Migrando active-directory a sw libre

Moisés Rubiño García • Open South Code • ermoi@ermoi.es

OBJETIVOS

- Alternavias libres de Active Directory
- Mostrar una distribución precocinada
- Mostrar como se implementa

Premisas

- Red con Active Directory funcionando o planificada
- Equipos MS Windows en la red


SAMBA 4

Características

- Compartición de ficheros e impresoras
- Política de grupos y GPO
- Kerberos

Recomendaciones

- A día de hoy, no se recomienda más de 3 controladores de dominio

Limitaciones

- Sólo un dominio, en un único bosque, Samba no soporta múltiples dominios ni múltiples bosques
- El nivel funcional tanto del dominio como del bosque ha de ser mínimo 2003 y máximo 2012
- El nombre de host no puede coincidir con el nombre NETBIOS, el nombre NETBIOS se genera a partir de la parte izquierda del nombre de dominio, por ejemplo, si el nombre de host es 'zentyal', el nombre de dominio no puede ser 'zentyal.lan', pero si 'zentyal-domain.lan'
- Las relaciones de confianza entre dominios y bosques no están soportadas
- Las GPO se sincronizarán desde los servidores Windows® hacia los servidores Zentyal, pero no a la inversa
- No se soportan usuarios con nombres no-ASCII (tildes, eñes, guión)

DISTRIBUCIONES PRECOCINADAS

- Zentyal
- Univention
- nethserver
- ...


ZENTYAL

CARACTERÍSTICAS

Mail

- Native compatibility with Microsoft® Exchange Server Protocols
- Support for Microsoft Outlook® 2007, 2010
- Native compatibility with Microsoft Active Directory®
- Multiple Virtual Mail Domain
- Email, calendars, contacts
- Webmail
- Synchronization with mobile devices (ActiveSync® support)
- Antivirus and antispam
- Extension and MIME type Filters

Basic Networking and Firewall

- Static and DHCP interfaces
- Objects & Services
- Packet Filter
- Port Forwarding

Domain & Directory

- Central domain directory management
- Users, Security Groups, Distribution Lists, Contacts
- Multiple Organizational Units (OUs)
- Single Sign-On (SSO) authentication
- Supported OS: Windows® XP, Windows Vista®, Windows® 7, Windows® 8
- File sharing in Windows® environments (CIFS)
- Users & Groups access and modification permissions (ACLs)
- Advanced domain management through the RSAT tools
- Printers Management
- Antivirus with integrated quarantine for file server

Infrastructure

- DNS Server
- DHCP Server
- NTP Server
- Certification Authority
- VPN Server & Client

Hay versión comercial

- www.zentyal.com
- Soporte técnico ilimitado
- Versiones más estables
- Preparado para entornos de producción
- Cada versión está soportada durante 4,5 años
- ANS - Max. 2 Días Laborables

Precios

- Precio al año
- Primer servidor 395 euros
- Servidores adicionales 275 euros

Edición Development

- Gratis
- Sw más actual pero menos estable
- Nueva versión cada 3 meses
- Necesario actualizar (incluso reinstalar) para continuar recibiendo actualizaciones
- Sin soporte, solo la comunidad

Recomendaciones

- No es recomendable mezclar servidores comerciales con servidores development: llevan distintas versiones de software lo cual causaría errores de sincronización y mal funcionamiento de todo el despliegue

INSTALACIÓN

- www.zentyal.org
- Descargamos la versión Zentyal Server (development edition)
- Actualmente versión 4.2

- Se realiza una instalación típica de una distribución
- Basada en ubuntu
- La administración se realiza toda vía web

Arrancando

Installing Zentyal core packages... Please wait.

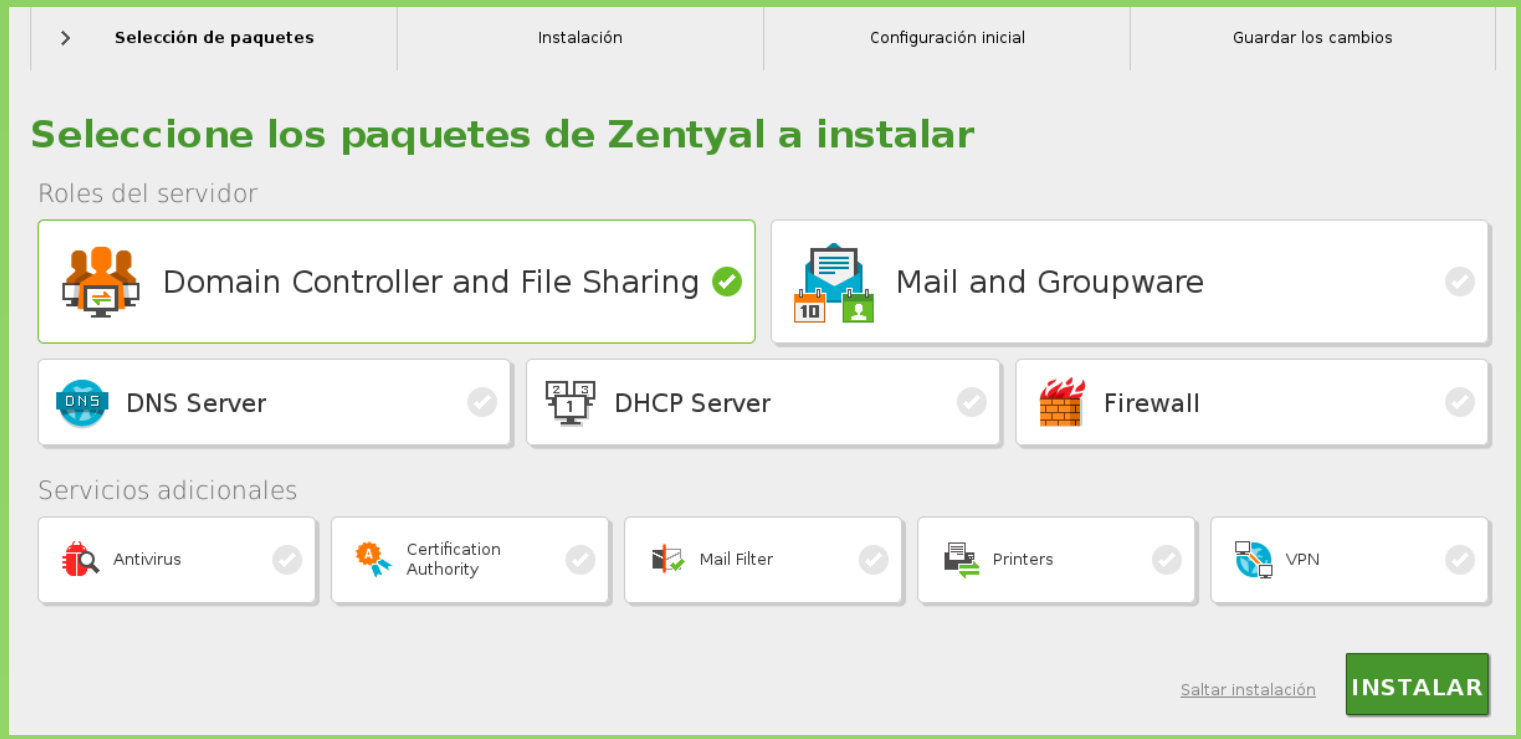

Zentyal - Mozilla Firefox
Zentyal
https://localhost:8443/Login/Index
Search
Most Visited
zentyal.com
zentyal.org
Documentation
Forum
Online Store
zentyal
Usuario
Contraseña
ENTRAR
Zentyal - Mozilla Firefox
20:44

Configuración inicial

Gracias por escoger Zentyal, sólo quedan unos pocos pasos para empezar a disfrutar del producto:

Continuar

Seleccionamos el tipo de servidor Zentyal



Esperamos. . .


Selección de paquetes
Instalación
Configuración inicial
Guardar los cambios
Compatibilidad nativa con protocolos Microsoft® Exchange Server
¡Integración transparente en entornos Microsoft Outlook®!
Soporte para Microsoft Outlook® 2007 y 2010
Correo y Groupware (Contactos y Calendarios)
¡No es necesario instalar plug-ins o conectores en los clientes de correo!
Configuración automática del servidor con el servicio Autodiscover
¡Aprende más en wiki.zentyal.org!
Instalando paquetes
Operación actual: Unpacking postfix-ldap (2.11.0-1ubuntu1) ...
37%
218 de 600 operaciones realizadas

CONFIGURAMOS RED

✔ Selección de paquetes | ✔ Instalación | > **Configuración inicial** | Guardar los cambios

Asistente de configuración inicial

Interfaces de Red

Configurar red para interfaces externos

Ahora puede configurar direcciones IP y redes para cada interfaz

eth0

Método

Static

Dirección IP

Máscara de red

255.255.255.0

Puerta de enlace

Servidor de nombres de dominio 1

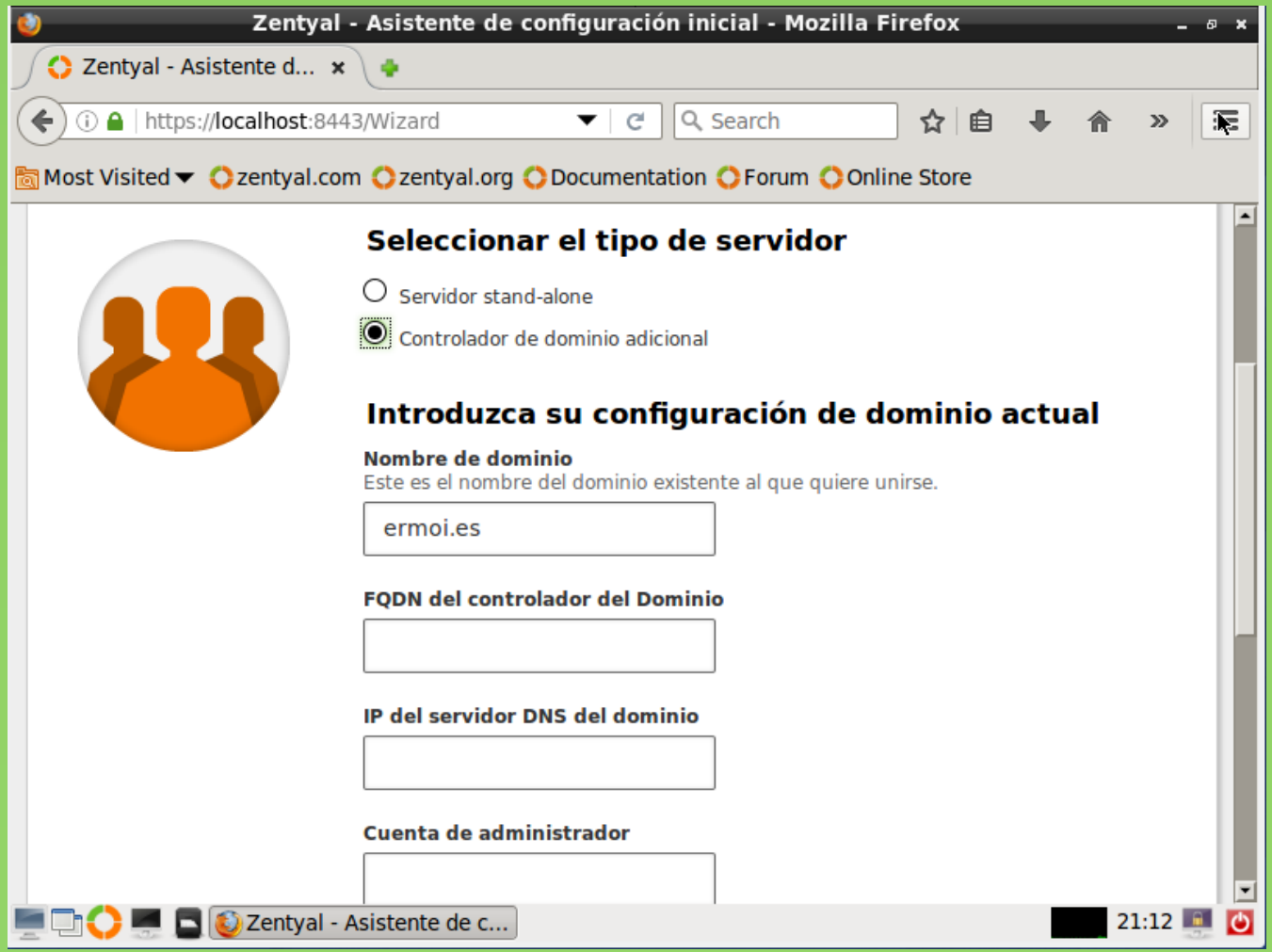
Servidor de nombres de dominio 2

SALTAR SIGUIENTE

Decidimos el tipo de controlador

- Standalone server (controlador principal)
- Aditional domian controler (para añadir a un dominio ya existente como secundario)


Zentyal - Asistente de configuración inicial - Mozilla Firefox
Zentyal - Asistente d...
https://localhost:8443/Wizard
Search
Most Visited
zentyal.com
zentyal.org
Documentation
Forum
Online Store
Asistente de configuración inicial
Usuarios y Grupos
Seleccionar el tipo de servidor
Servidor stand-alone
Controlador de dominio adicional
Seleccionar nombre de dominio del servidor
Nombre del dominio para esta máquina
Será usado como dominio de autenticación de Kerberos para sus usuarios.
ermoi.es
SALTAR
FINALIZAR
Zentyal - Asistente de c...
21:12


Zentyal - Asistente de configuración inicial - Mozilla Firefox
Zentyal - Asistente d...
https://localhost:8443/Wizard
Search
Most Visited
zentyal.com
zentyal.org
Documentation
Forum
Online Store
Seleccionar el tipo de servidor
Servidor stand-alone
Controlador de dominio adicional
Introduzca su configuración de dominio actual
Nombre de dominio
Este es el nombre del dominio existente al que quiere unirse.
ermoi.es
FQDN del controlador del Dominio
IP del servidor DNS del dominio
Cuenta de administrador
Zentyal - Asistente de c...
21:12

Finalizamos!!!!!

✔ Selección de paquetes | ✔ Instalación | ✔ Configuración inicial | ✔ Guardar los cambios

Instalación completada

¡Enhorabuena!

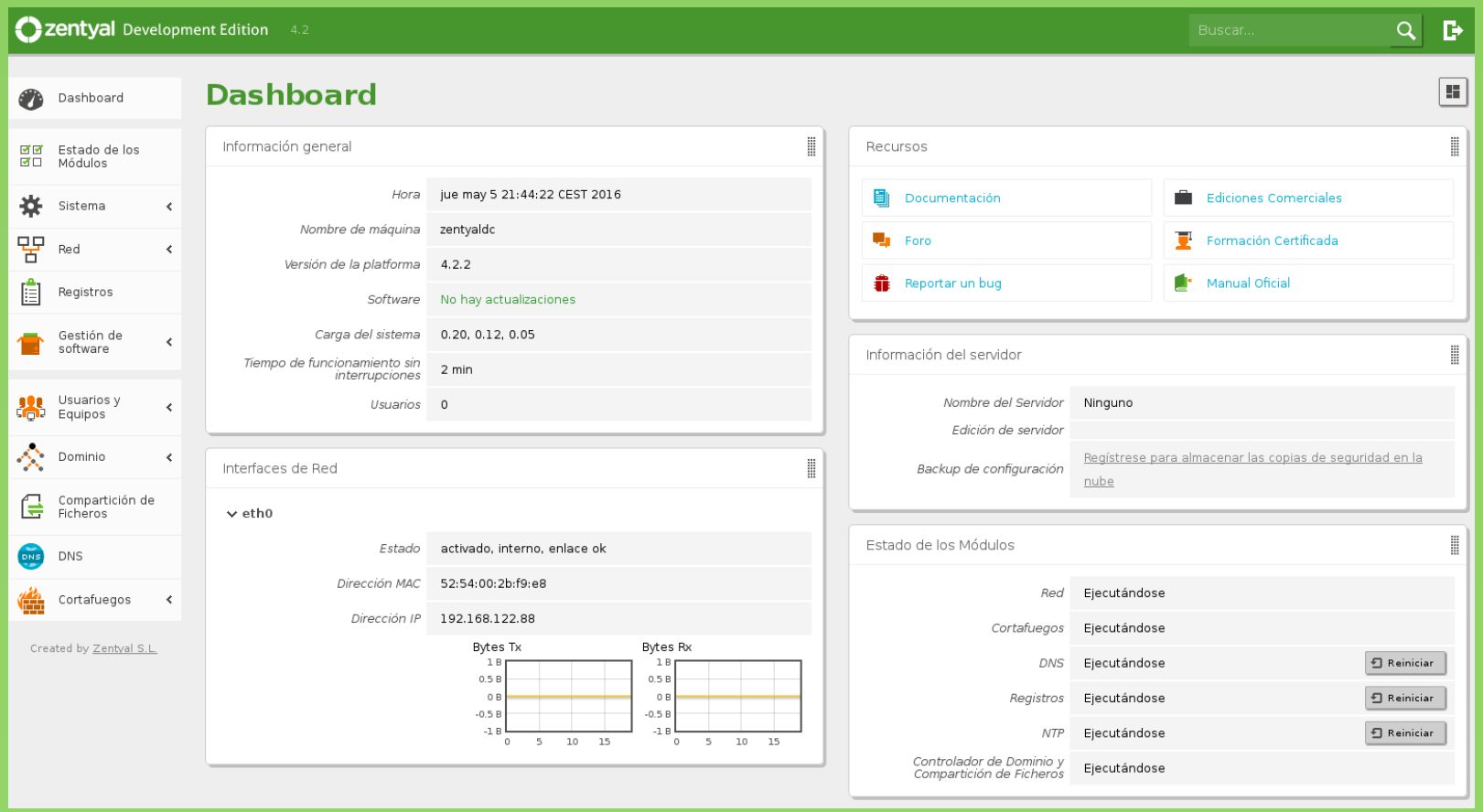
¡Tu instalación de Zentyal se ha completado con éxito!

Puedes ir al Dashboard y comenzar a usar tu servidor Zentyal recién instalado.

IR AL DASHBOARD

EXPLOTACIÓN

Dashboard


zentyal Development Edition 4.2
Buscar...
Dashboard
Estado de los Módulos
Sistema
Red
Registros
Gestión de software
Usuarios y Equipos
Dominio
Compartición de Ficheros
DNS
Cortafuegos
Created by Zentyal S.L.
Dashboard
Información general
Hora
jue may 5 21:44:22 CEST 2016
Nombre de máquina
zentyaldc
Versión de la platforma
4.2.2
Software
No hay actualizaciones
Carga del sistema
0.20, 0.12, 0.05
Tiempo de funcionamiento sin interrupciones
2 min
Usuarios
0
Interfaces de Red
eth0
Estado
activado, interno, enlace ok
Dirección MAC
52:54:00:2b:f9:e8
Dirección IP
192.168.122.88
Bytes Tx
Bytes Rx
Recursos
Documentación
Ediciones Comerciales
Foro
Formación Certificada
Reportar un bug
Manual Oficial
Información del servidor
Nombre del Servidor
Ninguno
Edición de servidor
Backup de configuración
Regístrese para almacenar las copias de seguridad en la nube
Estado de los Módulos
Red
Ejecutándose
Cortafuegos
Ejecutándose
DNS
Ejecutándose
Reiniciar
Registros
Ejecutándose
Reiniciar
NTP
Ejecutándose
Reiniciar
Controlador de Dominio y Compartición de Ficheros
Ejecutándose

Recomendaciones

- Para las actualizaciones, mejor descargar iso nueva y reestablecer copia de seguridad de la BD
- O actualizaciones desde el entorno web, nunca desde la consola, para mentener integridad de paquetes

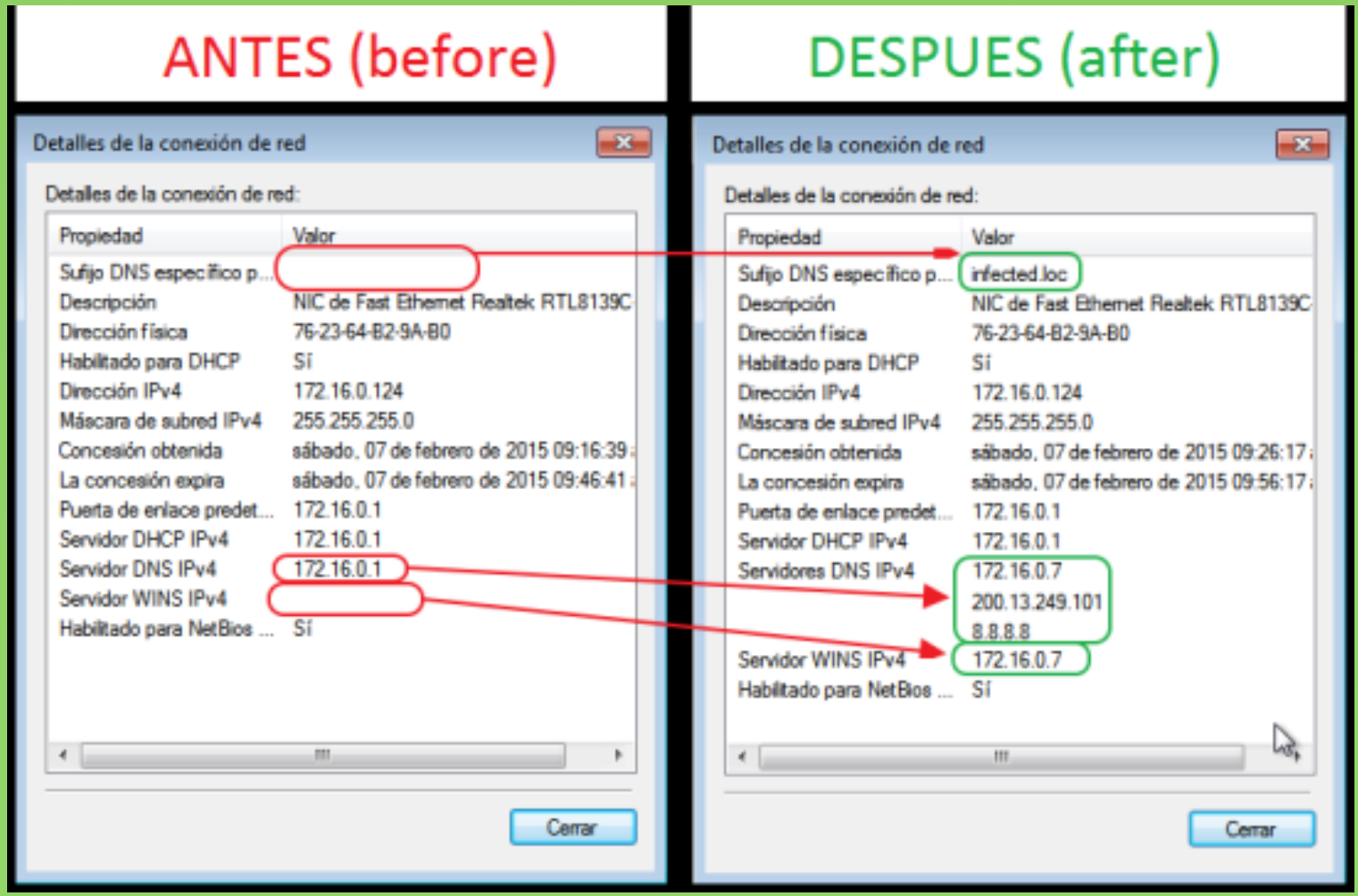
Backup del sistema

LISTO Y FUNCIONANDO

Pruebas para ver el funcionamiento

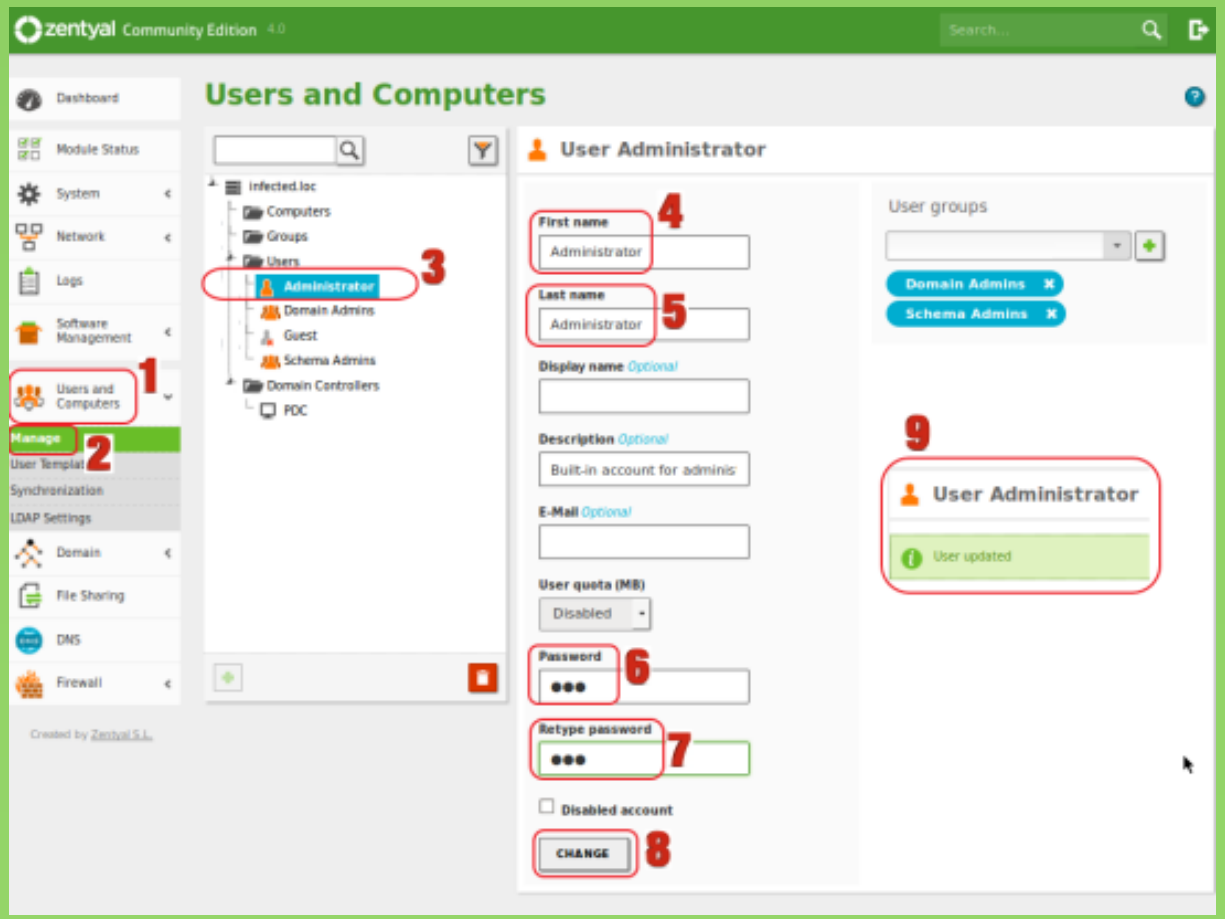
- Reconfiguramos red un equipo windows para que coja nuestra dhcpd
- Metemos un equipo dentro del dominio

Reconfiguración de red de un equipo

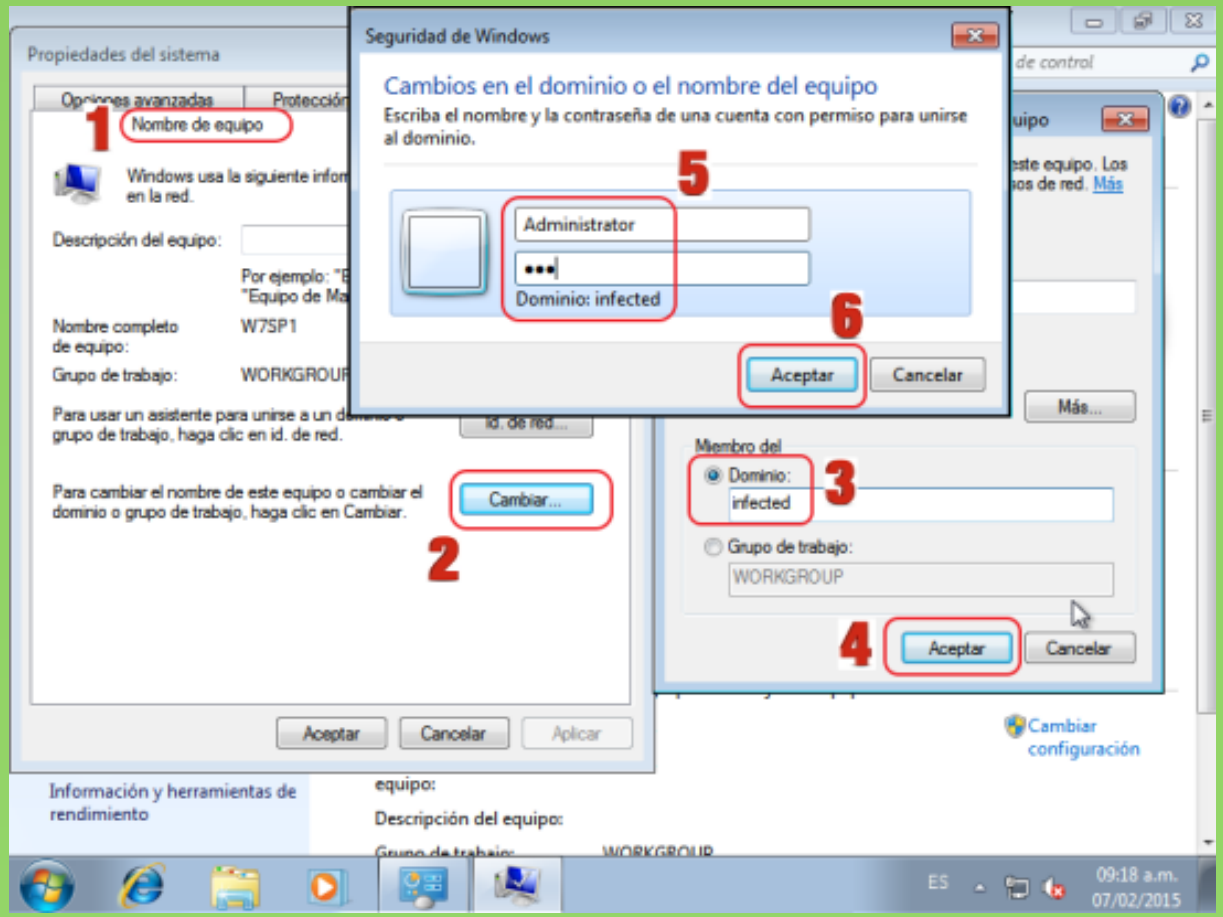


Metemos equipo en dominio

Cambiamos clave administrador del DC

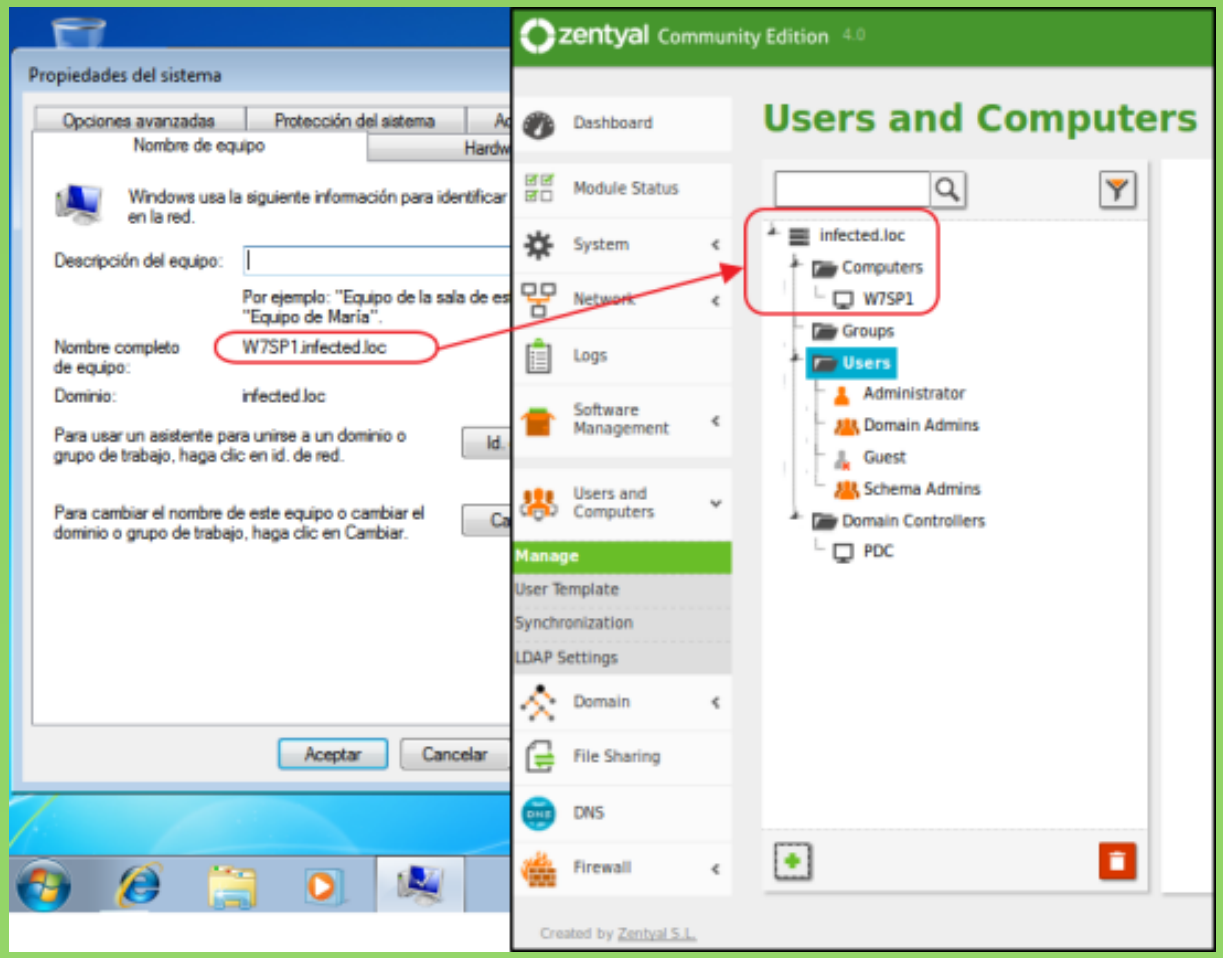


Metemos equipo en dominio



Metemos equipo en dominio

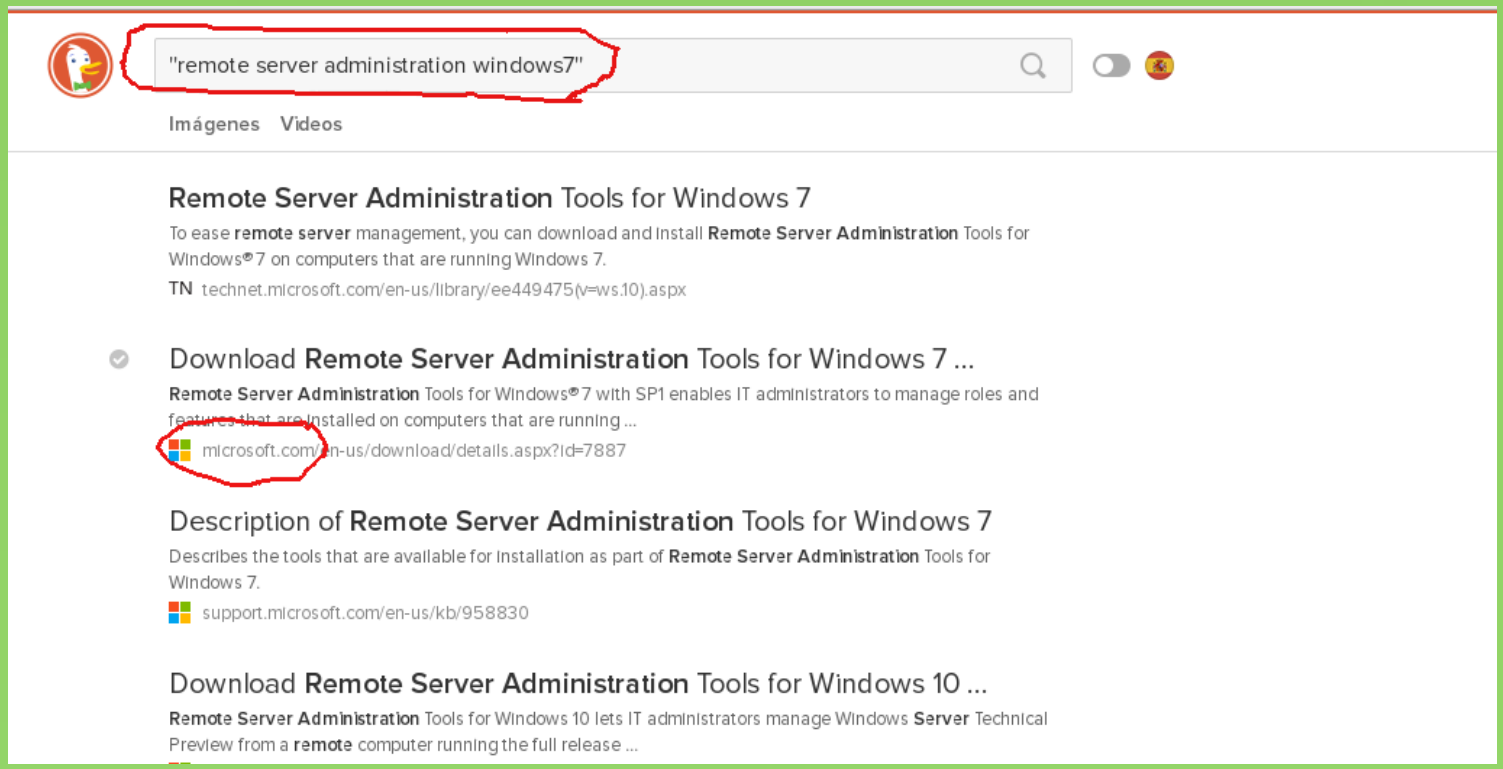
Verificamos en Zentyal



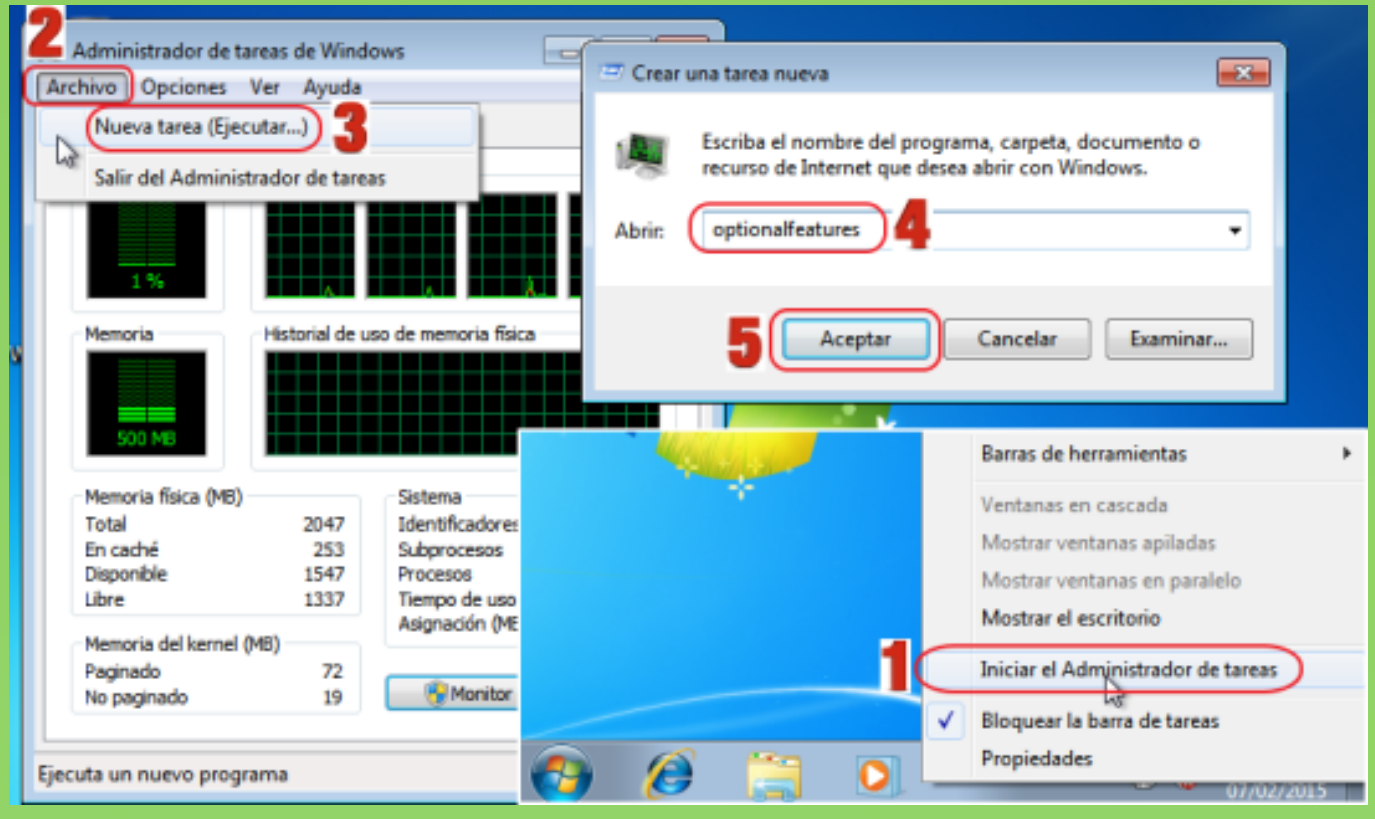
CREANDO Y ADMINISTRANDO POLÍTICAS

- Actualmente se realiza desde un equipo windows
- Mucho más comodo y visual
- Tiene sentido porque en realidad estás administrando una red windows
- Hay que instalar ”remote server administration windows7”

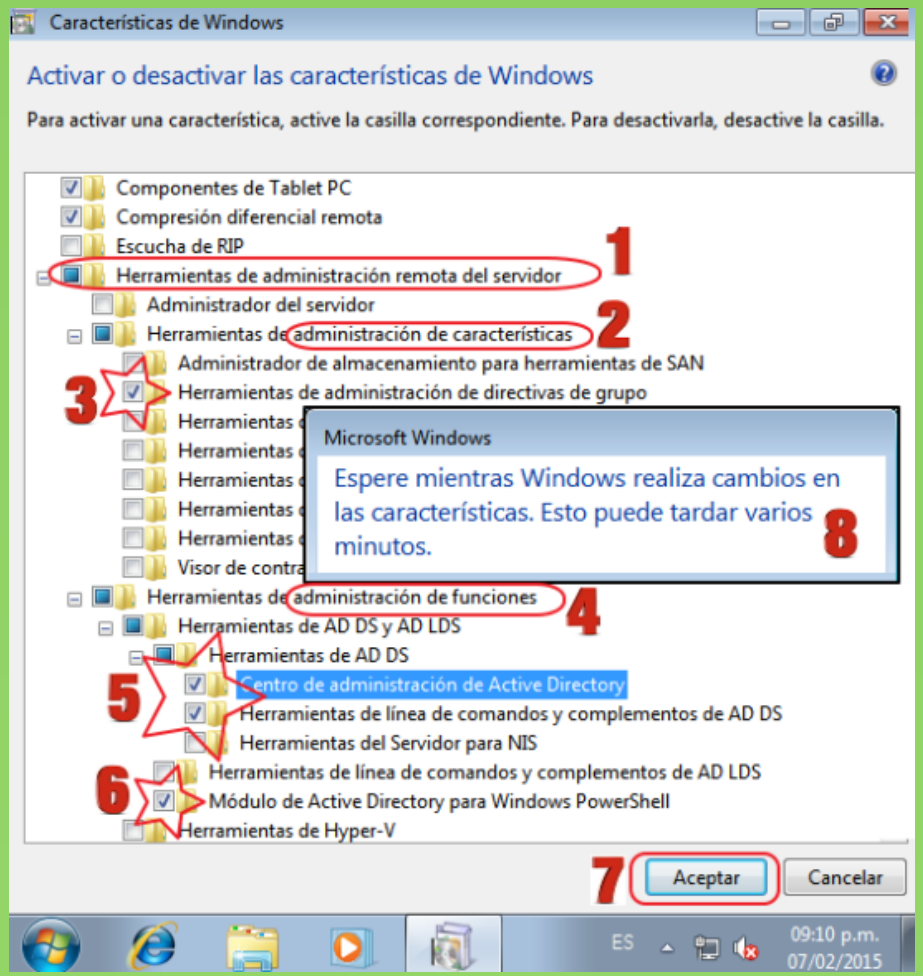
Descargamos ”remote server administration windows7”



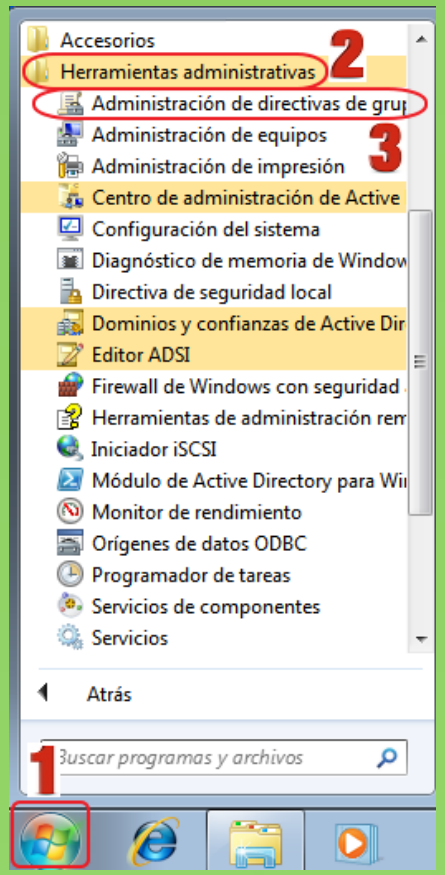
Instalamos


2
Administrador de tareas de Windows
Archivo
Opciones
Ver
Ayuda
Nueva tarea (Ejecutar...)
3
Salir del Administrador de tareas
Crear una tarea nueva
Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.
Abrir:
optionalfeatures
4
5
Aceptar
Cancelar
Examinar...
Memoria
Historial de uso de memoria física
Memoria física (MB)
Total 2047
En caché 253
Disponible 1547
Libre 1337
Memoria del kernel (MB)
Paginado 72
No paginado 19
Sistema
Monitor
Ejecuta un nuevo programa
Barras de herramientas
Ventanas en cascada
Mostrar ventanas apiladas
Mostrar ventanas en paralelo
Mostrar el escritorio
1
Iniciar el Administrador de tareas
Bloquear la barra de tareas
Propiedades

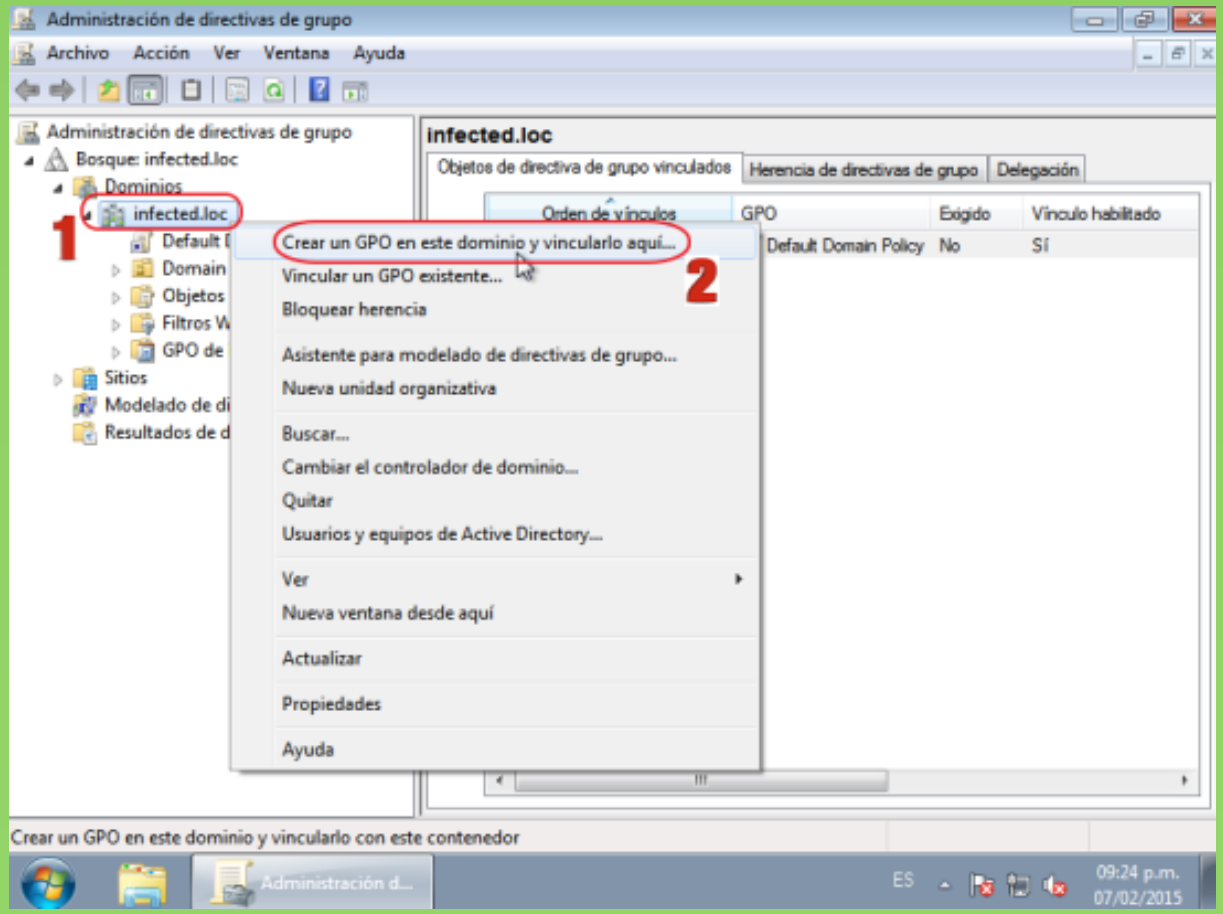
Activamos


Características de Windows
Activar o desactivar las características de Windows
Para activar una característica, active la casilla correspondiente. Para desactivarla, desactive la casilla.
Componentes de Tablet PC
Compresión diferencial remota
Escucha de RIP
Herramientas de administración remota del servidor
1
Administrador del servidor
Herramientas de administración de características
2
Administrador de almacenamiento para herramientas de SAN
3
Herramientas de administración de directivas de grupo
Microsoft Windows
Espere mientras Windows realiza cambios en las características. Esto puede tardar varios minutos.
8
Herramientas de administración de funciones
4
Herramientas de AD DS y AD LDS
Herramientas de AD DS
5
Centro de administración de Active Directory
Herramientas de línea de comandos y complementos de AD DS
Herramientas del Servidor para NIS
Herramientas de línea de comandos y complementos de AD LDS
6
Módulo de Active Directory para Windows PowerShell
Herramientas de Hyper-V
7
Aceptar
Cancelar
ES
09:10 p.m.
07/02/2015

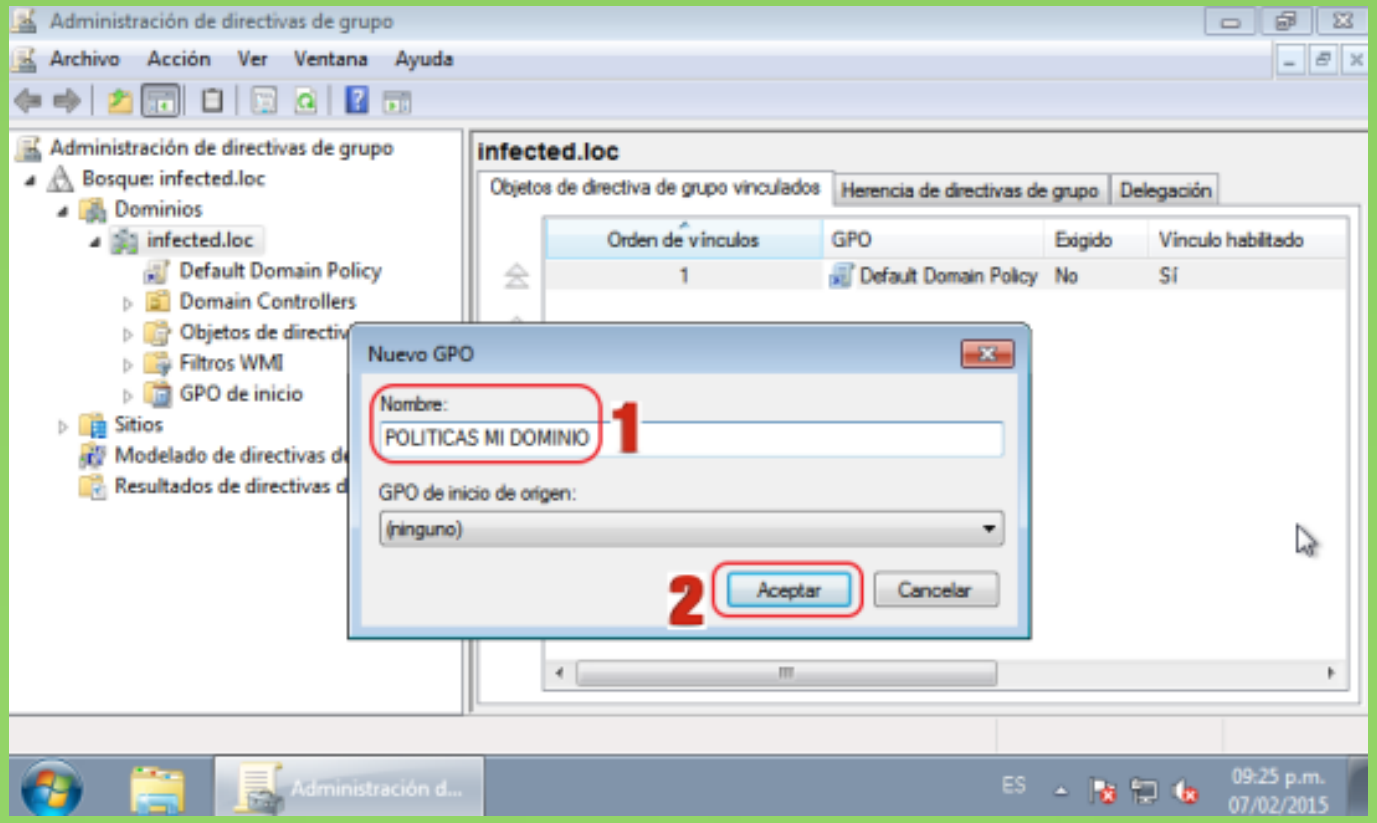
Y verificamos



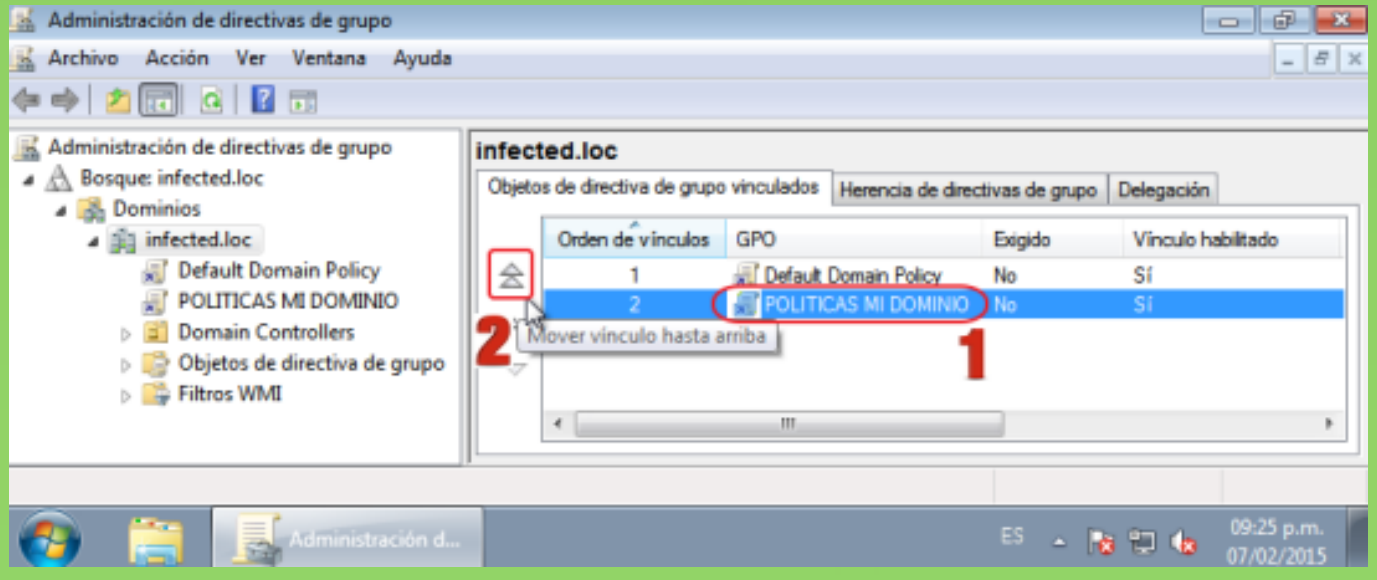
Creando una GPO



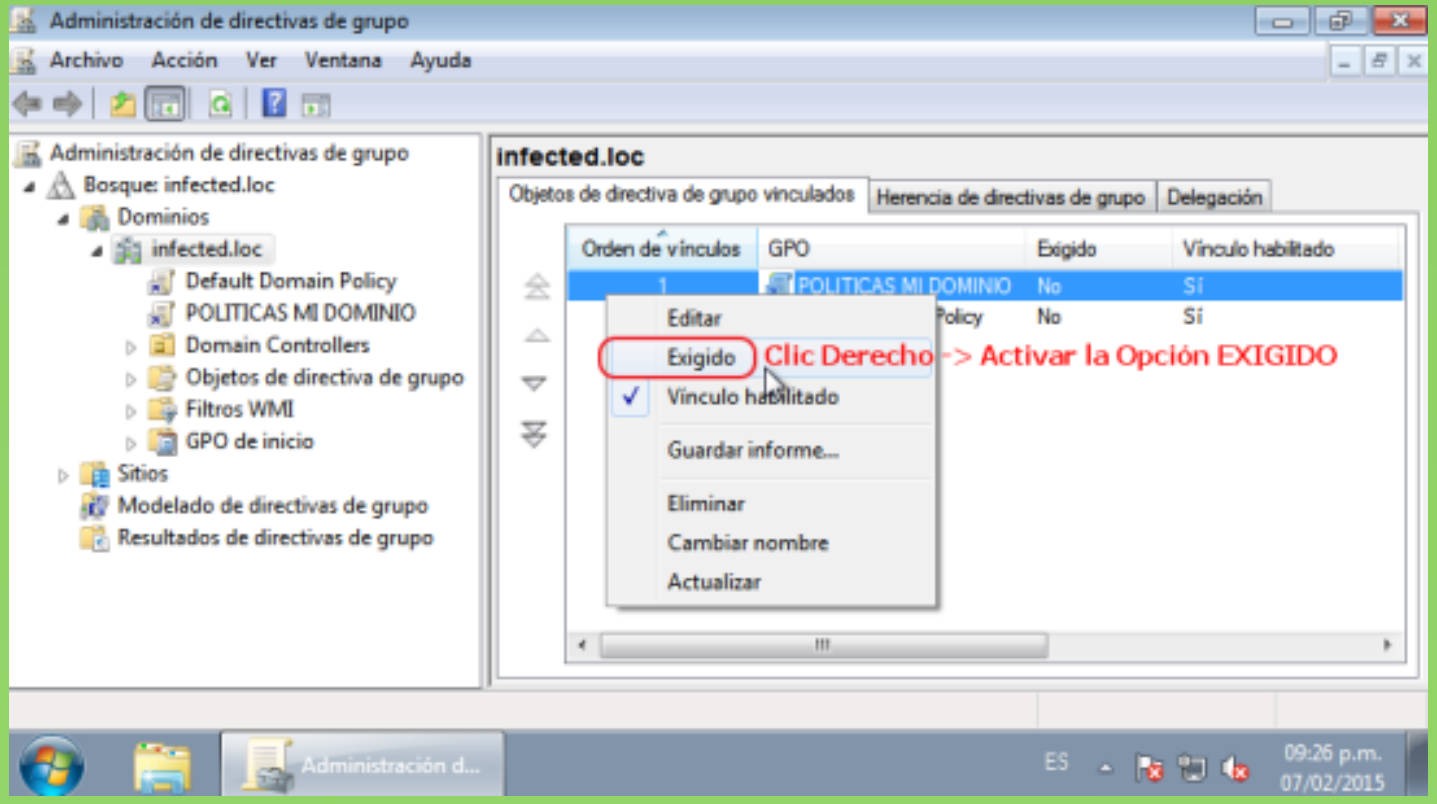
Creando una GPO



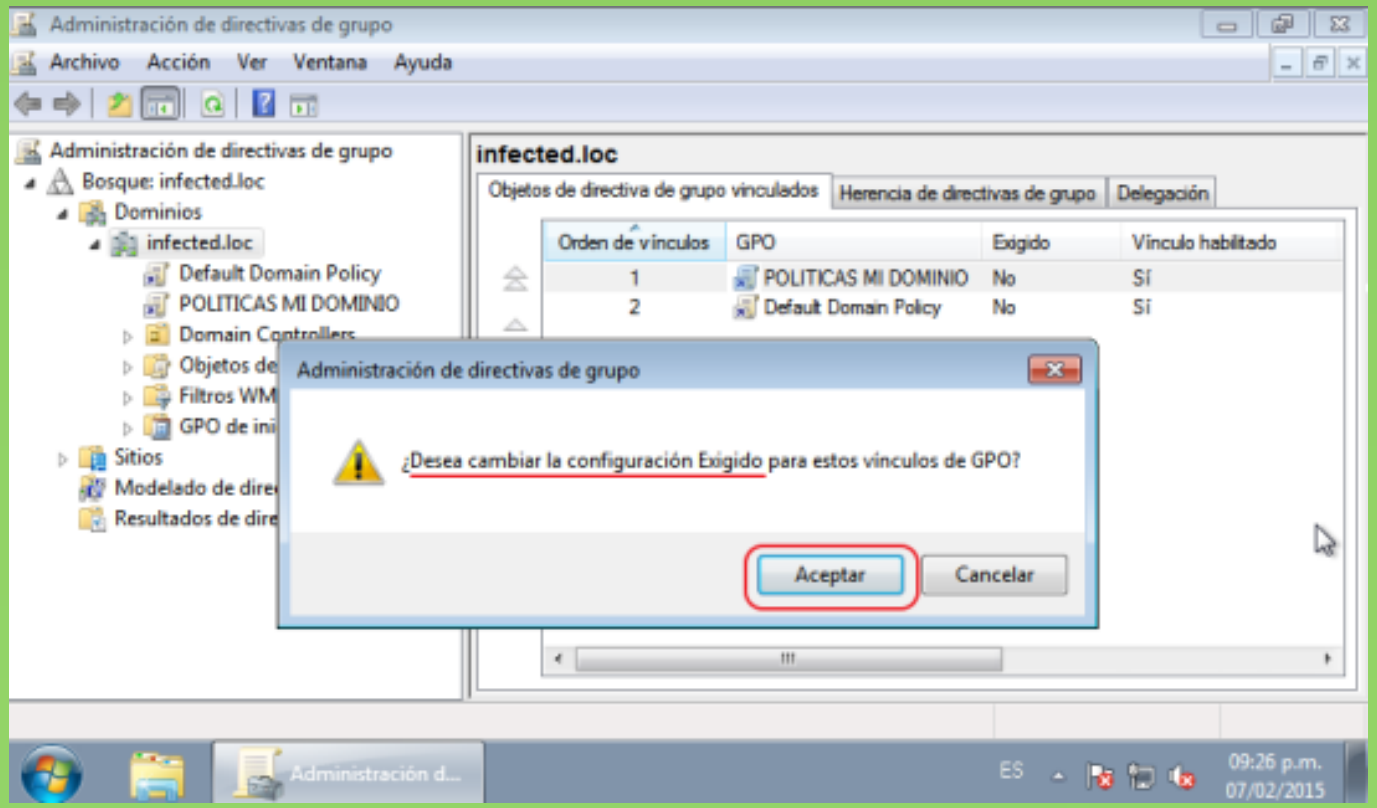
Creando una GPO



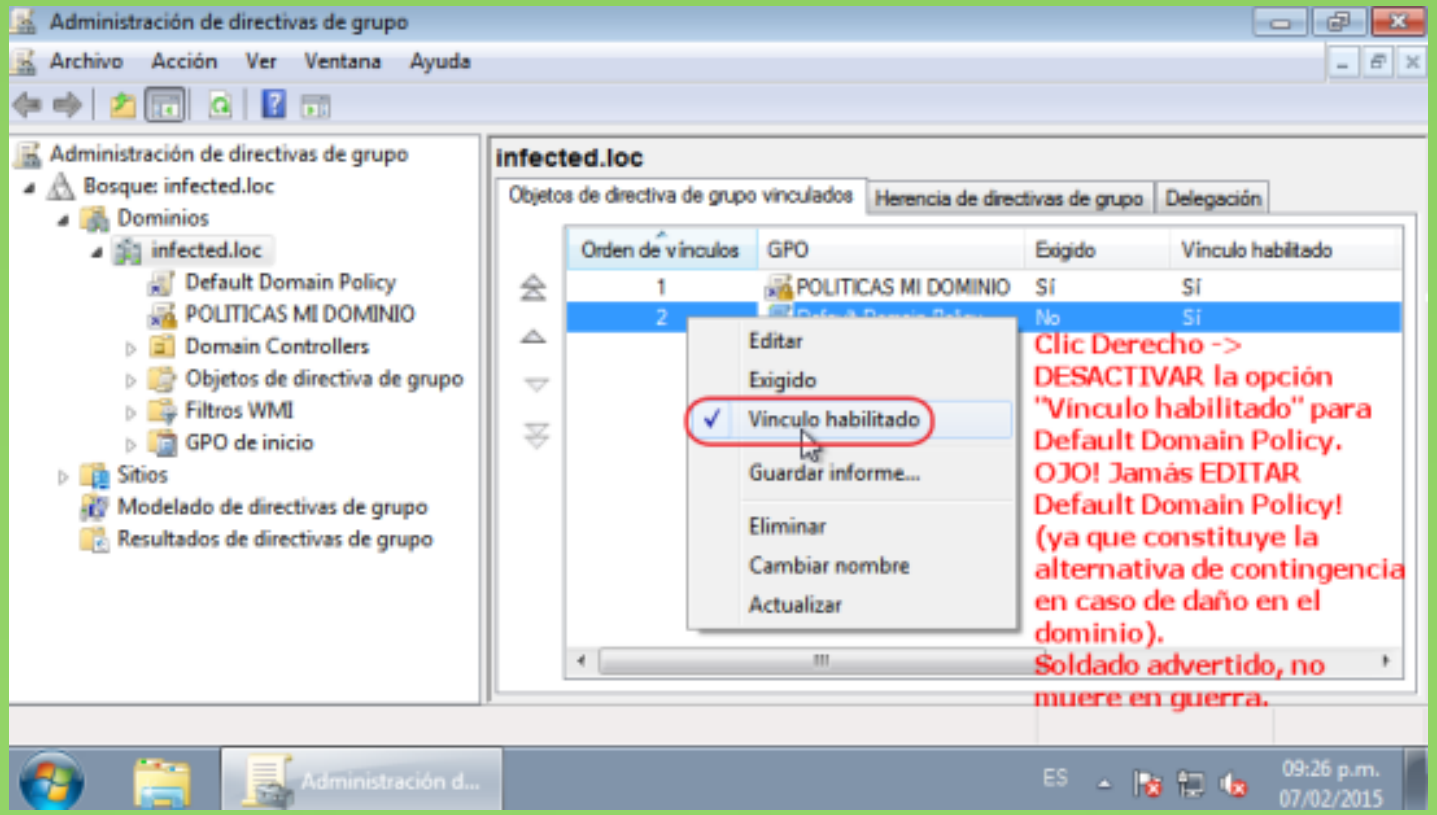
Creando una GPO



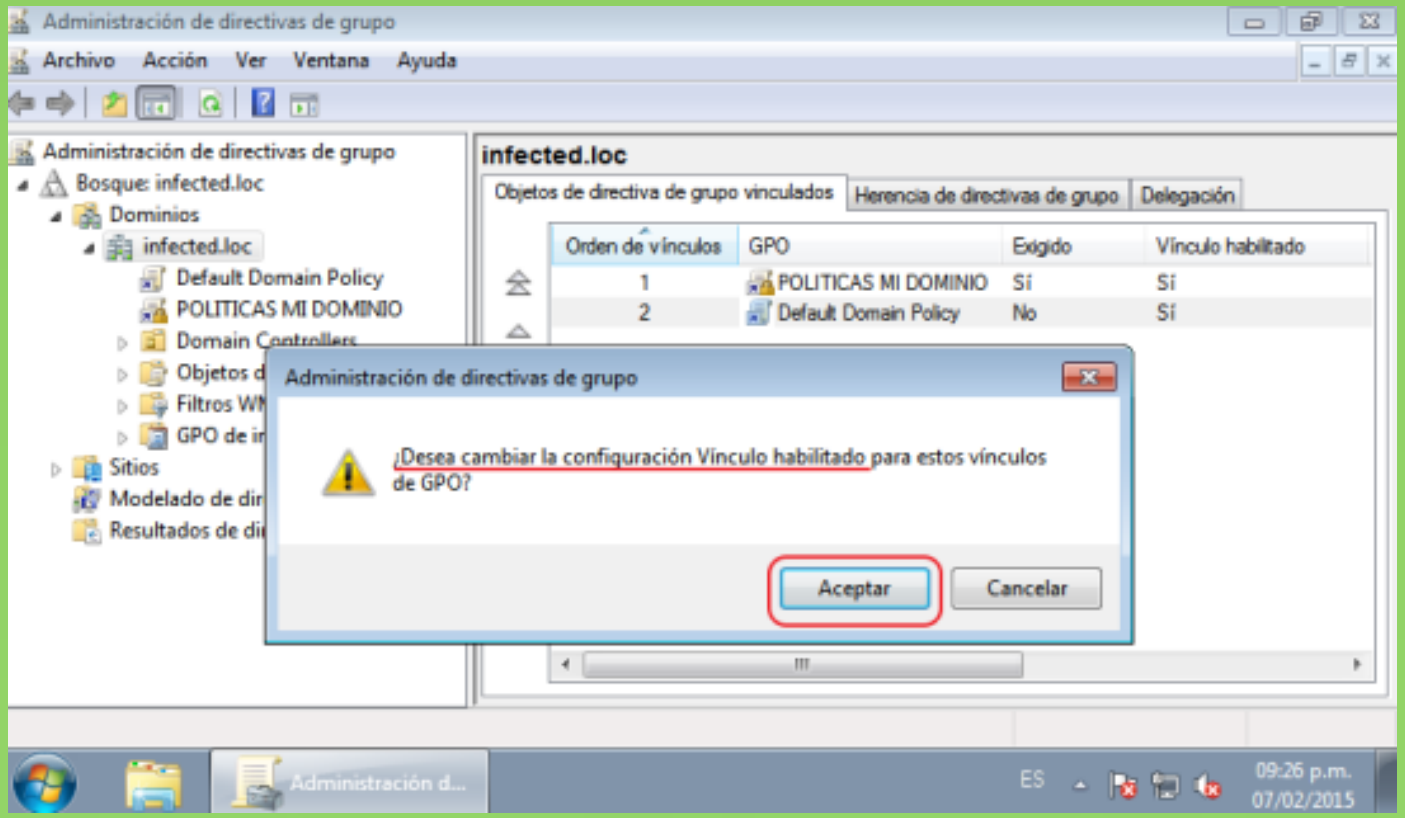
Creando una GPO



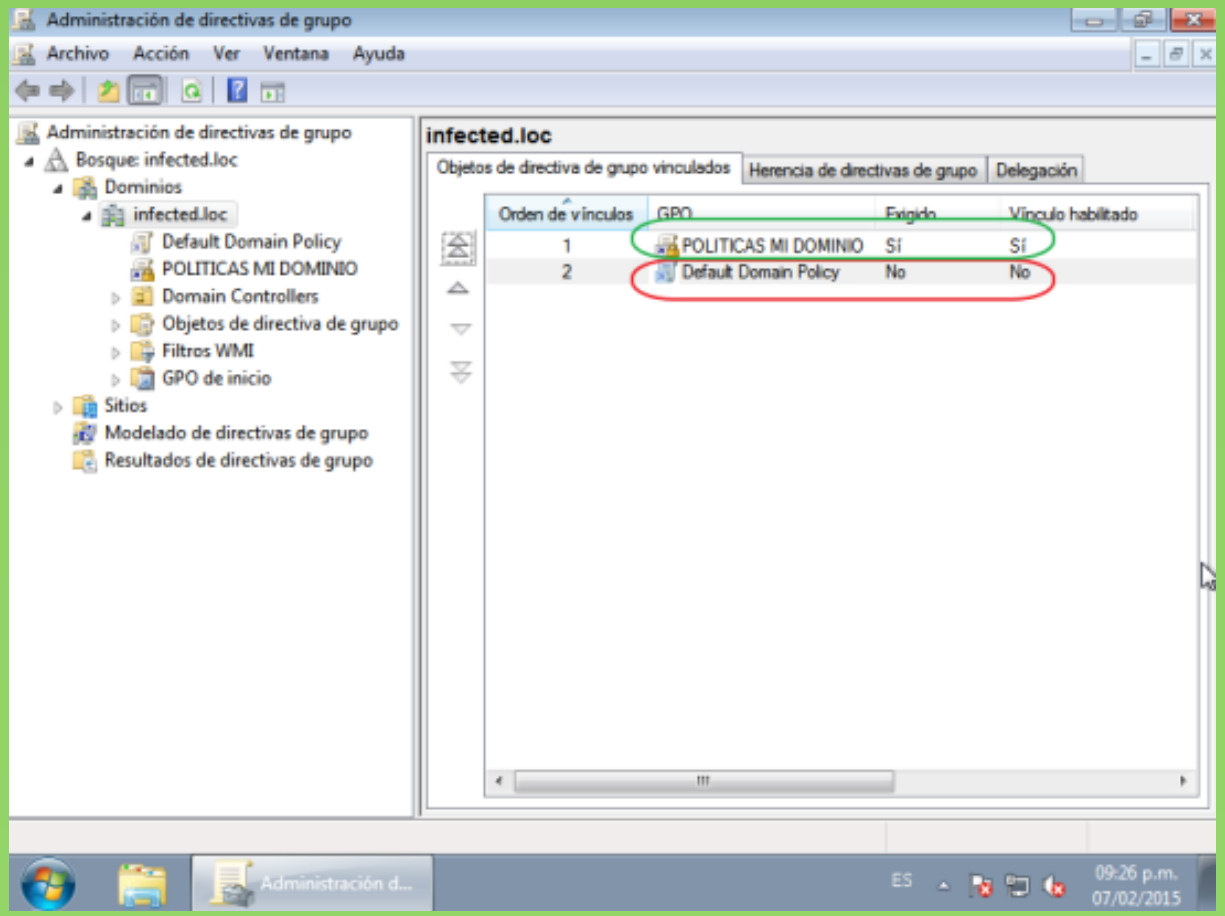
Creando una GPO



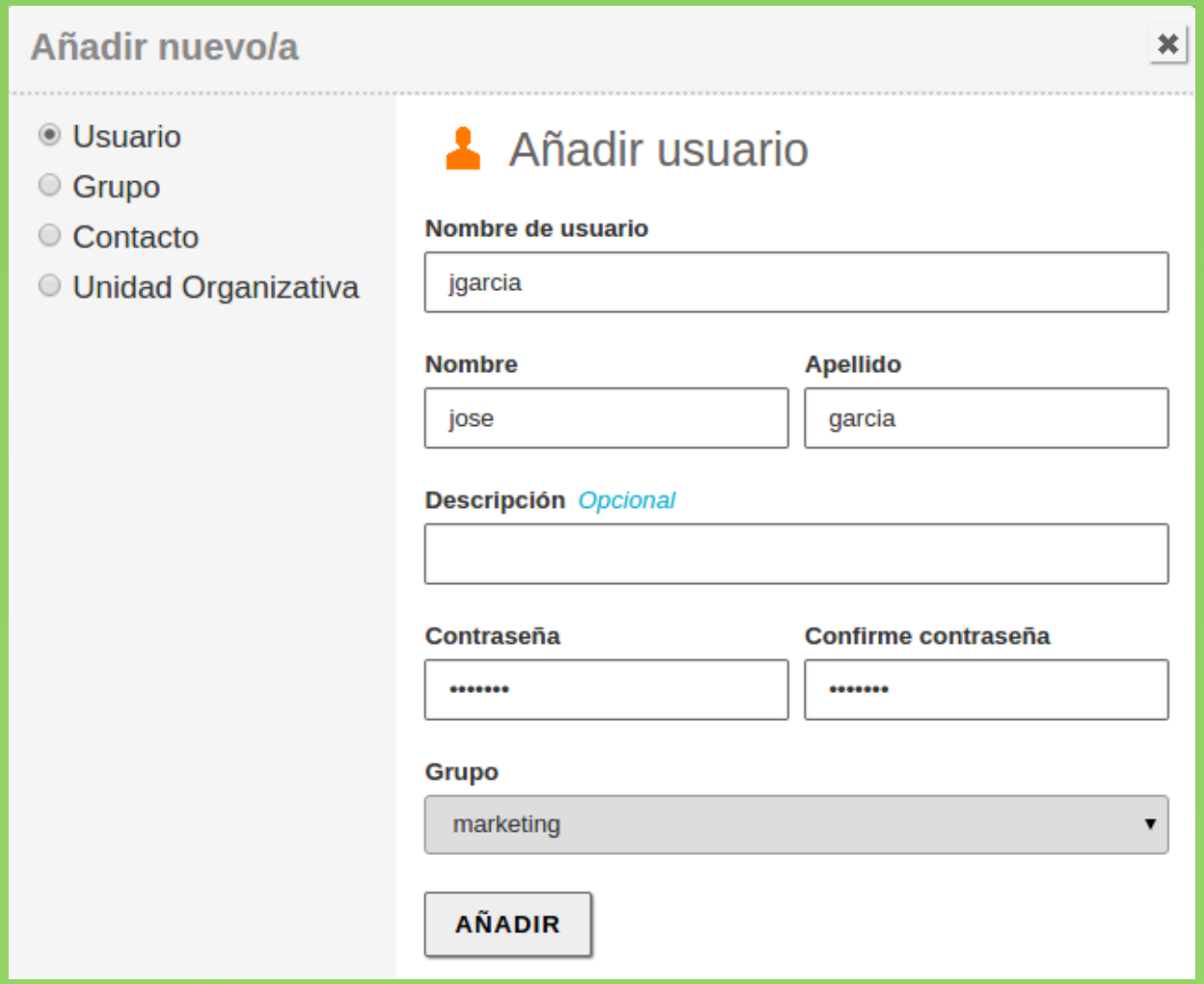
Creando una GPO



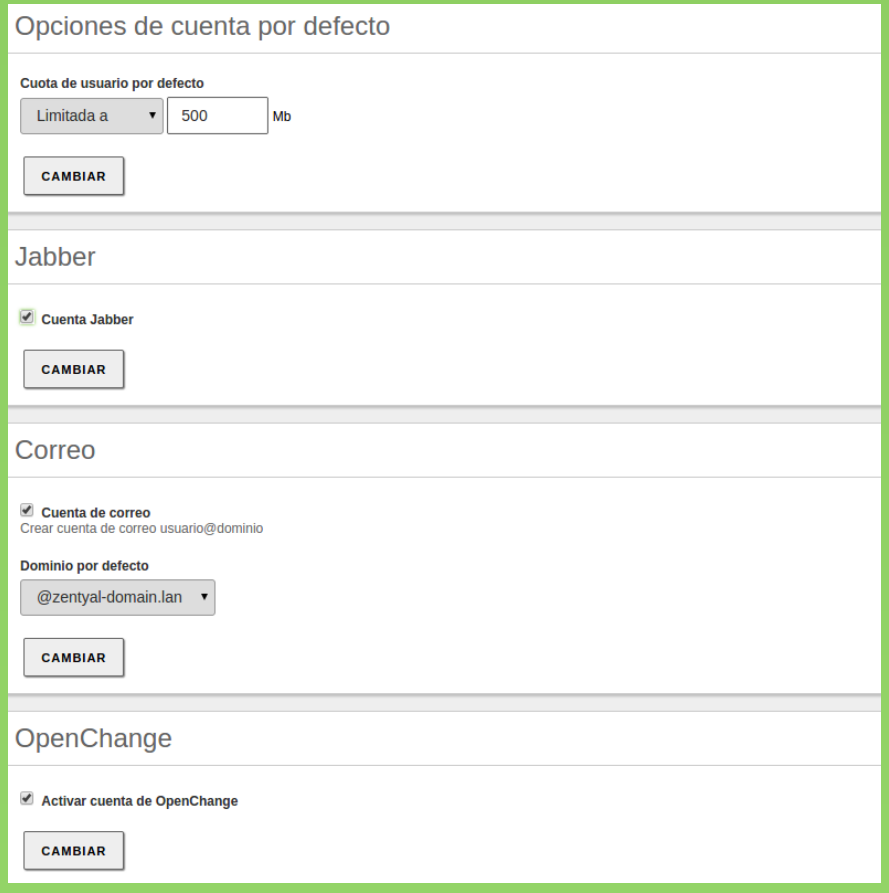
Creando una GPO



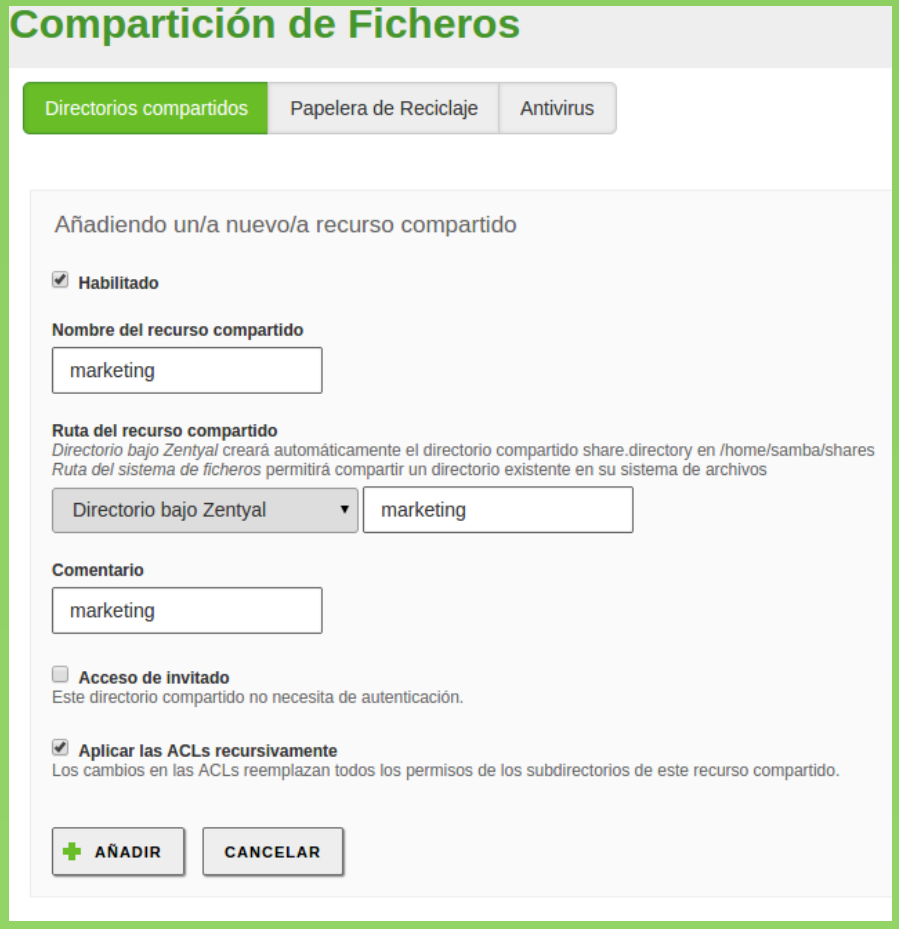
GESTIÓN DE USUARIOS/OU/GRUPOS

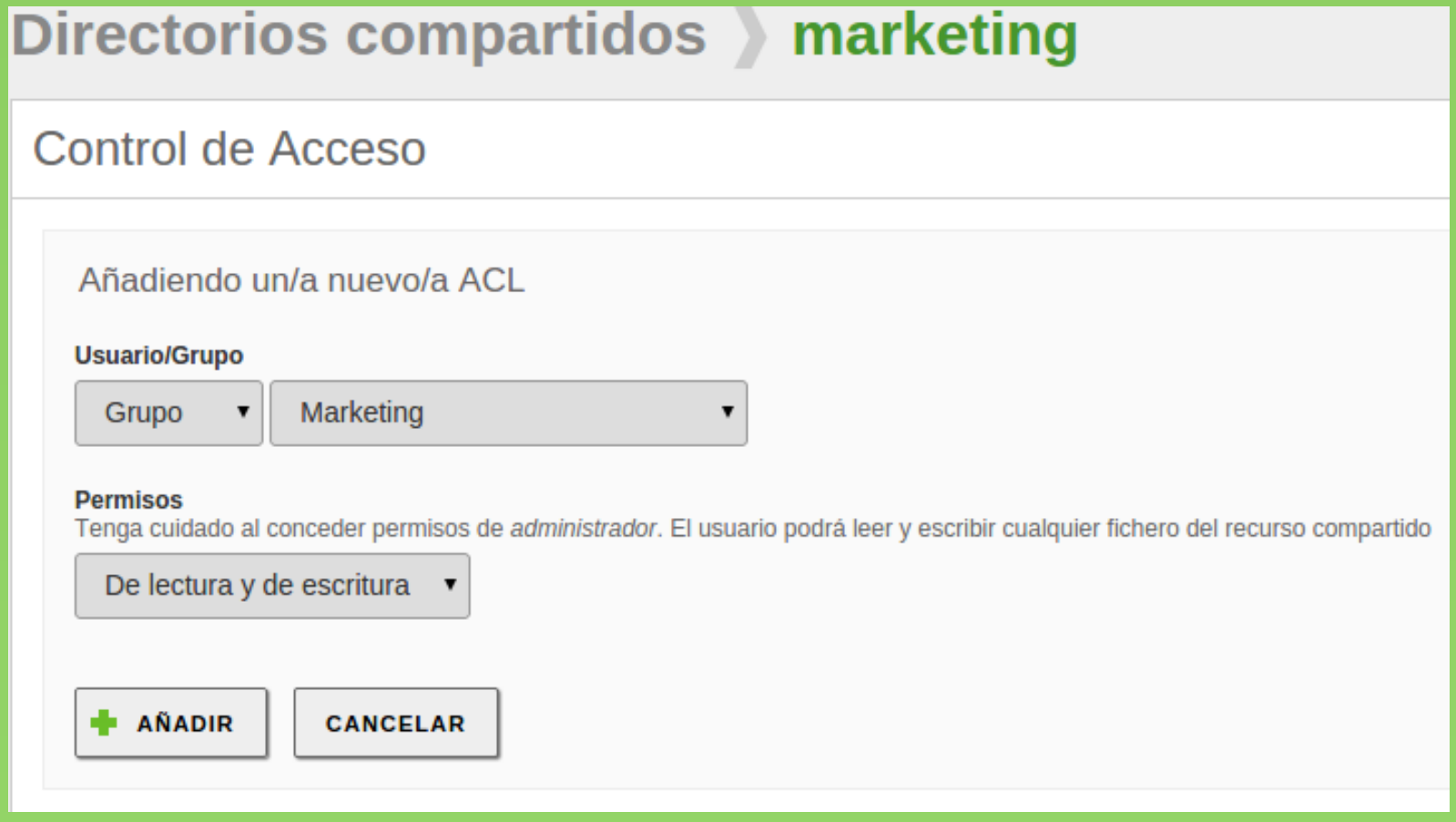

Añadir nuevo/a
Usuario
Grupo
Contacto
Unidad Organizativa
Añadir usuario
Nombre de usuario
jgarcia
Nombre
jose
Apellido
garcia
Descripción Opcional
Contraseña
Confirme contraseña
Grupo
marketing
AÑADIR


ntyal Community Edition 4.0
Search...
Dashboard
Module Status
System
Network
Logs
Software Management
Users and Computers
1
Manage
2
User Templ
Synchronization
LDAP Settings
Domain
File Sharing
DNS
Firewall
Created by Zentyal S.L.
Users and Computers
infected.loc
Computers
W7SP1
Groups
Users
3
Administrator
Domain Admins
Guest
Schema Admins
Domain Controllers
PDC
4
Add new
User
Group
Contact
Organizational Unit
Add User
User name
julio.restrepo
5
First name
Julio
6
Last name
Restrepo
7
Description Optional
Password
8
Retype password
9
Group
ADD
10


Opciones de cuenta por defecto
Cuota de usuario por defecto
Limitada a
500
Mb
CAMBIAR
Jabber
Cuenta Jabber
CAMBIAR
Correo
Cuenta de correo
Crear cuenta de correo usuario@dominio
Dominio por defecto
@zentyal-domain.lan
CAMBIAR
OpenChange
Activar cuenta de OpenChange
CAMBIAR

CARPETAS COMPARTIDAS


Compartición de Ficheros
Directorios compartidos
Papelera de Reciclaje
Antivirus
Añadiendo un/a nuevo/a recurso compartido
Habilitado
Nombre del recurso compartido
marketing
Ruta del recurso compartido
Directorio bajo Zentyal creará automáticamente el directorio compartido share.directory en /home/samba/shares
Ruta del sistema de ficheros permitirá compartir un directorio existente en su sistema de archivos
Directorio bajo Zentyal
marketing
Comentario
marketing
Acceso de invitado
Este directorio compartido no necesita de autenticación.
Aplicar las ACLs recursivamente
Los cambios en las ACLs reemplazan todos los permisos de los subdirectorios de este recurso compartido.
AÑADIR
CANCELAR


Directorios compartidos
marketing
Control de Acceso
Añadiendo un/a nuevo/a ACL
Usuario/Grupo
Grupo
Marketing
Permisos
Tenga cuidado al conceder permisos de administrador. El usuario podrá leer y escribir cualquier fichero del recurso compartido
De lectura y de escritura
AÑADIR
CANCELAR

MIGRACIÓN TOTAL

- Existen roles específicos que pertenecen al controlador master, llamados los roles FSMO o Operations Masters. Hay cinco roles FSMO:

  - Schema master: a cargo de la definición del árbol LDAP, envía actualizaciones de este formato
  - Domain naming master: Crear y borrar dominios en el bosque
  - Infrastructure master: Provee de identificadores GUID, SID y DN únicos en el dominio
  - Relative ID Master: ID relativas asignadas a los principales de seguridad
  - PDC Emulator: Compatibilidad con máquinas Windows 2000/2003® hosts, servidor de hora principal

- Usando el script de Migración Total, podemos transferir estos roles a un servidor Zentyal unido al dominio
- administrator@zentyal:/usr/share/zentyal-samba$ sudo ./ad-migrate


administrator@zentyal:/usr/share/zentyal-samba$ sudo ./ad-migrate
WARNING: This script will transfer all FSMO roles from the current owners to the local server.
After all roles has been successfully transferred, you can shutdown the other domain controllers.
Do you want to continue [Y/n]? Y
Checking server mode...
Checking if server is provisioned...
Synchronizing sysvol share... syncing [SYSVOL] files and directories including ACLs, without DOS Attributes
Transferring FSMO roles... Transferring Schema Master role from owner: CN=NTDS Settings,CN=WINDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=zentyal-domain,DC=lan Transferring Domain Naming Master role from owner: CN=NTDS Settings,CN=WINDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=zentyal-domain,DC=lan Transferring PDC Emulation Master role from owner: CN=NTDS Settings,CN=WINDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=zentyal-domain,DC=lan Transferring RID Allocation Master role from owner: CN=NTDS Settings,CN=WINDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=zentyal-domain,DC=lan Transferring Infrastructure Master role from owner: CN=NTDS Settings,CN=WINDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=zentyal-domain,DC=lan
Migrated successfully!

Referencias

- https://wiki.zentyal.org/wiki/Es/4.1/Zentyal_4.1_Documentacion_Oficial