Administración del acceso al dominio.

Caso práctico

En los contenidos de las unidades anteriores hemos gestionado nuestro entorno de red instalando un dominio y configurando sus controladores. El usuario "Carlos" de la empresa "Gestisa" aprovecha el servidor de dominio para administrar los recursos compartidos como son las aplicaciones, impresoras, carpetas y ficheros. En nuestra estructura de red deberemos aplicar una política de compartición de recursos en el dominio para que los usuarios, desde cualquier terminal, puedan acceder a ellos bajo una supervisión de permisos y derechos, procurando como responsables de la administración gestionar un buen control de seguridad en el acceso.

Recordemos que desde un terminal de Windows 7, uno de los caminos **para acceder a un recurso compartido** que sirve otro equipo es desde *Inicio-Equipo* del panel derecho, pulsar en *Red*, se visualizarán los equipos que han iniciado sesión en la red, seguidamente pulsamos en el icono del terminal deseado y veremos los recursos compartidos como impresoras carpetas o directorios, unidades, etc., si pinchamos en el recurso deseado podremos acceder siempre que tengamos los permisos correspondientes.

Cuando el recurso que comparte el servidor es un directorio, desde el equipo cliente de Windows 7 **podemos crear accesos directos o conexiones directas** para no tener que realizar todos los pasos anteriores cada vez que necesitemos utilizar el recurso, para ello desde la misma ventana donde estamos, seleccionamos el recurso y pulsamos el botón derecho del ratón y del menú escogemos la opción *Conectar e una unidad de red*, entonces aparecerá un ventana de edición y en el campo *Unidad* desplegamos para seleccionar una letra que será asignada al directorio compartido, marcamos el campo *Conectar de nuevo al iniciar sesión*, para terminar pulsar en el botón *Finalizar*. Cuando demos a *Inicio-Equipo*, veremos que el sistema ha creado una nueva unidad con la letra asignada en los pasos anteriores, si pulsamos en ella accederemos directamente al directorio compartido.

También sabemos que con la instalación de la aplicación smbclient (normalmente ya se integra en la mayoría de los sistemas Linux durante el proceso de instalación), **podemos acceder desde un terminal Linux a recursos compartidos por una máquina Windows mediante el protocolo SAMBA**. Así en el escritorio de Linux desde el menú *Lugares-Conectar con el servidor* o desde el propio explorador podemos acceder a los recursos compartidos por otros equipos.

Una de las tareas del administrador es la de gestionar la seguridad en el acceso a los recursos compartidos y servicios que ofrece el servidor, con el fin de ofrecer una total integridad de los datos y aplicaciones del servidor, y de esta forma proteger el dominio. Para conseguirlo, los sistemas operativos disponen de herramientas que ofrecen políticas de seguridad en el acceso y la posibilidad de aplicar propiedades a los recursos con el fin de atribuirles características de permisos de uso para los usuarios y grupos.

Debes conocer

Como hemos aprendido en unidades anteriores, para la administración de usuarios y grupos podemos utilizar el grupo de comandos net. En el siguiente documento puedas ampliar conocimientos para gestión del uso y acceso de recursos en los equipos de una red, desde el símbolo de sistema o consola de comandos en sistemas Windows.

Configuración de recursos con comandos net. (64.0 KB)

Equipos del domino.

Caso práctico

En los contenidos de las unidades anteriores ya hemos gestionado las cuentas de equipo de un controlador de dominio. La estructura de red de la empresa "Gestisa" la han ampliado instalando maquinas virtuales Linux en los equipos con más prestaciones en Hardware y que disponen de base el sistema operativo Windows. De esta forma, los usuarios pueden acceder al dominio desde los dos sistemas sin necesidad de comprar nuevos equipos. En nuestra estructura de red, si hacemos lo mismo, deberemos aprender a integrar terminales Linux en el controlador de dominio Windows Server 2008.

En muchos entornos de red las estaciones de trabajo pueden estar configuradas con un sistema operativo Windows o Linux, pudiendo formar las llamadas redes mixtas.

En la unidad anterior ya aprendimos a gestionar un dominio mediante la instalación de un controlador de dominio. También comprobamos que un controlador de dominio, con más o menos posibilidades de administración, puede estar habilitado en servidores Windows o en un Servidores Linux.

Debido a la extensión de los posibles casos de acceso, también estudiamos la forma de crear cuentas de equipo en un controlador de dominio Windows cuando los terminales se ejecutaban bajo Windows, y vimos como añadir cuentas de equipo Windows a un controlador de dominio bajo Linux.

En esta unidad aprenderemos a añadir terminales Linux a controladores de dominio Windows. Para ello se tendrán que realizar las siguientes tareas:

1. Configurar los parámetros de la red.
2. Instalar el software necesario para la gestión.
3. Configurar Kerberos (presentación del login para el acceso seguro al servidor Windows desde el cliente Linux).
4. Crear los tickets de Kerberos.
5. Configurar el servicio de Samba.
6. Configurar Winbind para resolver nombres y grupos de usuarios en el dominio.
7. Añadir el terminal de Linux al controlador de dominio Windows.
8. Podemos utilizar alguno de los siguientes comandos para consultar información del dominio desde Linux:
   - *net ads info*: Información del controlador de dominio.
   - *net rpc testjoin*: Comprueba si la integración es correcta mostrando un mensaje, como por ejemplo: *"Join to 'INFOALISAL' is ok"*
   - *wbinfo –u –g*: Visualiza los usuarios y grupos del dominio.
   - *net rpc info –U nombre_usuario*: Muestra información del usuario del dominio.

Debes conocer

En el siguiente documento podrás aprender a configurar un terminal Linux para que se integre en un controlador de dominio Windows Server 2008 y poder acceder como usuario del Active Directory.

Configuración de cuenta de equipo Linux para un controlador de dominio en Windows. (0.21 MB)

Autoevaluación

¿Qué ocurrirá después de ejecutar el comando "*net ads join -S distancia.infoalisal.local -U administrador*" necesario para añadir una máquina de Linux al Active Directory de un controlador de dominio gestionado por Windows Server?

- No ocurrirá nada.
- Dará error ya que la orden no existe.
- Nos soliciará la contraseña del usuario administrador del dominio.
- Ninguna es correcta.

Permisos y derechos.

Caso práctico

Carlos, el administrador de la red local de "Gestisa", ha gestionado un plan de seguridad de dominio, mediante el cual restringe y permite al acceso a los recursos del servidor dependiendo del tipo de usuario y de los grupos a los que pertenezca. De esta manera, cada usuario solamente puede acceder a los recursos que necesita para su actividad en la empresa. Carlos tiene que compartir los recursos y gestionar los permisos pertinentes para su correcto y seguro uso. Por ejemplo, existen tres impresoras en red compartidas para todos los usuarios, también cada usuario puede acceder a su directorio particular en el servidor con todos los permisos que le permitan escribir y leer para poder guardar sus trabajos, mientras que los usuarios del mismo grupo al que pertenece solamente podrán acceder con permiso de lectura.

Una de las tareas del administrador es la de gestionar la seguridad en el acceso a los recursos compartidos y servicios que ofrece el servidor, para ello por una parte, tendrá que autorizar las diferentes acciones o tareas que los usuarios o grupos de usuarios pueden realizar en todo el dominio desde el momento que entran en el sistema, estas acciones se identifican como **derechos**. Por otra parte, deberá atribuir a cada recurso compartido los **permisos** u operaciones que pueden realizar los usuarios o grupos a la hora de actuar sobre él como pueden ser leer, modificar, borrar, etc.

Es importante realizar una buena administración de los permisos y derechos, con el fin de no dejar al descubierto, por una mala planificación, información valiosa para el sistema o información privada de los usuarios. Los diferentes permisos de acceso que puede tener un recurso como puede ser una carpeta, impresora, dispositivo, fichero, etc., dependerán de las operaciones que se puedan realizar que pueden ser: lectura, ejecución, modificación, borrado, apertura, creación, cierre, copiar, mover, renombrar, escritura, etc. Cada recurso dispondrá de un listado con los permisos que tiene cada usuarios y grupos sobre él, según hayan sido asignados por el administrador. Cada servidor dispone de diferentes niveles de permisos sobre ficheros y capetas dependiendo de la posibilidad que ofrezca el sistema de ficheros utilizado (FAT, NTFS, EXT3, etc.).

Mediante la gestión de derechos, el administrador indica las políticas de control para el acceso de usuarios y grupos de usuarios al sistema. **La administración de derechos se basa, principalmente, en la aplicación de reglas llamadas directivas de seguridad que definirán características relacionadas con la seguridad del sistema**. Para facilitar la gestión de derechos el propio sistema dispone de grupos de usuarios predeterminados con unas directivas asignadas por defecto. Algunas reglas son: poder acceder localmente o remotamente al sistema, poder o no instalar aplicaciones, solamente tener acceso al sistema durante un periodo de tiempo determinado, no poder ejecutar una aplicación concreta, etc.

La seguridad en el acceso a sistemas Linux no dispone de una herramienta para gestión de directivas de seguridad como dispone Windows, podemos

aplicar un control de acceso seguro mediante el protocolo *OpenSSH* y la aplicación de comandos como *chage* (gestiona la caducidad de contraseñas), asignación al usuario a que pertenezca grupos predeterminados del sistema, gestión de *iptables* en acceso por interface de red (actuaciones de cortafuegos), etc.

En el dominio Windows la información de cada usuario referente a los derechos de uso y acceso al sistema se gestiona mediante el Active Directory, que contiene datos como el número **SID** identificador de usuario y los **SID** de grupos a los que pertenece, así como la lista de directivas otorgadas. En Linux dicha la información se almacena en ficheros como *shadow* y *passwd* donde **SUID** es el número identificados de usuario y **SGID** a los grupos. **En Windows Server 2008 para poder configurar recursos compartidos será necesario tener instalada la función de Servicio de Archivos**, en distribuciones anteriores viene instalado de forma predeterminada.

Debes conocer

En el siguiente podrás aprender a instalar la función de servidor de archivos necesaria en Windows Server 2008.

Instalación del servicio de archivos en Windows Server 2008. (0.21 MB)

Autoevaluación

¿Qué opción u opciones deberemos señalar en el asistente de agregar funciones que permita al Windows Server 2008 gestionar los archivos de los usuarios?

- Servidor de archivos y Administrador de recursos del servidor de archivos.
- Administrador de recursos del servidor de archivos.
- Administrador de recursos del servidor de archivos.
- Servicio Búsqueda de archivos.

Permisos en Windows Server 2008: Compartir recursos y listas de control.

Caso práctico

En el equipo controlador de Windows del dominio de la red de “Gestisa” se gestionan tres directorios compartidos, uno para cada grupo de usuarios que representan a cada de las asesorías con las que se trabaja (laboral, financiera y empresarial). Los usuarios dependiendo de los grupos a los que pertenezcan dispondrán de todos los derechos en cada directorio; además cada usuario dispondrá de su propia carpeta particular en el dominio para alojar sus trabajos personales. Cuando acceda el usuario, automáticamente aparecerán en el entorno del equipo las carpetas sobre las que tiene permiso se acceso conectadas como unidades de red.

En Windows, con diferencia de los sistemas de archivos FAT, en las **particiones NTFS podemos utilizar permisos y cifrado para restringir el acceso a los ficheros**. Al asignar permisos a un objeto estamos indicando que usuarios o grupos puede acceder y que operaciones pueden realizar.

El servidor guarda toda la información relacionada con los objetos y sus permisos (descriptores de seguridad) en las **listas de control de acceso** o **ACLs** (exclusivas de particiones con formato NTFS) que son listas que le dicen al Sistema Operativo qué o quién tiene permiso para acceder a un objeto determinado. Una ACL contiene una **ACE** para cada usuario o grupo, indicando qué permisos tiene. Todos estos permisos pueden ser modificados con los comandos *cacls* (para acceder a la ayuda ejecutamos desde símbolo del sistema:*calcs /?*).

Para saber más

En el siguiente enlace puedes ampliar la información que te proporcionamos sobre la orden *calcs*.

El comando calcs. (100 KB)

Para poder gestionar permisos en recursos compartidos debemos de tener en cuenta algunas **características, como son**:

- **Los derechos tienen prioridad ante cualquier permiso.**
- **Los permisos son acumulativos**, por ejemplo puedes tener permisos como usuario y además como miembro de un grupo.
- Los **permisos de los archivos preceden o tienen prioridad sobre las carpetas** y **los ficheros o carpetas heredan los permisos de sus contenedores**.

- Un permiso puede tener dos valores **Permitir y Denegar**, en caso de disponer de los dos a la vez se considera el de Denegar por ser el más restringido. Los permisos **explícitos tienen prioridad sobre los heredados**.
- **Es conveniente asignar permisos a nivel de grupos de usuarios**, no individualmente a cada usuario de manera que no compliquemos y sobrecarguemos la tarea de administración.
- Los permisos que se asignan a una carpeta compartida se determinan por los permisos de recurso compartido más los NTFS, aunque al final **se aplicarán siempre los permisos más restrictivos**; por ejemplo, "podemos definir los permisos de un recurso para *Control total* al grupo *Todos* y usar los permisos NTFS para restringir el acceso de una manera más exclusiva".
- Cada recurso tiene al menos **un propietario que puede configurarlos permisos del recurso** y a quien se le conceden, así que un Administrador que necesite modificar los permisos en un recurso debe tomar posesión del archivo
- **Los permisos de recursos compartidos aplican sólo a carpetas,** y **los permisos NTFS se aplican a carpetas y ficheros**.
- **No se permiten las conexiones múltiples para un servidor o recurso compartido compatible por el mismo usuario, usando más de un nombre de usuario.**

Windows server puede gestionar los permisos mediante dos modos o niveles de acceso:

- **Permisos para el acceso local** (desde el mismo ordenador) deberemos de utilizar los permisos NTFS.
- **Permisos para el acceso a través de la red** (desde otro terminal al servidor del recurso) se deben de utilizar los llamados permisos para recursos compartidos (SHARE), junto con los permisos NTFS (será necesario que el volumen esté formateado con este tipo de sistema de archivos) para potenciar la seguridad. En el caso de disponer de una partición FAT32 solamente podemos establecer permisos para carpetas o recursos compartidos.

Debes conocer

En este enlace se estudia la forma de compartir recursos desde Administración de almacenamiento y recursos compartidos.

Compartir recursos en un controlador de dominio de Windows Server 2008. (0.44 MB)

Para saber más

Te recomendamos ver el siguiente vídeo sobre compartir recursos desde herramientas de administración de equipos.

Compartir recursos en Windows Server 2008 desde Herramientas de administración de equipos.

se ha podido cargar el compleme

Autoevaluación

De forma predeterminada los permisos de acceso a la carpeta Acceso público serán asignados para el grupo *Todos*.

- Verdadero.
- Falso.

Permisos para recursos compartidos y Permisos NTFS en Windows Server 2008.

Para acceder a gestionar los permisos de un recurso, Windows Server 2008 ofrece varios caminos. Nosotros utilizaremos en muchas explicaciones la consola **mmc** de *Administración de almacenamiento y recursos compartidos* con la que podemos realizar tareas como: crear o eliminar volúmenes y carpetas compartidas, decidir que protocolo gestiona el recurso compartido, aplicar los permisos NTFS, decidir cuántos y que usuarios acceden, publicar el recurso en un espacio DFS (Sistema de Ficheros distribuido), etc.

Se accede desde *Inicio-Herramientas administrativas- Administración de almacenamiento y recursos compartidos*, donde si seleccionamos un recurso compartido, pulsamos al botón derecho del ratón y elegimos *Propiedades*, en la pestaña *Permisos* podemos administrar los *Permisos de los recursos compartidos* o *Permisos NTFS*.

Los permisos de las carpetas o **recursos compartidos** que el sistema nos deja configurar son:

- **Control total**: el usuario o grupo tomará propiedad del recurso y puede realizar cualquier tarea.
- **Cambiar**: crear, eliminar y modificar archivos y carpetas.
- **Lectura**: permite leer y ejecutar.

Los permisos estándar o predeterminados NTFS que se pueden asignar a una carpeta son:

- **Control total**: para leer, cambiar, crear y ejecutar bien sean programas o carpetas.
- **Lectura y ejecución**: para ver el contenido y ejecutar programas de una carpeta.
- **Modificar**: para poder cambiar los ficheros y las carpetas, pero sin crear y eliminar ficheros ni carpetas nuevas.
- **Lectura**: para poder ver y abrir el contenido.
- **Escritura**: para poder crear y cambiar los ficheros y carpetas existentes.
- **Mostrar el contenido de la carpeta.**

Debes conocer

Cada uno de estos permisos se compone de un grupo lógico de **permisos especiales NTFS**, que puedes conocer a continuación en el siguiente enlace.

Permisos NTFS especiales aplicados a recursos en Servidor Windows.

Para saber más

Lo que se permite o deniega con cada Permiso especial NTFS.

Debes conocer

En estos vídeos podrás ver cómo compartir recursos en un Servidor Windows 2008 que actúa de controlador de dominio.

Gestionar Permisos a recursos en un controlador de dominio de Windows Server 2008 (primera parte).

se ha podido cargar el compleme

Gestionar Permisos a recursos en un controlador de dominio de Windows Server 2008 (segunda parte).

se ha podido cargar el compleme

Para saber más

En este enlace aprenderás a compartir una impresora desde Windows.

Compartir una impresora desde el sistema Windows. (0.46 MB)

Autoevaluación

Si un usuario tiene solamente el permiso de lectura sobre una carpeta compartida en un dominio Windows, ¿puede crear nuevas carpetas dentro de la carpeta compartida?

- Sí, siempre que sea el propietario.
- Sí, siempre que tengas activado Permitir.
- Sí, ya que lo que no puedes es añadir ficheros.
- No.

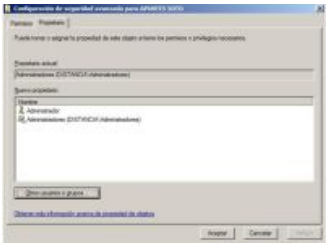
Permisos Especiales y Heredados. Concepto de Propiedad. Publicar permisos.

Además de los permisos estándar NTFS, podemos personalizar mejor las tareas que un usuario o grupo puede realizar sobre un recurso compartido **aplicando los permisos especiales NTF**S. Se establecen así:

1. Vamos a la consola **mmc** *Administración de almacenamiento de recursos compartidos*, seleccionamos al recurso, dar al botón derecho de ratón y del menú dar en *Propiedades*, en la pestaña *Permisos*, *pulsar* en el botón de*Permisos NTFS*, luego en *Opciones avanzadas*.
2. Pulsamos en la pestaña de *Permisos*. Podemos *Agregar* y *Quitar* nuevos usuarios o grupos como ya hemos aprendido anteriormente (recordamos que si el botón *Quitar* no está disponible, desactivar la casilla *Incluir todos los permisos heredables del objeto primario de este objeto*); también se puede establecer los permisos especiales seleccionando el grupo o el usuario y pulsando al botón de *Editar*.

Los **permisos explícitos** son aquellos que se establecen de forma predeterminada en objetos, mientras que se consideran **permisos heredados** los que se propagan a un objeto desde un objeto ya creado que actúa como contendor de recursos. Por ejemplo, la carpeta Mis documentos de un usuario tiene permisos explícitos, mientras que las carpetas y ficheros que se graban en sus interior ya disponen de permisos heredados. Los permisos explícitos tienen prioridad sobre los permisos heredados, incluidos los permisos Denegar heredados. Para administrar la herencia:

1. Vamos a *Administración de almacenamiento de recursos compartidos*, seleccionamos al recurso, dar al botón derecho de ratón y en *Propiedades*, en la pestaña *Permisos* pulsar en el botón de *Permisos NTFS*, luego en *Opciones avanzadas*.
2. Pulsamos en la pestaña *de Permisos*. Si no deseamos que se hereden los permisos, activar *Sólo esta carpeta* cuando se configura los permisos especiales para la carpeta contenedora. Si desea evitar que sólo algunos archivos o subcarpetas hereden los permisos desactive la casilla *Incluir todos los permisos heredables del objeto primario de este objeto*.



El concepto de propiedad de un recurso se aplica a los usuarios o grupos que tienen el control sobre él, de forma predeterminada el que crea el recurso es el propietario. Podemos transferir la propiedad, y también puede tomarse por cualquier usuario o grupo que tiene el permiso *Tomar posesión* o de *Restaurar archivos y directorios*para el recurso en cuestión. El actual propietario puede conceder el permiso *Tomar posesión* a otro usuario. También, un usuario con derecho de *Restaurar archivos y directorios* puede elegir un usuario o grupo para asignarles la toma de propiedad. Para transferir la propiedad debemos de:

1. Vamos a *Administración de almacenamiento de recursos compartidos*, seleccionamos al recurso, dar al botón derecho de ratón y en *Propiedades*, en la pestaña *Permisos* pulsar en el botón de *Permisos NTFS*, luego en *Opciones avanzadas*.
2. Pulsamos en la pestaña *de Propietario*, damos en *Editar*. En esta ventana podemos agregar nuevos propietarios desde el botón *Otros usuarios o grupos* y modificar la cualidad de propiedad seleccionando la opción *Reemplazar propietario en subcontenedores y objetos*.

El concepto de publicar es inscribir un recurso compartido en el catálogo global del Active Directory (AD). Los permisos de los recursos publicados sólo se aplican cuando se accede a esos recursos a través del AD. Para publicar una carpeta compartida deberemos de ir a la consola de Usuarios y equipos del DA, hacemos clic en *nuevo* y después *carpeta compartida*. Rellenamos la ruta que nos lleva a la carpeta.

Windows dispone la herramienta **Permisos efectivos** que permite solamente consultar los permisos o privilegios que tiene sobre un recurso dependiendo de los grupos a los que pertenece. Para ver los premisos efectivos NTFS:

1. Buscar el recurso y seleccionar, dar al botón derecho de ratón y del menú dar en *Propiedades*, pulsar en la pestaña *Seguridad*, luego en *Opciones avanzadas*.
2. Pulsamos en la pestaña de *Permisos efectivos*. No podemos cambiar los permisos solo comprobar cuales tiene.

Autoevaluación

¿Qué estamos configurando al hacer clic en "Sólo esta carpeta" en el cuadro "Aplicar" en al configurar permisos especiales para la carpeta principal?

- Permitimos publicar una carpeta compartida.
- Los nuevos archivos y subcarpetas que se crean en la carpeta heredan los permisos.
- No deseamos que los archivos y las carpetas hereden los permisos.
- Asignamos quien es el propietario de un recurso compartido.

Administración de permisos en Linux Ubuntu.

Caso práctico

Al servidor de Linux de "Gestisa" pueden acceder varios empleados simultáneamente. Para garantizar la confidencialidad de la información y la estabilidad del sistema, Carlos, como usuario **root**, tiene la responsabilidad de gestionar los permisos de acceso a los diferentes recursos de manera que cada usuario podrá acceder a su carpeta personal con todos los derechos, y dependiendo del grupo al que pertenezca estará autorizado para ejecutar y leer otros recursos.

Debemos aclarar que en Linux podemos establecer permisos de recursos para una estructura en red de cliente-servidor permitiendo acceder mediante el protocolo de seguridad ssh al servidor Linux desde terminales Windows (aplicación *Putty*) o Linux; también podemos compartir recursos entre equipos Windows y Linux gracias al protocolo **Samba** (mediante un grupo de trabajo o dominio); y existe otro protocolo el NFS que permite montar recursos compartidos entre equipos Linux (Windows Server 2008 ya incorpora este protocolo para poder compartir con este sistema con equipos Linux).

El sistema Linux, de forma predeterminada, permite establecer sobre cada fichero o carpeta los siguientes permisos de acceso:

- **Lectura** (*r*): Quien tiene este permiso sobre un archivo puede leerlo pero no modificarlo ni borrarlo. Si se trata de una carpeta podrá listar su contenido pero no podrá ver las características de los archivos o carpetas que contenga, como tampoco podrá borrarla o crear otras carpetas en su interior.
- **Escritura** (*w*): Quien tiene este permiso puede modificar o incluso borrar el archivo. Si se trata de una carpeta podrá eliminarla o crear nuevas carpetas dentro de ella.
- **Ejecución** (*x*): Si se trata de un fichero binario quien posea este permiso podrá ejecutarlo. Si se trata de una carpeta podrá ver su contenido y acceder también a las propiedades de los archivos o carpetas que contenga.
- **No asignado** (-): según el orden (rwx) donde aparece un "**-**" indica que no tiene asignado ese tipo de permiso.

El sistema establece permisos para el propietario, para uno de los grupos existentes, y para el resto de usuarios, utilizando una serie de bits cuyo contenido se interpreta según se muestra en la figura siguiente obtenida al ejecutar desde un terminal de comando la orden *ls –l*. Como norma, para cualquier agrupamiento de premisos **el sistema adopta por utilizar los más restrictivos.**

Para **administrar los permisos desde el entorno grafico**seleccionamos el recurso desde el explorador y pulsamos al botón derecho del ratón, seleccionamos del menú en *Propiedades*, pulsamos en la pestaña *Permisos*, seguidamente de la ventana completar cada uno de los campos según las posibilidades dadas en los valores de las listas despegables y las restricciones a aplicar. Otra forma de administrar permisos a ficheros y carpetas es desde la consola de entrada de comandos con la orden *chmod* (Podemos ver la ayuda del comando ejecutando *man chmod*). Este comando es similar al comando *cals* de Windows que permite gestionar los permisos de las tablas ACLs de un recurso desde la línea de comandos. Hay dos formatos posibles a usar*chmod*:

root@servidorcarlos:~# *chmod [número_octal] nombre_fichero*
root@servidorcarlos:~# *chmod [ugo][+-][rwx] nombre_ficheo*
Donde [*u=user, g=group y o=other*]; [*+/- activa o desactiva los atributos siguientes r=read, w=write, x=execute*]

Para saber más

En el siguiente enlace podrás completar el aprendizaje de gestionar permisos con la orden *chmod* de Linux.

Administración de permisos dentro del sistema de ficheros con el comando *chmod* en Linux.

Debes conocer

En el siguiente enlace podrás ver ejemplos de administración de permisos con la orden *chmod* de Linux.

Ejercicios de permisos con chmod en Linux. (60.0 KB)

Autoevaluación

El fichero fic1.txt. tiene los permisos 777, ejecutando sudo chmod 676 fic1.txt quitamos todos los permisos de escritura.

- Verdadero.
- Falso.

Permisos adicionales en Linux.

Con referencia a las ACLs en Linux podemos decir los comandos *chmod* y *chown* equivalen al comando *calcs* de Windows.

Cuando se utiliza la notación octal podemos **aplicar unos permisos especiales aplicando los llamados bits de permanencia** SUID, SGID y sticky que tienen las siguientes características:

1. **El bit SUID o setuid**: se aplica añadiendo o sumando 4000 a la representación octal del permiso del archivo o con "g+s" en notación textual, además debe tener permiso de ejecución para el propietario; esta operación producirá que se cambie la "x" del permiso del propietario por una" s". Por ejemplo:

```
root@servidorcarlos:~# chmod 4777 /home/carlos/apuntes.doc
root@servidorcarlos:~# ls –l /home/carlos/apuntes.doc
-rwsrwxrwx 1carlos other 10 Ene 1 10:01 /home/carlos/apuntes.doc
```

El bit SUID generalmente se activa sobre un fichero ejecutable indicando que todo aquél que ejecute el archivo va a tener durante la ejecución los mismos privilegios que el propietario en el proceso creado.

2. **El bit SGID o setgid**: se aplica añadiendo 2000 a la representación octal del permiso del archivo "u+s" en notación textual, además debe tener permiso de ejecución para el grupo; esta operación producirá que se cambie la "x" del permiso del grupo por una" s"; el bit SGID activado sobre un directorio, fuerza a todos los archivos y subdirectorios creados en él a pertenecer al grupo del dueño del directorio y no al grupo del usuario que crea el archivo o subdirectorio, y sobre un fichero indica que todo usuario que ejecute un programa tendrá los privilegios del grupo al que pertenece el archivo. Por ejemplo:

```
root@servidorcarlos:~# chmod 1777 /home/carlos/apuntes.doc
root@servidorcarlos:~# ls –l /home/carlos/apuntes.doc
-rwxrwsrwx 1carlos other 10 Ene 1 10:01 /home/carlos/apuntes.doc
```

3. **El bit stick**: se aplica añadiendo 1000 a la representación octal del permiso del archivo o con "+t" en notación textual, además debe tener permiso de ejecución el resto de usuarios; esta operación producirá que se cambie la "x" del permiso de otros por una" t", si no le hemos dado permiso de ejecución al archivo veremos una "t" indicando que no está activado. El bit stick en un directorio indica que independientemente de los permisos que tenga el directorio sólo el propietario y el administrador pueden borrar un archivo guardado en un directorio. Por ejemplo:

```
root@servidorcarlos:~# chmod +t /home/carlos/
root@servidorcarlos:~# ls –l /home/carlos/
drwxr-xr-t 13 carlos 403 Apr 12 2011 carlos
```

Es importante que el administrador impida la ejecución de archivos con el bit SUID activado en aquellos directorios en los que los usuarios tienen permiso de escritura. Si listamos los permisos relacionados con el fichero *shadow* podemos comprobar que son restrictivos (600 en octal, permiso de lectura para el propietario root), haciendo sumamente difícil que cualquier usuario que no sea root lo lea.

```
root@servidorcarlos:~# ls -l /etc/shadow
-rw------- 1 root shadow 1100 2011-02-03 11:03 /etc/shadow
```

Para saber más

En el siguiente enlace podrás completar el aprendizaje de gestionar permisos para recursos de Linux Ubuntu.

Administración de permisos dentro del sistema de ficheros en Linux Ubuntu.

Autoevaluación

¿Qué estamos permitiendo con la orden: chmod 4755 programa.sh?

- Que todos los usuarios puedan ejecutar el fichero programa.sh.
- Que solamente puede ejecutar el fichero programa.sh el propietario.
- Que solamente puede ejecutar el fichero programa.sh el grupo al que pertenece el usuario.
- Ninguna es correcta.

Gestión de recursos compartidos vía Samba: El fichero smb.conf en Linux.

Caso práctico

La red informática de "Gestisa" reparte la compartición de recursos entre sus servidores. Utiliza el servidor de Linux para descongestionar los accesos al servidor de Windows. Por ejemplo, el servicio de impresión compartido está gestionando y administrado en el servidor de Linux mediante el protocolo Samba, algunas aplicaciones realizan las copias de seguridad de sus bases de datos en un directorio compartido alojado en el servidor de Linux, etc. Por eso, **Carlos** considera que es importante saber aprovechar las posibilidades que ofrece **Samba** a la hora de compartir recursos entre redes mixtas.

El protocolo predeterminado para compartir recursos en Windows es **SMB** , es el que hemos utilizado hasta ahora, basado en permisos NTFS y permisos de recurso compartido. Linux también utiliza Samba, recordemos que en la unidad anterior nos iniciamos en su administración con entornos gráficos Linux(mediante una **GUI** como es SWAT, System-Config-Samba o mediante el entorno de trabajo Webmin que permite la administración remota del sistema operativo de un servidor desde un navegador).

Ahora estudiaremos con más atención su fichero particular de **configuración *smb.conf* para conseguir que Linux actúe de servidor de archivos e impresión permitiendo compartir recursos para los otros ordenadores de la red**. Antes de comenzar la configuración deberemos saber que:

- Hay que comprobar si tenemos instalado el servicio, desde un terminal de línea de comandos en Linux Ubuntu ejecutamos:
  dpkg -s samba
  Si no lo está procederemos a su instalación con la orden:
  sudo aptitude install samba-client samba-common samba system-config-samba
- Seguidamente realizaremos una copia de seguridad del fichero de configuración, para ello movemos el archivo de configuración smb.conf con otro nombre, por ejemplo *smb.conf.copia*: *sudo mv /etc/samba/smb.conf /etc/samba/smb.conf.copia*
- Para realizar cualquier modificación como usuario root debemos de editar el fichero *smb.conf*, por ejemplo ejecutando:
  sudo gedit /etc/samba/smb.conf
- Es recomendable comprobar la integridad del fichero *smb.conf* después su modificación ejecutando:
  sudo /usr/bin/testparm
- Deberemos recordar que siempre que cada vez que configuremos el servicio samba deberemos reiniciarle ejecutando:
  sudo /etc/init.d/samba restart
- Para que al iniciar el sistema Samba se arranque automáticamente, desde el directorio */etc/init.d* ejecutamos la orden:
  sudo update-rc.d samba defaults
- Ya sabemos, de la unidad anterior, que será necesario añadir al sistema los usuario samba mediante la orden:
  sudo smbpasswd [opciónes] nombre_usuario
- Samba también dispone de la posibilidad de configurar el sistema Access Control Lists utilizando el comando *smbcacls* que gestiona las ACLs de Windows en archivos y directorios compartidos por el servidor Samba.:
  smbcacls / / servidor / share nombre de archivo [opciones]
- Cuando accedemos desde un equipo cliente, por ejemplo Windows, a varios recursos compartidos por Samba **no se permiten las conexiones múltiples para un servidor o recurso compartido compatible por el mismo usuario, usando más de un nombre de usuario**, para solucionar el problema deberemos reiniciar sesión y volver a intentar acceder al siguiente recurso compartido.
- **Para evitar conflicto entre los permisos del sistema y los permisos del servicio Samba muchos administradores optan por ser más restrictivos a la hora de aplicar los permisos** del sistema que en los permisos de recurso compartido por samba, de ésta forma serán efectivos para otros servicios como *FTP, web, ssh,* etc., instalados en el sistema.

Debes conocer

En el siguiente enlace podrás completar el aprendizaje de gestionar recursos compartidos configurando el fichero smb.conf.

Definir recursos compartidos desde smb.conf. (0.13 MB)

Acceso a recursos compartidos con el servicio cliente de Samba: smbclient.

Ya sabemos que con la aplicación Samba smbclient, hemos accedido a recursos compartidos en máquinas Windows con los interfaces gráficos del propio explorador de Linux; para ello desde el menú *Lugares-Conectar con servidor*, aparece una ventana que completando los campos podemos tener acceso a un recurso de Windows desde la conexión de red creada en el escritorio. Para realizar una **conexión a una unidad de red desde la consola de comandos Linux**seguimos los siguientes pasos:

a. Instalamos el cliente Samba y la herramienta que nos permite montar directorios para el acceso a recursos por red. root@servercarlos:*~#apt-get install smbclient smbfs*

b. Crear un directorio donde montar el recurso, por ejemplo: root@servercarlos:*~#mkdir /mnt/carlos*

c. Podemos hacer un listado de los recursos que dispone el ordenador que deseamos acceder, por ejemplo.

root@servercalos:~*#smbclient -L 192.168.1.174*
Password:

Sharename	*Type*	*Comment*
Apuntes	*Disk*	*Trabajos de distancia*
Temas	*Disk*	

d. Ahora montamos el directorio compartido, con la orden ***smbmount*** o ***mount –t smbfs.***
root@servercarlos:~*# smbmount //192.168.1.174 /Apuntes /mnt/carlos*
También realizamos la misma tarea utilizando el comando *mount –t smbfs –o guest //192.168.1.174 /Apuntes /mnt/carlos*. **(dependiendo de la versión cuando se montan directorios de servidores Windows utilizaremos cifs en lugar del parámetro smbfs)**. *Por ejemplo, mount –t cifs –o guest //192.168.1.174 /Apuntes /mnt/carlos.*

Ahora podemos manejar los archivos del directorio compartido "Apuntes" ubicados en el ordenador *192.168.1.23*, en nuestro ordenador desde la carpeta */mnt/carlos*. Todos los cambios que realicemos afectaran de forma remota a la maquina que comparte. Ejecutando la orden *man smbmount*obtenemos una ayuda por pantalla sobre las opciones del formato.

e. Cuando ya no sea necesario utilizar esto se desmonta el directorio:
root@servercarlos:~*# smbumount /mnt/carlos*

También podemos acceder a un recurso compartido mediante el demonio o proceso ***smbclient***, por ejemplo si pretendemos acceder al recurso "Apuntes" de equipo Linux "EQU1" de la red por el usuario "Carlos" (**es importante recordar que si el servidor es del sistema Windows deberemos de utilizar el separador de componentes "\"**), ejecutamos:

root@servercarlos:~*#smbclient //EQU1/Apuntes –U Carlos*

added interface ip=192.168.1.174 bcast=192.168.1.255 nmask=255.255.255.0
Password:
Domain=[Distancia] OS=[Unix] Server=[Samba 3.2.1a]
smb: >

Seguidamente el sistema solicitará que se le proporcione la clave de acceso del usuario "Carlos" para acceder al equipo "EQU1". Aparece el prompt de entrada de smb y ahora ya pueden utilizarse casi los mismos mandatos que en el intérprete del servicio *ftp*, como serían *ls*, *get*, *mget*, *put*, *del*, etc., para realizar operaciones con el contenido del recurso compartido. Para obtener ayuda sobre la forma de utiliza el comando ejecutamos la orden *man smbcliente*.

Podemos automatizar el montaje de recursos compartidos mediante Samba añadiéndolos al fichero **/etc/fstab** una línea teniendo en cuenta el siguiente formato:
//host_servidor/recurso_compartido /directorio_donde_montar smbfs username= < usuario >,password= < contraseña >.

Un ejemplo de ello podría ser la siguiente línea, donde nos pedirá contraseña ya que no la hemos especificado:
//192.168.1.174/Apuntes /mnt/carlos smbfs username=Ana

Para saber más

Para completar el aprendizaje aprendiendo a compartir una impresora desde Linux.

Compartir una impresora desde Linux. (0.11 MB)

Sistema de archivos NFS: Uso compartido NFS en Windows Server 2008.

Caso práctico

Carlos, aprovechando la red Wifi instalada en la empresa "Gestisa", ha realizado la compra de ordenadores Notebook que disponen en su preinstalación el sistema operativo Linux. Dichos dispositivos se están utilizando para facilitar la movilidad de los empleados por la empresa y para el acceso a los recursos compartidos utilizando los servicios ofrecidos por el protocolo NFS.

Además de Samba, el sistema estándar recomendado para compartir carpetas entre equipos Linux por red **es el sistema NFS**, por el cual un servidor gestiona la compartición de sus recursos, a los cuales accederán los usuarios desde otros PCs mediante la tarea de montar los recursos compartidos en un directorio del disco. Windows también dispone del protocolo NFS para compartir recursos con el fin de permitir su acceso a los usuarios basados en Linux.

Para poder usar permisos NFS en Windows Server 2008, primero hay que instalar la función: Servicios para Network File.

System (NFS), mediante *Administrador del servidor*. Seguidamente desde símbolo del sistema ejecutando la aplicación *nfsshare* (para más ayuda ejecutar desde símbolo del sistema ***nfsshare /?***), o desde la ventana de *Administración de almacenamiento y recursos compartidos*, podemos especificar los recursos compartidos y permisos NFS de las siguientes formas:

a. Desde ***Administración de almacenamiento y recursos compartidos*** podemos especificar permisos para los **nuevos recursos compartidos basados en NFS**. En el *Asistente para crear carpetas compartidas*, si seleccionamos *NFS como protocolo de uso compartido*, la página **Permisos NFS** estará disponible en el asistente.

Seguidamente podemos agregar, editar o quitar permisos (sin acceso, sólo lectura, lectura-escritura) para grupos de clientes y hosts. El valor por defecto es acceso de *Sólo lectura* para el grupo *Todos los equipos*. Existe la aplicación *NFSAdmin* para crear grupos de clientes (para más ayuda ejecutar desde símbolo del sistema ***nfsadmin server /?***). Lo atributos NFS predeterminados son:

- **Propietario**: tiene permisos de **Leer, Escribir** y **Ejecutar**.
- **Grupo**: El grupo principal al que pertenece la persona que crea el archivo, tiene permisos de **Leer** y **Ejecutar**.
- **Otros**: equivalente a **Todos** en un sistema operativo Windows, tienen permisos de **Leer** y **Ejecutar**.

b. Desde el **explorador de Windows**, seleccionamos el recurso a compartir y damos al botón derecho del ratón, pulsamos en la opción *Propiedades*, damos a la pestaña *Uso compartido de NFS* y hacemos clic en *Administrar uso compartido de NFS* (para desactivar desmarcamos esta opción), seguidamente marcamos la opción *Compartir esta carpeta*, escribimos un nombre para el recurso que verán los equipos Linux.
Por seguridad no conviene activar el recurso para el **acceso anónimo**. Pode defecto los equipos Linux disponen del acceso de sólo lectura, para modificar los permisos pulsamos en *Permisos* y seleccionamos los permisos en la ventana de *Permisos de recurso compartido NFS*.

Después de establecer el recurso compartido por NFS **desde un equipo cliente Linux, podemos utilizarle montando dicho recurso en un lugar desde el directorio raíz**. Para ello desde una shell de comandos o un termina de línea de comandos del equipo Linux que ejecute software de cliente NFS, escribimos la orden con el siguiente formato:

mount -t nfs nombre_del_equipo_Windows :/nombre_del_Recurso_Compartido /lugar_de_Montaje_en_equipo_Linux

Para saber más

Para completar el aprendizaje sobre el servicio NFS en Windows Server 2008 puedes acceder al siguiente enlace.

Guía paso a paso de Servicios para NFS para Windows Server 2008.

Autoevaluación

Con la orden "sudo smbclient //WIND/Apuntes" podemos acceder al recurso Apuntes del equipo Windows "WIND".

- Verdadero.
- Falso.

Gestión de recursos compartidos en Linux con NFS.

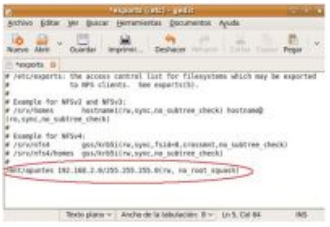
Como usuario *root* seguir los siguientes pasos **para compartir recursos en Linux con NFS**:

a. Deberemos tener instalado el paquete *nfs-user-server*, tanto en el ordenador cliente como en el servidor, con el gestor de paquetes de Synaptic o saliendo a un terminal desde *Aplicaciones-Accesorios-Terminal* y escribir:
root@carlos-laptop:*~# aptitude install nfs-user-server*

Después de la instalación el sistema ha creado los siguientes ficheros de configuración:

- */etc/init.d/nfs-user-server*: representa el script de inicio del servicio.
- */etc/exports*: contiene la lista de los sistemas de archivos NFS que se compartirán con los usuarios.
- */var/log/syslog*: contiene la lista de registros de las acciones realizadas al intentar las conexiones NFS sobre el servidor.

b. Cada vez que quiera compartir un directorio, se deberá añadir una línea al fichero */etc/export*, indicando la ruta del directorio a compartir y el equipo de la red que permitimos acceder a dicho recurso con una serie de opciones en la que podemos indicar los permisos. Por ejemplo, para compartir la carpeta creada "/mnt/Apuntes" para todos los equipos de la red 192.168.1.0 con permisos de lectura y escritura. Editamos el fichero:
root@carlos-laptop:*~# gedit /etc/export*



Añadimos la siguiente línea (marcada en rojo en la imagen), que permite compartir la carpeta " /mnt/Apuntes", con el parámetro (*rw*) damos permisos de lectura y escritura, con *no_root_squash* no permitimos que el usuario *root* pueda acceder remotamente al recurso, si llegamos a poner (*ro*) damos permiso de lectura, con * indicamos que permitimos a todos, etc. Guardamos el fichero desde el menú *Archivo-guardar*.

Los permisos de compartición por NFS no excluyen a los permisos del sistema Linux sino que **prevalecen los más restrictivos**. Por ejemplo, si una carpeta está compartida con permiso NFS de lectura y escritura pero en los permisos del sistema solo disponemos de permiso de lectura, no podremos escribir.

c. Deberemos reiniciar el servicio NFS para que el sistema tenga en cuenta los cambios realizados, ejecutamos:
root@carlos-laptop:*~# service nfs-user-server reload*

d. Desde cualquier ordenador Linux de la red que deseemos acceder al recurso compartido deberemos de realizar la operación de montar el recurso, iremos a dicho equipo y como usuario *root*, instalamos la aplicación cliente *nfs-common* del servicio NFS con la siguiente orden:
root@carlos-laptop:*~# aptitude install nfs-common*

e. Es importante que creemos en el ordenador el mismo usuario que comparte el recurso en el servidor o que es propietario del recurso compartido. Seguidamente montamos el directorio, por ejemplo en la carpeta ya creada " /mnt/temporal", con la siguiente orden (192.168.1.22 es el equipo servidor NFS que comparte el recurso):

root@carlos-laptop:~# *mount –t nfs 192.168.1.22:/mnt/apuntes /mnt/temporal*

Para saber más

Para completar el aprendizaje sobre el servicio NFS en Linux puedes consultar el siguiente enlace:

Sistema de archivos NFS en Linux.

Autoevaluación

¿Qué línea deberemos de añadir el fichero /etc/exports de un servidor NFS de Linux para compartir la carpeta /home/carlos con los permisos de escritura y lectura para que puedan acceder los equipos de la red 192.168.1.0/24?

- /home/carlos +rw.
- export /home/carlos 192.168.1 .* (rw).
- /home/carlos *(ro).
- /home/carlos 192.168.1.0/255.255.255.0 (rw).

Derechos de usuarios y grupos: Políticas de seguridad.

Caso práctico

Carlos ha analizado las necesidades que tienen cada usuario y grupo de usuarios a la hora de acceder al sistema, y ha creado unas directivas de grupo con el fin de controlar la seguridad en el acceso y uso de los equipos del dominio. Dicho agrupamiento de políticas de seguridad permitirá asegurar los recursos que ofrece el controlador de dominio Windows Server 2008 frente a posibles malos usos del sistema. Cada vez que se incorpora un usuario o equipo al dominio deberá volver a gestionar las directivas de seguridad de grupo.

La gestión de los derechos en el inicio de sesión de usuarios y grupos dentro de los sistemas operativos permiten la concesión o denegación de privilegios (políticas de seguridad) para la operatividad con el entorno de la computadora y de los servicios que disponga.

Los usuarios administradores serán los encargados de asignar derechos específicos a las cuentas de grupo o a cuentas de usuario individuales, con el fin de permitir a los usuarios el realizar tareas en el entorno del sistema, de esta manera podrán mantener un control en el uso y la seguridad en el acceso local y global. También servirá para evitar conflictos entre permisos a los servicios y recursos compartidos dentro de las estructuras de dominio, grupo de trabajo o cliente-servidor.

Mientras que los permisos se asignan a los objetos como carpetas, impresoras, archivos, etc., los derechos se aplican a las cuentas de usuario y cuentas de grupo de usuario que estará sometidos al protocolo de seguridad de la red en la que trabajan. Los sistemas disponen de herramientas que permiten la administración de los derechos de usuarios; en Windows estas políticas de seguridad de acceso al sistema y recursos se conocen como Directivas.

Directivas de seguridad en Windows.

Las directivas de seguridad son un conjunto de reglas de seguridad, referentes a características y permisos que se pueden configurar con el fin de garantizar el acceso a los recursos del sistema. En sistemas Windows la aplicación que resuelve su administración es gpedit.msc que se puede ejecutar desde un termina de línea de comandos, y gestiona los permisos o privilegios y derechos, mediante una planificación de reglas a aplicar a las contraseñas, normas de acceso, etc.

El sistema aporta desde la instalación unas directivas de seguridad predeterminadas, que son suficientes para la mayoría de las situaciones, las cuales se pueden clasificar en:

- **Directiva de seguridad local**: se gestionan cuando el servidor no actúa de controlador de dominio.
  Para acceder a la gestión de estas directivas iremos a *Inicio-Panel del control-Herramientas administrativas-Directivas de seguridad local* (el comando que se ejecuta para entrar en este modo es *secpol.msc* que se encuentra en *%windir%\System32\secpol.msc*).
  Para gestionar una regla de directiva, se selecciona, clic en el botón derecho del ratón y pulsamos la opción *Propiedades* y de la ventana de asistente de configuración *Activar/desactivar* o completar los campos deseados. Permite establecer, entre otras cosas: **Política de cuentas, Directivas locales de auditoría del sistema y directivas de claves públicas**.

- **Directiva de seguridad de dominio y de seguridad de controlador de dominio**: se administran cuando el servidor actúa de controlador de dominio, y se utiliza para gestionar los usuarios del dominio y los controladores de todo el dominio. Para acceder a la gestión de estas

directivas iremos a *Inicio-Panel del control-Herramientas administrativas-Administración de directivas de grupo*.

Los administradores pueden agrupar, modificar o personalizar las directivas para que se ajuste a las necesidades específicas de la organización del sistema.**Las políticas o directivas de grupo pueden estar contenidas en cuatro tipos de objetos:**

- **Equipos Locales o directiva de grupo local**: son aplicadas únicamente en el equipo que las tiene asignadas independientemente del dominio al que pertenezcan. Son modificadas con "gpedit.msc". Estas son las únicas políticas que se aplican a los equipos que no están en un dominio, como servidores independientes (stand alone) o clientes en redes de igual a igual (peer to peer).
- **Sitios de Active Directory o directiva de sitio de grupo**: se aplican para todos los equipos y/o usuarios de un sitio, independientemente del dominio del mismo bosque al que pertenezcan.
- **Dominios de Active Directory o directiva de grupo de dominio**: se aplican a todos los equipos y/o usuarios de dominio.
- **Unidades Organizativas de Active Directory directiva de grupo de unidad organizativa**: se aplican únicamente a los equipos y/o usuarios que pertenezcan a la propia unidad organizativa (OU).

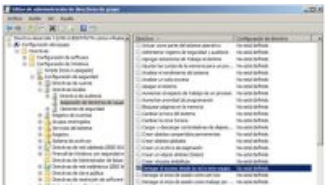
Para saber más

Debido a la importancia que tienen la administración de las directivas de seguridad dentro de los entornos Windows, TechNet de Microsoft dispone de su propia ayuda on-line. Si deseas profundizar en la configuración y administración de las directivas de grupos podemos acceder a:

Directivas de grupo en Windows.

Introducción a las directivas de grupo (GPO) en Windows.

La directiva de grupo es un conjunto de una o más políticas del sistema. Cada una de las políticas o reglas del sistema establece una configuración del objeto al que afecta. Gracias a las reglas de directiva de grupo podemos controlar los entornos de trabajo de los usuarios del dominio, los equipos y el comportamiento de los diferentes objetos y elementos que conforman la estructura del dominio en red.



Cuando se instala el AD se crean un conjunto de directivas de grupo predeterminadas y editables, los usuarios pasarán a ser usuarios del dominio y lo mismo ocurrirá con lo referente a la directiva de seguridad. Esto ocurre debido al modo en que la directiva de grupo se hereda mediante la estructura de AD.

Algunas de las características a considerar sobre las directivas de grupo son:

- Para la administración de la directiva de grupo podemos entrar en el editor de directiva complemento de Microsoft Management Console o MMC). Este complemento MMC se encuentra en la siguiente ubicación: *%windir%\System32\gpedit.msc*. Para **abrir el Editor de directivas de grupo local**, hacer clic en *Inicio*, luego en *Ejecutar* y escribir *gpedit.msc*.
- **La herramienta de administración que gestiona las directivas de grupo en el interfaz gráfico en Windows Server 2008 es el llamado complemento de** *Administración de directivas de grupo* y se accede desde *Inicio-Panel del control-Herramientas administrativas*.
- En cada ordenador hay unos objetos de directiva grupo local (GPO) encontrada en el directorio *SystemRoot\System32\GroupPolicy*. Además, en el controlador de dominio se encuentran los objetos de las directivas de grupo (GPO) de Active Directory (tienen prioridad sobre las directivas locales) y se guardan en el directorio *Sysvol*.
- **Un dominio ya dispone de dos directivas predeterminadas Default Domain Policy y Default Domain Controllers** formadas por un conjunto de reglas utilizadas para administrar distintas áreas.
- La forma de trabajar con una directiva de grupo predeterminada consistirá en localizar la directiva deseada o una plantilla y habilitarla configurándola de un modo personalizado.
- **Las directivas se pueden heredar de contenedores padres (sitios, dominios o unidades organizativas) a contenedores hijos acumulándose con las que ya disponga. La herencia se puede bloquear para no recibir directivas de ningún otro dominio, sitio o unidad organizativa.**
- Las directivas pueden estar en estado de **no configurada, habilitada para usuarios y grupos o deshabilitada**, se encuentra configurada pero no se aplica a usuarios y grupos. También se pueden aplicar plantillas de GPO para facilitar la asignación de las mismas directivas a varios usuarios.

Para saber más

A continuación puedes ver el vídeo creado por TechNet de Microsoft recomendado para los administradores de Windows relacionado con la administración de directivas de seguridad en Windows.

Definir directivas de seguridad en Windows Server 2008.

se ha podido cargar el compleme

Autoevaluación

Gracias a las reglas de directiva de grupo podemos controlar los entornos de trabajo de los usuarios del dominio, indicar de las siguientes actuaciones, ¿cuáles pueden ser controladas por directivas en el sistema Windows?

- [ ] Activa o no los scripts que se ejecutan al inicio y final de sesión de equipo o usuario.
- [ ] Cambiar la actuación de los permisos de usuarios y grupos.
- [ ] Bloquear cuentas.
- [ ] Limitar las funcionalidades de los equipos.

Mostrar Información