1 Directivas de Grupo en Windows 2008

As Directivas de Grupo son obxectos de *Active Directory* que permiten unha configuración completa e centralizada dos equipos e dos contornos de usuario.

1.1 Sumario

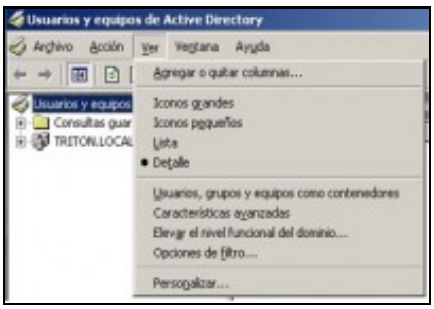
1.2 Introdución

Coas Directivas de Grupo podemos configurar: A seguridade, a instalación de programas, as secuencias de comandos, as plantillas administrativas, o servizo de instalación remota, o explorador de internet, a redirección de carpetas, etc.

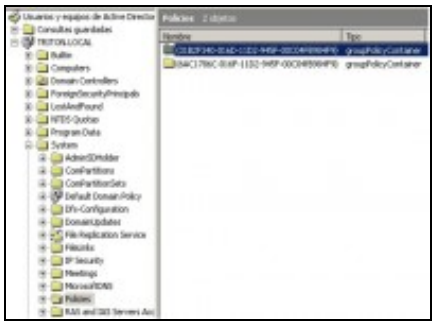
Hai que ter en conta que as Directivas de Grupo só se poden aplicar aos sistemas operativos Windows 2000 e posteriores (XP, Server 2003, Windows 7, Server 2008,?).

O obxecto Directiva de Grupo contén dous compoñentes: *Group Policy Container* (GPC) e *Group Policy Template* (GPT).

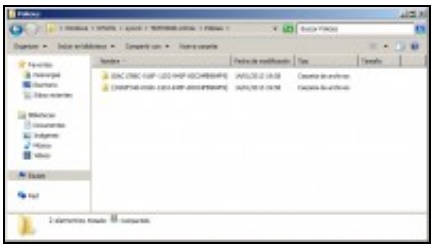
- ***Group Policy Container* (GPC):** Está referenciado na base de *Active Directory*, na carpeta *Policies*.



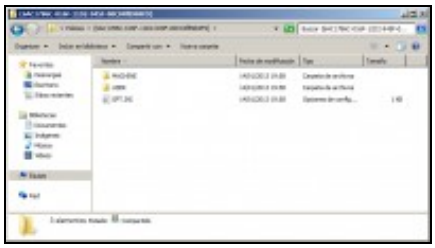
Mostrar as "Características avanzadas".


En *System-Policies* vemos as **GUID** (*Global Unique IDentifier*) das dúas directivas creadas por defecto no Dominio

- ***Group Policy Template* (GPT):** O GPT cós parámetros de directiva almacénanse na carpeta *Sysvol*.



Contido de C:\Windows\SYSVOL\sysvol\TRITON00.LOCAL\Policies.



Contido dunha das dúas GPTs creadas ao promocionar o equipo a Servidor de Dominio.

A existencia destes dous compoñentes pode ter repercusións na administración de AD, pois a súa replicación é disxunta:

- O GPC replícase durante a replicación de AD.
- O GPT replícase mediante o servicio de replicación de arquivos (*File Replication Service* ? FRS).

Aplicación das Directivas de Grupo:

As Directivas de Grupo defínense para as contas de equipo e de usuario, e só para elas. Non se aplican aos obxectos de grupo.

◊ *Directivas de Grupo de Equipo.* Aplícanse ao arrancar a máquina e se refrescan a intervalos de 5 minutos para os Controladores de Dominio e 90 minutos para os equipos.

◊ *Directivas de Grupo de Usuarios.* Aplícanse ao iniciar sesión e se refrescan cada 90 minutos.

Así e todo, estes valores pódense configurar e se queremos que se fagan efectivas nun momento dado podemos executar o comando gpupdate.

Herdanza das directivas:

As Directivas de Grupo poden estar definidas en distintos niveis da árbore de AD: sitio, dominio e OU. Ademais os equipos membros poden ter unha directiva local.

A Prioridade na aplicación das directivas de grupo é: Directiva local ? Sitio ? Dominio ? Unidade Organizativa Principal ? Unidade Organizativa Secundaria.

Este orden significa que a GPO local procésase en primeiro lugar e que as GPOs vinculadas á unidade organizativa da que é membro directo o equipo ou o usuario procésanse en último lugar, có que se sobrescribe a configuración das GPOs anteriores en caso de conflicto. (Se non hai conflicto, simplemente se agregan a configuración anterior e a posterior).

Como sempre, esta herdanza pode ser modificada?

1.3 A Consola de Administración de Directivas de Grupo (GPMC)

A Consola de Administración de Directivas de Grupo (GPMC) é un complemento de scripts de Microsoft Management Console (MMC), que proporciona unha única ferramenta administrativa para administrar as directivas de grupo en toda a organización. Así, a GPMC é a ferramenta estándar para administrar as directivas de grupo.

1.4 Directivas de Grupo Interesantes

1.4.1 Mis Documentos

Ollo!!! Esta directiva non funciona nos usuarios que xa teñan gardado arquivos na súa carpeta personal.

Configuración del Usuario - Directivas - Configuración de Windows - Redirección de carpetas - Documentos - Configuración: Avanzada (especificar ubicaciones para diversos grupos de usuarios):

- Grupo: TRITON00\G-Triton
- Ubicación de la carpeta de destino: Redirigir el directorio particular del usuario

  - Ruta: %HOMESHARE%%HOMEPATH%

En *Opciones* recordar habilitar: "Aplicar también directiva de redirección a los sistemas operativos Windows 2000?"

1.4.2 No Acceder a C desde Mi PC

1.4.2.1 Windows 2008

Configuración del Usuario - Directivas - Plantillas administrativas - Componentes de Windows - Explorador de Windows:

- Directiva: Impedir acceso a las unidades desde Mi PC
- Configuración: Habilitado
- Elegir una de las siguientes combinaciones: Restringir sólo la unidad C

1.4.2.2 Windows 2012

Configuración del Usuario - Directivas - Plantillas administrativas - Componentes de Windows - Explorador de archivos:

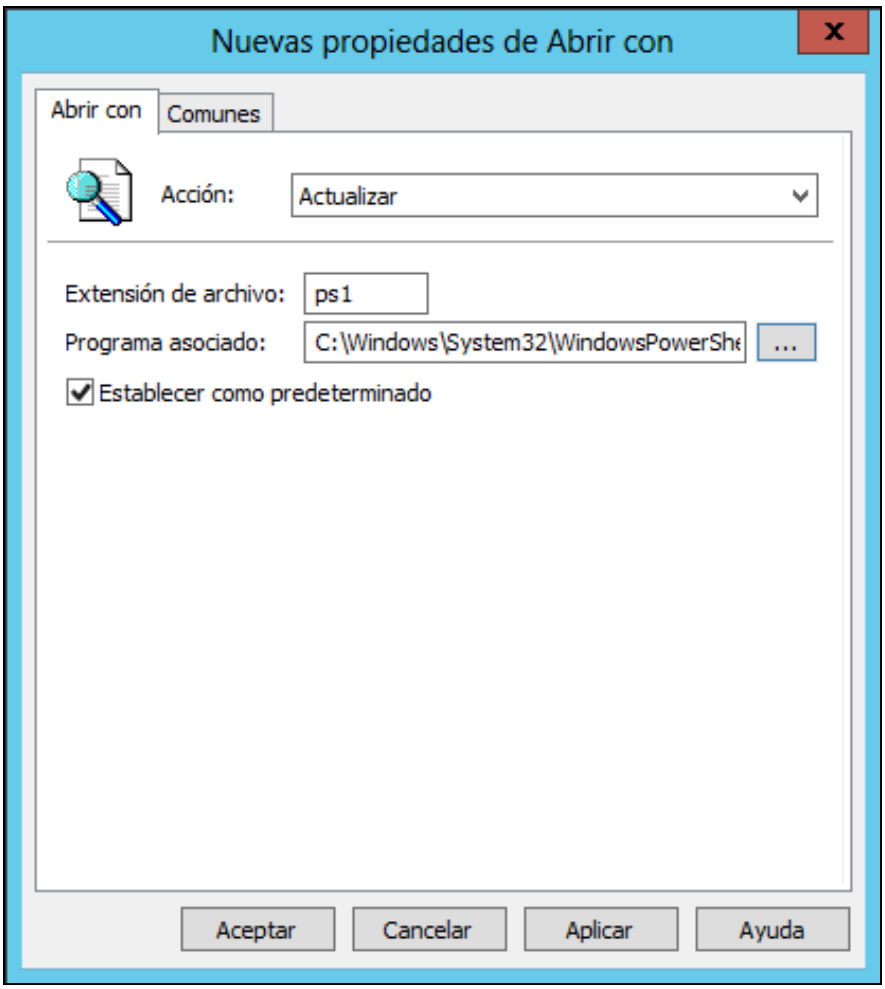
- Directiva: Ocultar estas unidades específicas en Mi PC
- Configuració: Habilitada
- Elegir una de las siguientes combinaciones: Restringir sólo la unidad C

1.4.3 Abrir archivos .ps1 con PowerShell

Configuración del Usuario - Preferencias - Configuración del Panel de control - Opciones de carpeta - Abrir con:

- Extensión de archivo: ps1
- Programa asociado: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Group Policy to change open with file associations.



1.4.4 Agregar el grupo Administradores a las carpetas de Perfiles móviles

Configuración del equipo - Directivas - Plantillas administrativas - Sistema/Perfiles de usuario:

- Directiva: Agregar el grupo de seguridad de administradores a los perfiles de usuarios móviles.
- Configuración: Habilitado.

Group Policy Settings for Roaming User Profiles.

NOTA: Para que a configuración da directiva surta efecto, ten que configurarse no equipo cliente e non no servidor.

- Para eliminar un perfil móbil completamente hai que ir a "todos" os ordenadores onde o usuario iniciou sesión e borrar a clave do rexistro: HKEY-LOCAL...\SOFTWARE\MICROSOFT\WINDOWSNT\CURRENTVERSION\PROFILELIST\...

1.4.5 Agregar Grupo Global del Dominio a Grupo Administradores equipo local

Enlace.

GPO de Equipos en la OU de los Clientes donde queremos instalar el software

1.4.6 Contraseña de Longitud 0

Configuración del equipo - Directivas - Configuración de Windows - Configuración de seguridad - Directivas de cuenta/Directivas de contraseñas:

- Directiva: Las contraseñas deben cumplir los requisitos de complejidad - Deshabilitado.
- Directiva: Longitud mínima de la contraseña - 0 Caracteres

1.4.7 Páxina de inicio do navegador

Neste enlace está ben explicado.

1.4.8 Configurar que usuarios poden iniciar sesión nun equipo

Cando existe unha unidade organizativa que contén os equipos aos que se quere **permitir** o inicio de sesión, crearase unha directiva de grupo para esa unidade organizativa:

Configuración de equipo - Directivas - Configuración de Windows - Configuración de seguridade - Directivas locais - Asignación de dereitos de usuarios - Permitir o inicio de sesión local

Defínese a directiva engadindo o grupo de usuarios que teñen permitido o inicio de sesión. Tamén se deben engadir o grupo administradores e o grupo dos administradores do dominio.

1.4.9 Configurar que usuarios NON poden iniciar sesión nun equipo

Cando existe unha unidade organizativa que contén os equipos aos que se quere **restrinxir** o inicio de sesión, crearase unha directiva de grupo para esa unidade organizativa:

Configuración de equipo - Directivas - Configuración de Windows - Configuración de seguridade - Directivas locais - Asignación de dereitos de usuarios - Denegar o inicio de sesión local

Defínese a directiva engadindo o grupo de usuarios que NON teñen permitido o inicio de sesión.

1.4.10 Control remoto máis dunha conexión simultánea

Temos dúas GPOs a configurar: Configuración del equipo - Directivas - Plantillas administrativas - Componentes de Windows - Servicios de Escritorio remoto - Host de sesión de escritorio remoto - Conexiones:

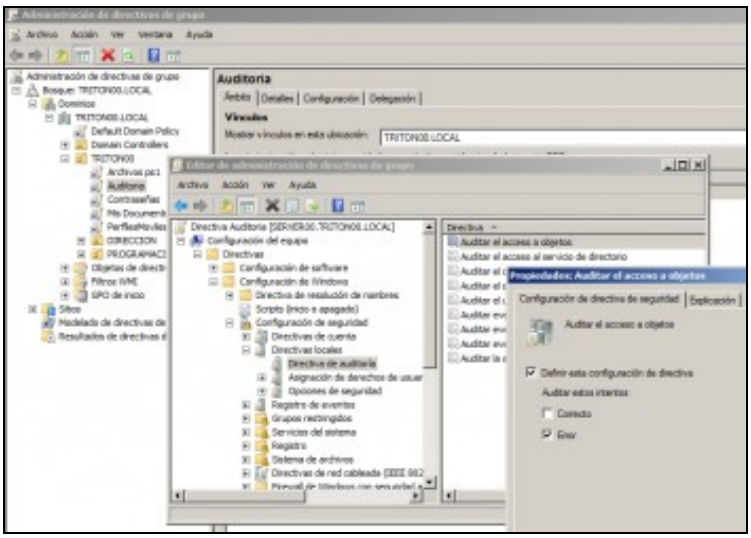
1. Directiva: Limitar a los usuarios de Servidios de Escritorio remoto a una única sesión de Servicios de Escritorio remoto - Deshabilitado.
2. Directiva: Limitar número de conexiones - Habilitada - [O número que nos interese]

1.4.11 Auditar o acceso a arquivos e carpetas

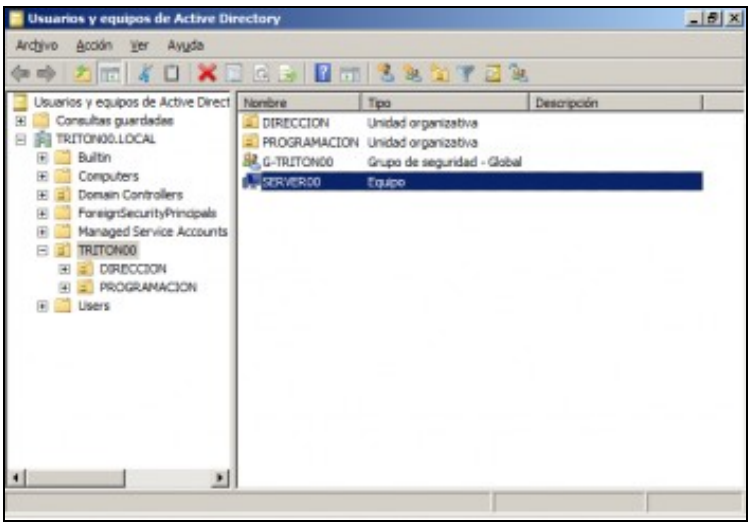
Windows 2008 soporta a auditoría granular baseándose nas contas do usuario ou grupo e as accións específicas realizadas por esas contas. Para configurar a auditoría, débense completar tres pasos: Crear e activar a auditoría específica (GPO), configurar a Ficha Auditoría no directorio que nos interese e avaliar os eventos no rexistro de seguridade.

- **Crear e activar a auditoría específica (GPO).**

  - Agregar unha nova directiva GPO na OU que nos interese, hai que ter moi en conta que o "servidor de arquivos" onde se atope o directorio a auditar se atope no seu interior.
  - Editar a directiva: Configuración de equipo - Directivas - Configuración de Windows - Configuración de seguridad - Directivas locales - Directiva de auditoría... Aí temos "Auditar el acceso a objetos" e debemos escoller:
    · Definir esta configuración de directiva.
    · Auditar estos intentos: E seleccionar "Correcto", se nos interesa auditar o acceso correcto a directorios, e/ou "Error", se nos interesa auditar os accesos erróneos.

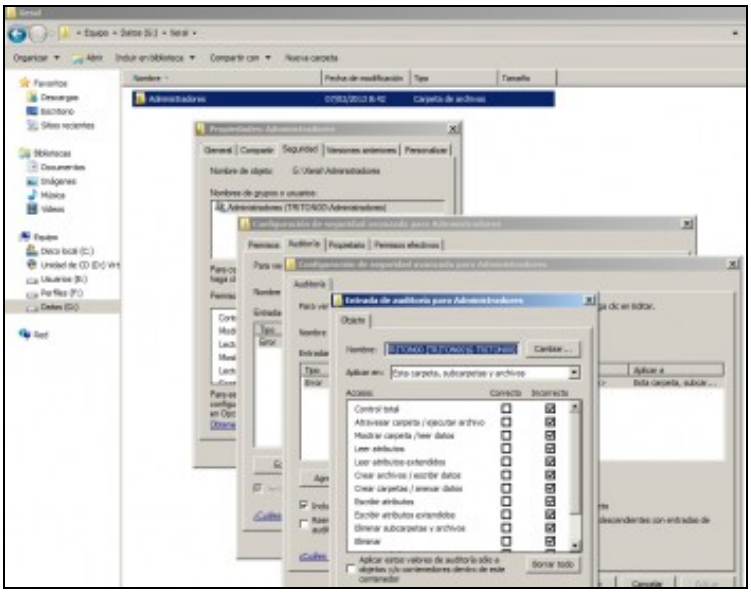


· Neste intre non hai que esquecer "mover" o servidor de arquivos (onde se atope o directorio que queremos auditar o seu acceso) á UO correspondente (no exemplo da imaxen seguinte trátase de SERVER00).



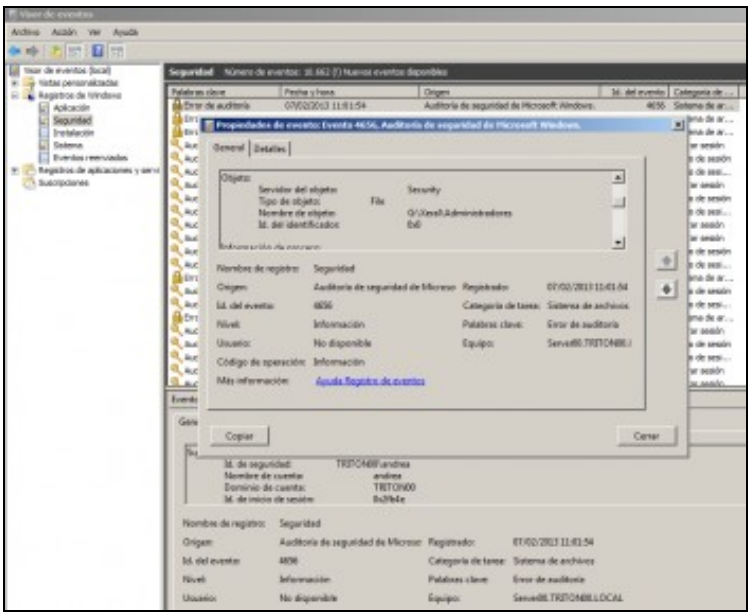
- **Configurar a Ficha Auditoría no directorio a auditar.**

  - Logo de configurar os permisos de acceso do directorio a auditar (Neste exemplo o fago dunha carpeta chamada "Administradores" dentro do directorio compartido "Xeral"). Fago que só os Administradores poden acceder a ela.
  - Por último, acceder á Ficha Auditoría do directorio "Administradores" e configurar que se quere auditar o Acceso Incorrecto a ela do grupo ou grupos a Auditar.



- **Comprobar os eventos xerados.**

  - Xa só nos queda intentar acceder a esa carpeta cun usuario do grupo a auditar e comprobar no "Visor de eventos" que queda o acceso rexistrado.
  - Abrir o "Visor de eventos" e acceder a "Registro de Windows - Seguridad", ordenar todos os eventos por "Fecha y Hora" e comprobar a existencia do envento correspondente (será un "Error de auditoría").



1.4.12 Administración de impresoras

Seguir el siguiente enlace

1.4.13 Borrar directivas de grupo

Para borrar unha directiva de grupo debemos ir ao contenedor **Group Policy Objects**, seleccionar a GPO a borrar e premer Delete. Ollo, pois unha GPO borrada non se poderá recuperar máis.

1.4.14 Grupo Global en Grupo Administradores Locales de Equipos Clientes

Para que un grupo global se añada a los administradores locales de equipos clientes:

Abrimos la GPO y vamos a la siguiente ruta Configuración del equipo -> Políticas -> Configuración de Windows -> Configuración de seguridad -> Grupos restringidos.

--Vieites 2 feb 2013