Grupo 5

**Actividades relacionadas a la inteligencia de negocios**

**Introducción a la administración de recursos**

La administración de *cuentas de usuario* y *grupos* es una parte esencial de la administración de sistemas dentro de una organización.

La razón principal para las cuentas de usuario es verificar la identidad de cada individuo utilizando un computador. Una razón secundaria (pero aún importante) es la de permitir la utilización personalizada de recursos y privilegios de acceso.

**Administración de grupos**

Windows también permite que la administración de usuario mediante grupo. Esto significa que puede definir grupos de usuarios con el mismo tipo de permisos, organizándolos en categorías.

Un grupo es un conjunto de cuentas de usuario. Un usuario que se agrega a un grupo obtiene todos los permisos y derechos de ese grupo. Los grupos de usuarios hacen más sencilla la administración, ya que es posible otorgar permisos a varios usuarios a la vez. Hay dos tipos diferentes de grupos:

Grupos locales: Otorga a los usuarios permisos para que accedan a un recurso de red. También sirven para conceder a los usuarios privilegios para abrir tareas de sistema (como cambiar la hora, hacer copias de seguridad, recuperar archivos, etc.). Existen grupos locales preconfigurados.

Grupos globales: Se usan para organizar las cuentas de usuario de dominio. También se usan en redes de varios dominios, cuando los usuarios de un dominio necesitan tener acceso a recursos de otro dominio.

**Administración de cuentas de usuarios**

Como se indicó anteriormente, las cuentas de usuarios es la forma a través de la cual se identifica y autentifica a un individuo con el sistema. Las cuentas de usuarios tienen diferentes componentes. Primero, esta el nombre de usuario. Luego, está la contraseña, seguida de la información de control de acceso.

Componentes de las cuentas de usuarios

**El nombre de usuario**

Desde el punto de vista del sistema, el nombre de usuario es la respuesta a la pregunta "quién es usted?". Como tal, los nombres de usuarios tienen un requerimiento principal — deben ser únicos. En otras palabras, cada usuario debe tener un nombre de usuario que sea diferente a todos los otros usuarios en ese sistema.

**Contraseñas**

Si el nombre de usuario responde a la pregunta "¿Quién es usted?", la contraseña es la respuesta a la pregunta que inevitablemente sigue:

"Demuéstralo!"

En términos más prácticos, una contraseña proporciona una forma de probar la autenticidad de la persona que dice ser el usuario con ese nombre de usuario. La efectividad de un esquema basado en contraseñas recae en gran parte sobre varios aspectos de la contraseña:

La confidencialidad de la contraseña

La resistencia de adivinar la contraseña

La resistencia de la contraseña ante un ataque de fuerza bruta

Es importante para la seguridad de la organización crear contraseñas robustas, mientras más robustas sean las contraseñas, hay menos chances de que estas sean descubiertas o que se adivinen. Hay dos opciones disponibles para reforzar el uso de contraseñas robustas:

El administrador del sistema puede crear contraseñas para todos los usuarios.

El administrador del sistema puede dejar que los usuarios creen sus propias contraseñas, a la vez que se verifica que las contraseñas sean lo suficientemente robustas.

**Cuentas de usuario**

• W2008 ofrece cuatro tipos de cuentas de usuario:W2008 ofrece cuatro tipos de cuentas de usuario:

**Cuentas de usuarios locales**

• Cuentas de usuario definidas en el equipo local, con acceso solamente al equipo local y, por tanto, a los recursos del mismo.

• Los usuarios pueden tener acceso a los recursos de otro equipo de la red si disponen de una cuenta en dicho equipo

• Para poder acceder a los recursos que un equipo comparte, es necesario autenticarse en él

•Estas cuentas de usuario residen en el administrador de cuentas de seguridad (*Security Account Manager*, *SAM*) del equipo, que es la BD de cuentas de seguridad local

• Se pueden crear en estaciones de trabajo o en servidores miembros pero NO en *controladores de dominio*

• Al usar cuentas locales de un servidor miembro, el usuario no podrán usar los recursos del dominio (al no estar autenticadas en él)

**Cuentas de usuario de dominio**

• Permiten a un usuario iniciar sesión en el dominio para obtener acceso a los recursos de la red

• El usuario tendrá acceso en cualquier equipo de la red con una única cuenta y contraseña

• Estas cuentas de usuario residen en el servicio de directorio AD y se crean definiéndolas en un *controlador de dominio*

• Un usuario puede acceder a los recursos del dominio utilizando un inicio de sesión único.

**Cuentas de usuario integradas**

• Permite a un usuario realizar tareas administrativas u obtener acceso temporalmente a los recursos de red

• Existen dos cuentas de usuario integradas que no pueden eliminarse: *Administrador* e *Invitado*

• Las cuentas de usuario locales *Administrador* e *Invitado* residen en SAM

• Las cuentas de usuario integradas de dominio residen en AD

• Estas cuentas se crean automáticamente durante la instalación de Windows o la de un dominio del Active Directory

• Son cuentas instaladas con el sistema operativo y las aplicaciones o servicios.

**Cuentas de usuario implícitas**

• Creadas de forma implícita por el sistema operativo o aplicaciones, se usan para asignar permisos en ciertas situaciones

• SistemaLocal (Localsystem): permite ejecutar procesos del sistema y administrar las tareas relativas al sistema. No se puede iniciar una sesión con esta cuenta, pero algunos procesos se ejecutan con ella:

– Por ejemplo, esta cuenta es la que se usa para ejecutar muchos de los servicios del sistema

• LocalService: acceso al sistema local

• NetworService: acceso al sistema local y en la red

• Otras cuentas son, por ejemplo, las de Internet

Information Services o los servicios de terminales.

**Manejo de acceso a los recursos**

**Herramientas *Usuarios y equipos de Active Directory***

• *Usuarios y equipos del Active Directory* es la herramienta

de administración más importante de Active Directory.

• Permite manejar todas las tareas relativas a cuentas de usuarios, grupos y equipos, además de administrar las unidades organizativas unidades organizativas

• *Inicio* / *Programas* / *Herramientas administrativas*/

*Usuarios y equipos del Active Directory*

• Por defecto se trabaja con el dominio al que esté conectado el equipo.

• También es posible conectarnos a otro controlador de dominio de ese dominio, o de otro dominio el mismo.

**Herramienta *Usuarios y equipos* Herramienta *Usuarios y equipos***

***de AD* (active directory)*.***

Al acceder a un dominio con *Usuarios y equipos del AD*.

Existen por defecto una serie de unidades organizativas:

– **Integrada**(*Builtin*): Contiene los objetos que definen las cuentas

integradas,

(como los Administradores y Operadores de cuentas)

**– *Equipos***(*Computers*): La unidad organizativa predeterminada para las cuentas de los equipos de los servidores miembro

– **Controladores de dominio**(*Domain Controllers*): La unidad organizativa predeterminada para los equipos que son

controladores de dominio

– **Usuarios**(*Users*): La unidad organizativa para los usuarios

– ***ForeignSecurityPrincipals*:** La unidad organizativa por defecto para los identificadores de seguridad (SIDs) asociados con los objetos de dominios externos en los que se confía

**Implementación de impresión:**

La implementación de impresión permite compartir impresoras en una red y centralizar las tareas de administración del servidor de impresión y las impresoras de red mediante el complemento Administración de impresión, que ayuda a supervisar las colas de impresión y a recibir notificaciones cuando dichas colas interrumpen el procesamiento de los trabajos de impresión. Además permite migrar los servidores de impresión e implementar conexiones de impresora con directivas de grupo.

Esta función puede interesar a aquellos administradores de redes pequeñas, medianas o grandes que necesiten administrar y supervisar varias impresoras y varios servidores de impresión de Windows.

**Administración de impresión:**

En aquellos equipos en los que se ejecuta Windows® 7 y Windows Server® 2008 R2, se puede compartir impresoras en una red y centralizar las tareas de administración del servidor de impresión y de las impresoras de red mediante el complemento Administración de impresión de Microsoft Management Console (MMC). Administración de impresión le ayuda a supervisar las colas de impresión y recibir notificaciones cuando las colas de impresión interrumpen el procesamiento de los trabajos de impresión. Además permite migrar los servidores de impresión e implementar conexiones de impresora con directivas de grupo.

**Herramientas para administrar un servidor de impresión:**

*Hay dos herramientas principales que se pueden usar para administrar un servidor de impresión de Windows:*

**Administrador del servidor.**

**Administración de impresión.**

*En Windows Server 2008 R2, se puede usar el Administrador del servidor para instalar el rol de servidor y los servicios de rol de Servicios de impresión y documentos.*

*Administración de impresión proporciona detalles actualizados sobre el estado de las impresoras y los servidores de impresión de la red. Puede usar Administración de impresión para instalar conexiones de impresora en un grupo de equipos cliente de forma simultánea y para supervisar de forma remota las colas de impresión. Administración de impresión facilita la búsqueda de impresoras con errores mediante filtros.*