Síntesis conceptual

Grado: Administración de Sistemas Informáticos en Red
Asignatura: Implantación de Sistemas Operativos
Unidad: 8, Directivas de seguridad y auditorías

Resumen

Las directivas de seguridad de Windows se dividen en dos tipos, directivas de seguridad local, a las que se accede usando los siguientes pasos:

Menú de inicio → Herramientas administrativas → Directivas de seguridad local

Las otras directivas son las directivas de seguridad de dominio, a las que se accede mediante los siguientes pasos:

Inicio → Herramientas administrativas → Administración de directivas de grupo

Dentro de estas últimas, existen las directivas de seguridad del controlador de dominio.

Las directivas de grupo, a las que se suelen llamar GPO, por su nombre en inglés, son las siguientes:

- Directiva de equipo local.
- Directiva de usuario local.
- Directiva de grupo del sitio.
- Directiva de grupo del dominio.
- Directiva de grupo de la unidad organizativa.
- Directiva de grupo del controlador de dominio

Dentro de cada directiva, cuando vamos a crearla o editarla, tenemos dos grupos fundamentales: **configuración del equipo** y **configuración de usuario.** Por defecto, en Windows Server tenemos las siguientes directivas de grupo: ***Default Domain Policy*** y ***Default Controller Domain Policy***. Para crear una directiva de grupo, lo más normal es crearla automáticamente vinculada a un objeto del AD. Dentro del **Administrador de directivas de grupo**, además de crear GPO, podemos:

- Cambiar el orden de actuación de cada GPO.
- Evitar que se anulen las peticiones de una directiva por otras.
- Modificar los permisos de alguna de las directivas de grupo.
- Visualizar las siguientes propiedades de una GPO:
    - **Ámbito.**
    - **Detalles.**
    - **Configuración.**
    - **Delegación.**

Las auditorias que tratan de monitorizar sucesos en relación con la seguridad del sistema se configuran por las directivas de auditoría, las cuales pueden ser para los siguientes casos:

- Auditar el acceso a objetos.
- Auditar el acceso al servicio de directorio.
- Auditar el cambio de directivas.
- Auditar el seguimiento de procesos.
- Auditar el uso de privilegios.
- Auditar eventos de inicio de sesión de cuenta.
- Auditar eventos del sistema.
- Auditar la administración de cuentas.

Estas directivas de auditorías se establecen sobre GPO ya creadas previamente. Se puede además auditar el acceso a objetos, para ello, en el descriptor de seguridad contamos con una lista de control de acceso al sistema o SACL, es común que se basen en el atributo **Acierto o Error** para determinar esta auditoría. Para auditar el acceso a archivos y carpetas, debemos de tener activadas las directivas de auditoría: **Auditar el acceso a objetos** y **Auditar el acceso al servicio de directorio**. Por último, si lo que queremos es comprobar los sucesos que han registrados las auditorías, nos dirigiremos al **Visor de eventos**.

Conceptos fundamentales

- **Directiva de seguridad:** serie de normas donde se refleja el comportamiento que debe de tener el equipo o usuario en temas referentes a la seguridad del sistema.
- **GPO**: directivas específicas del sistema que nos ayudan a identificar una serie de normas para reforzar la seguridad del equipo y del usuario, afecta a todos los objetos del dominio.
- **Administración de directivas de grupo:** herramienta incorporada en el sistema para poder administrar las GPO del dominio.
- **Ámbito de una GPO:** se trata del recorrido que tiene la GPO, es decir, a que aplica y en qué modo.
- **Auditoría**: sistema usado para la monitorización de los sucesos del sistema en relación con la seguridad de este.
- **Sucesos de seguridad**: son las acciones ocurridas sobre el sistema que implican un posible problema con la seguridad de la información.
- **Directiva de auditoría:** nos indica sobre que sucesos de seguridad van a actuar ciertas auditorías, es decir, que se va a auditar.
- **Procesamiento de una directiva:** modo de ejecución de una directiva.
- **Descriptor de seguridad:** sistema de almacenamiento de información acerca de la seguridad del objeto en cuestión.
- **Visor de eventos:** herramienta nativa de Windows donde ver todos los registros acerca de lo sucedido en el sistema.