CONCEPTOS BÁSICOS

Dominio

Es un grupo lógico de máquinas que comparten cuentas de usuarios y seguridad de los recursos. Un dominio está integrado por una máquina NT **servidor de dominio** que administra las cuentas y recursos del dominio en cuestión, y/o servidores y /o estaciones de trabajo. Los usuarios de un mismo dominio tendrán un inicio de sesión único en el **servidor del dominio** para acceder a los recursos de cualquier parte de la red, una cuenta única para acceder a las máquinas del dominio...

Cuentas de usuarios

En las cuentas de los usuarios se establecen datos como el propietario de la misma, contraseña de acceso, localización de su directorio de inicio de sesión, grupo al que pertenece etc. Windows NT distingue las **cuentas locales** y las **cuentas de dominio**:

- Cuenta local de usuario: pertenecen a una única estación Windows NT. El procedimiento de login de las mismas se valida en una base de datos local de la estación. La herramienta administrativa de la estación para crearlas, modificarlas, borrarlas y establecer políticas de seguridad es el **Administrador de usuarios** o el **Administrador de usuarios para dominios**.

- Cuenta de dominio : pertenecen al dominio en cuestión. El procedimiento de login requiere, además del nombre de usuario y contraseña, el dominio al que se está haciendo login. La validación se hace en una base de datos existente en el servidor de dominio. La herramienta administrativa del servidor para crearlas, modificarlas, borrarlas y establecer políticas de seguridad del dominio es el **Administrador de usuarios para dominios**.

Tanto si se hace login en un tipo de cuenta u otro, para acceder al menú de seguridad de la estación o el servidor (para cambiar el password, bloquear el terminal, o cierre de sesión e incluso del sistema) teclear CRTL+ALT+SUPR

Las cuentas que por defecto crea NT son la de **Invitado** (*guest*), deshabilitada por defecto -, y la del **Administrador**, para configuración y control de usuarios y recursos.

Cuentas de grupos

Las cuentas de usuarios se organizan en grupos. Cuando se añade un usuario a un grupo, el usuario tendrá los **derechos y permisos** asignados a ese grupo.

Windows NT distingue dentro del concepto de grupo, dos categorías: **grupos locales y globales**.

- Grupo local: lo forman cuentas locales de usuarios y grupos globales de otros dominios. Se usan para asignar a grupos de usuarios permisos para acceder a un recurso.

- Grupo global: lo forman únicamente cuentas de dominio. Aunque los grupos globales pueden usarse para asignar permisos a los recursos, su funcionalidad principal es agrupar las cuentas de un dominio. Para lo primero es mejor añadir los grupos globales como locales.

NT crea por defecto ciertos grupos locales - con ciertos derechos ya adquiridos, globales y de sistema. Los grupos locales que existen por defecto en cualquier máquina NT son:

Usuarios: Usuarios normales con cuenta.

Administradores: Usuarios con derechos para administrar el sistema.

Invitados: Usuarios sin cuentas que tienen derechos muy limitados.

Operadores de copia de seguridad: Usuarios con derechos de copia de seguridad y restauración de archivos.

Si es servidora de dominio, además de los anteriores grupos locales, NT crea:

Operadores de cuentas: Usuarios con derechos para administrar cuentas de usuarios.

Operadores de servidores: Usuarios con derechos para administrar servidores.

Operadores de impresión: Usuarios con derechos para administrar impresoras

y los siguientes grupos globales:

Admins de dominio

Usuarios de dominio

Invitados de dominio

Los usuarios se convierten en miembros de los grupos de sistema automáticamente al acceder a la red. Los grupos de sistema en cualquier máquina NT son:

TODOS: incluye a todos los usuarios que acceden a la red. No se puede controlar quién pertenece a este grupo, pero sí los permisos y derechos de este grupo.

CREATOR OWNER (propietario): usuario que creó el recurso o es propietario del mismo.

Es conveniente revisar qué derechos tienen todos estos grupos por defecto dentro del menú de políticas de derechos de usuarios

POLÍTICAS DE PASSWORDS Y CUENTAS

El administrador de la red debe establecer una política de passwords en la que se especifique:

Una duración máxima de la contraseña (aconsejable unos 90 días).

Una longitud mínima (aconsejable un mínimo de 8 caracteres).

Un histórico de la contraseña (unos 5 passwords).

Un bloqueo automático tras sucesivos fallos de login (unos 5 fallos de login).

La política se establece dentro del menú de Administrador de usuarios para dominios->Directivas->Cuentas->Plan de cuentas

Para desbloquear una cuenta, acceder dentro del menú de:

Administrador de usuarios para dominios->Usuario->Propiedades->Cuenta desactivada

También es útil establecer en el **Administrador de usuarios para dominios** restricciones de:

- Horas de login al dominio.
- Estaciones desde las que se puede acceder al dominio.
- Expiración de la cuenta si es temporal.
- Restricción de acceso dial-in.

así como templates para las cuentas de nueva creación.

PERMISOS Y DERECHOS DE USUARIO

Los **derechos de usuario** definen qué pueden hacer los usuarios . Algunos de los derechos más comunes son:

El derecho de inicio de una sesión local.

Derechos de administración de auditoría.

Derecho de apagar el equipo.

Derecho de acceder al equipo desde la red (Log On).

Derecho de hacer copias de seguridad o de recuperación de ficheros.

Para configurar los derechos de usuarios , se elige *Derechos de usuarios* del menú *Directivas* del *Administrador de usuarios de Dominio* y se autorizan para cada derecho los usuarios o grupos apropiados.

Hay que tener en cuenta que:

Es conveniente eliminar al grupo TODOS el derecho de LogOn (acceso desde red)

Los *permisos* definen qué recursos pueden usar los usuarios o grupos de usuarios , entendiendo por recurso un fichero, directorio o una impresora. Los permisos controlan el acceso a directorios y ficheros locales, y compartidos en la red y son configurados por el administrador o por el propietario de los mismos. Hay permisos estándar y permisos individuales. Los permisos estándar son una combinación de los permisos individuales.

Permisos para directorios

Permisos estándar	Permisos individuales	Permisos para nuevos ficheros
Sin acceso	Ninguno	Ninguno
Listar	R,X	-
Lectura	R,X	R,X
Añadir	W,X	-
Añadir y Lectura	R,W,X	R,X
Cambio	R,W,X,D	R,W,X,D
Control total	Todo	Todo

Permisos para ficheros

Permisos estándar para archivos	Permisos individuales
Sin acceso	Ninguno
Lectura	R,X
Cambio	R,W,X,D
Control total	Todos

En un sistema de ficheros NTFS, el administrador puede configurar los permisos de ficheros y directorios pulsando con el botón derecho del ratón sobre el fichero o directorio que se que desee proteger, y luego la secuencia:

propiedades -> seguridad -> permisos .

NOTA: *¡¡¡Cuando se formatea un volumen con NTFS, el grupo TODOS adquiere Control Total del volumen!!!*

Así, los directorios *systemroot* (normalmente *C:\winnt*), *systemroot\system32* y *systemroot\temp*, tienen derechos de CONTROL TOTAL , CAMBIO Y CONTROL TOTAL respectivamente al grupo TODOS.

Para corregirlo, una vez comprobado que el ADMINISTRADOR tiene CONTROL TOTAL sobre los mismos, cambiar a sólo LECTURA *systemroot* sin propagar estos cambios a los subdirectorios, y *systemroot\system32* a sólo LECTURA propagándolos, con la precaución de poner permiso de CAMBIOaTODOS a *\winnt\system32\RAS \winnt\system32\spool\Printer*.

De la misma manera, el volumen C: donde se encuentran ficheros relacionados con el arranque de la máquina, debería ser formateado NTFS y los ficheros críticos deberían tener:

C:\boot.ini -> Control total para Administradores y Sistema.

C:\ntdetect.com -> Control total para Administradores y Sistema.

C:\autoexec.bat -> Control total para Administradores y Sistema y Lectura a Todos.

C:\config.sys -> Control total para Administradores y Sistema y Lectura a Todos.

COMPARTICIÓN DE RECURSOS DE RED

Para compartir recursos a la red solo tendremos que pinchar con el botón derecho sobre un directorio o una impresora y veremos una opción que será compartir. Nos aparecerá un menú desde donde podremos compartir el recurso. Pulsaremos ahora en permisos...

Los recursos de la red se comparten de forma segura con los siguientes permisos:

CONTROL TOTAL: permite modificar permisos, tomar en propiedad y permisos de CAMBIO

CAMBIO: permite crear directorios, añadir ficheros, modificar datos y permisos de éstos, borrar ficheros y directorios, y permisos de READ.

LECTURA: permiten listar directorios, ficheros.

SIN ACCESO: este permiso sobreescribe cualquier otro y deniega el acceso al recurso.

NOTA!!! : estos permisos sólo son efectivos cuando se hace login en la red; en nada influyen si el usuario accede localmente. Para los accesos locales se usan los permisos NTFS. El grupo TODOS tiene asignado automáticamente CONTROL TOTAL ante cualquier recurso compartido. Nunca debe pues compartir directorios que contengan información crítica del sistema.

A diferencia de los permisos NTFS, no se pueden asignar diferentes permisos a distintos ficheros de un mismo directorio compartido.

Cuando se combinan los permisos de recursos compartidos y los permisos en un volumen NTFS, prevalece el más rectrictivo.

SEGURIDAD DEL REGISTRO

El registro es una base de datos que mantiene información sobre la configuración hardware, software y de entorno de la máquina. Se puede ver con REGEDT32. Windows NT 4.0 no permite el acceso remoto al registro por defecto. Es conveniente pues:

Deshabilitar el acceso remoto al registro, chequeando la existencia de la siguiente entrada en el registro:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

Deshabilitar (poner a 0) si es necesario el apagado del equipo en la opción *ShutdownWithoutLogon* de:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Proteger adecuadamente el registro de usuarios no autorizados.

Hacer copias periódicas del mismo con la utilidad REGBACK.EXE

AUDITORÍAS.

El *Sistema de auditorías* de Windows NT permite rastrear sucesos que ocurren en una máquina NT, servidor de dominio o estación o servidor NT . Las auditorías son esenciales para mantener la seguridad de los servidores y redes. Permiten un seguimiento de las actividades realizadas por los usuarios .

La política de auditorías se establece en cada máquina NT. Se pueden realizar tres tipos de auditorías en NT:

a) Auditoría de cuentas de usuario: rastrea los sucesos de seguridad y escribe apuntes en el registro de seguridad. Se activa en *Administrador de usuarios en dominios -> Directivas -> Auditoría*. PLAN DE AUDITORIAS.

Los eventos que se pueden auditar son:

Logon y logoff en la red

Acceso a ficheros , directorios o impresoras

Ejercicio de los derechos de un usuario

Seguimiento de procesos

Tirada o arranque del sistema...

b) Auditoría del sistema de archivos: rastrea sucesos del sistema de archivos. Se activa esta opción en *Propiedades*, tras pulsar con el botón derecho sobre el fichero o directorio que se desee auditar y luego seleccione *Seguridad -> Auditorías*.

Los eventos que se pueden auditar son: LECTURA, ESCRITURA, EJECUCIÓN, ELIMINACIÓN, CAMBIO DE PERMISOS Y TOMA DE POSESIÓN.

Para auditar ficheros y directorios, éstos deben estar localizados en un volumen NTFS.

c) Auditoría de impresoras: primero se establece la política de auditorías haciendo doble click en la impresora en cuestión, dentro del menú *Impresoras*, y luego seleccionar *Seguridad -> Auditorías*.

Algunos de los eventos que se pueden auditar son: uso de la impresora, cancelar trabajos de impresión, control total de la impresora...

Se debe tener derechos de administrador para configurar propiedades de auditoría.

Una vez que se activa una auditoría se utiliza el *Visor de sucesos* dentro de *Herramientas administrativas* para ver los eventos auditados.

Se debería tener cuidado y proteger los archivos de auditoría que están almacenados en el directorio *\winnt\system32\CONFIG* en los archivos:

APPEVENT.EVT : Registro de sucesos en aplicaciones.

SECEVENT.EVT : Registro de sucesos de seguridad.

SYSEVENT.EVT : Registro de sucesos del sistema.

Algo **muy importante** a la hora de mirar los registros es que la máquina tenga la hora correcta, ya que si tenemos que comparar con los registros de otras máquinas, si ambas no están sincronizadas será muy difícil. Para esto podemos usar NTP (Network Time Protocol)

SEGURIDAD DE LOS PROTOCOLOS. SEGURIDAD DE LOS SERVICIOS.

Debemos usar solo los protocolos que vayamos a necesitar. En principio y salvo que tengamos necesidad de usar más protocolos, podríamos dejar solo dos:
NetBEUI
TCP/IP
Con estos dos protocolos son solo de dos tipos los servicios que estamos ofreciendo a la red:
SMB: (**B**loques de **M**ensajes de **S**ervidor) de Microsoft que son servicios de archivos y red. Estos servicios están instalados por defecto normalmente.
Servicios TCP/IP e Internet como servidores Web y FTP. Se pueden instalar de modo opcional.
Estos son algunos de los puertos TCP/IP que podemos instalar en una máquina NT:

Servicio / Puerto / Protocolo	Descripción
FTP / 21 / tcp	Servidor FTP.
SMTP / 25 /tcp	Gestiona la distribución del correo de la máquina.
DNS / 53 / tcp-udp	Servidor de nombres (DNS)
GOPHER / 70 / tcp	Sistema de indexación de los servidores FTP (obsoleto)
HTTP (WWW) / 80 / tcp	Servidor WWW
POP2 / 109 / tcp	Servidor de correo Pop versión 2
POP3 / 110 / tcp	Servidor de correo Pop versión 3
NEWS / 119 / tcp	Servidor de News
NETBIOS / 137-138-139 / tcp-udp	Windows for Workgroups

Conviene tener abiertos el menor número de servicios. Al ser estos opcionales, no vienen instalados por defecto y hay que instalarlos a posteriori. Salvo que se necesiten y que se sepa lo que se está haciendo, conviene no instalar ninguno.
También se pueden configurar las opciones de seguridad TCP/IP para permitir o bloquear la dirección del (los) puerto(s) que se necesiten según los servicios que se quieran ejecutar. Para hacer esto, siga la siguiente secuencia:
Panel de Control -> Red -> Protocolos -> Protocolo TCP/IP -> Propiedades -> Avanzadas
Marque: *Activar seguridad*
Pulse el botón *Configurar*
Seleccione el adaptador correspondiente y marque el número de puerto/s del servicio/s que quiera permitir.

SERVICE PACK

Los Service Pack (SP) no son más que un conjunto de parches que Microsoft saca de vez en cuando para solucionar fallos, bugs, dar nuevas funcionalidades, etc... Lo bueno de estos parches es que de una sola vez aplicas todos (a veces más de 100) rápida y fácilmente.
Todo NT debería tener instalado al menos el SP5. En la actualidad ya ha salido el SP6a. La versión española del SP6a también está disponible.
IMPORTANTE: Nunca instalar un SP en ingles en un NT en español. Nos causará un sinfín de problemas y en algunos casos habrá que reinstalar el sistema.
El sitio web donde conseguira los ultimos Service Pack es:
http://www.microsoft.com/ntserver/nts/downloads/

IMPORTANTE

- No conviene que NT esté instalado en una máquina con arranque dual, ya que esto haría que muchas de sus garantías de seguridad perdieran efectividad.

- Es casi obligado que la partición sea NTFS, no encontraremos ninguna razón para instalar NT en una partición FAT.

- Conviene dar a cada uno de los usuarios del sistema unas ciertas normas sobre el uso de la máquina que podría empezar con la frase de "Todo lo que no esta explícitamente permitido, esta prohibido" y continuar explicando todo lo que está permitido. Si se dejan las cosas claras desde un principio, no ahorraremos muchos quebraderos de cabeza.

- Administrador no hay más que uno. Aunque NT permite que haya varios administradores para tareas determinadas, es muy importante delimitar estas tareas al máximo si son de una persona las que administran la máquina. A medida que el número de administradores tiende a infinito, la funcionalidad en la máquina tiende a cero.

- Los usuarios *solo* deben tener los privilegios necesarios para ser usuarios. En un exceso de celo, podemos cometer el error de limitar demasiado los privilegios de los usuarios. Esto hace que el usuario no pueda usar la máquina normalmente y perdamos de vista el objetivo por el que hacemos todo esto. Por otro lado, si los usuarios tienen excesivos privilegios (algunos administradores irresponsables lo permiten para no tener que hacer las cosas ellos y que las hagan los usuarios) nos podemos encontrar que por desconocimiento, experimentación o maldad se cause daño al sistema.

- Una buena política de passwds es conveniente, obligar a cambiar el passwd cada 3 meses, chequear las passwd de los usuarios contra diccionarios para encontrar passwds fáciles, no dejar repetir passwds, etc.

Por último decir que esta guía no es por supuesto exhaustiva, así que donde esta no llegue, puede pedir más información a atención@ula.ve . De todas formas recomendamos como receta general, una búsqueda exhaustiva de información, una buena dosis de sentido común y un pellizco de paranoia

RECURSOS EN LA WEB

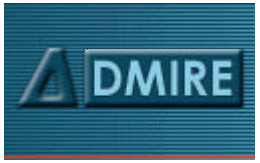
Pagina Principal de Microsoft Win NT Server:
http://www.microsoft.com/ntserver/default.asp

Pagina Principal de Win Nt Workstation:
http://www.microsoft.com/ntworkstation/default.asp

Windows NT, Recursos e Información:
http://www.infosyssec.com/infosyssec/winnt1.htm

Guia del Registro de Windows:
http://www.regedit.com/

Win NT FAQ
http://www.ntfaq.com/



Referencia Rápida de Seguridad en Windows NT

La intención principal de esta Referencia Rápida, es constituirse en un punto de partida para mejorar la seguridad de su sistema y buscar información más profunda al respecto. No puede reemplazar de modo alguno, la lectura exhaustiva de la abundante documentación ya existente, sobre la seguridad de los sistemas basados en Windows NT.