Informe práctica 2
Usuarios y protección en Windows 2000

Alejandro Samarín Pérez - alu3862
José Lucas Grillo Lorenzo - alu3181

22 de mayo de 2011

Resumen

El objetivo de la práctica consiste en familiarizarse con la gestión de usuarios y protección en Windows 2000. Para ello, se plantea una organización ficticia a la que hay que dotar con un sistema de cuentas y de seguridad a nivel de recursos.

Parte I
Configuración previa

Previamente a la resolución de esta práctica hubo que realizar una serie de procesos para configurar correctamente el servidor W2K3:

1. Establecer el nombre de dominio del servidor a aso11.org
2. Cambiar la IP DNS primaria a 10.0.2.15
3. Instalar el servicio DNS en el servidor a través de los componentes de Windows
4. Herramientas administrativas→DNS→ Agregar zonas en resolución forward y reverse
5. Instalar el Active Directory, y activarlo mediante el comando *dcpromo*.

Parte II
Organización del dominio

Para mantener un cierto orden en la aplicación de permisos y futuras políticas de grupos, se han definido tres unidades organizativas, una por cada proyecto (Auditorio, Aeropuerto y Parque). Dentro de cada una de las OU, se han creado dos grupos locales (directores y participantes) a los que les serán concedidos o revocados los permisos pertinentes, y cuyos únicos miembros son los grupos globales correspondientes. Además, se ha incluido otro grupo local para los ejecutivos cuyo único miembro es el grupo global del mismo nombre.

La finalidad que esto tiene es implementar una estructura de directorio adaptada a posibles ampliaciones del esquema de la organización; en el caso de que la organización conste de varios dominios y no sólo de uno, como es el caso que se trata aquí, será posible establecer permisos sobre los grupos locales que controlan los recursos y dar así acceso a los usuarios de la organización que sean miembros de los grupos globales que están incluidos a su vez en los grupos locales.

Parte III

Resolución de requisitos de la organización

Se pasa a continuación a listar las exigencias a implementar en el Active Directory y seguidamente la ruta de ventanas/pestañas seguida para configurarlos, o una pequeña descripción de los pasos realizados para esta tarea:

a) Sistema

- Cualquier usuario debe poder apagar el sistema
Admin Tools → Default Domain Security Settings → Local Policies → User Rights Assignment → Shut down the system

- Los usuarios tienen restringidas las horas de acceso al sistema
Admin Tools → Active Directory Users and Computers → (Click derecho sobre el usuario en cuestion) → Properties → Pestaña account → Logon hours

También se ha optado por automatizar esta tarea tediosa mediante un VBScript que invoca al comando 'net user' (Ver anexos).

b) Contraseñas

- A fin de facilitar la gestión, asignar como contraseña el nombre del usuario
Admin Tools → Active Directory Users and Computers → (Click derecho sobre el usuario en cuestion) → Reset password

- Los usuarios deben cambiar las contraseñas cada tres meses
Admin Tools → Default Domain Security Settings → Account Policies → Password Policy → Maximum password age → 90 days

- Los usuarios no pueden cambiar las contraseñas hasta 2 semanas después de haberla cambiado
Admin Tools → Default Domain Security Settings → Account Policies → Password Policy → Minimum password age → 14 days

- No se permiten contraseñas en blanco. Longitud mínima: 4 caracteres
Admin Tools → Default Domain Security Settings → Account Policies → Password Policy → Minimum password length → 4 characters

- La nueva contraseña no debe coincidir con las dos últimas introducidas por el usuario
Admin Tools → Default Domain Security Settings → Account Policies → Password Policy → Enforce password history → 2 passwords remembered

- Si se producen 4 intentos de autenticación fallidos a una cuenta de usuario en un intervalo de 10 minutos, ésta debe quedar permanentemente bloqueada
Admin Tools → Default Domain Security Settings → Account Policies → Account Lockout Policy → Account lockout threshold → 4 invalid logon attempts

Admin Tools → Default Domain Security Settings → Account Policies → Account Lockout Policy → Account lockout duration → 0 (Permancece bloqueada hasta que el administrador intervenga)

Admin Tools → Default Domain Security Settings → Account Policies → Account Lockout Policy → Reset account lockout counter after → 10 minutes

- Deben quedar registrados los intentos fallidos de entrada en el sistema

Admin Tools → Default Domain Security Settings → Local Policies → Audit Policy → Audit account logon events → Define these policy settings → Marcar "Failure"

Se realiza el mismo paso en "Default Domain Controller Security Settings" para evitar que entren en conflicto las políticas de seguridad del dominio y las políticas de seguridad del controlador de dominio.

c) Directorio privado de los usuarios

- Todo usuario debe disponer de un directorio propio a partir del directorio \home del servidor, cuyo nombre coincida con el de la cuenta del usuario. El usuario podrá acceder automáticamente a este directorio a partir de la unidad N: desde cualquier máquina del dominio.

- En este directorio, el usuario debe tener control total

- El resto de los usuarios no podrá tener ningún tipo de acceso sobre este directorio

Crear directorio "C:\home" → (Click derecho) → Sharing and security → Pestaña Sharing → Share this folder → Permissions → Full control for Everyone (permisos de red)

De nuevo click derecho → Propiedades → Pestaña security → Advanced → Desmarcar "Allow inheritable permissions..." → Remove en el cuadro de diálogo

Admin Tools → Active Directory Users and Computers → (Click derecho sobre el usuario en cuestión) → Properties → Pestaña Profile → Home folder → Connect N: to \\ORD11\home\empleX

(No hace falta crear la carpeta del empleado previamente)

d) Proyectos de la organización.

- Cada proyecto dispondrá de un directorio para almacenar la información relativa al mismo bajo el directorio \proyectos. Cada usuario podrá acceder automáticamente a los proyectos en los que participe a partir de las unidades p:, q:,... desde cualquier máquina del dominio

Se crea una carpeta 'proyectos' en C:\ , y se le da "Full Control" a "Everyone" en permisos de red. En los permisos NTFS de 'proyectos' se permite acceso exclusivamente a los administradores, y se desactiva la herencia de permisos como con la carpeta 'home'. Dentro de la carpeta 'proyectos', se crean dentro tres carpetas, una por proyecto. Se le da acceso por NTFS a cada unidad organizativa responsable de su proyecto.

Para que los usuarios puedan acceder automáticamente a los proyectos, en "C:\Windows\SYSVOL\sysvol\aso11.org\scripts se guarda el siguiente script batch (unidades_proyectos.bat):

```
@echo off

net use p: \\ord11\proyectos\auditorio
net use q: \\ord11\proyectos\aeropuerto
net use r: \\ord11\proyectos\parque
```

A continuación, para cada usuario se repiten los mismo pasos:

Active Directory Users and Computers → Click Derecho sobre el usuario → Properties → Pestaña Profile → Logon Script → unidades_proyectos.bat (sin rutas, solo nombre y extensión)

Esto es automatizable mediante el uso del script "xcacls.vbs" para los permisos NTFS y el comando "net user" para los permisos de red.

- Todos los usuarios que participan en un proyecto deben tener la posibilidad de leer y modificar los archivos que forman parte del proyecto

Se agregan a los participantes y directores de cada proyecto como grupos privilegiados en sus respectivas carpetas de proyectos. A los participantes se les da permiso de 'Modificar' y 'Lectura'.

- Los usuarios no podrán crear ni borrar archivos del proyecto. Esta función la realizará el director del mismo

Dentro de las propiedades de cada proyecto → Security → Advanced → Pinchar sobre participantes → Edit.

Se crearán dos permisos por cada participante y carpeta de proyecto. Para los permisos sobre las carpetas y subcarpetas se selecciona en 'Apply onto' 'This folder and subfolders', y se desmarca 'Create Folder' y 'Create Files' y ambos 'Delete (...)' ('Write atributes', 'Read Attributes', 'List Folder/Read Data', 'Traverse Folder/Execute File' se dejan marcados).

Para los permisos sobre archivos, se selecciona 'Files only' en 'Apply onto', y se repiten los permisos anteriores pero marcando ahora 'Write Data' y 'Append Data'.

En cuanto a los directores, véase la sección ***f***.

e) Usuarios de la organización

- Los usuarios implicados en los proyectos tendrán restringida la hora de acceso al sistema
Véase sección ***a***, punto 2.

- Les debe ser asignado un perfil flotante que no puedan modificar
Para ello, la manera más eficiente es crear primero un usuario "por defecto" y loguearse en su cuenta. A continuación, tras instalar los programas de usuario pertinentes o ajustar cualquier otro parámetro con el que se desea que cuenten los usuarios, se copia este perfil a alguna carpeta compartida del servidor (C:\netlogon\default por ejemplo). Para realizar esta acción, se siguen los sigiuentes pasos: Start → Control Panel → System → Advanced → User Profiles → Settings → Copy To → C:\netlogon\default.

En esta carpeta, se ha de cambiar la extensión del archivo "ntuser.dat" a "ntuser.man", para indicar que es un perfil mandatorio. Ahora, en "Active Directory Users and Computers, se seleccionan todos los usuarios a la vez y se ejecuta click derecho → Properties → Account → Cambiar 'Profile path' y hacer que apunten todos al perfil de este usuario ('\\ORD11\default'). Los cambios en los perfiles de los usuarios se pueden automatizar con el comando "net user" (Ver script "config_cuentas.vbs").

f) Directores de los proyectos

- Tienen control total sobre los archivos del proyecto que dirigen
Dentro de las propiedades de cada proyecto → Security → Pinchar sobre el grupo de directores → y marcar 'Full Control', para así dar permisos totales a los directores de su correspondiente proyecto.

g) Ejecutivos de la organización

Se crea un nuevo grupo "Ejecutivos", y se le incluyen los ejecutivos correspondientes.

- Podrán acceder a cualquiera de los directorios de los proyectos en curso
Se crea un nuevo script en SYSVOL que mapee 'p:' a 'C:\proyectos', asignándoselo a los ejecutivos en el campo 'Logon script' como fue explicado anteriormente.

- Pueden leer la información de estos proyectos
Desde la carpeta raíz de 'proyectos' se añade un nuevo permiso de lectura y ejecución para el grupo ejecutivos (que será subsecuentemente heredado por las carpetas de todos los proyectos).

- No pueden alterar dicha información
En el punto anterior, al especificar los permisos del grupo ejecutivos sobre la carpeta proyectos, se le indica que no pueden cambiar los permisos de dicha carpeta.

h) Resto de usuarios

- No dispondrán de ningún derecho de acceso a los directorios de los proyectos

Por defecto el resto de usuarios no tienen permiso alguno para acceder a las carpetas compartidos, puesto que no se han dado permisos para 'Everyone' a ningún recurso de los administrados. Esta opción es preferible a denegar explícitamente el acceso a todos los usuarios ajenos a la organización, puesto que sería una opción menos eficiente y más propensa a dar problemas.