Introducción

La administración de seguridad basada en grupos es más sencilla y rápida que la basada en objetos individuales. En esta práctica trabajaremos con objetos del tipo Grupo.

Objetivos

1. Entender el concepto de Grupo, ámbito de grupo y nivel funcional.
2. Saber administrar grupos de distintos ámbitos del dominio

Notas de ayuda

Necesitamos:

- Máquina virtual con Windows 2012 Server con DA y usuarios creados en prácticas anteriores que usaremos como miembros de nuestros grupos.
- Máquina virtual con Windows para conectarnos al dominio como cliente.

Recuerda:

Un grupo de usuarios permite establecer permisos y restricciones a todos los miembros del grupo de una vez.

De forma análoga a las cuentas de usuario, una cuenta de grupo posee un nombre y un identificador interno o SID, además de una lista de los usuarios que pertenecen a dicho grupo.

Existe una serie de grupos integrados: Administradores, Operadores de Copia, Usuarios Avanzados, Usuarios, e Invitados.

- El **grupo Administradores** recoge a todos aquellos usuarios que deban poseer derechos administrativos completos. Inicialmente posee un solo usuario, el Administrador.
- El **grupo Usuarios** son los usuarios normales del sistema. Tienen permisos para conectarse al sistema interactivamente y a través de la red.
- **Operadores de copia**. Estos usuarios pueden hacer (y restaurar) una copia de todo el sistema.
- **Usuarios avanzados**. Son usuarios con una cierta capacidad administrativa. Se les permite cambiar la hora del sistema, crear cuentas de usuario y grupos, compartir ficheros, etc.

Al crear las cuentas de los usuarios, podemos hacer que cada una pertenezca al grupo (o grupos) que consideremos conveniente.

Se define una serie de grupos especiales, cuyos miembros no se establecen de forma manual, sino que son determinados de forma dinámica y automática por el sistema. Estos grupos se denominan genéricamente identidades especiales (special identities) y se utilizan normalmente para facilitar la labor de establecer la protección del sistema. De entre estos grupos, destacan:

- **Usuarios Interactivos** (Interactive) representa a los usuarios que tienen el derecho de iniciar sesión local en la máquina.

- **Usuarios de Red** (Network). Usuarios que tienen el derecho de acceder al equipo desde la red.
- **Todos** (Everyone). Agrupa a todos los usuarios que el sistema conoce. Puede agrupar a usuarios existentes localmente y de otros sistemas (conectados a través de la red). A partir de Windows Server 2003, este grupo no incluye las conexiones anónimas (sin aportar usuario y contraseña).
- **Usuarios autentificados** (Authenticated Users). Usuarios que poseen una cuenta propia para conectarse al sistema. La cuenta de "invitado" pertenecen a "Todos" pero no a "Usuarios autentificados".

Windows Server define dos conceptos distintos y complementarios: el concepto de derecho y el concepto de permiso, respectivamente.

- Un **derecho o privilegio de usuario** (user right) son la habilidad de hacer determinadas tareas, por ejemplo, Backup. (Qué). Son atributos de un usuario (o grupo) que le permite realizar una acción.
- Un **permiso** (permission) es una característica de cada recurso (carpeta, archivo, impresora, etc.) del sistema, que concede o deniega el acceso al mismo a un usuario/grupo concreto. (quien) Cada recurso del sistema posee una lista en la que se establece qué usuarios/grupos pueden acceder a dicho recurso, y con qué tipo de acceso (lectura, modificación, ejecución, etc.).

En el DA pueden crearse dos tipos de grupos: grupos de distribución y grupos de seguridad. Los primeros se utilizan exclusivamente para crear listas de distribución de correo electrónico, mientras que a los segundos se les pueden asignar permisos, y por tanto son los que se utilizan con fines administrativos.

El ámbito de un grupo define sobre qué recursos se asignan los permisos y para qué miembros

En concreto, en dominios Windows Server 2012 los grupos de seguridad pueden definirse en tres ámbitos distintos: Grupos locales de dominio, grupos globales y grupos universales:

- **Grupos globales**: permiten asignar permisos a recursos de cualquier dominio a miembros sólo del dominio del que fue creado. A menudo se utilizan para reunir los usuarios y equipos del mismo dominio que comparten el mismo trabajo o función dentro de la empresa y necesitan el mismo tipo de acceso a los recursos.
- **Locales de dominio**: permite aplicar permisos a recursos del dominio donde fue creado a miembros de cualquier dominio. Pueden incluir a miembros de cualquier dominio del bosque y de los dominios de confianza de otros bosques.
- **Grupos universales**: Recursos y miembros de cualquier dominio

Trabajo a realizar:

Enunciado

En esta práctica se van a crear y configurar cuentas de grupo en el dominio. Abrir la consola **Usuarios y equipos de Active Directory** y sigue los pasos indicados:

-Proceso a seguir:

1. Vamos a ver el nivel funcional del DA:
    a. Selecciona el contenedor del dominio y en el menú contextual selecciona Elevar el nivel funcional del dominio…
    b. ¿Qué nivel funcional tiene?
    c. Puede elevar más el nivel funcional
2. En el contenedor **Users** vamos a crear dos grupos globales denominados "Funcionarios" y "Mecanógrafas", para ello:
    a. Con el botón derecho pulsa el contenedor Users y selecciona Nuevo y luego Grupo.
    b. Teclea "Funcionarios" como nombre del grupo y selecciona el ámbito de grupo Global y el tipo de grupo Seguridad.
    c. Repite los pasos para el grupo "Mecanógrafas"
3. Vamos a incluir en los grupos a los usuarios miembros. En primer lugar, vamos a hacerlo con los "Funcionarios", cuyos miembros van a ser los agentes del contenedor "Agentes":
    a. Sobre el grupo en cuestión, selecciona en el menú contextual Propiedades.
    b. Rellena la descripción con: "Funcionarios Agentes del dominio".
    c. En la pestaña "Miembro", pulsa Agregar… y en el cuadro Seleccionar Usuarios, Contactos, Equipos o Grupos:
        i. En Tipos de objetos, marca la opción Usuarios.
        ii. En Ubicaciones, selecciona dentro del dominio el contenedor "Usuarios agentes" y pulsando en Avanzadas… pulsa Buscar ahora. Aparecerán los dos usuarios creados en la práctica sobre Usuarios
        iii. Selecciona a los dos usuarios (manteniendo pulsada la tecla Control) y Acepta.
        iv. Aparecerán en la ficha Miembros, presiona Aceptar.
        v. Comprueba que cada usuario se ha añadido al grupo, en Propiedades del usuario, en la ficha "Miembro de".
4. Para agregar las secretarias al grupo "Mecanográficas" hazlo de la siguiente forma:
    a. Abre el contenedor "Secretarias" y selecciona simultáneamente a los dos usuarios (Ofelia y La dulce Irma)
    b. Pulsa el botón derecho sobre la selección y, a continuación, Agregar a un grupo
    c. Localiza el grupo "Mecanográficas" y Acepta.

d. Por último, añade una descripción al grupo, por ejemplo: “Personal administrativo del dominio”.

5. Crea una nueva unidad organizativa llamada, Vigilantes.

6. Crea ahora un grupo con ámbito de dominio local y tipo de grupo seguridad en el contenedor recién creado, denominado “Investigadores casos Agencia”, con la descripción siguiente: “Investigadores del caso La Misión Intergaláctica Espacial Rebóllez”. Después de crear el grupo, abre sus propiedades. Muestra información del grupo creado.Incluye en el grupo creado a los “Agentes” y, además, a los usuarios “El Superintendente Vicente” y “Saturnino Bacterio”.

7. Vamos a configurar los permisos de esos grupos y usuarios implicados en el dominio sobre una carpeta compartida en red con documentos del caso, denominada “CASOS NUEVOS”, que se va a encontrar en la ruta: “c:\”:

   a. Crea la carpeta “CASOS NUEVOS” en la unidad indicada.

   b. Edita las Propiedades de la carpeta y comparte la carpeta:

      i. Recurso compartido: “CASOSNEWS”.

      ii. Comentario del recurso compartido: “Documentos e informes de los casos nuevos de la Agencia”.

      iii. En el botón “Permisos” quita al grupo Todos y añade al grupo “Investigadores caso Agencia”.

      iv. Permite al grupo el acceso al recurso sólo para Leer.

   c. Fíjate que los permisos que hemos fijado son sólo para el acceso a la carpeta compartida a través de la red para el grupo “Investigadores principales del caso Agencia”. Ahora comprueba los permisos de esa carpeta como recurso local (en la ficha Seguridad). ¿Quiénes pueden leer los documentos, además de los miembros del grupo en cuestión si inician sesión interactiva?

   d. Antes de terminar, añade un agente nuevo al contenedor “Agentes”, nombre y apellidos “Rompetechos Gafotas”, nombre de inicio de sesión y contraseña “rompetechos”, además “el usuario no puede cambiar la contraseña”.