

Migrando active-directory a sw libre

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



OBJETIVOS

- Alternativas 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 sí '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 antisпам

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:



Seleccionar



Instalar



Configurar



Guardar


Continuar


Seleccionamos el tipo de servidor Zentyal


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


Seleccione los paquetes de Zentyal a instalar


Roles del servidor

 **Domain Controller and File Sharing** ✓


 **Mail and Groupware** ✓


 **DNS Server** ✓


 **DHCP Server** ✓


 **Firewall** ✓


Servicios adicionales

 **Antivirus** ✓

 **Certification Authority** ✓

 **Mail Filter** ✓

 **Printers** ✓

 **VPN** ✓

[Saltar instalación](#) **INSTALAR**

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



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)
- Adicional domain controller (para añadir a un dominio ya existente como secundario)

Zentyal - Asistente de configuración inicial - Mozilla Firefox

Zentyal - Asistente d... x

https://localhost:8443/Wizard

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.

SALTAR **FINALIZAR**


Zentyal - Asistente de C... 21:12

Zentyal - Asistente de configuración inicial - Mozilla Firefox

Zentyal - Asistente d... x

https://localhost:8443/Wizard

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.

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!

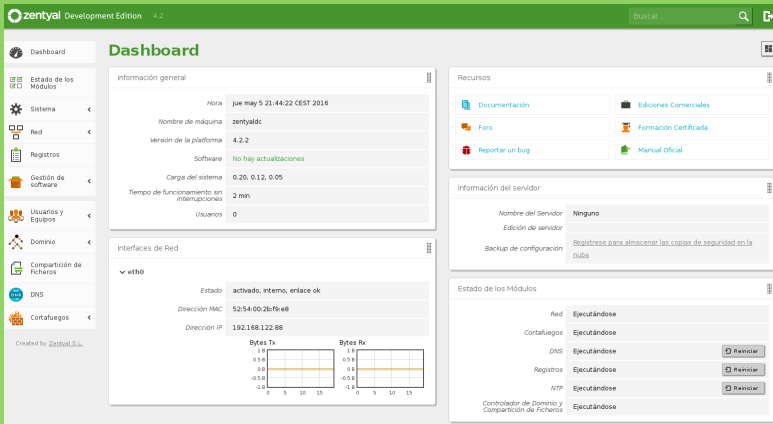
Puedes ir al Dashboard y comenzar a usar tu servidor Zentyal recién instalado.



[IR AL DASHBOARD](#)

EXPLOTACIÓN

Dashboard



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 mantener integridad de paquetes

Backup del sistema

The screenshot displays the Zentyal web interface for system backup configuration. The top navigation bar includes the Zentyal logo, 'Development Edition 4.2', and a search field. The left sidebar contains a menu with categories like 'Dashboard', 'Estado de los Módulos', 'Sistema', 'General', 'Fecha/Hora', 'Backup de la configuración', 'Apagar o reiniciar', 'Red', 'Registros', 'Gestión de software', 'Usuarios y Equipos', 'Dominio', 'Compartición de ficheros', and 'DNS'. The main content area is titled 'Backup de la configuración' and features a 'Local' tab selected over 'Cloud'. It contains three sections: 'Backup del estado actual' with a 'COPIA DE SEGURIDAD' button; 'Restaurar backup desde un archivo' with a 'Browse...' button and a 'RESTAURAR' button; and 'Informe de configuración' with a 'GENERAR Y DESCARGAR FICHERO DE INFORME' button. A footer note states 'Created by Zentyal S.L.'.

zentyal Development Edition 4.2 Buscar

Backup de la configuración

Cloud Local

Backup del estado actual

Descripción

Restaurar backup desde un archivo

No file selected.

Informe de configuración

Puede generar un fichero con información sobre el estado de su sistema. Este fichero puede ser de utilidad si desea enviar un informe de error o recibir soporte.

Created by [Zentyal S.L.](#)

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

ANTES (before)

Detalles de la conexión de red

Detalles de la conexión de red:

Propiedad	Valor
Sufijo DNS específico p...	
Descripción	NIC de Fast Ethernet Realtek RTL8139C
Dirección física	76-23-64-B2-9A-B0
Habilitado para DHCP	Si
Dirección IPv4	172.16.0.124
Máscara de subred IPv4	255.255.255.0
Concesión obtenida	sábado, 07 de febrero de 2015 09:16:39
La concesión expira	sábado, 07 de febrero de 2015 09:46:41
Puerta de enlace predet...	172.16.0.1
Servidor DHCP IPv4	172.16.0.1
Servidor DNS IPv4	172.16.0.1
Servidor WINS IPv4	
Habilitado para NetBios ...	Si

Cerrar

DESPUES (after)

Detalles de la conexión de red

Detalles de la conexión de red:

Propiedad	Valor
Sufijo DNS específico p...	infected.loc
Descripción	NIC de Fast Ethernet Realtek RTL8139C
Dirección física	76-23-64-B2-9A-B0
Habilitado para DHCP	Si
Dirección IPv4	172.16.0.124
Máscara de subred IPv4	255.255.255.0
Concesión obtenida	sábado, 07 de febrero de 2015 09:26:17
La concesión expira	sábado, 07 de febrero de 2015 09:56:17
Puerta de enlace predet...	172.16.0.1
Servidor DHCP IPv4	172.16.0.1
Servidores DNS IPv4	172.16.0.7 200.13.249.101 8.8.8.8
Servidor WINS IPv4	172.16.0.7
Habilitado para NetBios ...	Si

Cerrar

Metemos equipo en dominio

Cambiamos clave administrador del DC

zentyal Community Edition 4.0

Users and Computers

1 Users and Computers

2 Manage

3 Administrator

4 First name
Administrator

5 Last name
Administrator

Display name *Optional*

Description *Optional*
Built-in account for admins

E-Mail *Optional*

User quota (MB)
Disabled

6 Password
●●●

7 Retype password
●●●

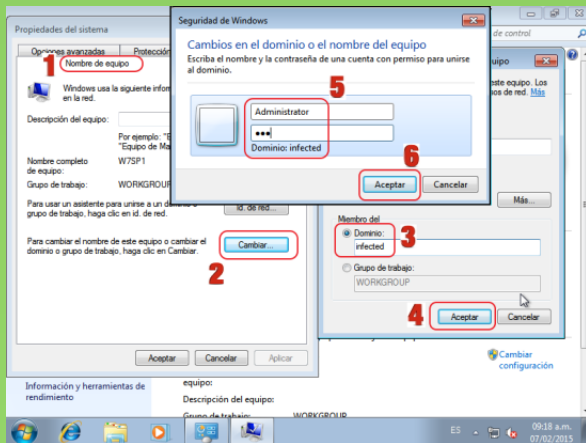
Disabled account

8 CHANGE

9 User Administrator

User updated

Metemos equipo en dominio



Metemos equipo en dominio

Verificamos en Zentyal

The image displays two overlapping windows. On the left is the Windows 'Propiedades del sistema' (System Properties) dialog box, specifically the 'Opciones avanzadas' (Advanced) tab. The 'Nombre de equipo' (Computer name) field is set to 'W7SP1.infected.loc', which is circled in red. A red arrow points from this field to the 'Users and Computers' interface on the right. The Zentyal interface shows a tree view of the domain 'infected.loc', with 'Computers' and 'W7SP1' highlighted in red boxes. The 'Users' folder is also highlighted in blue. The Zentyal interface includes a sidebar with navigation options like 'Dashboard', 'Module Status', 'System', 'Network', 'Logs', 'Software Management', 'Users and Computers', and 'Manage'. The 'Users and Computers' section is currently selected, showing a list of users and groups.

Propiedades del sistema

Opciones avanzadas

Nombre de equipo

Windows usa la siguiente información para identificar en la red.

Descripción del equipo:

Por ejemplo: "Equipo de la sala de es
"Equipo de María"

Nombre completo de equipo: **W7SP1.infected.loc**

Dominio: infected.loc

Para usar un asistente para unirse a un dominio o grupo de trabajo, haga clic en id. de red.

Para cambiar el nombre de este equipo o cambiar el dominio o grupo de trabajo, haga clic en Cambiar.

Aceptar Cancelar

zentyal Community Edition 4.0

Dashboard

Module Status

System

Network

Logs

Software Management

Users and Computers

Manage

User Template

Synchronization

LDAP Settings

Domain

File Sharing

DNS

Firewall

Users and Computers

infected.loc

Computers

W7SP1

Groups

Users

Administrator

Domain Admins

Guest

Schema Admins

Domain Controllers

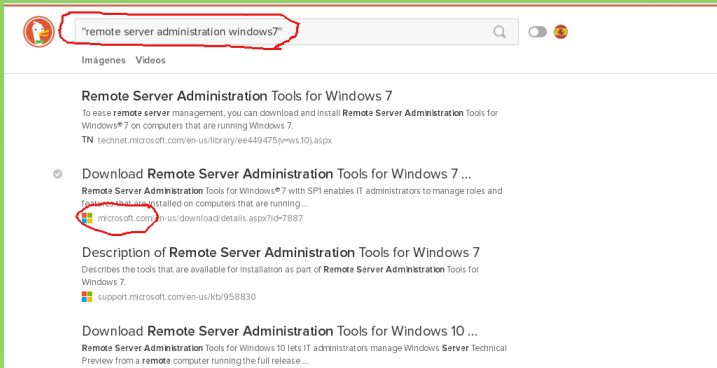
PDC

Created by Zentyal S.L.

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"

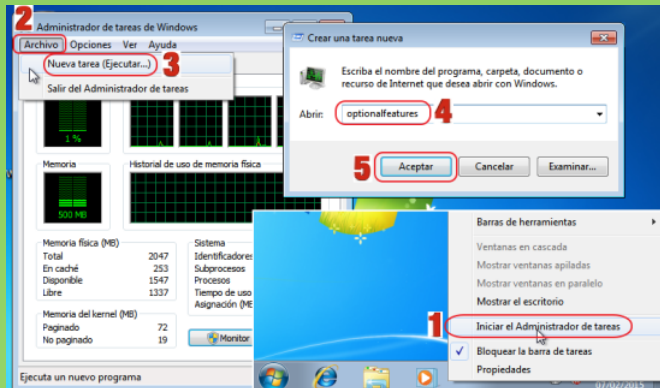
Descargamos "remote server administration windows7"



The screenshot shows a search engine interface with a search bar containing the text "remote server administration windows7". Below the search bar, there are tabs for "Imágenes" and "Videos". The search results are as follows:

- Remote Server Administration Tools for Windows 7**
To ease **remote server** management, you can download and install **Remote Server Administration Tools** for Windows® 7 on computers that are running Windows 7.
TN [technet.microsoft.com/en-us/library/ee449475\(y=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee449475(y=ws.10).aspx)
- Download **Remote Server Administration Tools** for Windows 7 ...
Remote Server Administration Tools for Windows® 7 with SP1 enables IT administrators to manage roles and features that are installed on computers that are running ...
microsoft.com/en-us/download/details.aspx?id=7887
- Description of **Remote Server Administration Tools** for Windows 7
Describes the tools that are available for installation as part of **Remote Server Administration Tools** for Windows 7.
support.microsoft.com/en-us/kb/958830
- Download **Remote Server Administration Tools** for Windows 10 ...
Remote Server Administration Tools for Windows 10 lets IT administrators manage Windows Server Technical Preview from a **remote** computer running the full release ...

Instalamos



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 **1**
- Herramientas de administración remota del servidor **2**
 - Administrador del servidor
 - Herramientas de administración de características **3**
 - Administrador de almacenamiento para herramientas de SAN
 - Herramientas de administración de directivas de grupo
 - Herramientas de administración de dispositivos de almacenamiento
 - Herramientas de administración de dispositivos de almacenamiento de red
 - Herramientas de administración de dispositivos de almacenamiento de red de alta velocidad
 - Herramientas de administración de dispositivos de almacenamiento de red de alta velocidad de almacenamiento de datos
 - Visor de control de dispositivos de almacenamiento de red
 - Herramientas de administración de funciones **4**
 - Herramientas de AD DS y AD LDS
 - Herramientas de AD DS **5**
 - Centro de administración de Active Directory **6**
 - 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
 - Módulo de Active Directory para Windows PowerShell
 - Herramientas de Hyper-V

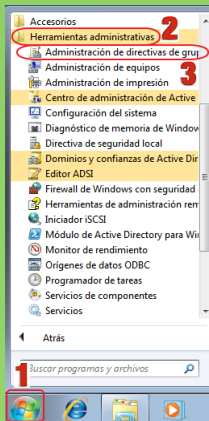
Microsoft Windows

Espere mientras Windows realiza cambios en las características. Esto puede tardar varios minutos. **8**

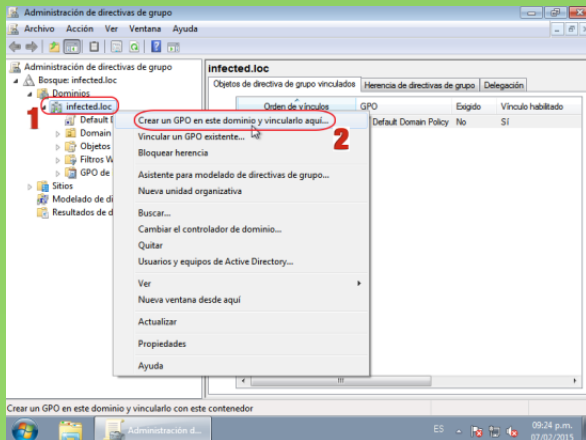
7

ES 09:10 p.m. 07/02/2015

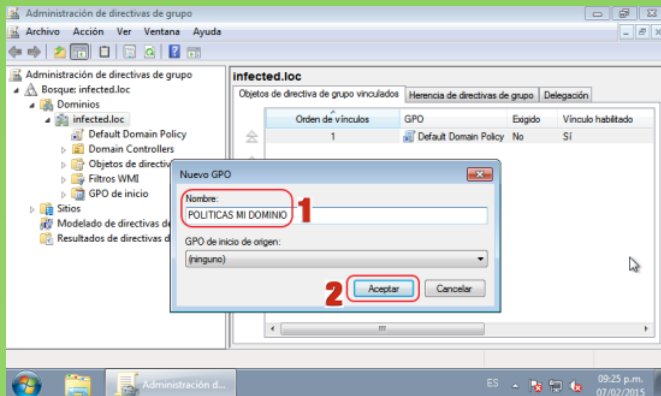
Y verificamos



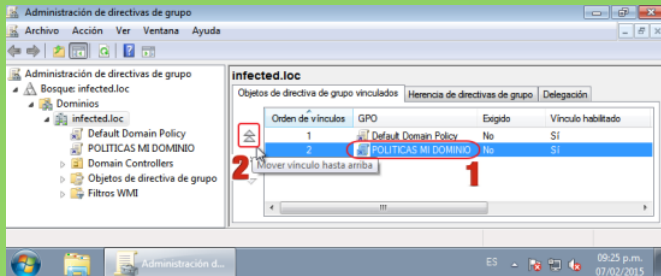
Creando una GPO



Creando una GPO



Creando una GPO



Creando una GPO

Administración de directivas de grupo

Archivo Acción Ver Ventanas Ayuda

Administración de directivas de grupo

Bosque: infected.loc

- infected.loc
 - Default Domain Policy
 - POLITICAS MI DOMINIO
 - Domain Controllers
 - Objetos de directiva de grupo
 - Filtros WMI
 - GPO de inicio
- Sitios
- Modelado de directivas de grupo
- Resultados de directivas de grupo

infected.loc

Objetos de directiva de grupo vinculados

Orden de vínculos	GPO	Exigido	Vínculo habilitado
1	POLITICAS MI DOMINIO	No	Sí
2	Policy	No	Sí

Exigido Clic Derecho -> Activar la Opción EXIGIDO

Vínculo habilitado

Guardar informe...

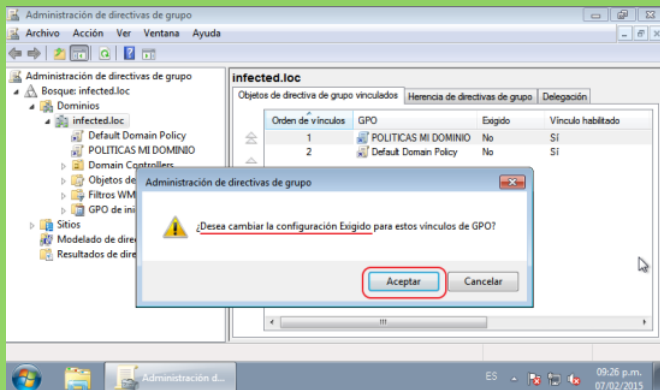
Eliminar

Cambiar nombre

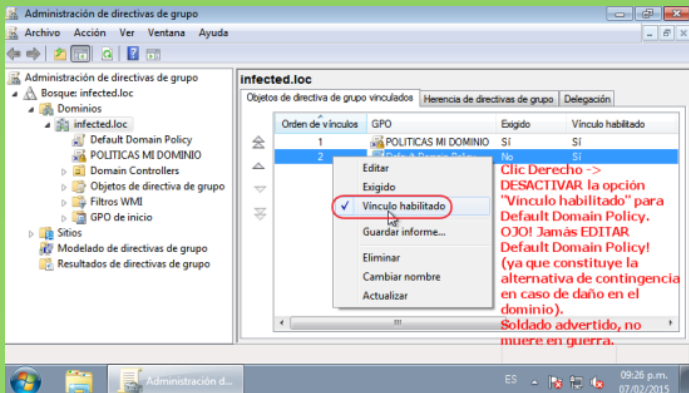
Actualizar

ES 09:26 p.m. 07/02/2015

Creando una GPO



Creando una GPO



Administración de directivas de grupo

Archivo Acción Ver Ventanas Ayuda

Administración de directivas de grupo

- Bosque: infected.loc
 - Dominios
 - infected.loc
 - Default Domain Policy
 - POLITICAS MI DOMINIO
 - Domain Controllers
 - Objetos de directiva de grupo
 - Filtros WMI
 - GPO de inicio
 - Sitios
 - Modelado de directivas de grupo
 - Resultados de directivas de grupo

infected.loc

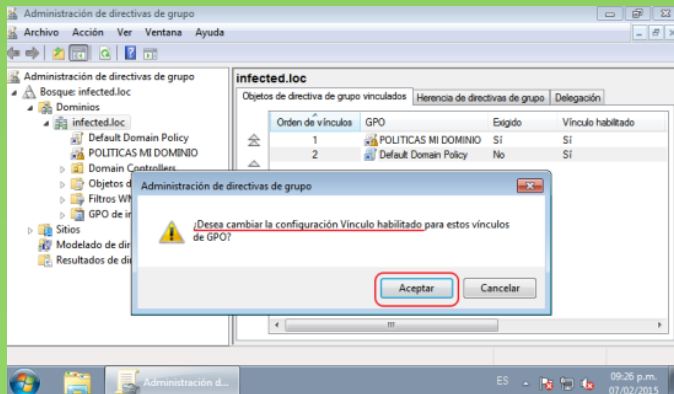
Objetos de directiva de grupo vinculados Herencia de directivas de grupo Delegación

Orden de vínculos	GPO	Exigido	Vinculo habilitado
1	POLITICAS MI DOMINIO	Sí	Sí
2	...	No	Sí

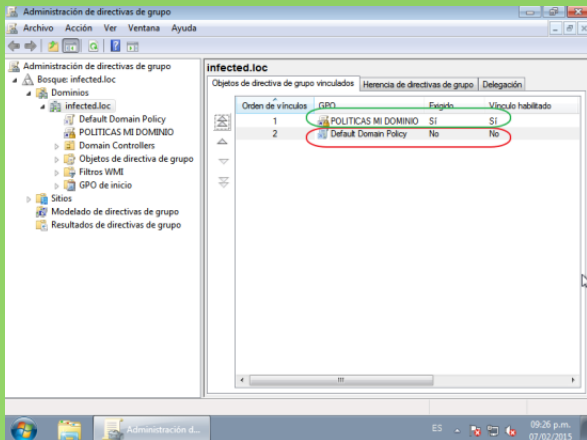
Clic Derecho ->
DESACTIVAR la opción "Vinculo habilitado" para Default Domain Policy.
OJO! Jamás EDITAR Default Domain Policy!
(ya que constituye la alternativa de contingencia en caso de daño en el dominio).
Soldado advertido, no muere en guerra.

ES 09:26 p.m. 07/02/2015

Creando una GPO



Creando una GPO



GESTIÓN DE USUARIOS/OU/GRUPOS

Añadir nuevo/a



- Usuario
- Grupo
- Contacto
- Unidad Organizativa



Añadir usuario

Nombre de usuario

Nombre

Apellido

Descripción *Opcional*

Contraseña

Confirme contraseña

Grupo

AÑADIR

Centrality Community Edition 4.0

Search...

Users and Computers

infected loc

- Computers
 - W7SP1
- Groups
 - Users** **3**
 - Administrator
 - Domain Admins
 - Guest
 - Schema Admins
- Domain Controllers
 - PDC

1 Users and Computers

2 Manage

4

Add new

User

Group

Contact

Organizational Unit

5 User name: julio.restrepo

6 First name: Julio **7** Last name: Restrepo

Description *Optional*

8 Password: ●●● **9** Retype password: ●●●

Group

10 ADD

Created by Centrality S.L.

Opciones de cuenta por defecto

Cuota de usuario por defecto

Limitada a 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/Espanol/4.1/Zentyal_4.1_Documentacion_Oficial