta sobre a que queremos operar e premeremos sobre propiedades:



Amosarse a seguinte pantalla:

Propiedades: Sergio Brandariz Fuentes

Entorno	Sesiones	Control remoto	Perfil de Servicios de Escritorio remoto	COM+			
General	Dirección	Cuenta	Perfil	Teléfonos	Organización	Miembro de	Marcado


Sergio Brandariz Fuentes

Nombre de pila:

 Iniciales:

Apellidos:

Nombre para mostrar:

Descripción:

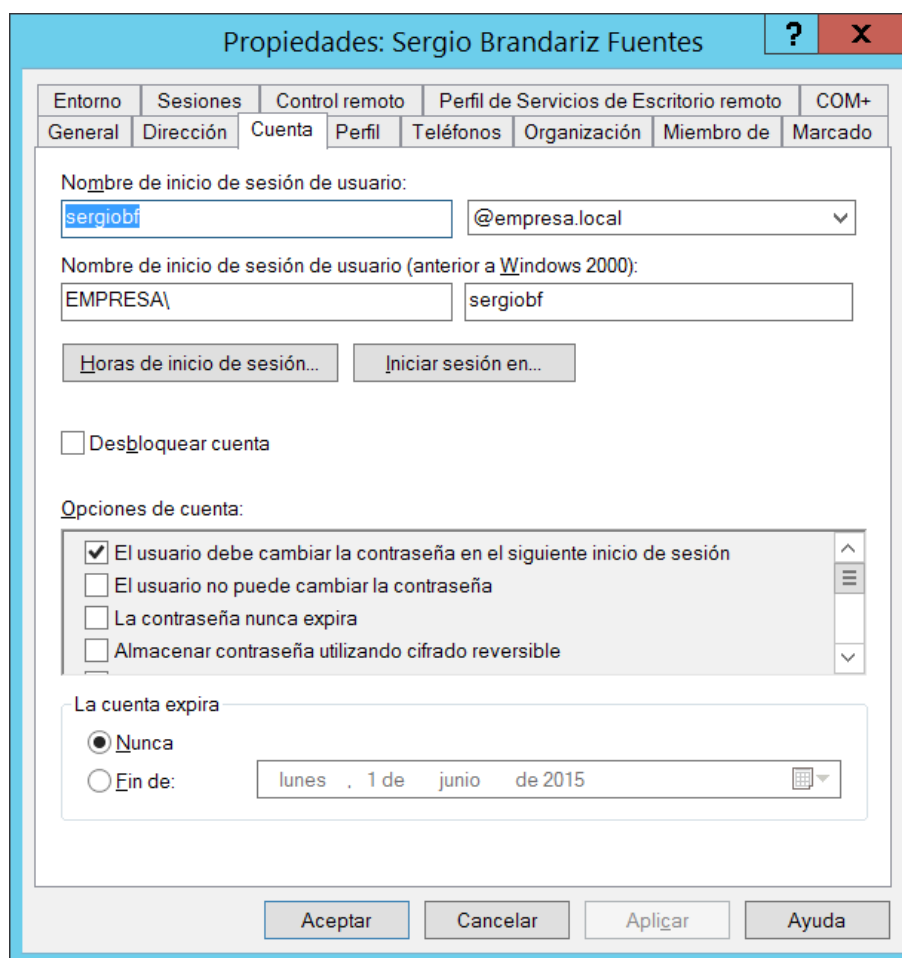
Oficina:

Número de teléfono:

Correo electrónico:

Página web:

Empregando as pestanas presentes nesta pantalla é posible xestionar un gran número de características dunha conta de usuario. Algunhas delas as veremos ao longo do desenvolvemento desta documentación. Agora ímonos centrar na pestana cuenta:



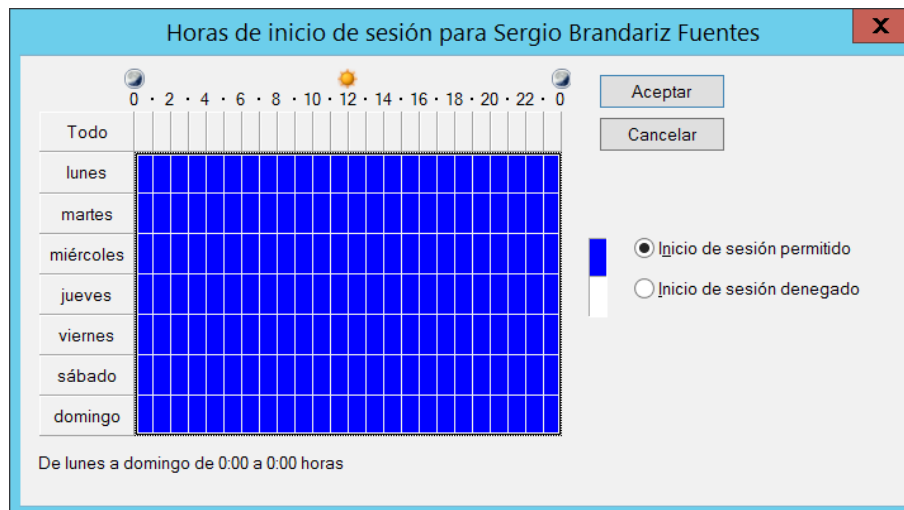
Vexamos as operacións que se soen realizar principalmente nesta pestaña:

- Indicar as horas de conexión permitidas a un usuario.
- Indicar desde que equipos do dominio pódese conectar un usuario.
- Desbloquear unha conta de usuario.
- Habilitar e deshabilitar unha conta de usuario.
- Fixar a data de expiración dunha conta de usuario.

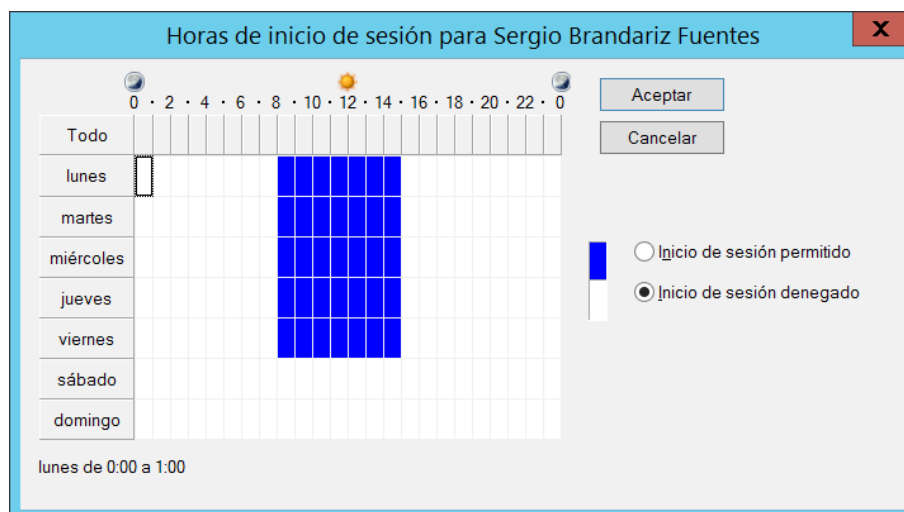
Vexamos estas operacións por partes.

Horas de conexión permitidas a un usuario

É posible que non nos interese que calquera usuario poida conectarse ao dominio en calquera momento. P.e. quizais so interéñenos que o persoal de contabilidade so pódase conectar de oito da mañá a seis da tarde de luns a venres. Para limitar as horas de acceso ao dominio dun usuario deberemos premer no botón Horas de inicio de sesión. Abrirase a seguinte xanela:



Mediante esta xanela poderemos indicar graficamente a que horas e que días pode iniciar sesión o usuario no dominio. P.e., se quixéramos que este usuario so poida conectar de luns a venres de oito da mañá a tres da tarde, configuraríamos esta pantalla deste xeito:



Equipos permitidos para realizar unha conexión

É posible que a pesar de que o dominio estea composto por varios equipos non queiramos que tódolos usuarios pódanse conectar desde calquera equipo. P.e., quizais queiramos que o usuario juanfvy unicamente podase conectar desde os equipos CONTABILIDADE1 e CONTABILIDADE2. Para limitar desde que equipos pódese conectar un usuario deberemos premer sobre o botón iniciar sesión en. Amosarase a seguinte pantalla:

Estaciones de trabajo de inicio de sesión

En Nombre de equipo, escriba el nombre NetBIOS o DNS (Sistema de nombres de dominio) del equipo.

Este usuario puede iniciar sesión en:

☒ Todos los equipos

☐ Los siguientes equipos

Nombre de equipo:

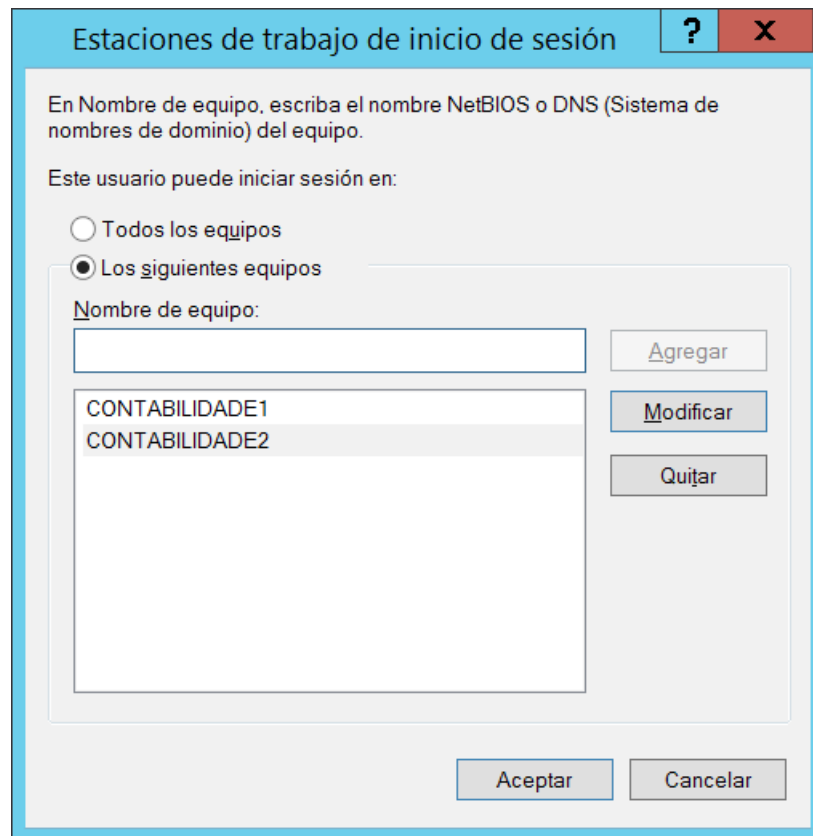
Agregar

Modificar

Quitar

Aceptar Cancelar

Esta pantalla danos dúas opcións. A primeira opción (todos los equipos) permite ao usuario conectarse desde tódolos equipos. A segunda opción (los siguientes equipos) permite indicar os equipos desde os que é posible que o usuario conéctese ao dominio. P.e., se quixéramos que o usuario que estamos configurando so poida acceder aos equipos CONTABILIDADE1 e CONTABILIDADE2 configuraremos a pantalla deste xeito:



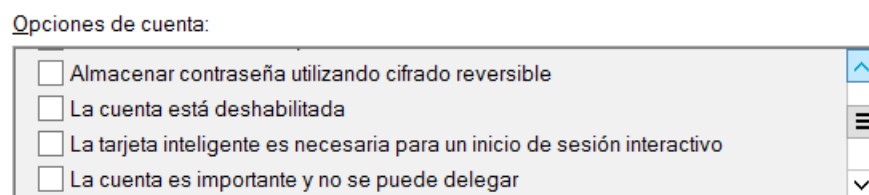
A maneira de identificar os equipos desde os que pode conectarse o usuario é ou ben mediante o seu nome NETBIOS ou ben mediante o seu nome DNS completo.

Desbloqueo dunha conta de usuario

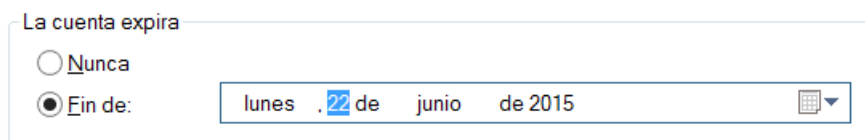
É posible que o administrador determine regras para minimizar a posibilidade de que unha conta de usuario sexa accedida ilegalmente. P.e, pódese establecer o número de veces que un usuario introduce un contrasinal erróneo. No caso de chegar ao límite de veces que o usuario pode introducir un contrasinal erróneo a conta de usuario queda bloqueada e é preciso que o administrador a desbloquee. Nun caso como o anterior, a conta podería ser desbloqueada facendo uso da casilla de verificación desbloquear cuenta.

Habilitación e deshabilitación dunha conta de usuario

Unha conta de usuario, a pesar de estar dada de alta no AD pode que sexa utilizable ou pode que non. Se unha conta esta habilitada é utilizable, pero se está inhabilitada non se pode empregar para acceder a ningunha máquina do dominio. Para habilitar ou deshabilitar unha conta de usuario desmarcaremos ou marcaremos respectivamente a casilla de verificación la cuenta está deshabilitada presente no listado Opciones de cuenta:



Fixar a data de expiración dunha conta de usuario. É posible que queiramos que unha conta sexa válida temporalmente ata unha data dada. Para limitar a duración dunha conta de usuario e fixar cando debe de expirar emprégase o panel la cuenta expira presente nas propiedades da conta de usuario:



Se non queremos que a conta expire seleccionaremos o botón de radio nunca. No caso contrario, seleccionaremos o botón de radio fin de e indicaremos a data de expiración da conta de usuario.

Familia de comandos ds

Ao igual que vimos anteriormente na xestión de UOs, tamén é posible xestionar as contas dos usuarios mediante comandos de consola. Aínda que existen varios métodos para facelo, neste caso ímonos centrar na familia de comandos ds. Os comandos da familia ds provistos polo sistema para xestionar contas de usuario son os mesmos que vimos para a xestión de UOs pero con pequenas variacións adaptadas á xestión de contas de usuario.

Dsadd

Para comezar, falaremos do comando dsadd user. Este comando é empregado para dar de alta unha conta de usuario. A súa sintaxe é a seguinte: dsadd user DN_do_obxecto_a_engadir [opcións]. É salientable reseñar cal é a estrutura dun DN dunha conta de usuario. Anteriormente vimos cal era a estrutura dos DNs das UOs. As UOs teñen a estrutura que teñen debido a que son contedores doutros obxectos do AD. En realidade son ramas na árbore do AD. Sen embargo, as contas de usuario son follas da árbore do AD e a súa sintaxe no referente á definición dos seus DNs é diferente. Por exemplo, supoñamos que temos o dominio definicion.local. Dentro deste dominio temos a UO usuarios e dentro da UO usuarios temos definido ao usuario marcos. Neste caso, o DN da UO é como xa ben sabemos ou=usuarios,dc=definicion,dc=local. Sin embargo, o DN para o usuario marcos é o seguinte: cn=marcos, ou=usuarios,dc=definicion,dc=local. Como podemos observar, o DN da conta do usuario marcos, ten dúas partes. Unha primeira parte, cn=marcos, na cal indicamos mediante cn (common name) o nome do obxecto na árbore do AD (o nome da folla dentro da árbore do AD). Ademais ahi unha segunda parte, ou=usuarios,dc=definicion,dc=local, mediante a cal definimos a localización do obxecto marcos dentro da estrutura da árbore do AD indicando tódalas ramas a seguir desde a raíz da árbore para alcanzar ao obxecto marcos.

Respecto ás opcións que podemos empregar co comando dsadd user, as máis salientables son as seguintes:

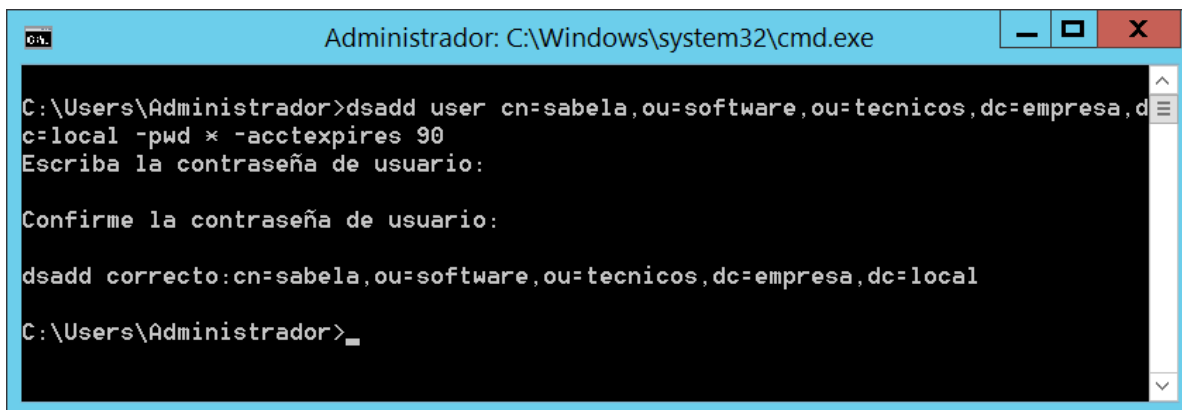
- -disabled valor. Mediante este parametro indicamos se a conta de usuario está ou non está deshabilitada. Valor pode valer yes, en cuxo caso a conta estará deshabilitada ou pode valer no, en cuxo caso o conta non estará deshabilitada. O valor por defecto é no.
- -pwd valor. A través deste parámetro podemos indicar o contrasinal a empregar para o conta de usuario. Valor pode tomar o valor do propio contrasinal ou o valor *. No caso

de que valor valga *, o comando dsadd solicitaranos o contrasinal da conta de usuario durante a súa creación.

- -mustchpwd valor. Mediante esta opción indícase se o usuario debe cambiar o contrasinal no próximo inicio de sesión. Valor pode valer yes, en cuxo caso o usuario deberá cambiar o contrasinal no seguinte inicio de sesión, ou pode valer no (valor por defecto) en cuxo caso non é necesario que o usuario cambie o seu contrasinal no seguinte inicio de sesión.
- -canchpwd valor. Mediante esta opción indícase se o usuario pode cambiar o contrasinal. Valor pode valer yes (valor por defecto), en cuxo caso o usuario pode cambiar o contrasinal, ou pode valer no en cuxo caso o usuario non pode cambiar o seu contrasinal.
- -acctexpires valor. A través desta opción podemos establecer a data de expiración dunha conta de usuario. Valor pode ser algún dos seguinte valores: 0, número positivo ou never. Se vale 0 a conta expiraráa ao final do día. Se é un número positivo, dito número indica o número de días que deben pasar para que a conta expire. Se vale never, a conta non expirará nunca.

Existe moitas máis opcións que se poden utilizar xunto ao comando dsadd user. Algunhas verémolas en apartados posteriores desta documentación, mentres que outras serán necesarias para a realización dos exercicios propostos de modo que requirirán de certo traballo de investigación co fin de coñecelas.

Para rematar, imos desenvolver un exemplo no cal crearemos un usuario de nome sabela na UO software. Ademais, indicaremos ao sistema que nos solicite o contrasinal da conta de usuario durante o proceso de creación da mesma e tamén indicaremos que dita conta de usuario debe de expirar en noventa días:



```
Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsadd user cn=sabela,ou=software,ou=tecnicos,dc=empresa,dc=local -pwd * -acctexpires 90
Escriba la contraseña de usuario:
Confirme la contraseña de usuario:
dsadd correcto:cn=sabela,ou=software,ou=tecnicos,dc=empresa,dc=local
C:\Users\Administrador>_
```

Dsmod, dsquery, dsget e dsrm

Os comandos dsmod, dsquery e dsget xa foron descritos á hora de explicar o seu funcionamento sobre as UOs. Respecto ao emprego destes comandos sobre a xestión de usuarios, a súa funcionalidade é similar, coa diferenza de que traballan sobre contas de usuario en lugar de sobre UOs. Unicamente imos indicar cal é a sintaxe básica para cada un deles, deixando o descrición das opcións para que sexan investigadas ao longo da resolución dos exercicios propostos:

- dsmod user DN_conta_usuario_a_modificar_atributos [opcións]
- dsquery user DN_contas_usuario_a_buscar [opcións]
- dsget user tipo DN_conta_usuario_a_detallar [opcións]

En canto ao comando dsrm, xa indicamos previamente que se emprega para eliminar diferentes elementos da árbore do AD, incluíndo entre os obxectos eliminables por este comando as contas de usuario.

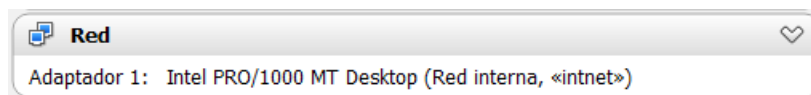
1.2.6 Engadir equipos ao dominio

Unha vez que creamos o dominio e que temos usuarios que poidan facer emprego del, chega o momento de facer que os equipos da rede formen parte do dominio. Para elo é necesario configurar cada un dos equipos que queiramos que formen parte do dominio.

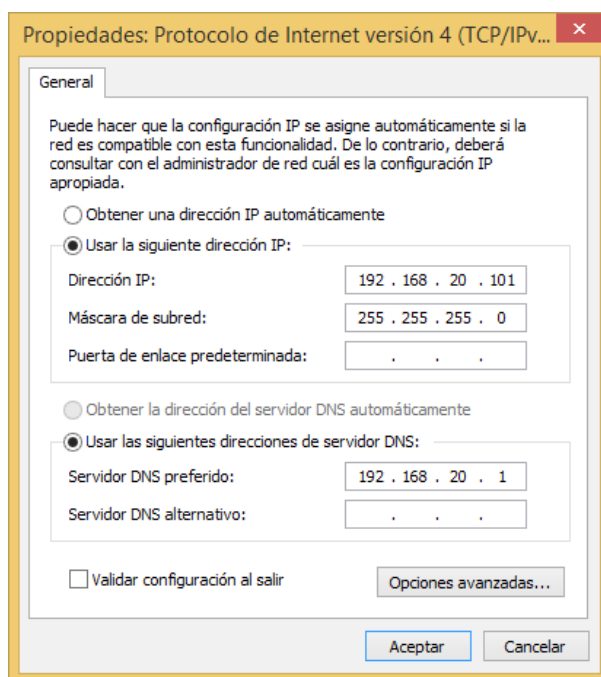
Engadir estacións de traballo Windows ao dominio

Imos describir o proceso que hai que realizar para unir unha estación de traballo de tipo Windows 8.1 Professional ao dominio empresa.local creado anteriormente (A estación de traballo estará virtualizada mediante VirtualBox). O nome do equipo vai ser CLIENTE1. Unicamente vai ter un usuario creado. O seu login é usuariolocal e o seu contrasinal é o mesmo co login. É un usuario de tipo administrador local.

Restauramos o servizo virtualizado de Windows 8.1 no entorno de VirtualBox. Unha vez restaurado o servizo virtualizado imos configurar a máquina virtual xerada para que teña unha tarxeta de rede. Dita tarxeta de rede deberá estar na mesma rede que a tarxeta de rede do controlador de dominio (a que atende á LAN):

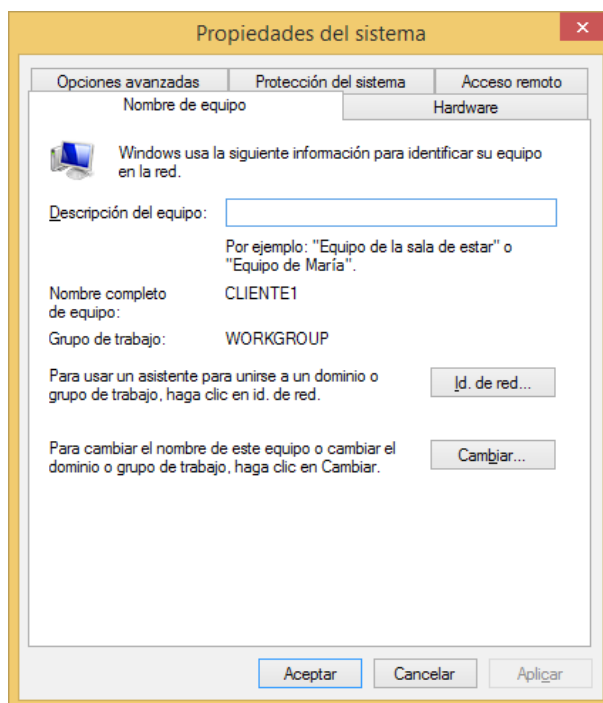


Unha vez que arranquemos a máquina de Windows 8.1 deberemos configurar a súa tarxeta de rede para que poida comunicarse co equipo SERVIDOR. Asignarémolle a dirección ip 192.168.20.101:



Fixémonos na imaxe anterior en que ademais de configurar a dirección do equipo tamén configuramos a dirección do servidor de DNS, indicando que dita tarefa será realizada polo equipo SERVIDOR (192.168.20.1) no cal, lembremos, temos instalado un servidor de DNS. Unha vez que temos configurada a rede e comprobado que temos visibilidade sobre o controlador de dominio, pasamos a engadir á estación de traballo Windows 8.1 ao dominio.

Evidentemente para engadir unha estación de traballo ao dominio é necesario que o controlador de dominio, que é o lugar onde vaise dar de alta o equipo, estea levantado. Unha vez dito isto, accedemos na estación de traballo á xanela empregada para cambiar o nome do equipo:



Como podemos observar na imaxe anterior a estación de traballo pertence a un grupo de traballo chamado WORKGROUP. Para cambiar este comportamento e facer que pase a pertencer ao dominio empresa.local, prememos sobre o botón cambiar. Amosarase a seguinte pantalla:

Cambios en el dominio o el nombre del equipo [X]

Puede cambiar el nombre y la pertenencia de este equipo. Los cambios podrían afectar al acceso a los recursos de red.

Nombre de equipo:
CLIENTE1

Nombre completo de equipo:
CLIENTE1

Más...

Miembro del

☐ Dominio:

☒ Grupo de trabajo:
WORKGROUP

Aceptar Cancelar

Esta pantalla permítenos cambiar o nome do equipo, pero tamén permítenos introducir un equipo nun dominio ou nun grupo de traballo. Neste caso como o que queremos facer é introducir á estación de traballo nun dominio, seleccionamos o botón de opción dominio e indicamos o nome do dominio ao cal queremos engadir a estación de traballo:

Cambios en el dominio o el nombre del equipo [X]

Puede cambiar el nombre y la pertenencia de este equipo. Los cambios podrían afectar al acceso a los recursos de red.

Nombre de equipo:
CLIENTE1

Nombre completo de equipo:
CLIENTE1

Más...

Miembro del

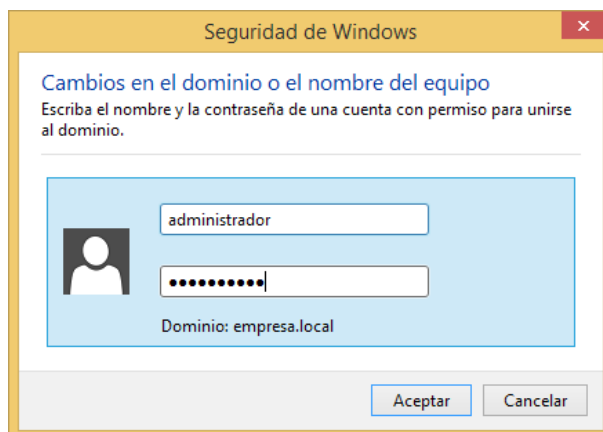
☒ Dominio:
empresa.local

☐ Grupo de trabajo:
WORKGROUP

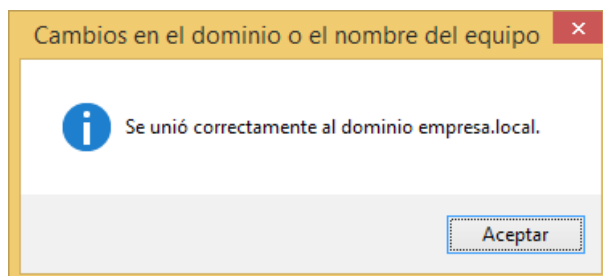
Aceptar Cancelar

Unha vez indicado o nome do dominio ao que queremos engadir a estación de traballo prememos sobre o botón aceptar. Amósase unha pantalla na cal vaise pedir un usuario do dominio xunto co seu contrasinal. Dito usuario deberá de ter os privilexios necesarios para

poder engadir máquinas ao dominio. Neste caso, lembremos, temos no dominio ao usuario administrador e a tódolos usuarios que creamos previamente no AD. De tódolos usuarios que acabamos de indicar unicamente o usuario administrador ten os privilexios suficientes para engadir máquinas ao dominio, polo tanto é o usuario que empregaremos:



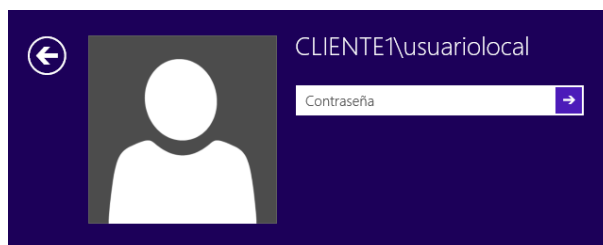
Unha vez introducido o login do usuario administrador e o seu contrasinal, prememos sobre o botón aceptar. Neste momento a estación de traballo vaise por en contacto co controlador de dominio para indicarlle que quere engadirse ao dominio que controla. Agora so resta esperar a resposta do controlador de dominio:



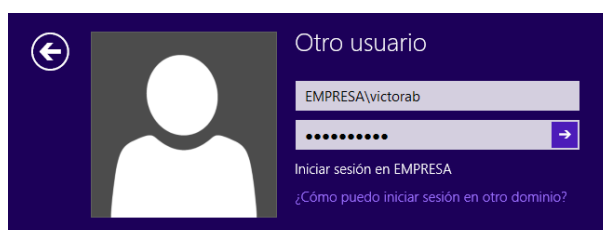
Comunícasenos que a operación de unión ao dominio da estación de traballo foi correcta. A pesar de que a operación foi correcta é necesario reiniciar a estación de traballo para que se apliquen os cambios, polo tanto procedemos a elo.

Autenticación no dominio

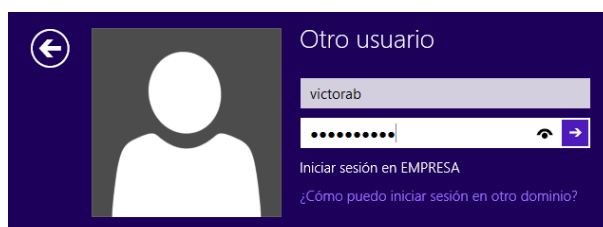
Unha vez reiniciada a estación de traballo poderemos identificarnos cun usuario local da máquina ou cun usuario do dominio. No caso de facelo cun usuario local da máquina non estaremos accedendo ao dominio e as restricións e os recursos aos que podamos acceder serán diferentes ás restricións aplicadas e aos recursos dispoñibles no caso de acceder como un usuario do dominio. Para acceder cun usuario local o login do usuario deberá ser do tipo `nome_equipo\login_usuario_local`:



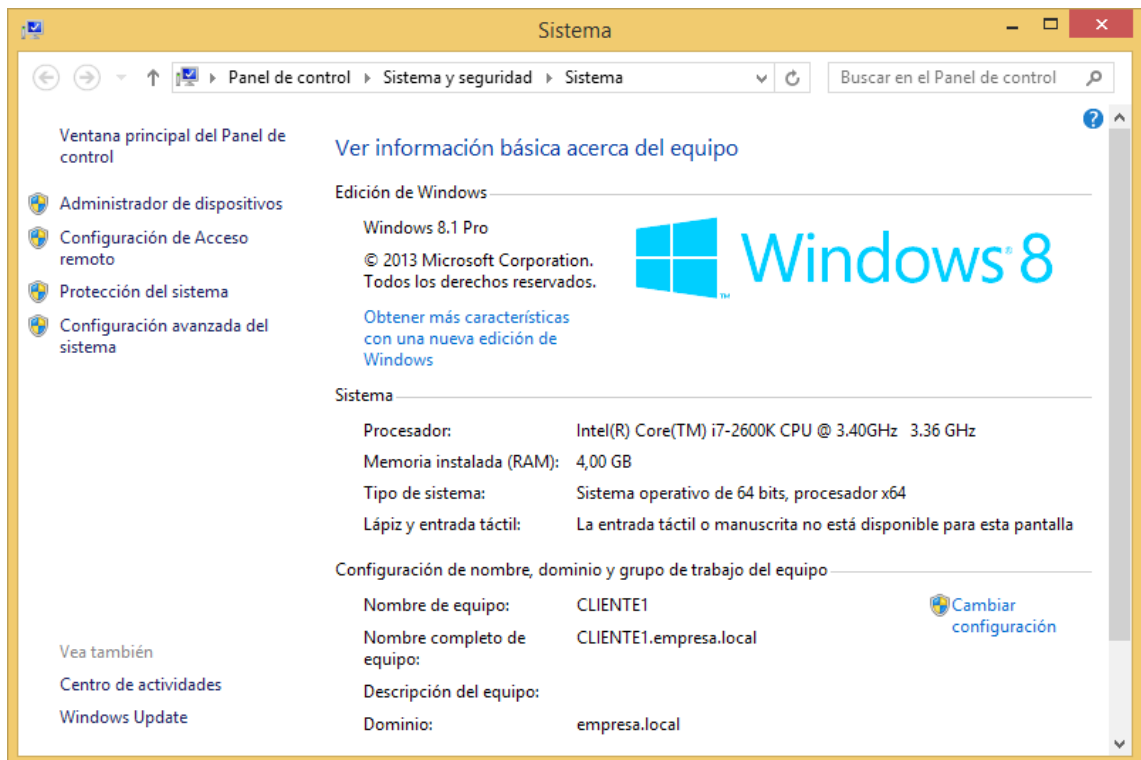
Para acceder como un usuario do dominio, o login do usuario deberá ser do tipo nome_dominio\login_usuario_dominio:



Se na parte inferior da pantalla de identificación se indica o nome do equipo ou o nome do dominio, será suficiente con indicar o login de usuario e o seu contrasinal:



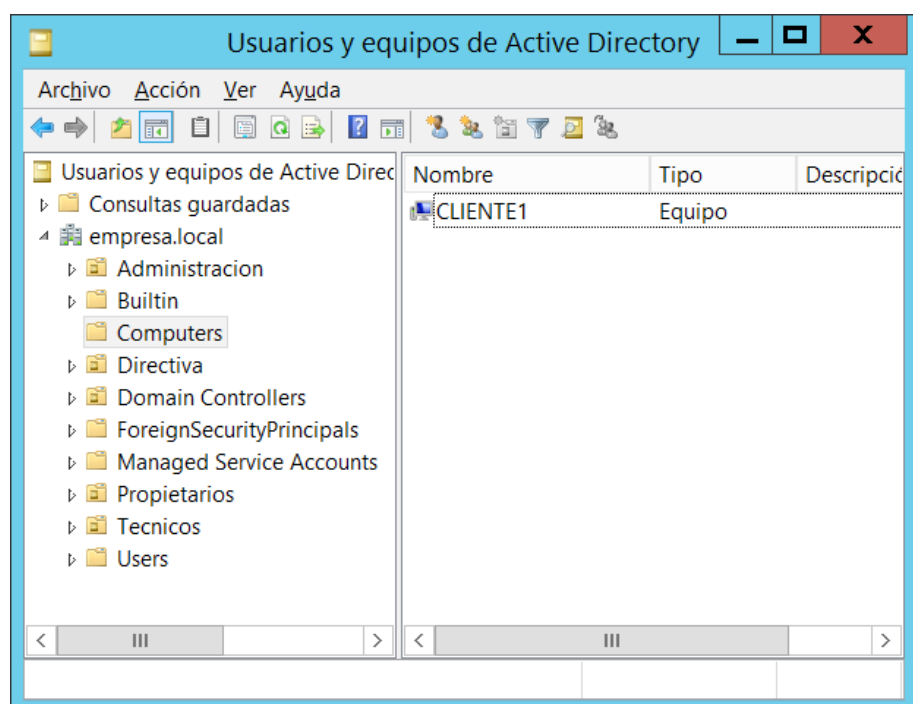
Unha vez identificados no dominio accederemos á estación de traballo. Esta operación de identificación a poderemos realizar con calquera usuario dado de alta no dominio. Será o controlador de dominio o que permitirá entrar ou non na estación de traballo en función das restricións establecidas sobre cada usuario. Para comprobar que realmente o equipo está engadido ao dominio podemos acceder ás propiedades do sistema:



Como pódese observar na imaxe anterior, o dominio ao que pertence esta estación de traballo é empresa.local, polo tanto podemos afirmar que a estación de traballo está engadida ao dominio.

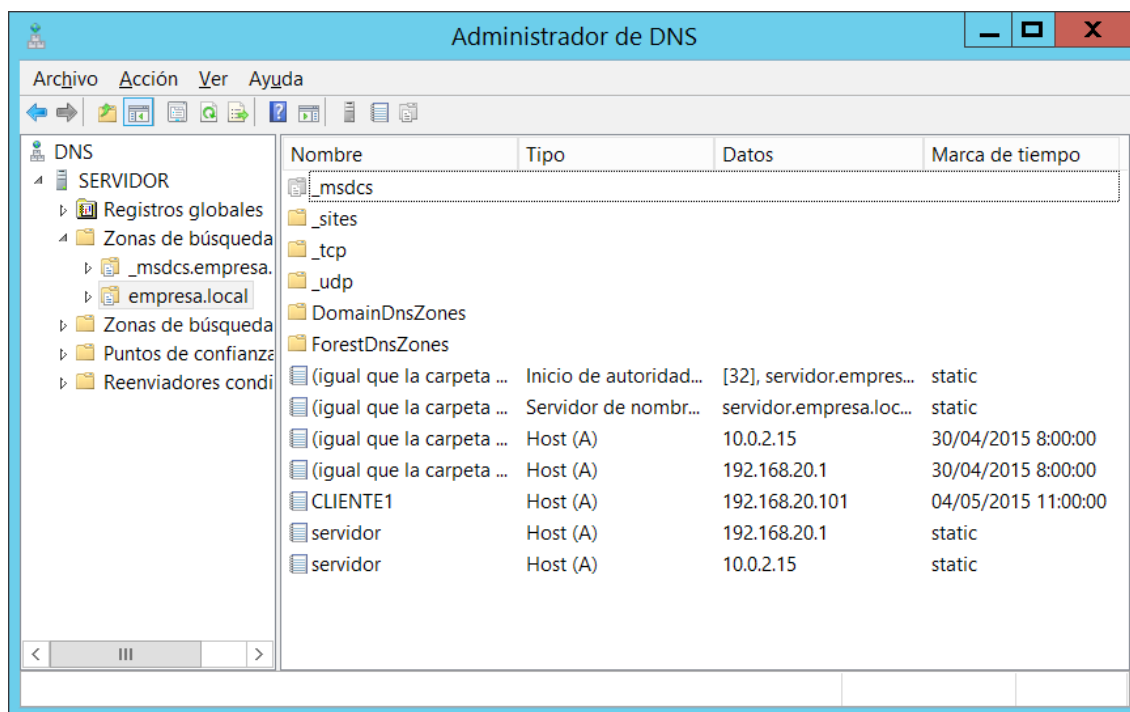
Estación de traballo vista desde o servidor

Se agora abrimos no controlador de dominio a ferramenta de usuarios e equipos de AD e accedemos á carpeta COMPUTERS amósase o seguinte:



Cada vez que engadamos unha nova máquina ao dominio esta pasa a ter un reflexo lóxico no AD. Por defecto o obxecto que representa a cada máquina engadida ao dominio é almacenado na carpeta Computers (aínda que nada impide movelo a outra localización dentro do AD). Neste caso podemos observar que creouse un novo obxecto que representa á estación de traballo que acabamos de engadir. Se accedemos ás súas propiedades podemos visualizar informacións sobre a máquina e realizar algunhas accións sobre ela.

Tamén comentar que ao engadir a máquina ao dominio deuse de alta automaticamente unha entrada no servidor DNS para identificar a máquina engadida mediante este servizo. Isto pódese visualizar mediante a consola de administración do servidor DNS:



1.2.7 Grupos

Os grupos son obxectos do AD. Serven para agrupar usuarios e equipos de modo que todo o contido no grupo pódase administrar como un único elemento. A finalidade dos grupos é facilitar a xestión administrativa do dominio.

Nun dominio hai recursos dispoñibles para os seus usuarios, pero non tódolos usuarios van ter o mesmo nivel de acceso sobre os recursos do dominio. Se non existiran os grupos teríamos que xestionar o acceso sobre os recursos do dominio usuario a usuario indicando explicitamente a que recursos pode acceder cada un deles. A existencia dos grupos libéranos desta tarefa. Na administración de recursos baseada en grupos asígnanse os permisos de acceso sobre un recurso ao grupo. Tódolos usuarios que pertencen a ese grupo van ter os mesmos permisos de acceso sobre o recurso. Isto evidentemente axiliza e aclara a administración do dominio. Supoñamos que p.e. administramos un dominio con cen usuarios e queremos dar permiso de lectura a oitenta deles (supoñamos que é o persoal de teleoperadores) sobre un arquivo. Se non existiran os grupos teríamos que dar permiso de lectura sobre o arquivo aos oitenta usuarios un a un. Coa existencia de grupos o que faremos será dar permiso de lectura ao grupo teleoperadores sobre o arquivo. Previamente teremos que crear un grupo chamado teleoperadores no cal engadiremos tódalas contas de usuario dos oitenta teleoperadores. Como vemos unha soa asignación de permisos sobre un grupo é

similar a realizar a asignación de permisos sobre cada uno dos membros do grupo o cal facilita enormemente a administración do dominio. Evidentemente a creación dun grupo debe planificarse axeitadamente para poder empregar os grupos correctamente á la hora de asignarlles permisos sobre os recursos.

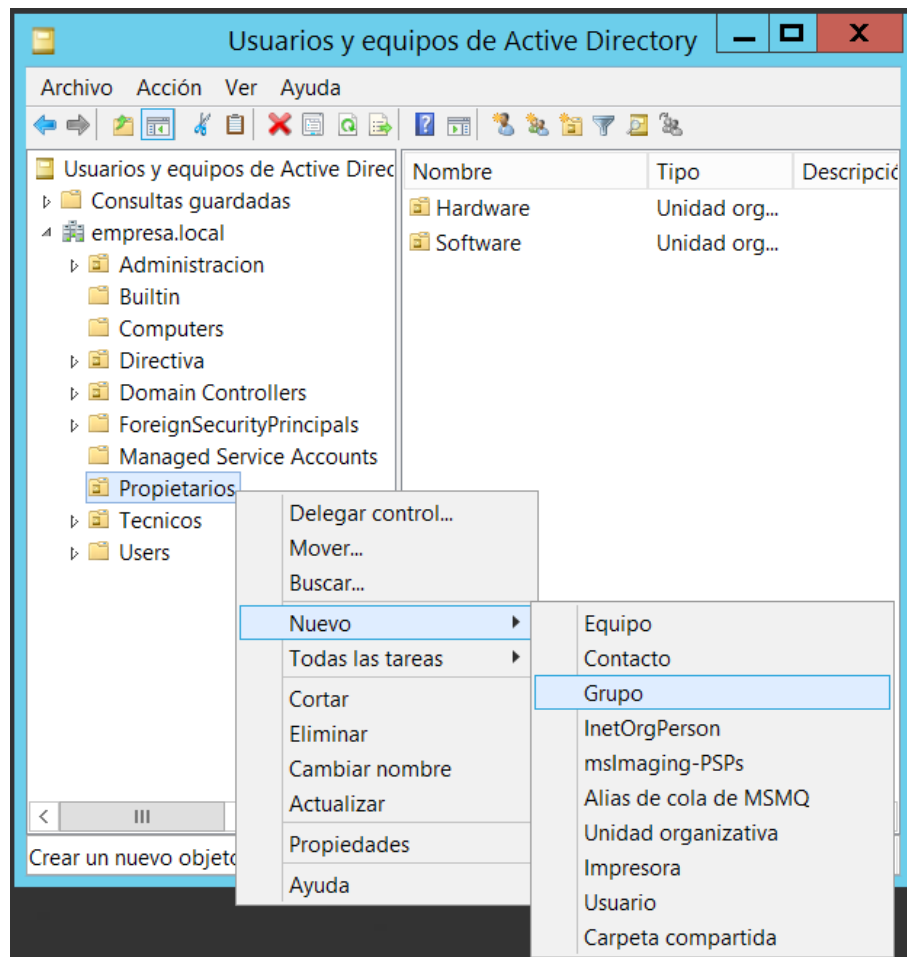
Non se deben confundir as UOs cos grupos. As UOs serven para aplicar directivas sobre seus membros. Os grupos serven para conceder permisos aos seus membros sobre os recursos do dominio.

Creación de grupos

Partindo dos usuarios creados para o dominio empresa.local imos crear os seguintes grupos no AD:

Grupo	Membros
G_Propietarios	Anafb mariac
G_Presidencia	adrianrv
G_Executivos	Iriasp iagomv
G_Administracion	Hectorrd juanfv lorenapg
G_SoftwareDesarrollo	Evarr saulll
G_SoftwareGestion	sergiobf
G_Hardware	victorab

Imos crear o grupo G_Propietario e a asignar os membros que compoñen o grupo. O primeiro que temos que facer é crear o grupo. Para elo desde a ferramenta de usuarios e equipos seleccionamos en que contedor queremos crear o grupo. Neste caso imos crear o grupo na UO Propietarios (podería crearse noutra UO o incluso nas carpetas predefinidas polo sistema. Simplemente vanse crear nesta UO por ter organizado o AD dunha maneira determinada). Prememos co botón dereito sobre a UO Propietarios. Despregarase un menú contextual. Neste menú eliximos a opción nuevo e no menú contextual que se desprega seleccionamos a opción grupo:



Abrirase a siguiente pantalla:

The screenshot shows the 'Nuevo objeto: Grupo' (New Object: Group) dialog box. The 'Crear en:' (Create in:) field is set to 'empresa.local/Propietarios'. There are two empty text boxes for 'Nombre de grupo:' and 'Nombre de grupo (anterior a Windows 2000):'. Below these are two sections: 'Ámbito de grupo' (Group Scope) with radio buttons for 'Dominio local', 'Global' (selected), and 'Universal'; and 'Tipo de grupo' (Group Type) with radio buttons for 'Seguridad' (selected) and 'Distribución'. At the bottom are 'Aceptar' (OK) and 'Cancelar' (Cancel) buttons.

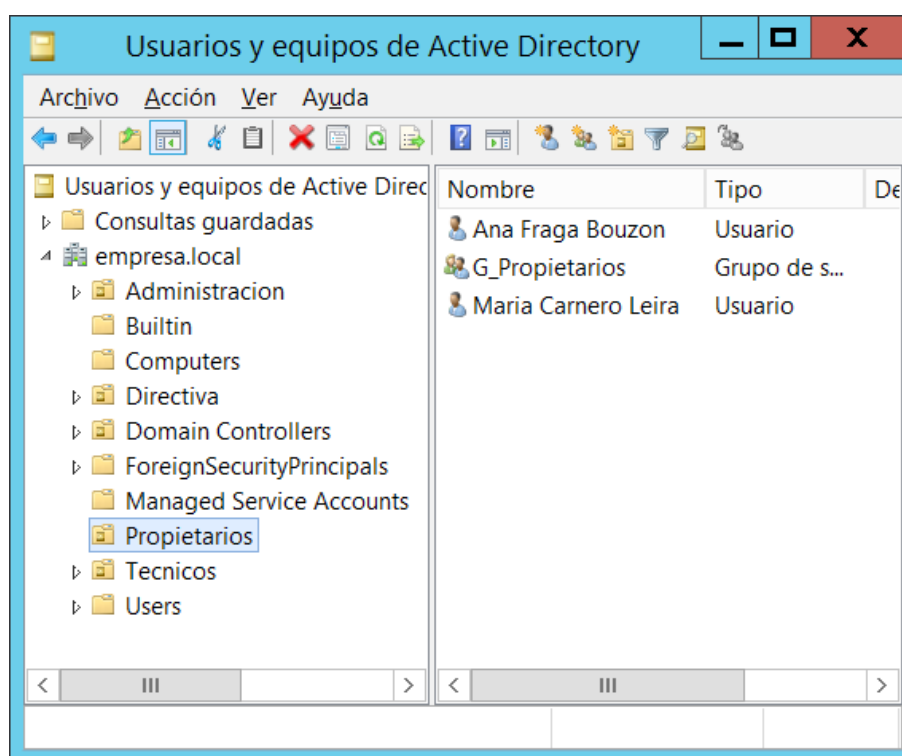
Empregando a caixa de texto Nombre de grupo introduciremos o nome do grupo que queremos crear, neste caso: G_Propietarios. Respecto ao botón de opción ámbito de grupo, serve para indicar cal é o alcance dos permisos dos usuarios pertencentes ao grupo:

- Dominio local: aos membros dun grupo local so pódeseles asignar permisos dentro dun dominio.
- Global: aos membros dun grupo global pódeseles asignar permisos en calquera dominio do bosque.
- Universal: aos membros dun grupo universal pódeseles asignar permisos en calquera dominio do bosque ou da árbore de dominios.

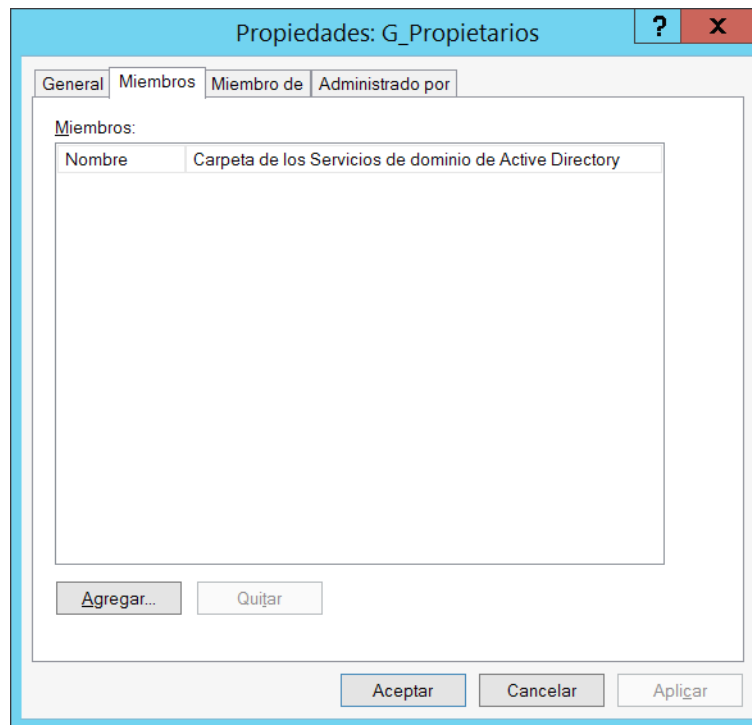
Respecto ao botón de opción tipo de grupo, serve para indicar cal é a utilidade do grupo:

- Seguridad: o grupo emprégase para asignar permisos sobre os recursos.
- Distribución: o grupo emprégase para crear listas de distribución de correo electrónico.

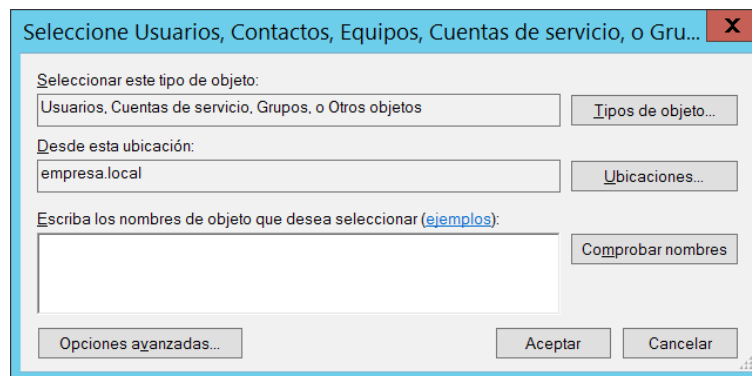
No noso caso imos crear os grupos para posteriormente xestionar os permisos sobre os recursos do dominio así que deixamos as opcións como están e prememos sobre o botón aceptar. Como podemos observar na ferramenta de usuarios e equipos de AD o grupo é creado satisfactoriamente:



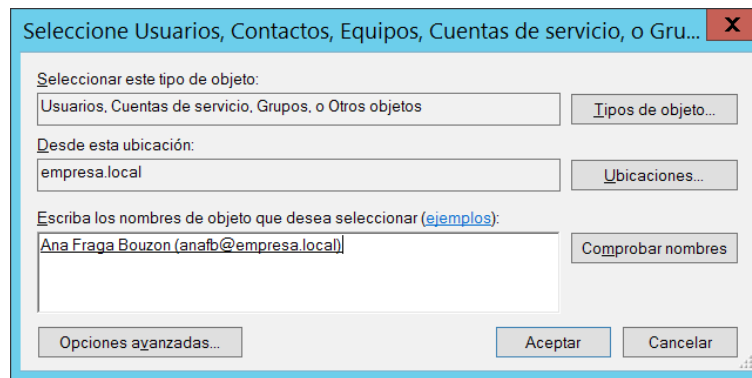
Agora restaría engadir os usuarios que pertencen ao grupo. Para elo prememos co botón dereito sobre o grupo G_Propietarios e accedemos ás súas propiedades. Dentro da xanela que se nos amosa seleccionamos a pestana membros:



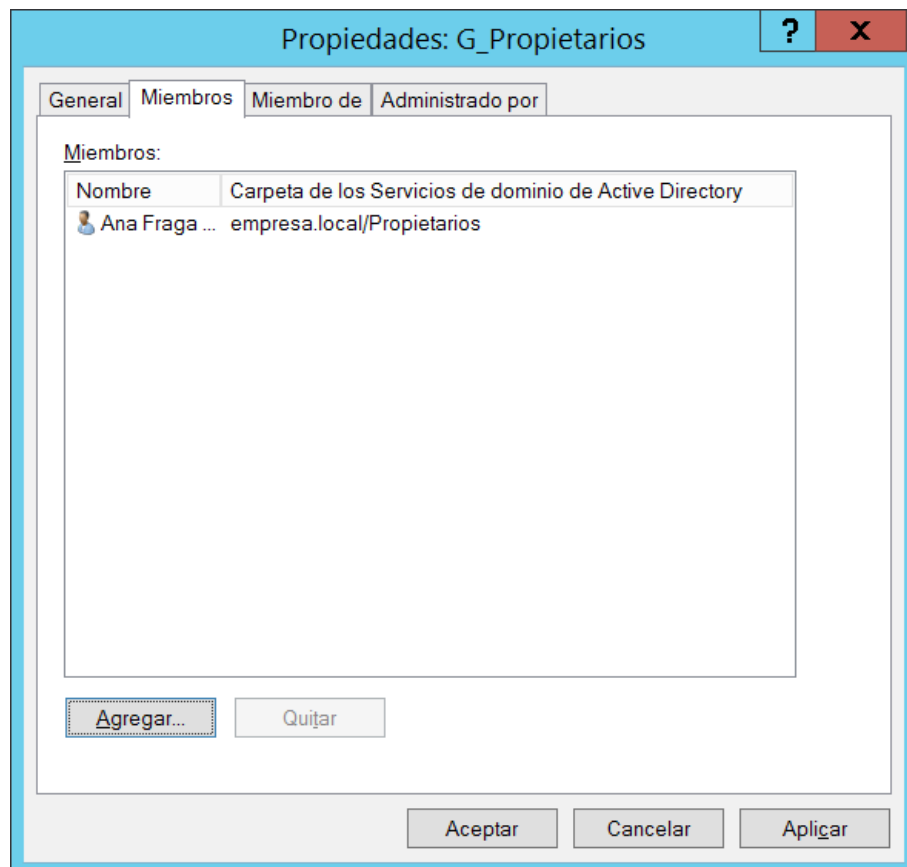
Mediante esta xanela podemos engadir ou eliminar os membros que forman parte do grupo. Para engadir un usuario prememos sobre o botón agregar. Abrirase a seguinte xanela:



Nesta xanela poderemos escribir o nome do membro ou membros que queremos engadir ao grupo, ou ben premer en opciones avanzadas. Se prememos sobre opciones avanzadas abrirase un buscador que vainos permitir buscar ao membro ou membros que queramos engadir ao grupo. Neste caso imos escribir no campo de texto o login do usuario anafb e adicionalmente imos premer sobre o botón comprobar nombres para asegurarnos de que o login introducido é correcto. Amosarase a seguinte pantalla:



Para finalizar prememos sobre o botón aceptar de modo que o usuario pasa a pertencer ao grupo G_Propietarios:

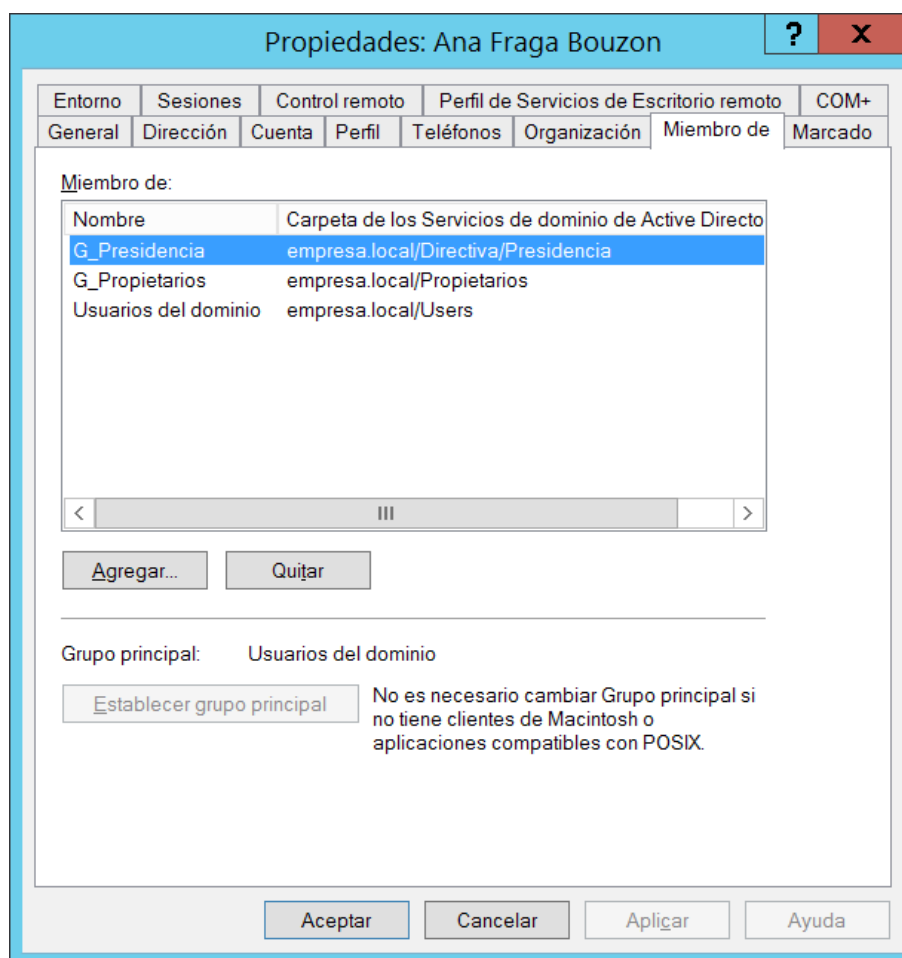


Se quixeramos eliminar do grupo a un usuario, unicamente teríamos que seleccionar nesta pantalla a dito usuario e premer sobre o botón quitar. Quitar a un usuario dun grupo non implica eliminar ao usuario do AD. Unha vez visto como agregar a un usuario a un grupo procedemos do mesmo modo para o resto dos grupos que queremos crear.

Pertenza dun usuario a varios grupos

Que un usuario pertenza a un grupo non limita que poida pertencer a outros. Supoñamos que os usuarios anafb e mariacl, que son as propietarias da organización queren poder acceder aos mesmos recursos que o presidente da organización. Para elo, o único que teríamos que

facér é agregar aos usuarios anafb e mariacl ao grupo G_Presidencia. Tras realizar este proceso, se amosamos as propiedades do usuario anafb e accedemos á pestana miembro de veremos a que grupos pertence:



Como se pode observar nesta pantalla, o usuario anafb pertence a máis dun grupo e polo tanto vai ter acceso a tódolos recursos accesibles polos usuarios dos grupos aos que pertence. Desde esta pantalla tamén é posible agregar ou eliminar a un usuario dun grupo. Respecto ao grupo que aparece na imaxe anterior chamado usuarios del dominio, calquera usuario polo mero feito de pertencer ao dominio é incluído nel.

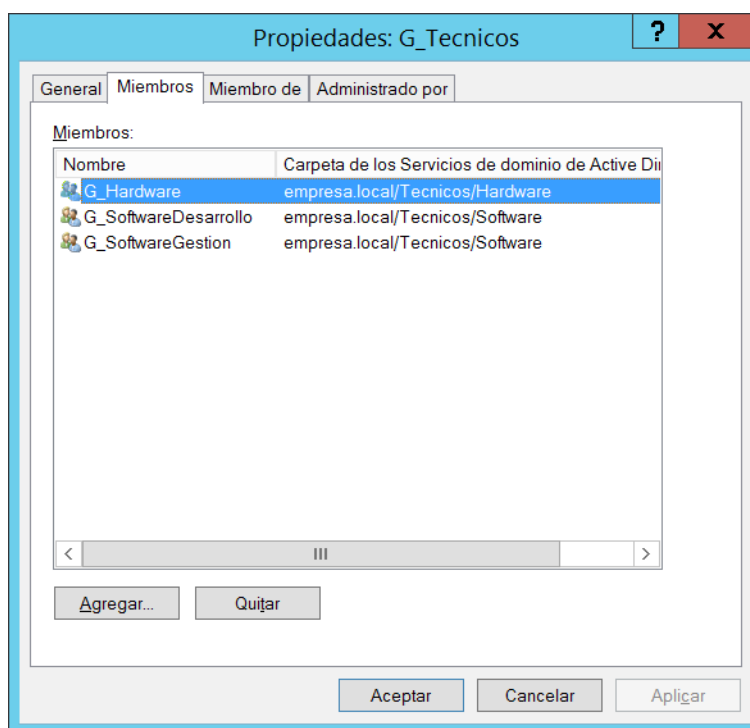
Pertenza dun grupo a outro grupo

Un grupo tamén pode pertencer a outro grupo, de modo que se asignamos a un grupo acceso sobre un recurso, o estaremos facendo para tódolos usuarios de dito grupo, así como recursivamente para tódolos usuarios dos seus subgrupos.

Imaxinemos que imos ter unha serie de recursos que queremos que sexan accesibles por tódolos usuarios do departamento técnico. Unha opción sería crear un grupo e agregarlle tódolos usuarios do departamento de software e tódolos usuarios do departamento de hardware. Outra solución aínda máis sinxela sería crear un grupo e asignarlle os grupos G_SoftwareDesarrollo, G_SoftwareGestion e G_Hardware de modo que tódolos usuarios pertencentes a ditos grupos tamén pasarán formar parte do novo grupo creado. A vantaxe deste último método é dobre:

- Por unha banda temos que realizar menos operacións xa que hai que agregar menos grupos que usuarios.
- Por outra banda e pensando no futuro, cada vez que chegue ou marche un técnico da organización unicamente vai ser necesario darlle de alta no seu grupo máis especializado.

Para agregar un grupo dentro doutro grupo seguiremos o mesmo procedemento visto para agregar usuarios. A única diferenza é que en lugar de indicar un nome de usuario como elemento a agregar indicaremos un nome de grupo. A continuación amósase o resultado de crear o grupo G_Tecnicos e agregarlle os grupos indicados anteriormente:



Familia de comandos ds

Ao igual que vimos anteriormente na xestión de UOs e usuarios, tamén é posible xestionar os grupos mediante comandos de consola. Aínda que existen varios métodos para facelo, neste caso ímonos centrar na familia de comandos ds. Os comandos da familia ds provistos polo sistema para xestionar grupos son os mesmos que vimos para a xestión de UOs e de usuarios, pero con pequenas variacións adaptadas á xestión de grupos.

Dsadd

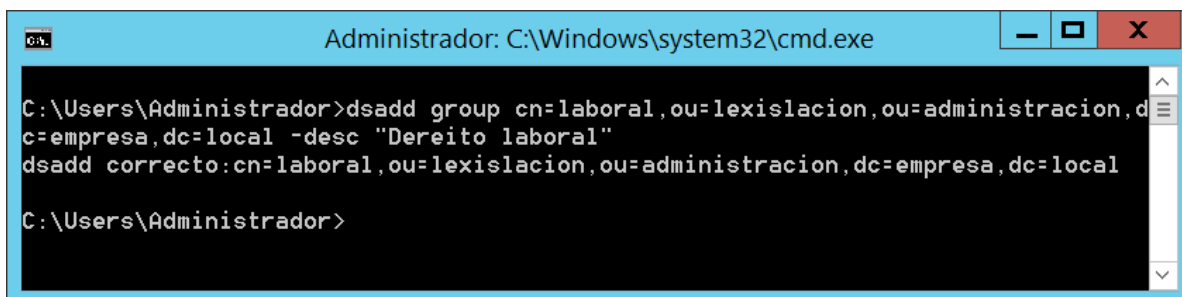
Para comezar, falaremos do comando `dsadd group`. Este comando é empregado para dar de alta grupos. A súa sintaxe é a seguinte: `dsadd group DN_do_grupo_a_engadir [opcións]`. Ao igual que ocorría cos usuarios, os grupos obxectos de tipo folia na árbore do AD e polo tanto emprégase a mesma nomenclatura que os usuarios á hora de contruír os seus DNs.

Respecto ás opcións que podemos empregar co comando `dsadd group`, as máis salientables son as seguintes:

- `-desc valor`. Mediante este parametro indicamos a descrición do grupo. Valor vai ser a descrición que vai ser asignada ao grupo.

- -members lista_DN_membros. A través deste parámetro podemos indicar que usuarios e/ou grupos van ser membros do grupo que estamos a dar de alta. Mediante lista_DN_membros indicaremos os DNs dos usuarios e grupos que queremos dar de alta como membros do grupo que estamos creando.
- -memberof lista_DN_grupos. A través deste parámetro podemos indicar a que grupos vai pertencer o grupo que estamos a dar de alta. Mediante lista_DN_grupos indicaremos os DNs dos grupos aos que queremos que pertenza o grupo que estamos creando.
- -secgrp valor. Mediante este parámetro indicamos se o grupo é un grupo de seguridade ou non. No caso de que valor teña o valor yes o grupo vai ser de seguridade. En caso de que o valor sexa no, o grupo non vai ser un grupo de seguridade. O valor por defecto é yes.
- -scope valor. Mediante este parámetro indicamos o ámbito do grupo. Se valor toma o valor l o grupo será local, se toma o valor g o grupo será global e se toma o valor u o grupo será universal. O valor por defecto é g.

Para rematar, imos desenvolver un exemplo no cal crearemos un grupo de nome laboral na UO Lexislacion. Ademais, indicaremos ao sistema que a descrición do grupo vai ser Dereito laboral:



```

Administrador: C:\Windows\system32\cmd.exe

C:\Users\Administrador>dsadd group cn=laboral,ou=lexislacion,ou=administracion,dc=empresa,dc=local -desc "Dereito laboral"
dsadd correcto:cn=laboral,ou=lexislacion,ou=administracion,dc=empresa,dc=local

C:\Users\Administrador>

```

Dsmod, dsquery, dsget e dsrm

Os comandos dsmod, dsquery e dsget xa foron descritos á hora de explicar o seu funcionamento sobre as Uos e sobre os usuarios. Respecto ao emprego destes comandos sobre a xestión de grupos, a súa funcionalidade é similar, coa diferenza de que traballan sobre grupos. Unicamente imos indicar cal é a sintaxe básica para cada un deles, deixando o descrición das opcións para que sexan investigadas ao longo da resolución dos exercicios propostos:

- dsmod group DN_grupo_a_modificar_atributos [opcións]
- dsquery group DN_grupos_a_buscar [opcións]
- dsget group tipo DN_grupo_a_detallar [opcións]

En canto ao comando dsrm, xa indicamos previamente que se emprega para eliminar diferentes elementos da árbore do AD, incluíndo entre os obxectos eliminables por este comando os grupos.

1.2.8 Carpetas persoais

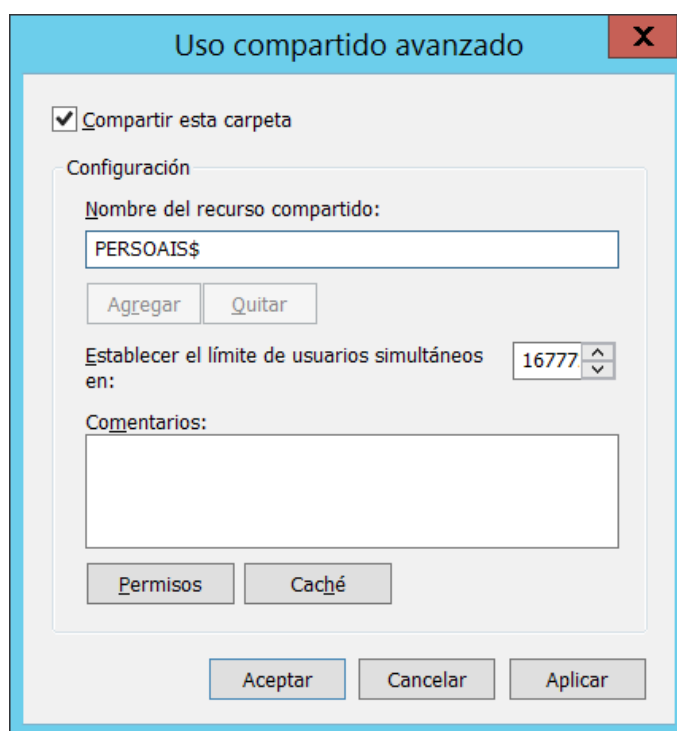
Cando un usuario identifícase nunha estación de traballo pode gardar os arquivos que xera en dita máquina de xeito local, pero no caso de que o usuario cambie de máquina e queira

empregar os arquivos que creou anteriormente será necesario que haia feito unha copia de ditos arquivos á nova máquina na que se atopa agora. Mediante o emprego de carpetas persoais no dominio un usuario, independentemente de que se conecta desde unha u outra máquina do dominio, poderá almacenar os seus arquivos nunha carpeta que será accesible desde calquera equipo do dominio. Esta carpeta chámase carpeta persoal. Trátase de unha carpeta que se encontra localizada fisicamente nun equipo do dominio. Cada vez que o usuario se conecte ao dominio, con independencia do equipo desde o que o faga, crearase automaticamente unha unidade de rede que se conectará á carpeta persoal de modo que todo o que teña almacenado en dita carpeta vai ser accesible desde calquera equipo do dominio. En función dos permisos establecidos sobre a carpeta persoal poderán acceder a ela máis ou menos usuarios, aínda que o habitual é, como o seu nome indica, que sexa unha carpeta accesible so polo seu propietario, quedando para este a responsabilidade de compartila ou non con outros usuarios.

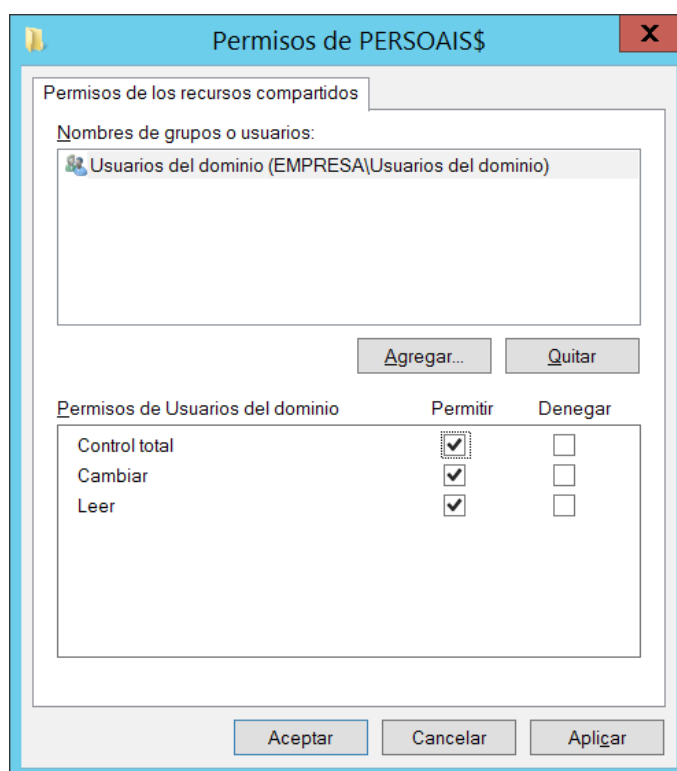
Creación de carpetas persoais

Vexamos a continuación o proceso de creación das carpetas persoais. Para elo partiremos da configuración que temos feita para o dominio empresa.local. Crearemos as carpetas persoais dos usuarios incluídos na UO Propietarios, é dicir, as carpetas persoais dos usuarios anafb e mariacl. Co fin de acelerar o proceso imos crear as carpetas persoais na unidade C: da máquina SERVIDOR, pero isto non é obrigatorio e de feito tampouco é o máis habitual. As carpetas persoais poderían estar en calquera sitio, nunha carpeta específica para carpetas persoais, noutra partición da máquina SERVIDOR o incluso noutra máquina do dominio. Como requisito de acceso neste caso vaise establecer que as carpetas persoais sexan accesibles unicamente polos seus propietarios.

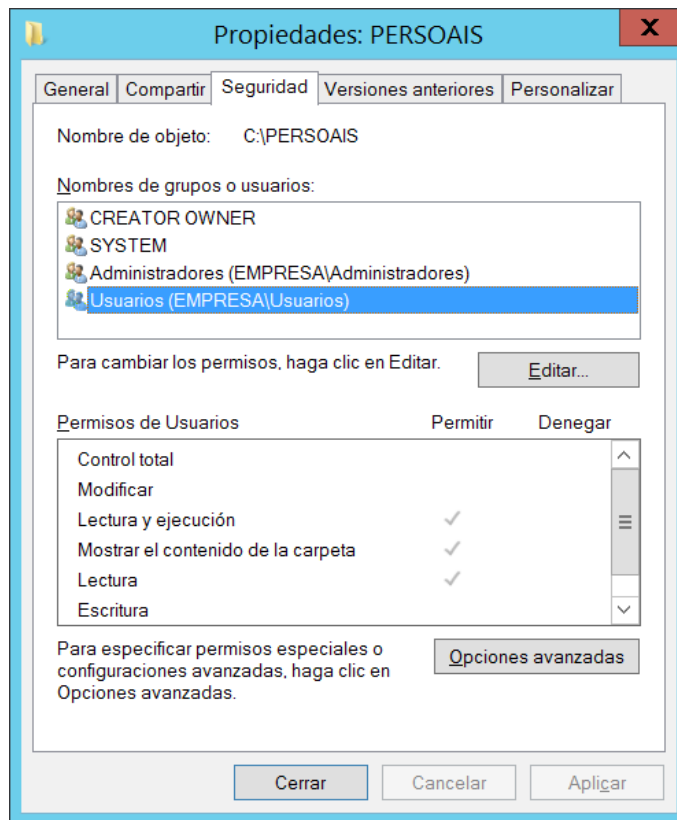
Para comenzar imos crear unha carpeta na raíz de C:. Dita carpeta vai conter tódalas carpetas persoais de tódolos usuarios do dominio. O seu nome será PERSOAIS. Unha vez creada ímola compartir como un recurso oculto (lembrems que isto xa foi visto nunha actividade previa):



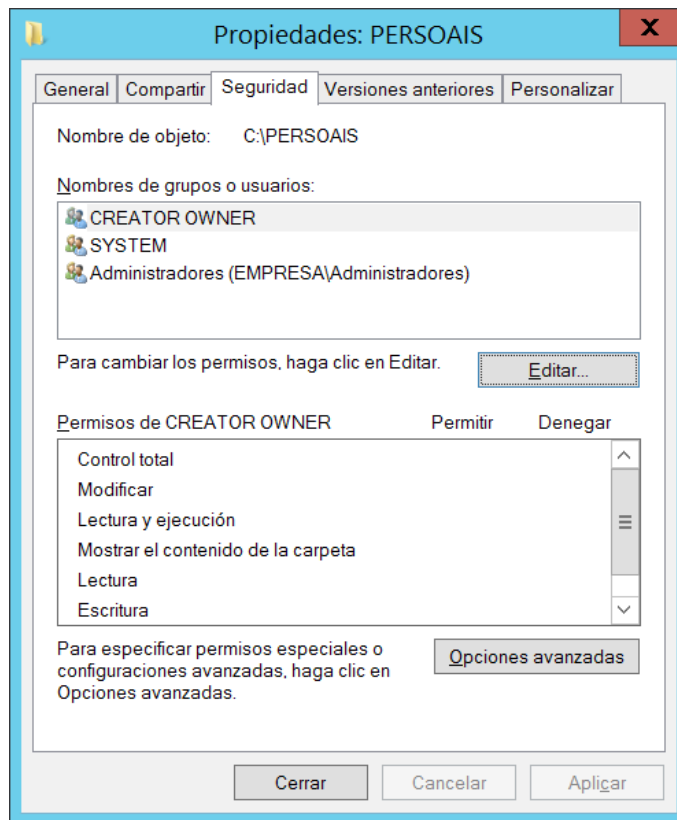
Realmente non é necesario compartir a carpeta como recurso oculto, pero deste modo evitamos que calquera usuario que escriba \\SERVIDOR no seu explorador de arquivos poida ver que existe unha carpeta compartida chamada PERSONAIS. Es unha forma de minimizar posibles ataques. Ademais de ocultar o nome do recurso compartido, imos cambiar os seus permisos de modo que a carpeta so sexa accesible polos usuarios do dominio (esta é unha configuración de seguridade habitual, pero dependendo dos escenarios é posible que haia que realizar outra configuración):



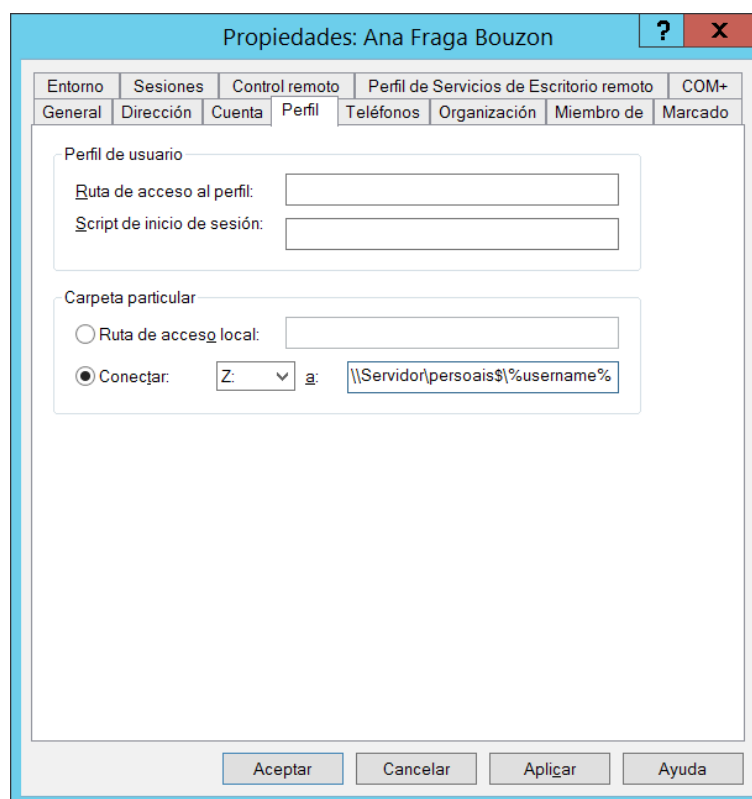
Dámoslle como permisos de compartición control total (obviase la explicación pois isto xa foi explicado nunha actividade previa), de modo que imos ter que axustar os accesos mediante a ficha de seguridade da carpeta. Para elo, accedemos á ficha de seguridade da carpeta PERSONAIS e estudamos cales son os permisos que ten preestablecidos e se nos valen:



Neste caso dixéramos que as carpetas persoais íanse crear dentro da carpeta PERSONAIS e ademais dixéramos que cada carpeta persoal so poderá ser accedida polo seu propietario. Como os permisos hérdanse ao longo da estrutura de carpetas, calquera carpeta que creemos dentro da carpeta PERSONAIS vai herdar os seus permisos e como pódese ver na imaxe, tódolos usuarios que pertencen ao grupo Usuarios van ter acceso de lectura sobre as carpetas persoais que creemos dentro de PERSONAIS. Para evitalo, eliminamos o problema de raíz, é dicir, eliminamos o permiso de lectura dos usuarios do grupo Usuarios sobre a carpeta PERSONAIS (xa viuse como facer isto nunha actividade previa) :

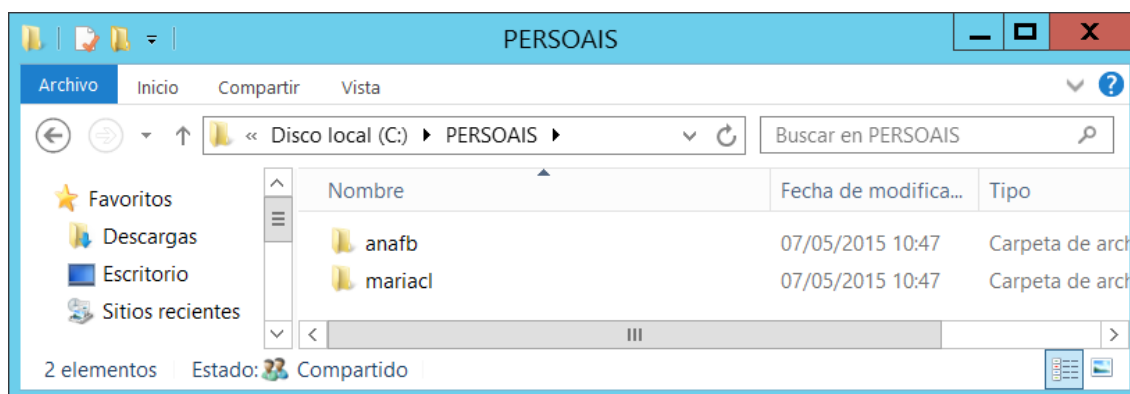


O resto dos permisos da carpeta PERSONAIS ímolos deixar como están. Unha vez preparada a carpeta que vai conter as carpetas persoais pasaremos a configurar os usuarios anafb e mariac1 para indicarlles onde están as súas carpetas persoais e como acceder a elas. Para elo desde a ferramenta de usuarios e equipos de AD accedemos á ficha perfil das propiedades do usuario anafb e configuramos o panel carpeta particular do seguinte modo:

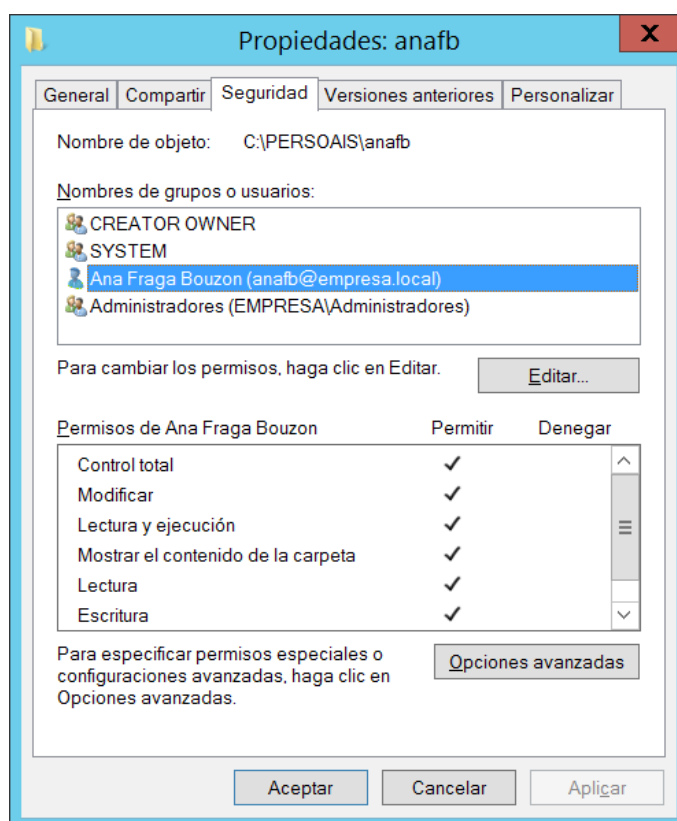


Por unha banda, mediante o despregable estamos indicando cal vai ser o identificador que empregará a unidade de rede que se conectará á carpeta persoal cando o usuario se conecte desde calquera equipo do dominio. Neste caso vai ser Z:. Por outra banda indicamos onde vai estar fisicamente a carpeta persoal do usuario anafb. Isto facémolo indicando a ruta do recurso compartido que a contén (\\Servidor\persoais) seguido da variable %username%. Esta variable vai ser substituída polo nome do usuario (de feito tamén poderíase escribir anafb en lugar de %username%). É dicir, a carpeta persoal vai estar en \\Servidor\persoais\anafb. No caso de que a carpeta non existira o sistema vai intentar creala. Se non ten permisos para creala (neste caso se que os ten xa que establecemos control total sobre a carpeta PERSONAIS) nos indicará que debemos creala manualmente.

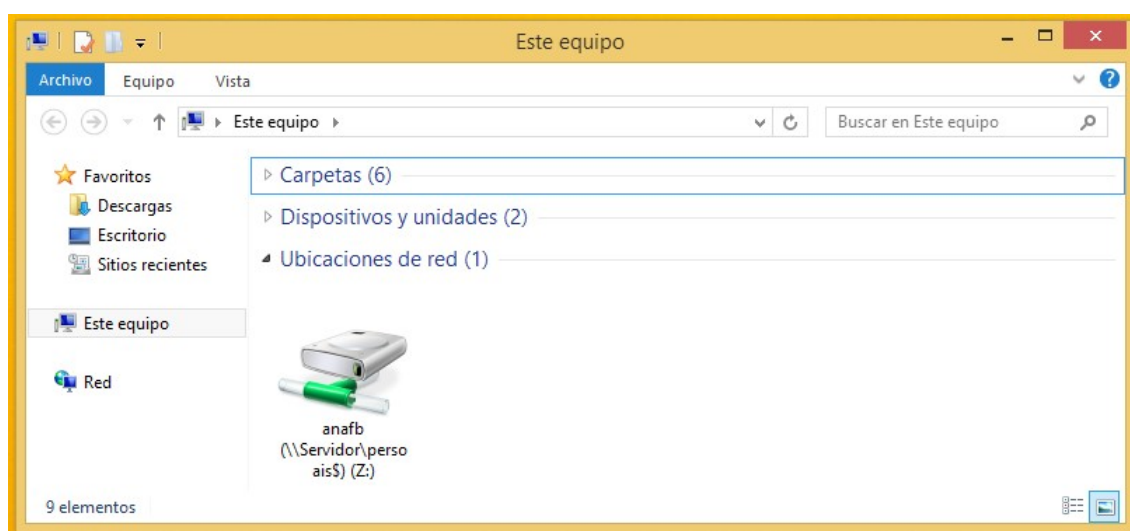
Unha vez configurada a pantalla prememos sobre o botón aceptar. Repetiremos o proceso para mariac. Unha vez terminado vemos que dentro da carpeta PERSONAIS créanse automaticamente as carpetas persoais dos usuarios:



Ademais, se accedemos aos permisos dalgunha destas carpetas vemos que son os correctos conforme aos requisitos previos:

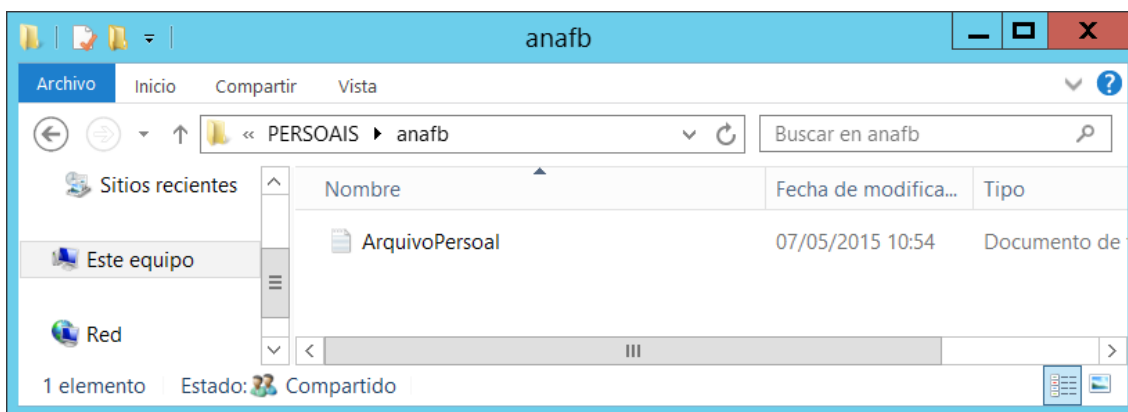


Poderíamos afinar máis os permisos no caso de ser necesario. Unha vez creadas as carpetas persoais comprobemos que funcionan correctamente. Para elo conectámonos co usuario anafb desde unha estación de traballo ao dominio e abrimos un explorador de arquivos:



Como podemos ver hai unha unidade de red Z: que apunta a \\Servidor\persoais\$\anafb. Finalmente para comprobar que funciona imos crear un arquivo de texto chamado

ArquivoPersoal en Z: desde a estación de traballo. Unha vez creado comprobaremos que o arquivo está no servidor dentro da carpeta anafb creada dentro de PERSOAIS:



Como podemos observar na imaxe previa, o arquivo creado desde a estación de traballo está situado fisicamente na carpeta persoal de anafb creada a tal efecto no servidor. Independentemente do equipo desde o que se conecte anafb, a súa carpeta persoal referenciada pola unidade de rede Z: sempre vai estar apuntando contra a carpeta física do servidor, de modo que sempre vai ser posible que o usuario anafb acceda á información que almacena na súa carpeta persoal.

Familia de comandos ds

É posible asignar e xestionar as carpetas persoais mediante comandos de consola. Imos ver como empregar os comandos da familia ds para facelo. O comando dsadd user, o cal xa víramos con anterioridade á hora de xestionar contas de usuario ten dúas opcións, as cales permiten asignar unha carpeta persoal, así como a letra para acceder a ela. Estas opcións son as seguintes:

- -hmdir ruta_da_carpeta. Mediante a opción hmdir indicamos a ruta na cal está situada a carpeta compartida do usuario que estamos a dar de alta. O valor ruta_da_carpeta contén a ruta na cal está situada a carpeta persoal do usuario.
- -hmdrv letra:. A través desta opción indicamos a letra a través da cal poderá o usuario que estamos a crear acceder á súa carpeta persoal. É importante lembrar que a letra indicada debe ir rematada polo caracter:.

Ademais de empregar estas opcións co comando dsadd user, tamén é posible empregalas cos comandos dsmod user e dsget user. Evidentemente o uso destas opcións no caso do comando dsmod vai ser para modificar o seu valor e no caso do comando dsget vai ser para amosar o seu valor. Non entraremos en máis detalles respecto a estes comandos, senón que os deixaremos para ser investigados á hora de resolver os exercicios propostos.

1.2.9 Carpetas compartidas no dominio

O concepto dunha carpeta compartida no dominio é parecido ao dunha carpeta persoal. Ao igual que esta última, unha carpeta compartida no dominio é unha carpeta que se atopa localizada fisicamente nun equipo do dominio. Este tipo de carpetas créanse co propósito de que sexan empregadas por varios usuarios do dominio para compartir os recursos, de modo que deben establecerse os permisos axeitados para que os diferentes usuarios que accedan á

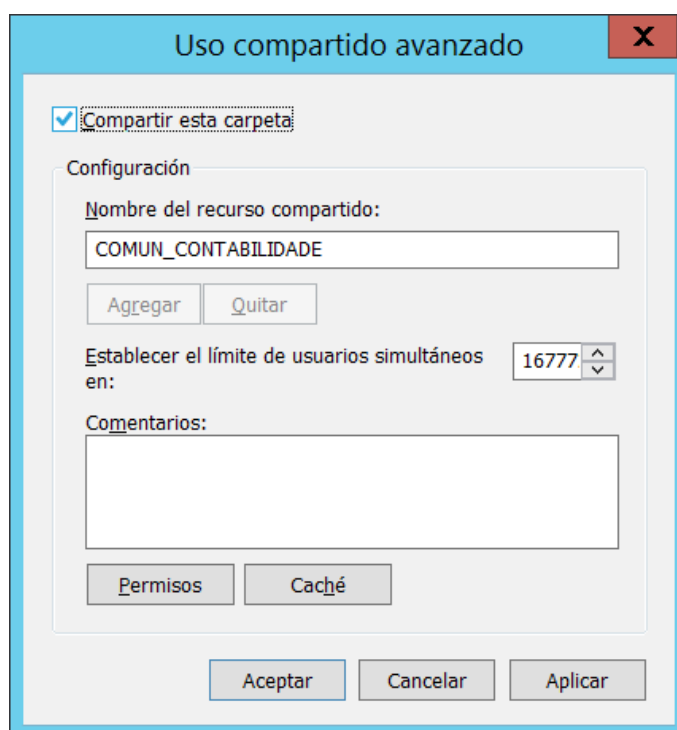
carpeta poidan facelo dun modo axeitado ás súas necesidades. Ao igual que ocorría coas carpetas persoais, as carpetas compartidas no dominio poden ser accedidas desde calquera equipo do dominio polos usuarios que teñen permiso para facelo.

Creación de carpetas compartidas no dominio

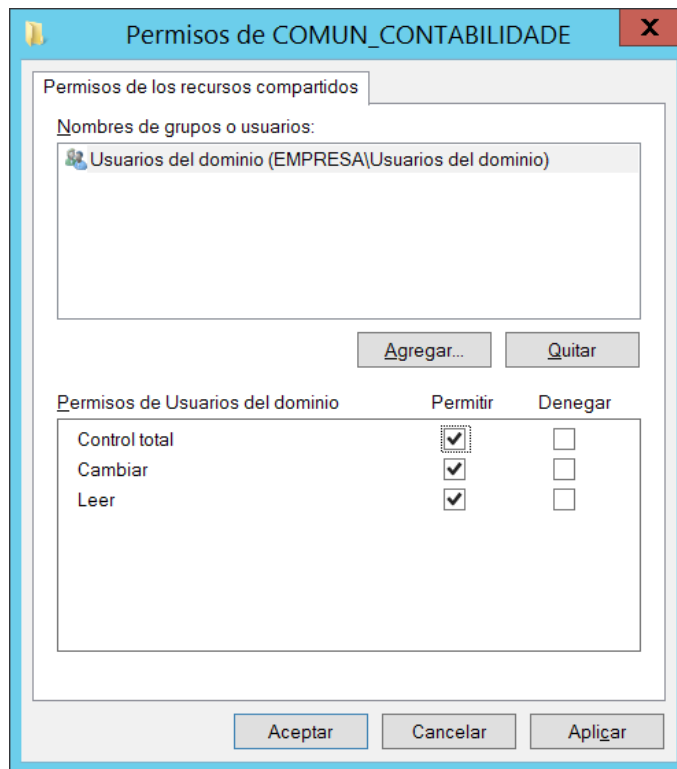
Vexamos de seguido o proceso de creación dunha carpeta compartida no dominio. Para elo partiremos da configuración que temos feita para o dominio empresa.local. Crearemos unha carpeta compartida no dominio que poderá ser accedida polos usuarios incluídos na UO Propietarios, polos usuarios da UO Presidencia e polos usuarios da UO Contabilidade. Ao igual que fixemos cando creamos as carpetas persoais dos usuarios, imos crear a carpeta compartida no dominio na unidade C: da máquina SERVIDOR (aínda que podería situarse en calquera outra localización física do dominio). Establécense os seguintes requisitos de acceso á carpeta compartida:

- Usuarios UO Propietarios: permiso de lectura.
- Usuarios UO Presidencia: permiso de lectura.
- Usuarios UO Contabilidade: permiso de lectura e escritura.

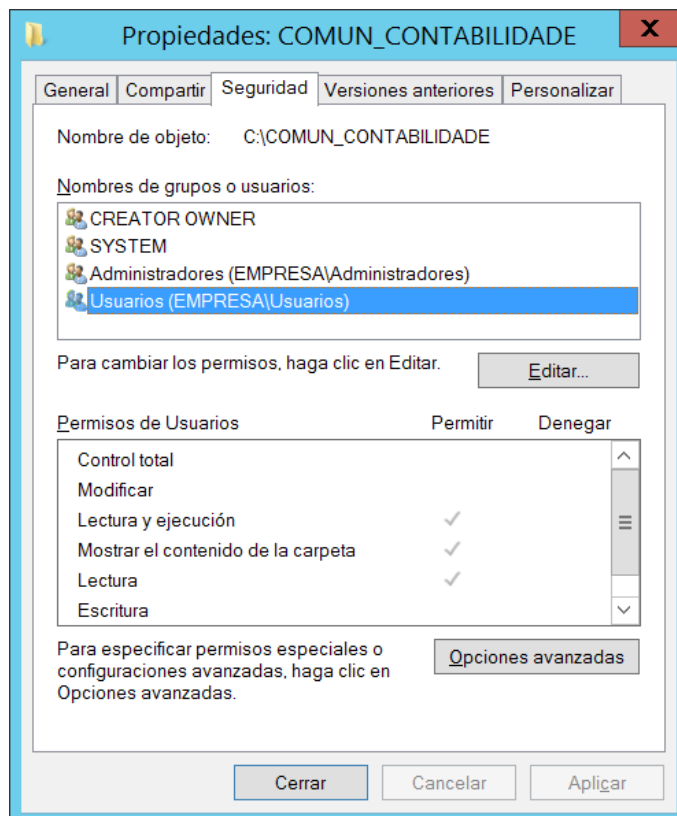
Para comezar imos crear a carpeta compartida no dominio na raíz de C:. O seu nome vai ser COMUN_CONTABILIDADE. Unha vez creada ímola compartir (esta vez non a compartiremos como un recurso oculto, aínda que sería unha opción a contemplar):



A continuación cambiamos los permisos de la carpeta de modo que sea accesible por los usuarios del dominio (esta es una configuración de seguridad habitual, pero dependiendo de los escenarios es posible que haya que realizar otra configuración):



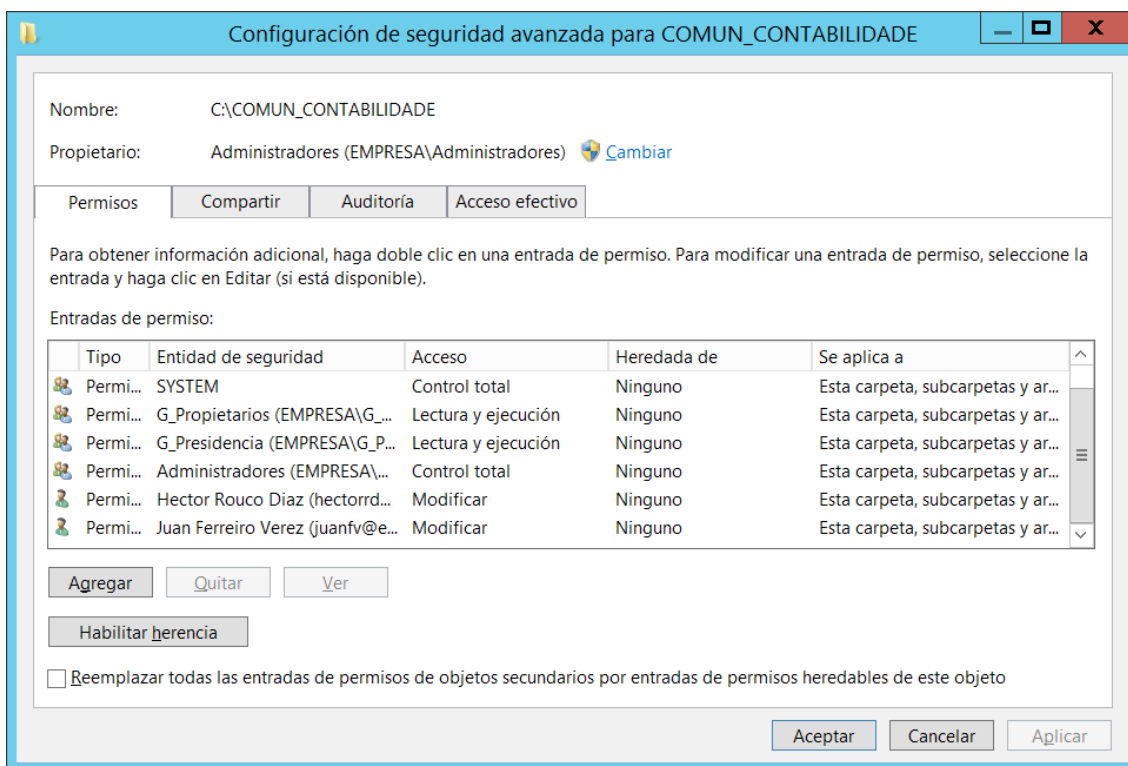
Dámoslle control total de modo que imos ter que axustar os accesos mediante a ficha de seguridade da carpeta. Para elo, accedemos á ficha de seguridade da carpeta COMUN_CONTABILIDADE e estudamos cales son os permisos que ten preestablecidos e se válenos algún deles:



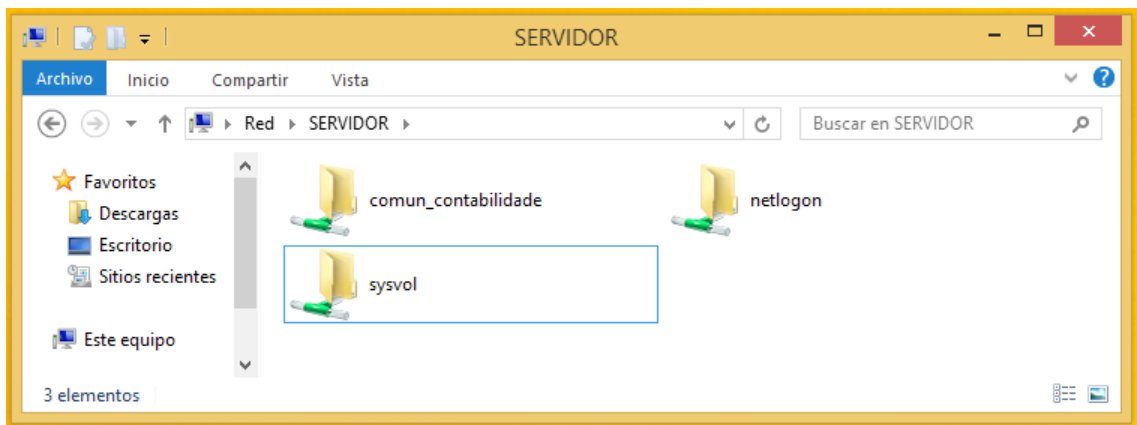
Evidentemente os permisos preestablecidos non son válidos para os nosos requisitos, así que ímolos modificar. Estableceremos os seguintes permisos:

- Usuarios grupo G_Propietarios: permiso de lectura. Establecer permiso de lectura para este grupo equivale a facelo para tódolos usuarios que forman parte do grupo.
- Usuarios Grupo G_Presidencia: permiso de lectura. Establecer permiso de lectura para este grupo equivale a facelo para tódolos usuarios que forman parte do grupo.
- Usuarios hectorrd e juanfv: permiso de lectura e escritura. En lugar de establecer os permisos individualmente, sería, máis eficiente crear un grupo que englobe aos usuarios de contabilidade e asignar os permisos sobre dito grupo, pero imos facer a asignación de permisos individualizadamente co fin de ver que é posible mesturar asignación de permisos a grupos e a usuarios sobre o mesmo recurso.

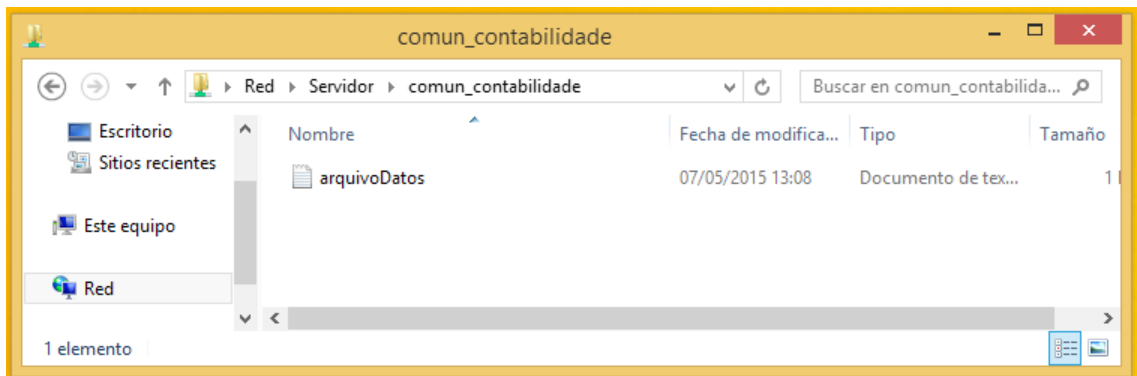
Como os permisos hérdanse ao longo da estrutura de carpetas, calquera carpeta que creemos dentro da carpeta COMUN_CONTABILIDADE vai herdar os seus permisos e como pódese ver na imaxe, tódolos usuarios que pertenzan ao grupo Usuarios van ter acceso de lectura sobre a carpeta COMUN_CONTABILIDADE e sobre as súas carpetas. Para evitalo, eliminamos o problema de raíz, é dicir, eliminamos o permiso de lectura dos usuarios do grupo Usuarios sobre a carpeta COMUN_CONTABILIDADE. Unha vez eliminado o permiso de lectura para os usuarios do grupo Usuarios, establecemos os permisos requiridos para a correcta xestión da carpeta compartida no dominio:



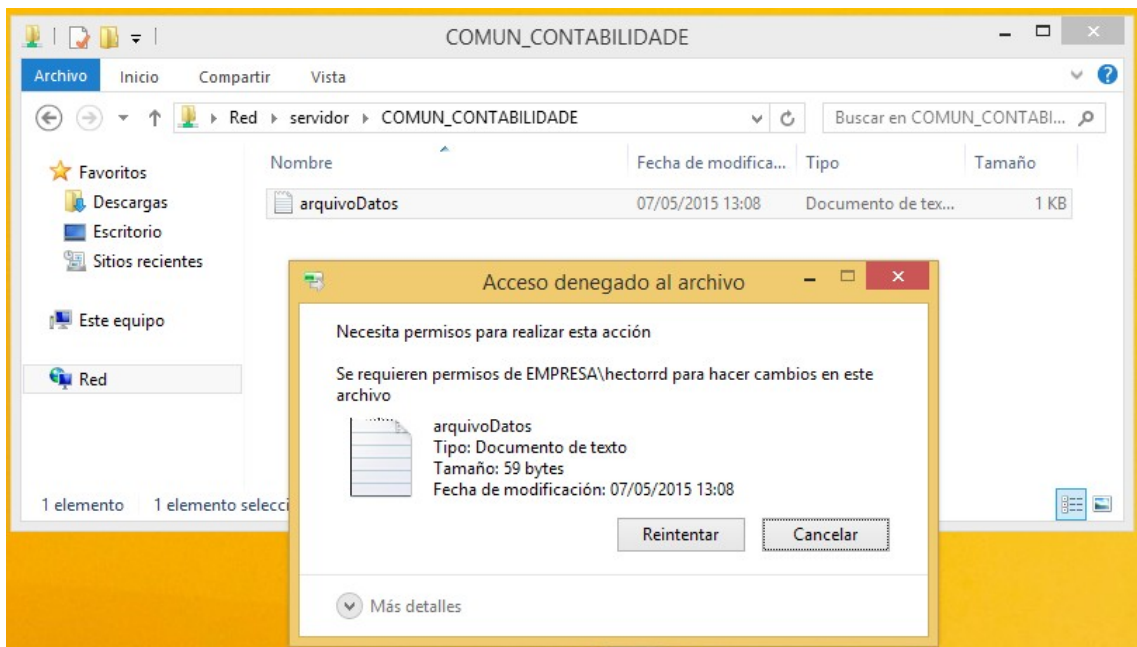
Unha vez configurada a carpeta COMUN_CONTABILIDADE imos probar que funciona correctamente. Para elo, desde unha estación de traballo abrimos unha sesión cun usuario de contabilidade, en concreto con hectorrd, e amosamos no explorador de arquivos os recursos compartidos na máquina SERVIDOR:



Como pódese observar, o explorador de arquivos indícanos que entre outros temos un recurso compartido na máquina SERVIDOR chamado comun_contabilidade. Este recurso fai referencia ao recurso que acabamos de configurar. Para probar se funciona e se os permisos están ben establecidos imos intentar crear un arquivo de texto chamado arquivoDatos no recurso compartido desde a sesión aberta na estación de traballo por hectorrd:



O arquivo pódese crear e pódese ler, polo tanto os permisos, ao menos para o usuario hectorrd, están establecidos correctamente. Imos abrir unha sesión no dominio desde unha estación de traballo cun usuario do grupo G_Propietarios, en concreto co usuario anaafb, e imos intentar eliminar o arquivo que acabamos de crear:



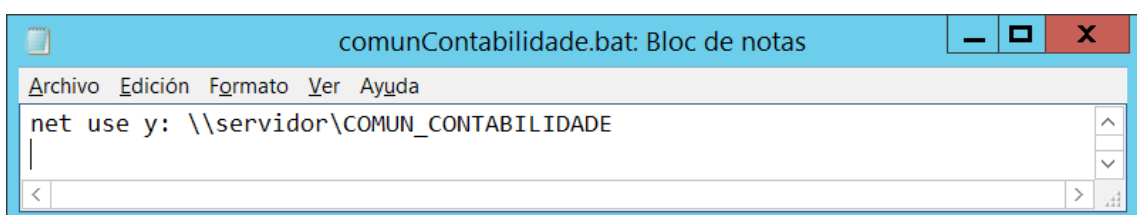
Como pódese observar na imaxe anterior, anafb pudo acceder ao recurso compartido, pero ao intentar eliminalo o sistema de permisos impediu facer a acción xa que o usuario non ten os suficientes permisos para realizar esta operación.

Acceso aos recursos compartidos mediante unidades de rede

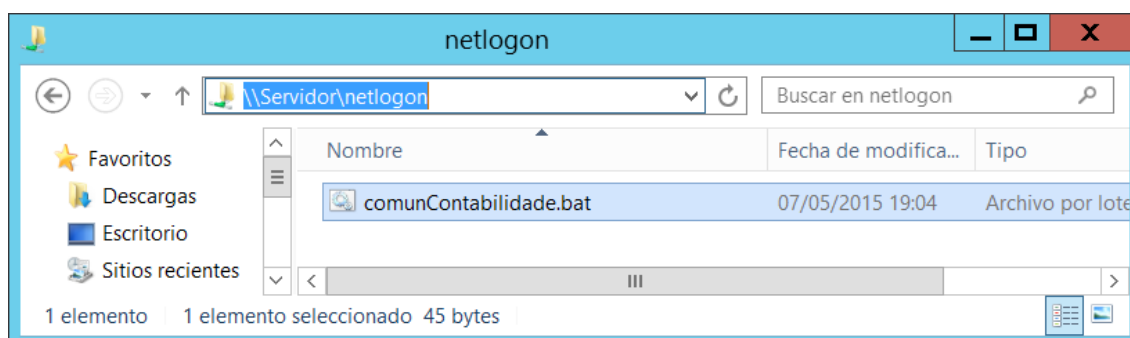
Acabamos de ver que para acceder ao recurso compartido no dominio o único que ten que facer o usuario é indicar a ruta do recurso e ter os privilexios suficientes para facer uso del. Aínda así, é posible simplificar o acceso ao recurso compartido e deixalo limitado a unha unidade de rede que apunte ao recurso. A continuación imos ver como configurar a conta dun usuario para crear automaticamente esta unidade de rede cada vez que se conecte ao dominio. Iremos realizar a configuración para o usuario hectorrd.

Nas máquinas Windows Server existe unha carpeta compartida chamada netlogon. É unha carpeta que crea o sistema e que se emprega para colocar nela scripts de inicio de sesión. Esta carpeta é accesible en lectura por tódolos usuarios. Dependendo da versión de Windows Server empregada, a localización física desta carpeta varía. Para acceder a ela, independentemente da versión de Windows Server empregada, o podemos facer mediante `\\NOMBRE_EQUIPO\netlogon`. Neste caso accederemos a ela mediante `\\SERVIDOR\netlogon`.

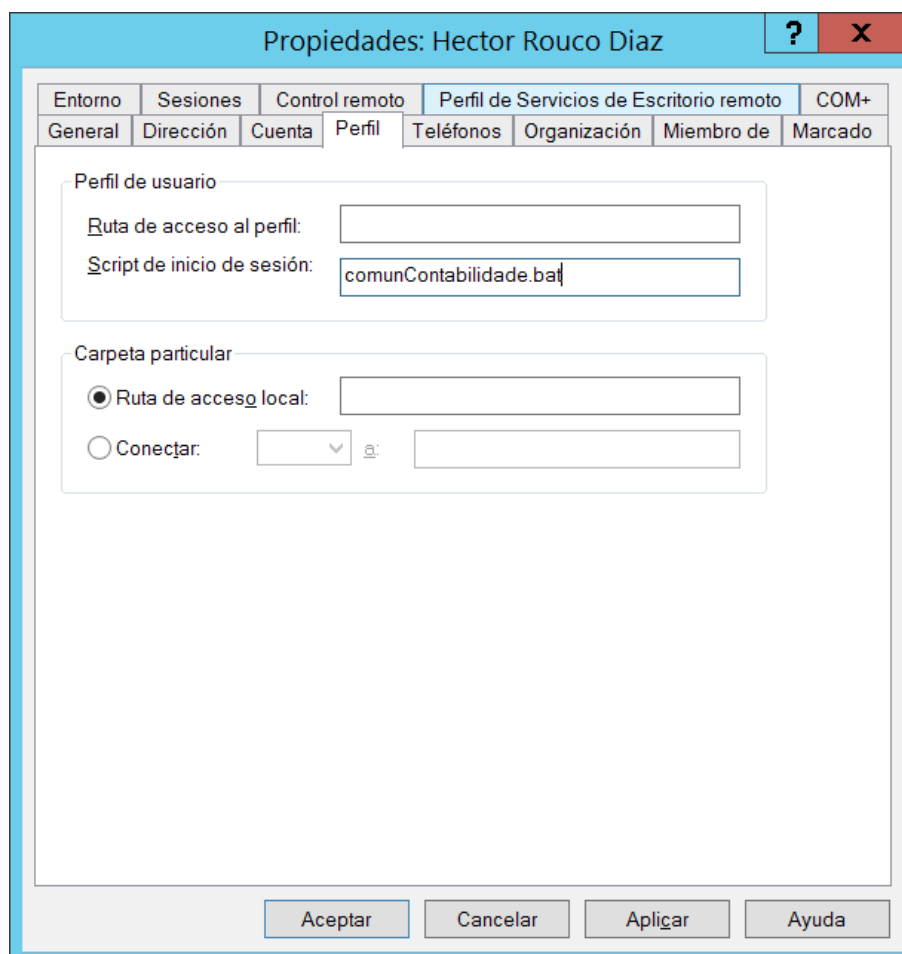
Para automatizar a xeración dunha unidade de rede ao inicio da sesión dun usuario o único que temos que facer é crear un ficheiro bat que cree a unidade de rede, colocar dito ficheiro bat na carpeta netlogon e por último indicar na configuración da conta do usuario que ao iniciar a sesión execute dito ficheiro bat. No caso que estabamos preparando, crearemos o ficheiro bat comunContabilidad.bat:



O comando indicado no ficheiro bat, tal e como vimos nunha unidade didáctica anterior crea unha unidade de rede contra a carpeta \\SERVIDOR\COMUN_CONTABILIDADE e mapéala mediante a letra y:. É fundamental almacenar este arquivo na carpeta netlogon:

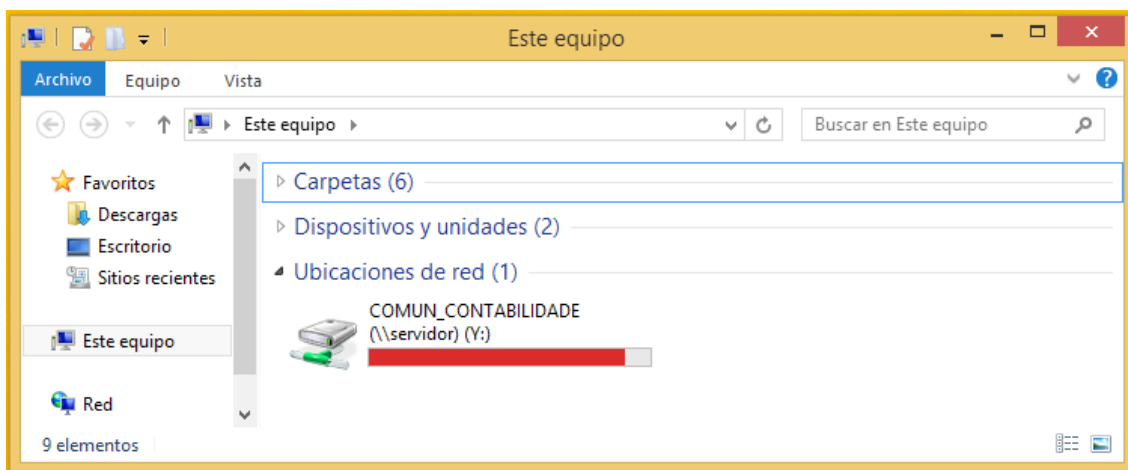


Agora unicamente resta configurar a conta do usuario hectorrd para que execute este script ao iniciar a súa sesión no dominio. Para elo desde a ferramenta de usuarios e equipos de AD accedemos á ficha perfil das propiedades do usuario hectorrd e configuramos o panel perfil de usuario do seguinte modo:

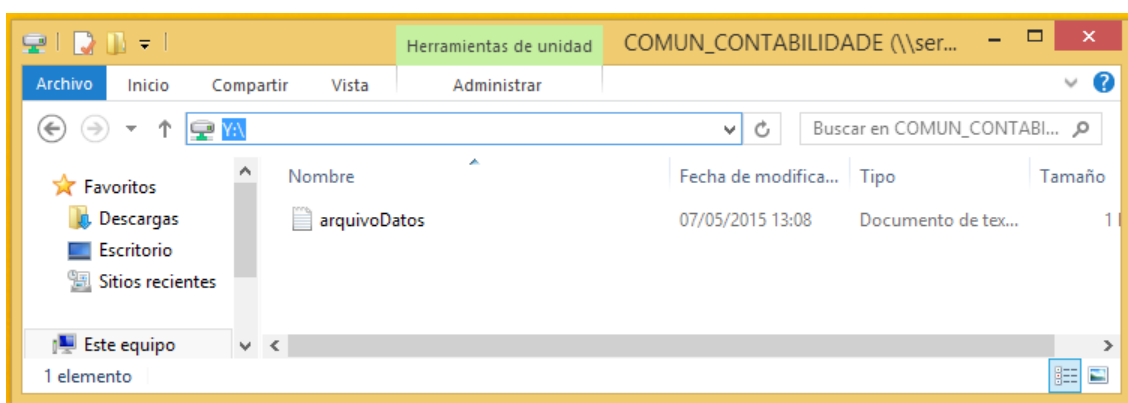


Simplemente indicamos o nome do ficheiro bat situado en netlogon que se ten que executar cando o usuario hectorrd inicie unha sesión no dominio. Evidentemente este ficheiro bat non

está limitado á creación dunha única unidade de rede. Dentro deste ficheiro bat poderán indicarse tódolos comandos que se considere que son necesarios realizar cando o usuario inicia unha sesión no dominio. Para comprobar que a unidade de rede indicada é creada, iniciamos unha sesión no dominio desde unha estación de traballo co usuario hectorrd:



Como pódese observar na imaxe, ao iniciar hectorrd a súa sesión no dominio, créase automaticamente unha unidade de rede Y: que apunta a \\SERVIDOR\\COMUN_CONTABILIDADE. Agora o acceso á carpeta compartida no dominio faise mediante unha letra de unidade, o cal sempre facilita o acceso desde o punto de vista do usuario final:



Familia de comandos ds

É posible asignar e xestionar as carpetas compartidas mediante comandos de consola. Imos ver como empregar os comandos da familia ds para facelo. O comando dsadd user, o cal xa víramos con anterioridade á hora de xestionar contas de usuario ten unha opción, a cal permite indicar o script de inicio de sesión do usuario. Esta opción é a seguinte:

- -loscr script. A través desta opción indicamos o nome do script de inicio de sesión do usuario que estamos a dar de alta. O valor script contén o nome do script de inicio de sesión a definir.

Ademais de empregar esta opción co comando dsadd user, tamén é posible empregala cos comandos dsmod user e dsget user. Evidentemente o uso desta opción no caso do comando

dsmod vai ser para modificar o seu valor e no caso do comando dsget vai ser para amosar o seu valor.

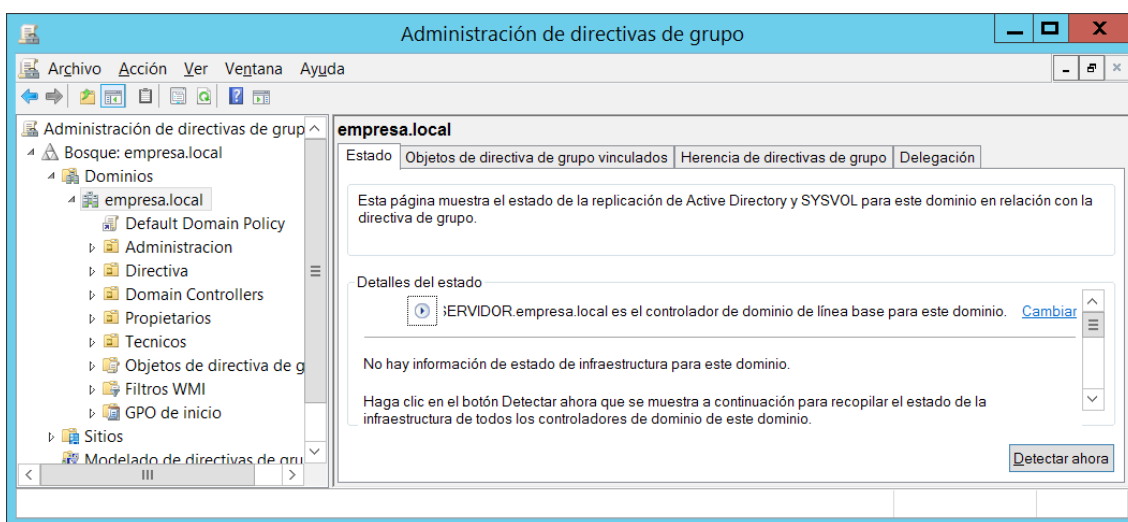
1.2.10 Directiva de grupos

Directiva de grupos é un sistema que permite implementar configuracións específicas para os usuarios e os equipos. As diferentes configuracións aplicadas polo sistema directiva de grupo establécense mediante os obxectos de directiva de grupo (GPO). Un GPO define unhas características determinadas de funcionamento para ser aplicadas sobre diferentes obxectos do AD. Os obxectos sobre os cales pódense aplicar GPOs son os sitios, os dominios e as UOs.

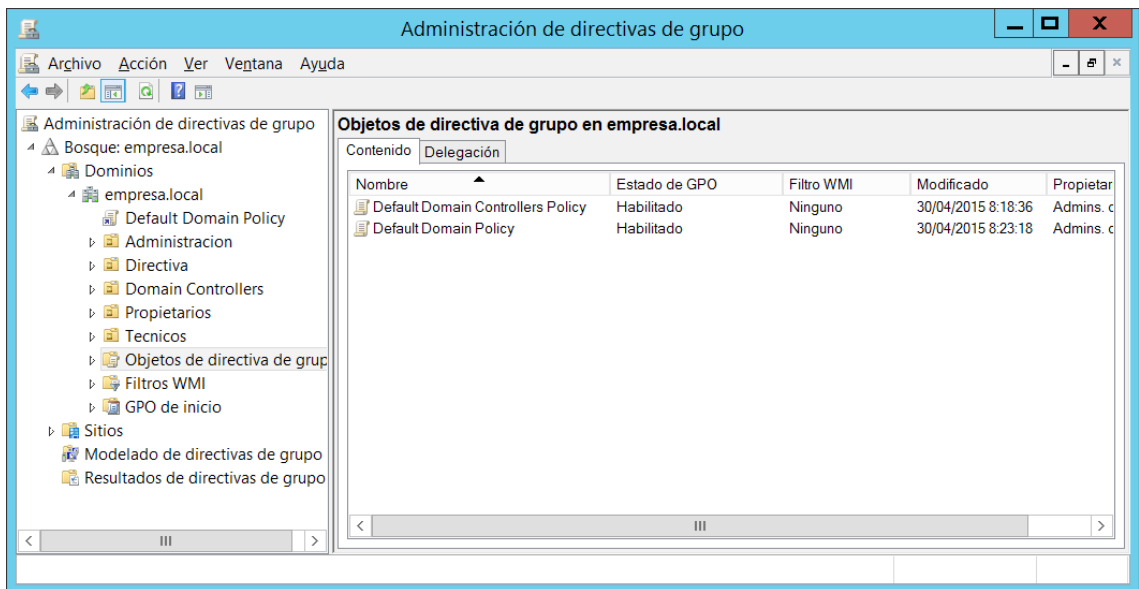
- A aplicación dun GPO sobre un dominio da lugar a que o GPO sexa aplicado sobre tódolos usuarios e tódalas máquinas que pertencen a dito dominio.
- A aplicación dun GPO sobre unha UO da lugar a que o GPO sexa aplicado sobre tódolos usuarios e tódalas máquinas que pertencen a dita UO (subUOs incluídas).

Creación dun GPO

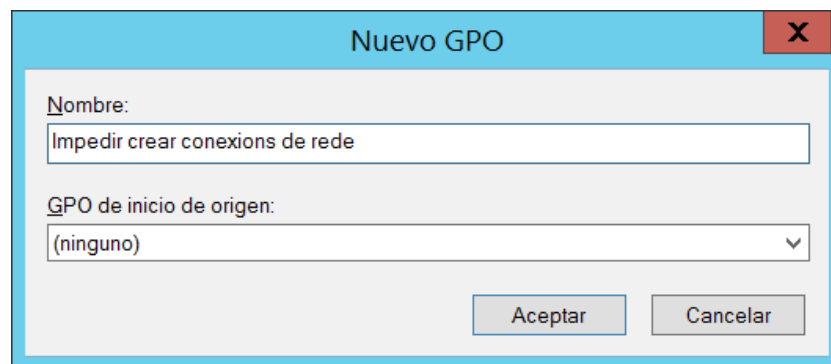
Para poder crear un GPO temos que acceder á consola de administración de directivas de grupo. Para elo, desde o administrador do servidor prememos en Herramientas e seleccionamos a opción administrador de directivas de grupo. Abrirase a seguinte xanela:



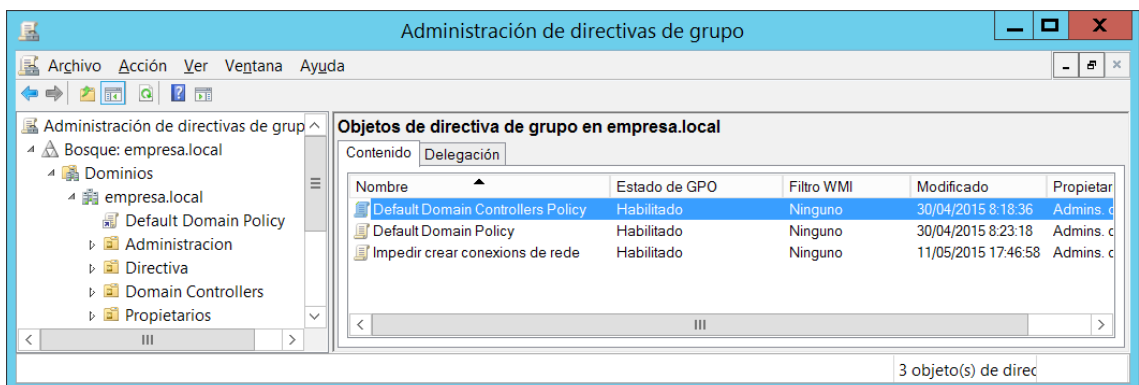
Para poder aplicar un GPO é necesario crealo. A continuación imos ver un dos métodos para crear un GPO. Crearemos un GPO que impida aos usuarios sobre os que se aplique que poidan empregar a opción de crear unidades de rede desde o explorador de arquivos. Para comezar prememos sobre o elemento Objetos de directiva de grupo. Amosarase un listado con tódolos GPOs existentes.



Prememos co botón dereito do rato sobre o listado de GPOs e seleccionamos a opción Nuevo. Abrirase unha nova pantalla que empregaremos para indicar o nome do GPO que imos crear. Neste caso chamarémolo Impedir crear conexións de rede:

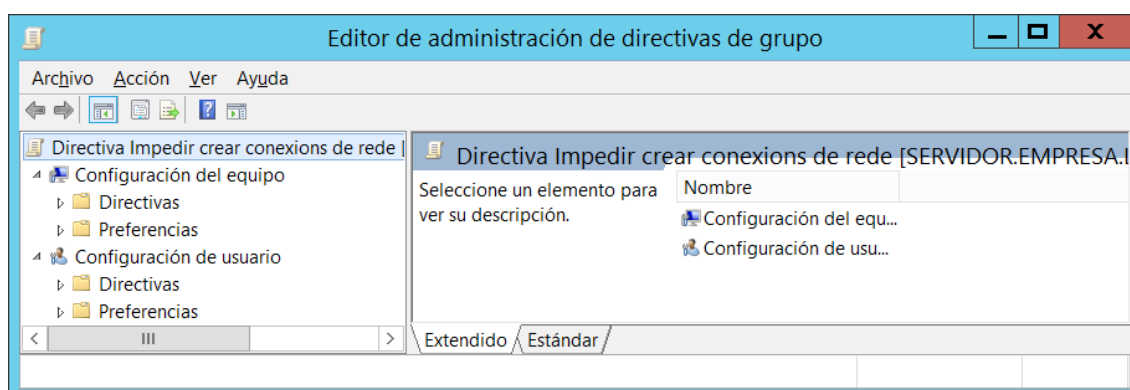


Prememos en Aceptar. Agora o GPO xa está creado:



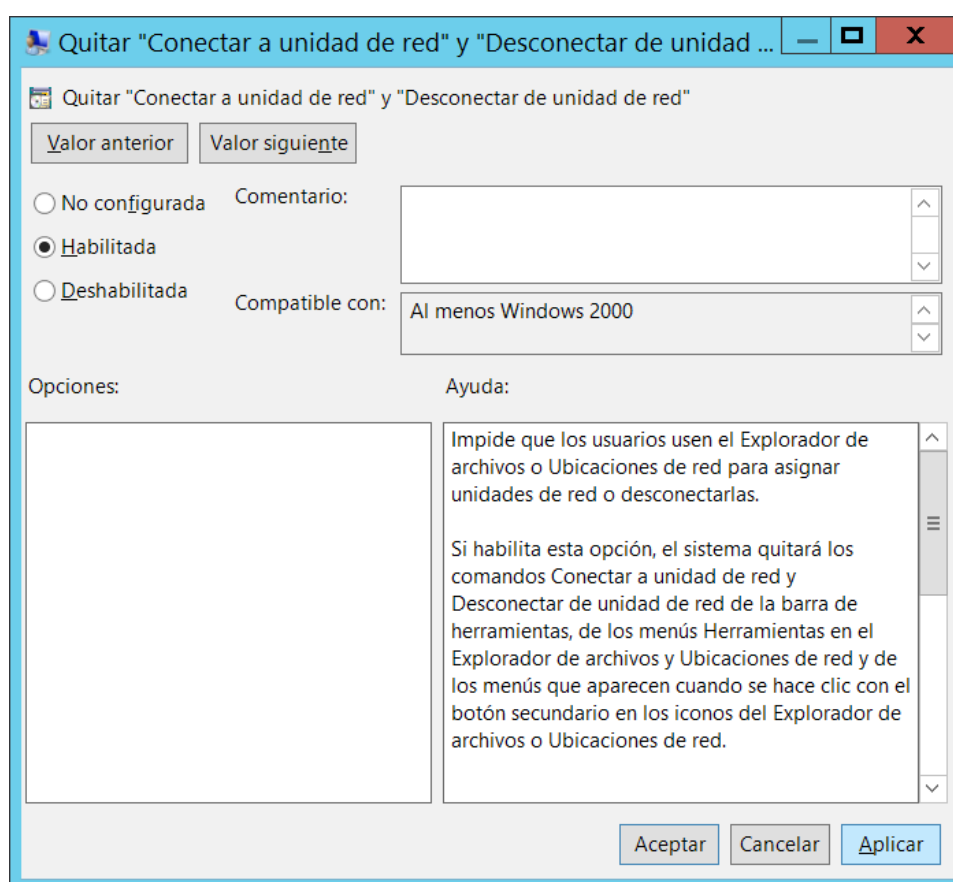
A continuación imos configurar o GPO para establecer as restricións que queiramos. Para elo, prememos co botón dereito sobre o GPO Impedir crear conexións de rede e

seleccionamos a opción Editar. Abrirase o editor de directivas para o GPO que estamos configurando:

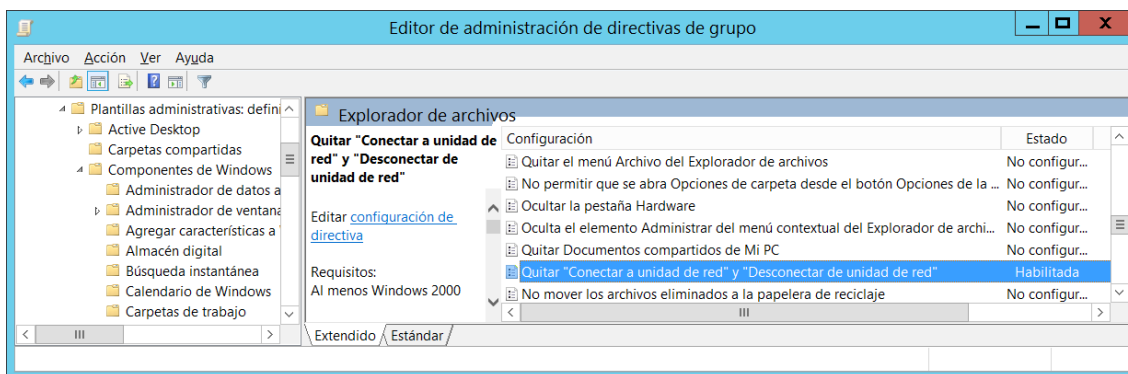


Como pódese observar esta xanela é similar á xanela de edición de directivas locais, a cal xa foi vista nunha unidade previa. Polo tanto non imos parar en detallar o seu funcionamento. Unicamente lembrar que as directivas que colgan da rama Configuración del equipo afectan aos equipos e que as directivas que colgan da rama Configuración de usuario afectan aos usuarios.

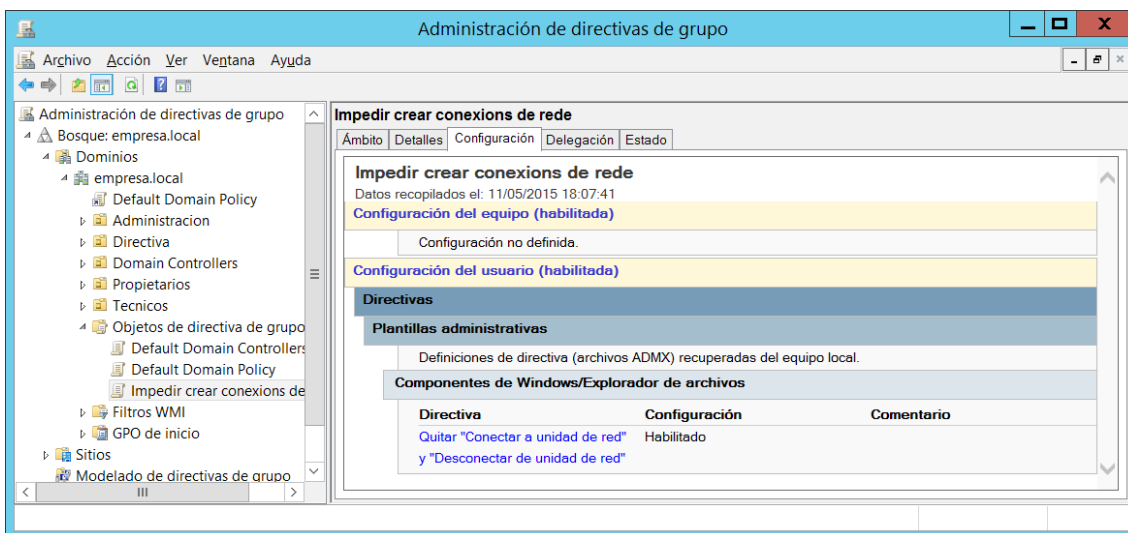
A directiva que imos modificar atópase en Configuración de usuario / Directivas / Plantillas administrativas / Componentes de Windows / Explorador de archivos e o seu nome é Quitar conectar a unidad de red y desconectar de unidad de red. Facemos dobre clic sobre a directiva e configurámola:



Marcamos a directiva como habilitada, de modo que no GPO que estamos definindo esta directiva vai estar habilitada. Prememos sobre o botón Aceptar, co cal regresaremos ao editor de directivas:

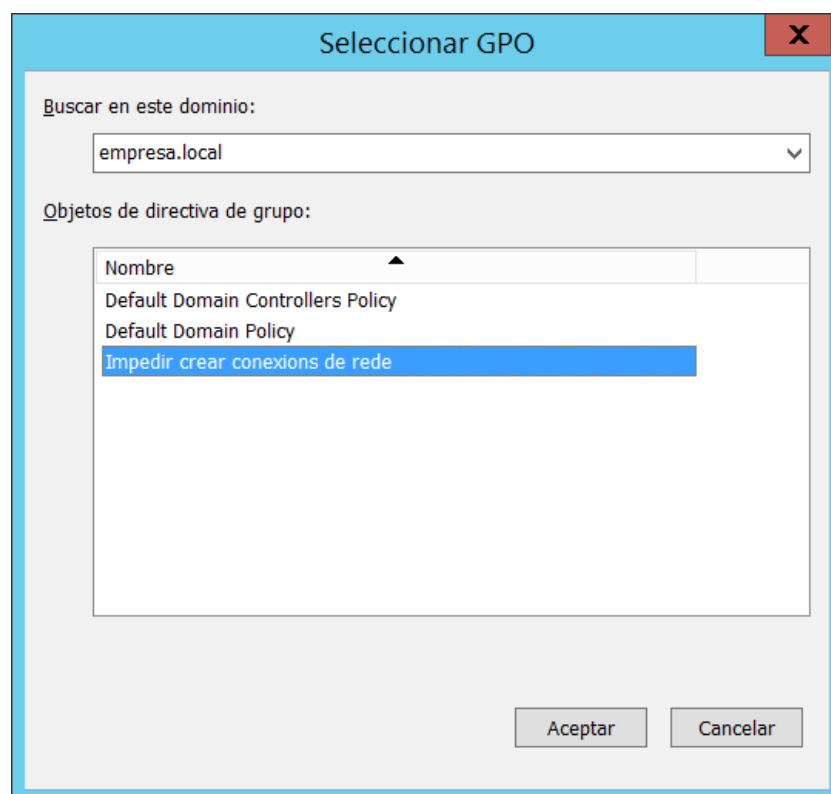


Como pódese observar na imaxe, a directiva agora aparece como habilitada. Agora poderíamos seguir modificando máis directivas para continuar coa configuración da GPO, pero neste caso ímonos limitar unicamente a modificar esta directiva. É importante lembrar que a maior parte das directivas aparecen como non configuradas. Isto non quere dicir que non se apliquen. Na axuda dalgunhas directiva indícase cal é o comportamento do seu estado no configurada, mentres que noutras directivas hai que deducilo mediante proba e erro. Unha vez que non temos que modificar ningunha directiva máis na GPO que estamos configurando, cerramos o editor de directivas. Se no panel da esquerda da xanela de administración de directivas de grupo seleccionamos o GPO que acabamos de crear, no panel da dereita cárgase información referente a dito GPO. É moi interesante a pestana Configuración xa que nos permite observar os cambios realizados para a configuración do GPO:

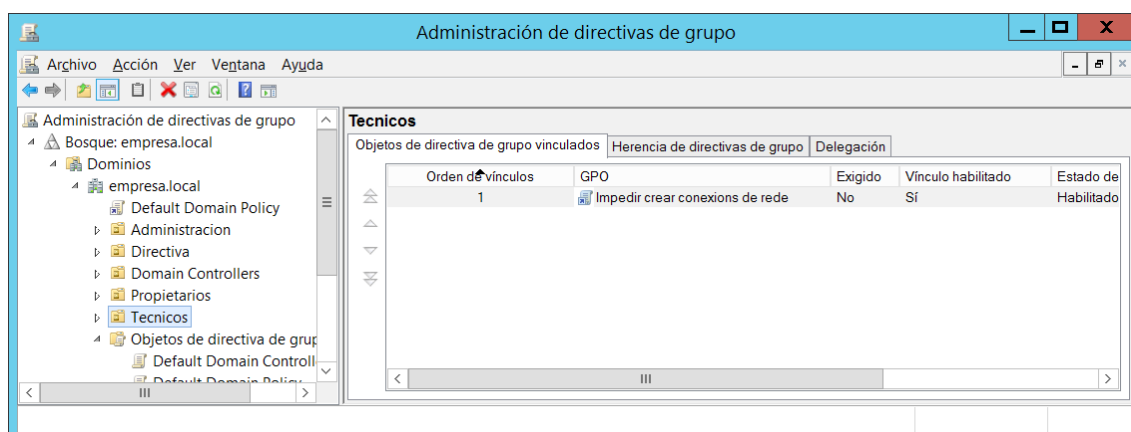


Unha vez configurada a GPO, imos aplicarlle sobre algún usuario para poder ver os seus resultados. Os GPOs non se aplican sobre usuarios directamente, senón que como xa dixéramos antes faise sobre dominios ou sobre UOs. Neste caso imos facer que o GPO sexa aplicado sobre tódolos usuarios que pertencen á UO Tecnicos. A aplicación dun GPO sobre unha UO implica que tamén sexa aplicada sobre todas sus subUOs (a aplicación dun GPO

realízase recursivamente). Para elo, na consola de administración de directivas de grupo prememos co botón dereito do rato sobre a UO á que queremos aplicar o GPO, neste caso a UO Tecnicos. Desprégase un menú contextual. Seleccionaremos a opción Vincular un GPO existente. Abrirase a seguinte xanela:

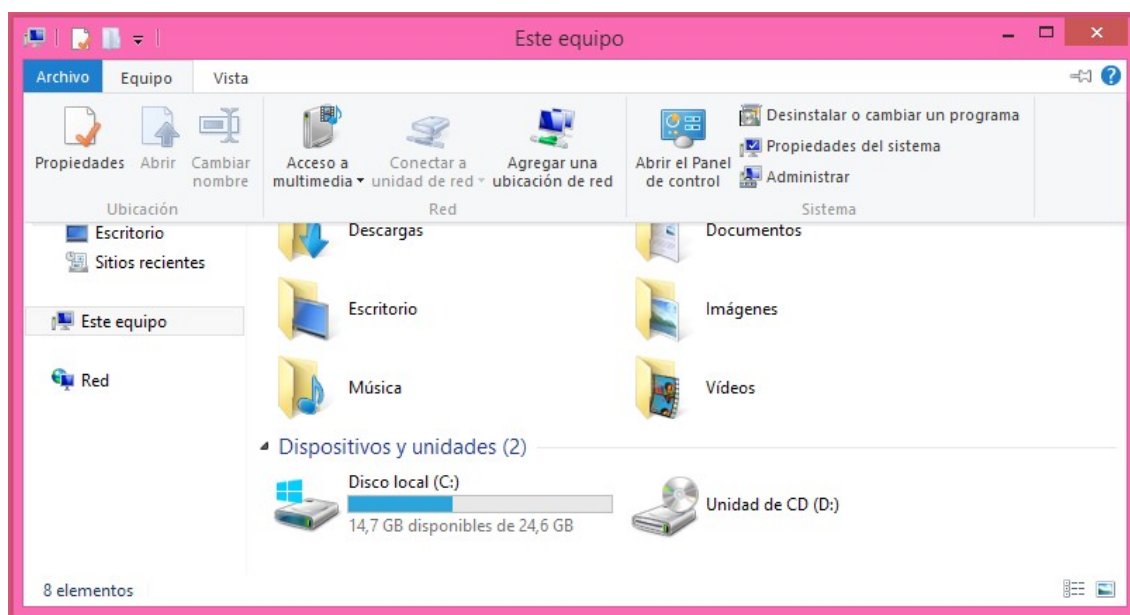


Nesta xanela lístanse tódolos GPOs que hai definidos no sistema. Elixiremos o GPO que queiramos aplicar sobre a UO seleccionada e premeremos sobre o botón Aceptar. Unha vez vinculado un GPO a unha UO, se na consola de administración de directivas de grupo seleccionamos dita UO, na pestana Objetos de directivas de grupo vinculados amósanse tódolos GPOs que se aplican sobre dita UO:



Comprobemos que o GPO funciona axeitadamente. Para elo iniciaremos sesión desde unha estación de traballo empregando un usuario que pertenza á UO Tecnicos. A UO Tecnicos

non ten usuarios, pero ten outras UOs que se que teñen usuarios. Como dixéramos anteriormente, os GPOs que se aplican sobre un obxecto, tamén aplícanse recursivamente sobre os obxectos que contén, así que o GPO Impedir conexións de rede tamén vaise aplicar sobre os obxectos das UOs Software e Hardware. Imos iniciar sesión co usuario evarr e imos comprobar se pódense crear conexións de rede desde o seu explorador de arquivos:



Como pódese observar na imaxe anterior, o elemento da barra de menú do explorador de arquivos de evarr que se emprega para crear unidades de rede está deshabilitado. Polo tanto, a aplicación da directiva foi correcta.

Aplicación das directivas de grupo

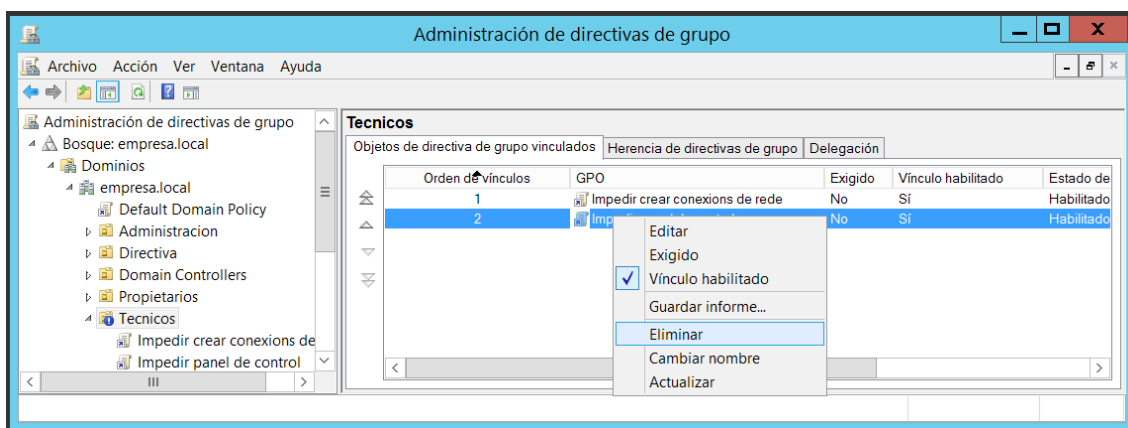
As directivas de grupo non se aplican inmediatamente trala súa creación. As directivas de grupo son aplicadas nas seguintes situacións:

- A configuración do equipo aplícase ao iniciar o sistema operativo.
- A configuración do usuario aplícase cando o usuario inicia a súa sesión.
- Ademais as directivas de grupo aplícanse con certa periodicidade sen necesidade de reiniciar máquinas nin sesións de usuario. Por defecto, cada noventa minutos (máis un tempo extra aleatorio para evitar sobrecarga na rede) actualízanse as directivas aplicadas sen que sexa necesario reiniciar a máquina nin a sesión de usuario. Este periodo de tempo chámase intervalo de actualización da directiva de grupo. Este intervalo pode ser modificado mediante a aplicación de directivas locais. É recomendable que este periodo de tempo non sexa reducido en exceso xa que a actualización de directivas é un proceso que sobrecarga a rede e no caso de que o intervalo de actualización de directivas sexa moi reducido teremos un tráfico excesivo e normalmente innecesario.

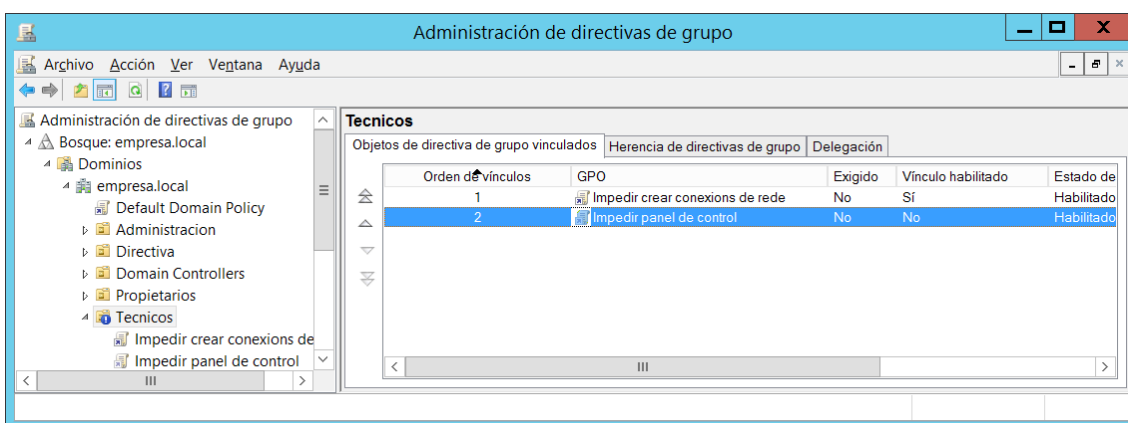
Desde calquera equipo podemos actualizar as directivas de grupo aplicadas sen ter que reiniciar a máquina, nin a sesión, nin ter que esperar o intervalo de actualización da directiva de grupo. Para elo unicamente debemos executar desde unha consola de comandos a orde gpupdate.exe (pero atención, hai certas directivas de grupo que non fan caso deste comando).

Habilitar e deshabilitar GPOs

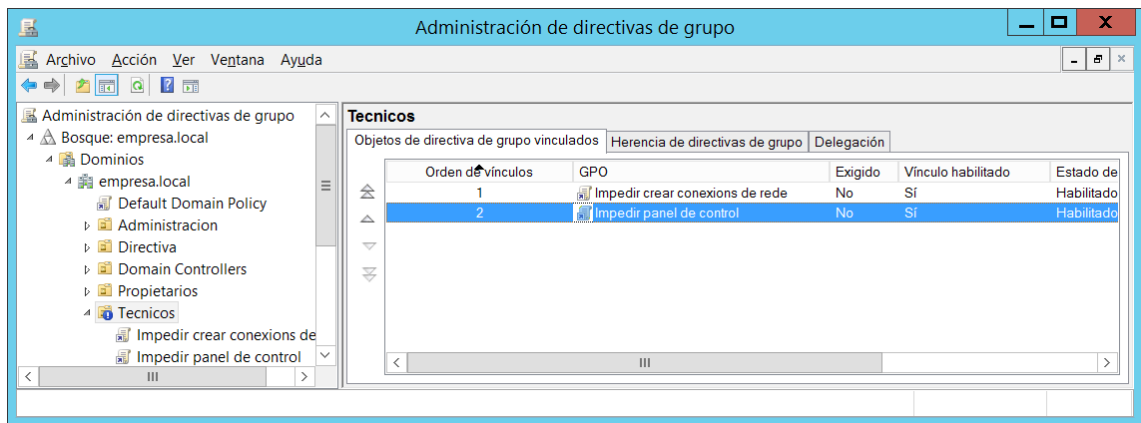
No caso de que queiramos que un GPO deixe de aplicarse sobre un obxecto podemos ou ben eliminar a vinculación do GPO ao obxecto ou ben inhabilitalo. Normalmente elimínase a vinculación cando esta deixa de ser necesaria para sempre e inhabilítase cando temporalmente pola razón que sexa non queremos asociar o GPO ao obxecto. Para eliminar o vínculo do GPO ao obxecto, seleccionamos o GPO no panel Objetos de directiva de grupo vinculados e prememos sobre el co botón dereito do rato. Despregarase un menú contextual. Seleccionamos a opción de eliminar e confirmamos a súa eliminación:



A eliminación non elimina o GPO definitivamente. Unicamente elimina o vínculo co obxecto, pero o GPO pode seguir sendo empregado para vinculalo con outros obxectos. Respecto á inhabilitación dun GPO vinculado a un obxecto, seleccionamos o GPO no panel Objetos de directiva de grupo vinculados e prememos sobre el co botón dereito do rato. Despregarase un menú contextual. Desmarcamos a opción vínculo habilitado, confirmamos a deshabilitación e a partir dese momento o GPO seguirá asociado ao obxecto, pero non será funcional:

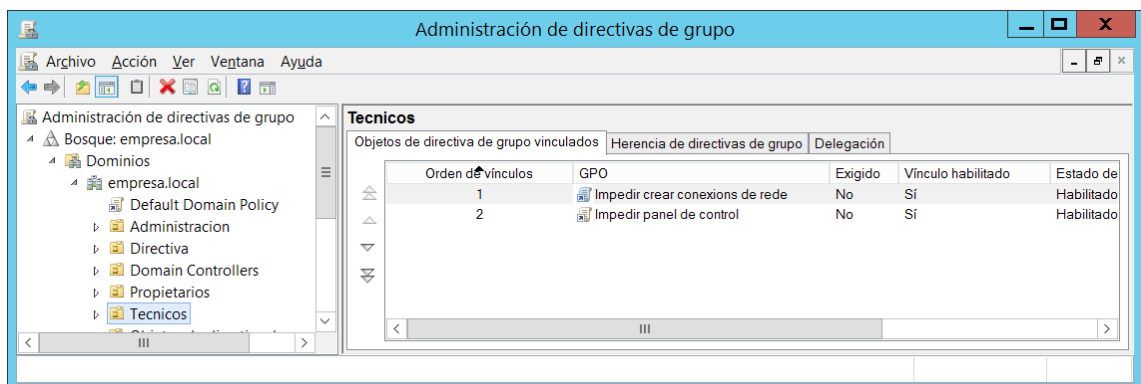


No momento que decidamos que o GPO volva a ser funcional repetiremos o proceso anterior, pero neste caso marcaremos a opción vínculo habilitado:



Aplicación de varios GPOs sobre un mesmo obxecto

É posible a aplicación de varios GPOs sobre un mesmo obxecto. Por exemplo imos crear un GPO que impida abrir o panel de control e ímolo vincular á UO Técnicos. Ao GPO ímolo chamar Impedir panel de control. A directiva a habilitar atópase en Configuración de usuario / Plantillas administrativas / Panel de control e chámase Prohibir el acceso a configuración de PC y a panel de control:



Como pódese observar na imaxe anterior, no panel da dereita aparecen os GPOs vinculados á UO Técnicos. Ademais o campo orden de vínculos indica en que orde vanse aplicar os GPOs. Os GPOs aplícanse partindo desde aquel que ten o valor de orden de vínculos máis alto (mínima prioridade) ata aquel que ten o valor máis baixo (máxima prioridade). Mediante as frechas presentes no panel Objetos de directiva de grupo vinculados podemos cambiar a prioridade da aplicación dos GPOs.

Neste caso, primeiro aplicárase o GPO Impedir panel de control e a continuación o GPO Impedir crear conexións de rede. Neste caso a orde de aplicación dos GPOs é indiferente xa que ningunha directiva das dous GPOs entra en conflito.

Imos modificar o GPO Impedir crear conexións de rede para que entre en conflito coa directiva Impedir panel de control. Para elo neste GPO deshabilitamos a directiva Prohibir el acceso a configuración de PC y a panel de control.

Se agora abrimos sesión co usuario evarr e intentamos acceder ao panel de control vemos que o usuario pode acceder sen ningún problema. ¿Porque?. Ao abrir sesión aplícanse os GPOs. O primeiro GPO a aplicar é o de Impedir panel de control, o cal deshabilita o acceso ao panel de control. A continuación aplícase o GPO Impedir crear conexións de rede o cal entre outras cosas habilita o acceso ao panel de control. Como resultado o usuario poderá

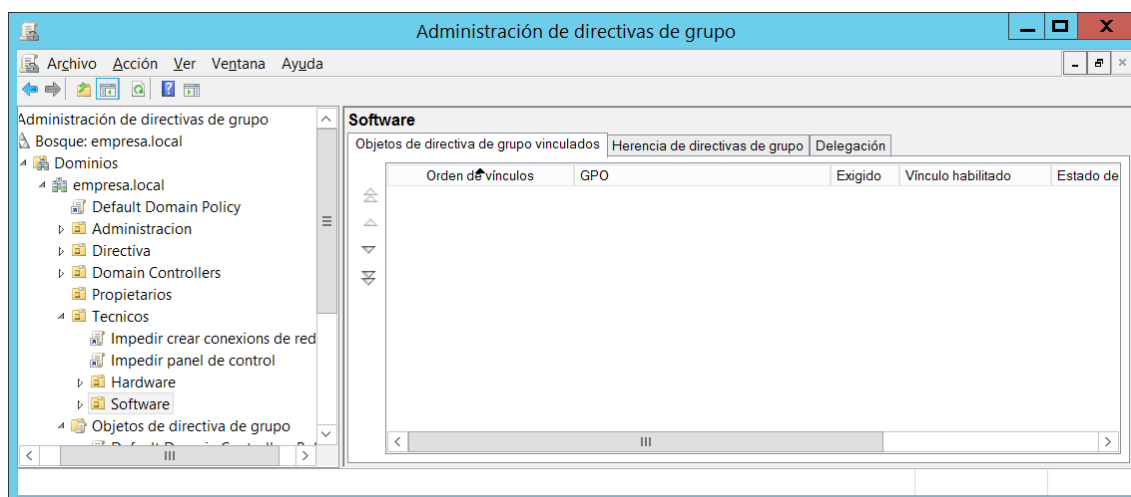
acceder ao panel de control, xa que o último GPO aplicado permítello.

Sen embargo, se configuramos o GPO Impedir crear conexións de rede de modo que a directiva Prohibir el acceso a configuración de PC y a panel de control quede en estado No configurado, ao abrir sesión co usuario evarr e intentar acceder ao panel de control vemos que o usuario non pode acceder. ¿Porque?. Ao abrir sesión aplícanse os GPOs. O primeiro GPO a aplicar é o de Impedir panel de control, o cal deshabilita o acceso ao panel de control. Ata o momento o valor da directiva que impide o acceso ao panel de control é o de habilitala. A continuación aplícase o GPO Impedir crear conexións de rede, o cal entre outras cosas non ten configurado que hai que facer ao intentar acceder ao panel de control. Polo tanto o valor da directiva que controla o acceso ao panel de control non se modifica xa que no GPO Impedir crear conexións de rede en ningún momento indícase que se faga. Unha directiva non configurada non modifica o seu valor na árbore de execución de GPOs.

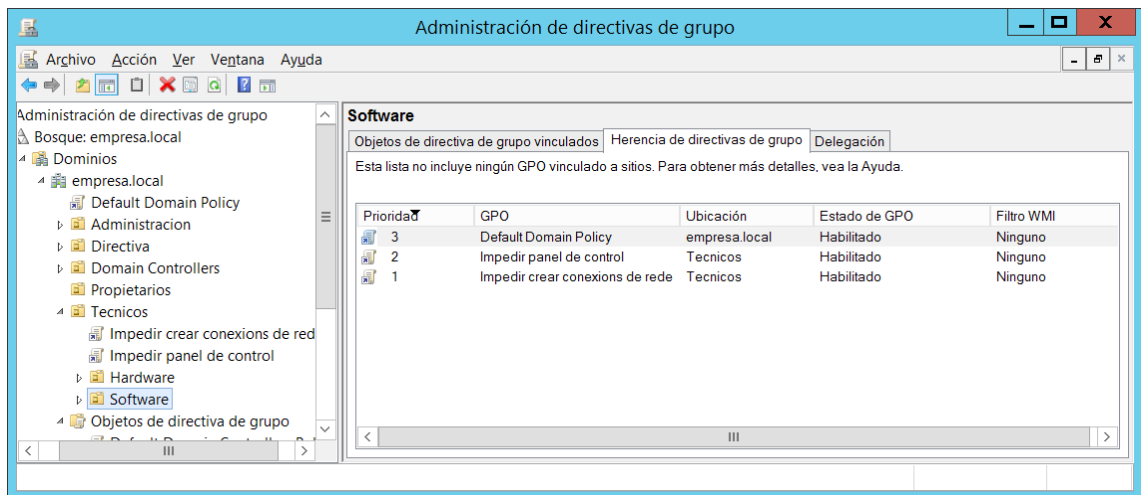
Evidentemente, polo visto ata o momento, se configuramos o GPO Impedir crear conexións de modo que a directiva Prohibir el acceso a configuración de PC y a panel de control quede en estado habilitado, ao abrir sesión co usuario evarr e intentar acceder ao panel de control, vemos que o usuario non pode acceder xa que o último valor dado á directiva que impide que se acceda ao panel de control é o de habilitada.

Herdanza de GPOs

Se amosamos os GPOs aplicados sobre a UO Software vemos que non hai ningún:



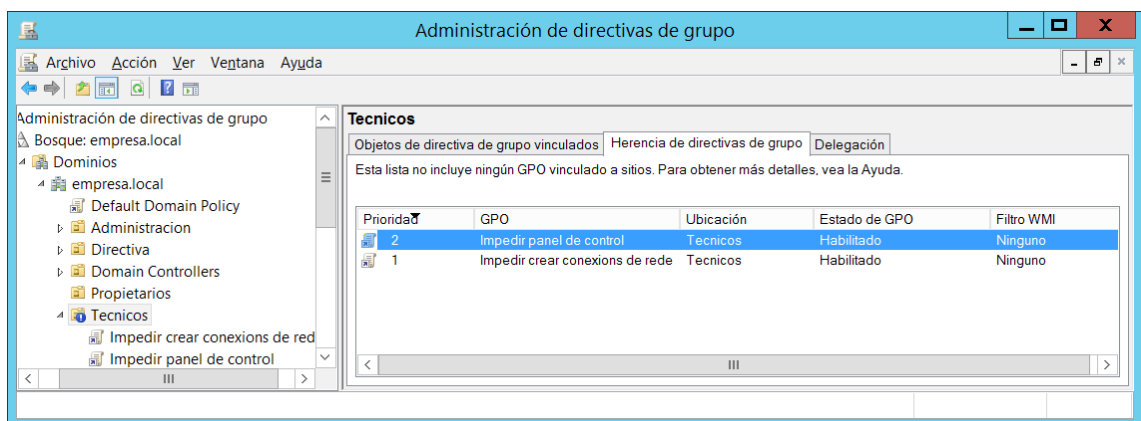
Sen embargo acabamos de comprobar que se aplican os GPOs Impedir panel de control e Impedir crear conexións de rede xa que ditos GPOs aplícanse sobre a UO Tecnicos e polo tanto sobre tódalas UOs contidas en Tecnicos. Neste caso dinse que os GPOs aplicados hérdanse. Para saber os GPOs que se aplican sobre un obxecto por herdanza, seleccionaremos a pestana Herencia de directivas de grupos. Neste panel amósase a información acerca de tódolos GPOs que se están aplicando sobre o obxecto:



O campo prioridad indícanos a orde de aplicación da GPO. Os GPOs aplícanse partindo desde aquel que ten o valor de prioridade máis alto ata aquel que ten o valor máis baixo. Neste caso primeiro aplicárase o GPO Default Domain Policy (este obxecto está predefinido polo sistema e define unha política de directivas de mínimos que se aplica a tódolos usuarios. O administrador, se consideralo oportuno, pode modificala), despois o GPO Impedir panel de control e por ultimo o GPO Impedir crear conexións de rede.

Anulación da herdanza

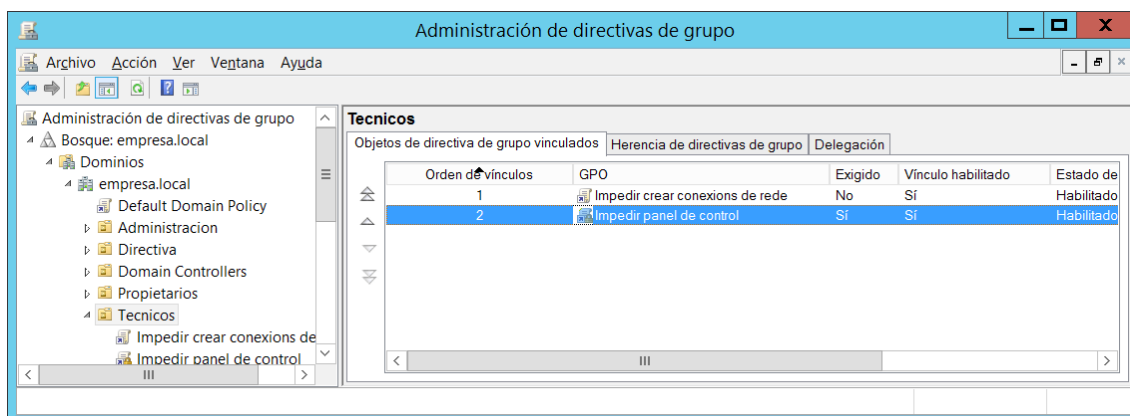
É posible que por algunha razón determinada non queiramos que sobre un obxecto aplíquense GPOs herdadas. Por exemplo, imaxinemos que non queremos que sobre a UO Tecnicos sexan aplicados os GPOs herdados. Para elo, prememos co botón dereito sobre a UO Tecnicos e activamos a opción de menú Bloquear herencia:



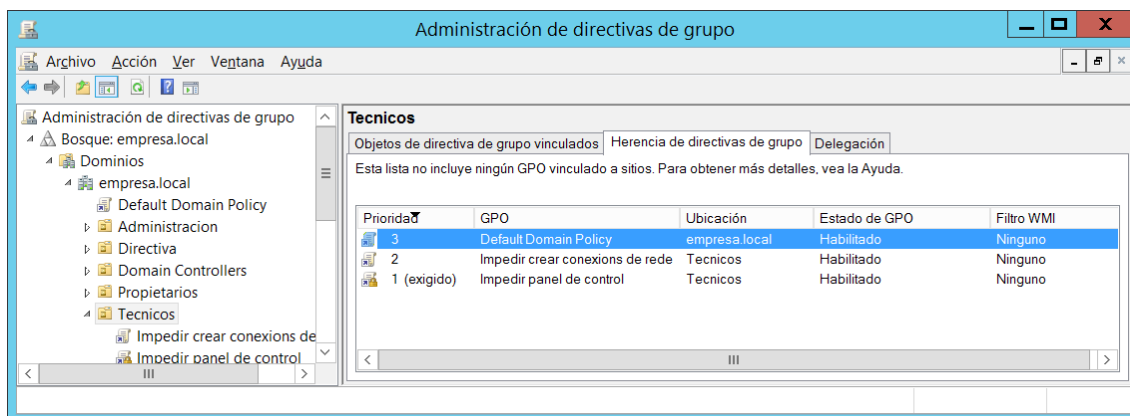
Como pódese observar na imaxe anterior, agora no panel Herencia de directivas de grupo unicamente amósanse os GPOs aplicados directamente sobre a UO Tecnicos, mentres que os GPOs herdados xa non aparecen debido a que non van ser aplicados. Evidentemente os GPOs non herdados pola UO Tecnicos tampouco serán herdados polas súas subUOs.

Exigir cumprimento dun GPO

Como xa vimos con anterioridade, é posible que algunha directiva dun GPO sexa sobrescrita por outra directiva doutro GPO que se executa posteriormente. No caso de que non queiramos que unha GPO sexa sobrescrita por outra o que faremos será asegurarnos de que dita GPO sexa a última en executarse. Para elo seleccionamos o GPO no panel Objetos de directiva de grupo vinculados e prememos sobre el co botón dereito do rato. Despregarase un menú contextual. Marcamos a opción Exigido e confirmamos a acción:



Se accedemos á información da pestana Herencia de directivas de grupo, podemos observar o seguinte:



O GPO Impedir panel de control será o último GPO en executarse na estrutura hereditaria de GPOs.

Advertencias sobre as directivas de grupo

As directivas de grupo son una ferramenta moi potente á hora de administrar un sistema informático pero non é fácil establecer unha política de directivas de grupos medianamente complexa. Require dun proceso de estudio, proba e refinamento. É recomendable ter ao menos unha estación de traballo de laboratorio dedicada á realización de probas de directivas de grupo, de modo que testemos estas sobre a máquina de laboratorio antes de aplicalas ao entorno de produción. Son moitas as sorpresas que nos podemos levar á hora de aplicar as directivas de grupo xa que non sempre fan o que supoñemos que van facer.

Ademais o seu comportamento pode variar en función do tipo de sistema operativo sobre o que se aplican. Polo tanto, lembémonos sempre de probar o funcionamento das directivas de grupo sobre unha máquina de laboratorio antes de aplicalas ao entorno de produción.

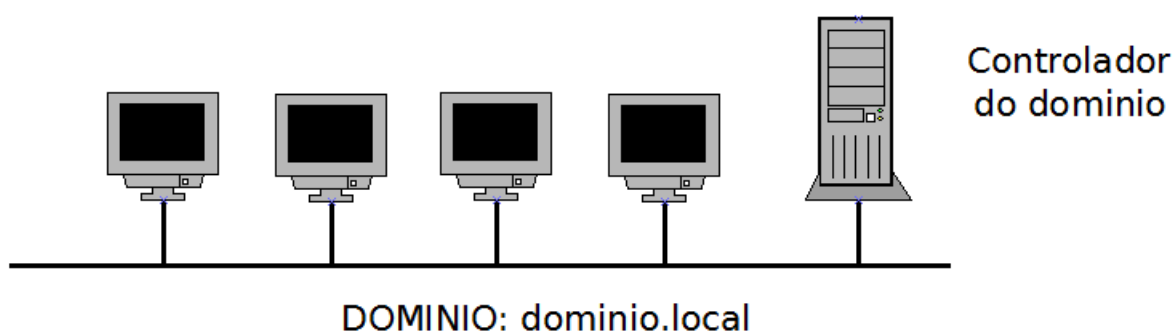


Realización da tarefa 9

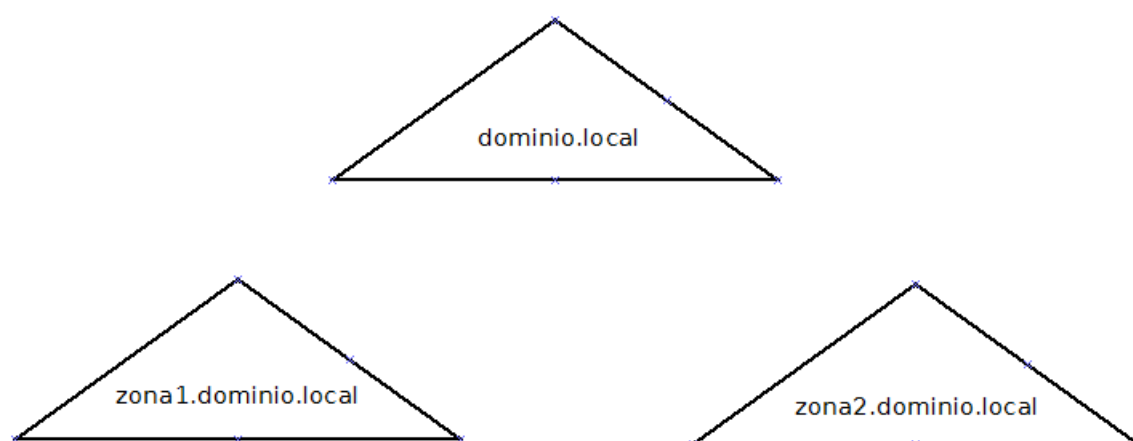
1.2.11 Estruturas de dominios

Aínda que non é intención deste material entrar en detalle sobre as diferentes estruturas de dominios que se poden configurar empregando Windows Server, si que imos polo menos a mencionalas para deixar constancia da súa existencia:

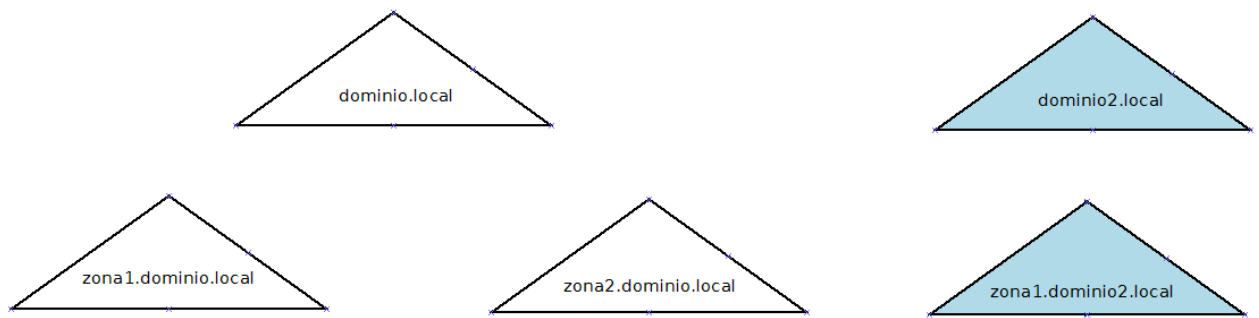
A estrutura máis sinxela é aquela composta por un único dominio. Nesta estrutura temos unha serie de equipos conectados en rede e un deles é o controlador do dominio. O dominio terá asignado un nome de dominio:



Esta estrutura de dominio é a estrutura típica dunha pequena organización. O dominio creado denomínase dominio raíz. Pode ocorrer que a organización por diversas razóns de funcionamento necesite crear dominios adicionais que dependan do dominio raíz:



Tódolos dominios que comparten o mesmo dominio raíz compoñen unha árbore de dominios. Adicionalmente pode ser que a organización estea composta por máis dunha árbore de dominios:



Neste caso, á suma de varias árbores de dominios denomínaselle bosque de dominios. A categorización dos dominios en subdominios, dominios, árbores e bosques permítenos limitar ou permitir a identificación dos usuarios e o acceso aos diferentes recursos desde as diferentes estruturas de dominio existentes. Para elo é necesario establecer relacións de confianza entre as diferentes estruturas de dominio existentes. Unha relación de confianza é unha relación entre dominios que permite aos usuarios dun dominio autenticarse por medio dun controlador de dominio noutro dominio. Non imos entrar en detalles, pero en función das relacións de confianza establecidas entre dominios, subdominios, árbores e bosques estableceremos que usuarios poden acceder ou non aos diferentes recursos existentes.