A S I R

Implantación de Sistemas Operativos

Windows Server 2008

Versión inicial: 1.0. Utiliza Windows Server 2008

(Sugerencias a sagsag@hotmail.es)

Índice de contenidos

1 INTRODUCCIÓN

Windows Server 2008 tiene ciertas características comunes con Windows Vista por formar parte ambos de un mismo proyecto de desarrollo. De su arquitectura se desprenden algunas particularidades:

- Modularización.- cada componente del sistema operativo se diseña como un módulo que puede añadirse o eliminarse fácilmente.

- Incluye un gestor de arranque.- permite iniciar los equipos con sistemas operativos instalados anteriormente. También permite realizar tareas de recuperación y resolución de problemas.

- Control de privilegios de administración.- se emite un aviso de seguridad cuando la tarea a realizar necesita privilegios de administración. Es configurable a través de las directivas de grupo.

Algunas diferencias con Windows Vista son:

- Windows Server no puede suspenderse, ni hibernar ni restaurarse.

- Dispone de menos opciones de diseño del Escritorio.

Las diferentes versiones de Windows Server 2008 son.

- Windows Server 2008, Standard Edition.- es el sustituto de Windows Server 2003. Admite multiproceso simétrico de dos y cuatro vias y maneja hasta 4 Gb. de memoria en sistemas de 32 bits y hasta 32 Gb. en sistemas de 64 bits.

- Windows Server 2008, Enterprise Edition.- ofrece servicios adicionales como el servicio de cluster y admite hasta 32 Gb. de memoria en sistemas de 32 bits y hasta 2 Tb. en sistemas de 64 bits y hasta 8 CPU's.

- Windows Server 2008, Datacenter Edition.- es el más potente permitiendo hasta 64 Gb. de memoria en sistemas de 32 bits y hasta 2Tb. en sistemas de 64 bits. Trabaja con un mínimo de 8 CPU's y un máximo de 64.

- Windows Web Server 2008.- versión diseñada para ofrecer servicios Web. Solamente incorpora herramientas y aplicaciones para este tipo de servicios. Carece de muchas de las características de las versiones anteriores; por ejemplo, no dispone de Active Directory por lo que no puede configurarse como servidor de un dominio.

Durante la instalación de Windows Server 2008 deberá configurarse el sistema como servidor individual que puede formar parte de un grupo de equipos o como servidor de un dominio.

Si se configura como servidor independiente, todos los recursos se administrarán de forma local, incluidas las cuentas de usuario y grupo. El equipo podrá incluirse en el mismo grupo de trabajo que otros servidores independientes pudiendo así compartir entre ellos ciertos recursos como son: ficheros, carpetas, impresoras, etc.

Si el equipo se configura como miembro de un dominio entrará a formar parte de un sistema donde los recursos y la seguridad se gestionan de forma centralizada. Una base de datos denominada Active Directory contendrá toda la información de los elementos, objetos o recursos incluidos en el dominio. Por ejemplo, las cuentas de usuario y de grupo se centralizarán en uno o varios equipos.

Los equipos que se configuren como controladores de dominio (DC) contendrán una copia del Active Directory; si un DC queda inactivo otro DC pasará a realizar sus funciones. Los demás equipos estarán registrados en el Active Directory mediante las correspondientes cuentas de equipo y podrán hacer uso de la información contenida en los DC's en la forma que los administradores de la red dispongan.

2 INSTALACIÓN

2.1 Conceptos previos

Antes de proceder a la instalación de Windows Server 2008 es conveniente conocer los siguientes conceptos:

- Active Directory.- base de datos que contiene la información de los elementos integrantes de la red y su seguridad: cuentas de usuario, cuentas de grupo, cuentas de equipos, recursos que se comparten , etc.

- Controlador de dominio o DC.- equipo que contiene el Active Directory. Es conveniente que exista más de uno para solucionar posibles fallos en los mismos.

- Dominio.- unidad administrativa que permite compartir ciertas capacidades y características. Deberá albergar uno o más DC's y cualquiera de ellos podrá autenticar cualquier identidad (usuario, grupo, máquina, …) del dominio. Un dominio también es el ámbito de las directivas administrativas tales como las directivas de complejidad de contraseña o las directivas de bloqueo de cuentas.

- Bosque.- es una colección de uno o más dominios de Active Directory. El primer dominio instalado en el bosque será el dominio raíz del bosque.

- Árbol.- los nombres de espacio DNS de los dominios en un bosque crean árboles dentro de éste. Si un dominio es un subdominio de otro dominio, los dos dominios se consideran un árbol. Los árboles son el resultado directo de los nombres DNS seleccionados para los dominios del bosque.

- Nivel funcional.- determina la versión más baja de Windows Server como controladores del dominio. Las posibilidades son Windows 2000, 2003 y 2008.

- Unidades Organizativas (OU).- permiten generar contenedores adicionales a los existentes por defecto (Usuarios, Equipos, …). A las nuevas unidades organizativas se las puede aplicar propiedades organizativas o parámetros de configuración que afectarán a los objetos incluidos: son las GPO u objetos de directivas de grupo.

- Sitio.- objeto de Active Directory que representa un fragmento de la empresa dentro del cual la conectividad de red es buena. Un sitio crea un límite de duplicación y de utilización de un servicio. Los controladores de dominio del mismo sitio duplican su información en segundos mientras que las comunicaciones entre sitios son lentas, caras y poco fiables. Por ejemplo, un cliente Windows intentará autenticarse en un controlador de dominio de su sitio y solamente si no lo consigue acudirá al controlador de otro sitio.

2.2 Instalación

Antes de proceder a la instalación deben conocerse o tenerse planificados los siguientes aspectos:

- El nombre del dominio y su nombre corto para Netbios. Por ejemplo, tiernogalvan.es y TIERNOGALVAN, respectivamente.

- Conocer si hay que dar soporte para versiones de Windows, para evitar problemas de compatibilidad entre servidores.

- Configuración IP para el controlador del dominio, que debe ser una dirección IP fija.

- Nombre de usuario y la contraseña del administrador. El usuario estará dentro del grupo Administradores del servidor.

  La contraseña deberá tener más de seis caracteres de tres de los cuatro tipos siguientes:

  - Letras mayúsculas: A-Z.
  - Letras minúsculas: a-z.
  - Números: 0-9.
  - Caracteres no alfanuméricos como: @ # $ & ? ¿ ...

- Ubicación del Active Directory.

Una de las formas más simples de instalar el Active Directory es ejecutar la instrucción “dcpromo.exe”.

Después de la instalación, al iniciar la sesión, aparece la ventana de “Tareas de configuración inicial” para configurar aspectos básicos iniciales. Dicha ventana aparecerá cada vez que se inicie sesión en el equipo o mediante el comando “Oobe.exe”.

Al cerrar la ventana de “Tareas de configuración inicial” aparece la de “Administración del servidor” que permite configurar y administrar las funciones y características del servidor. Esta ventana puede abrirse desde varios sitios, entre otros desde “Inicio – Herramientas administrativas”. Esta ventana dispone de varias opciones que permiten agregar funciones: “Acción – Agregar funciones”, “Subventana Resumen de funciones – Agregar funciones”, … Y algunas de las funciones a agregar pueden ser el Active Directory (aunque obligatoriamente después hay que ejecutar “dcpromo”) o el servicio DNS.

3 VENTANAS DE ADMINISTRACIÓN PERSONALIZADAS

3.1 Concepto

La totalidad de los programas o herramientas que permiten realizar tareas administrativas en el Active Directory se pueden encontrar en el Panel de Control y en la opción Herramientas Administrativas del menú Inicio o del menú Inicio – Todos los programas.

Pueden crearse ventanas de administración personalizadas o Microsoft Management Console (MMC) que contengan un subconjunto del total de las herramientas administrativas, que serán muy útiles en los siguientes escenarios:

- Generalmente son solamente unas pocas herramientas las que se utilizan con cierta frecuencia y hay que seleccionar diferentes opciones hasta llegar a las mismas.

- Es frecuente que las tareas administrativas se encuentren distribuidas entre varios usuarios de tal forma que cada uno de ellos solamente debe tener acceso a las herramientas que debe utilizar.

Las ventanas de administración personalizadas ofrecen un acceso rápido a las herramientas que contienen y además, por tratarse de un fichero, puede gestionarse qué usuarios tienen acceso al mismo.

Por ejemplo, puede crearse una ventana que contenga dos herramientas: “Usuarios y equipos de Active Directory” y “Copias de seguridad de Windows” y guardarse con el nombre de fichero “Mi_ventana.msc”. Este fichero solamente podrá ser leido o modificado por los usuarios que se considere oportuno, y podrán hacer uso de las herramientas contenidas en la ventana.

Otro aspecto a tener en cuenta es que no debe iniciarse la sesión de trabajo como usuario Administrador. Es aconsejable iniciar la sesión como un usuario sin privilegios y ejecutar haciendo uso del botón derecho y de la opción “Ejecutar como administrador”. Aquí las ventanas personalizadas también tienen su ventaja pues con pulsar una vez sobre la ventana con el botón derecho y elegir “Ejecutar como usuario administrador”, ya se podrán utilizar con los privilegios de usuario administrador todas las herramientas contenidas en la ventana.

Si una herramienta tiene que utilizarse muy frecuentemente como usuario administrador, puede crearse un acceso directo a la herramienta y configurar el acceso directo para que se ejecute siempre como usuario administrador, lo que se hace en las propiedades del acceso directo, botón “Avanzado”.

3.2 Creación y gestión

Para crear una MMC puede utilizarse la instrucción “mmc.exe”.

La opción “Agregar o quitar complemento” del menú Archivo permite elegir las herramientas o complementos que compondrán la ventana.

Las ventanas pueden guardarse en varios modos:

- Autor.- pueden modificarse las herramientas de la ventana.
- Usuario: acceso completo.- se pueden utilizar todas las herramientas pero no se pueden gestionar las herramientas de la ventana.
- Usuario: acceso limitado varias ventanas.- los usuarios podrán navegar y utilizar las herramientas de varias ventanas o subventanas.
- Usuario: acceso limitado una ventana.- los usuarios podrán utilizar las herramientas de una única ventana.

Los modos se eligen en la opción “Opciones” del menú Archivo o con el botón derecho sobre el icono de la ventana, opción “Autor”.

Las ventanas se guardan como un fichero con extensión “.msc”. El lugar donde se guarde permitirá o no el acceso a determinados usuarios: una carpeta compartida, un pen drive, …

4 Creación de objetos en Active Directory

4.1 Unidades organizativas

Active Directory es un servicio de directorio que mantiene la información acerca de los recursos de la empresa, incluyendo usuarios, grupos y equipos. Los recursos se dividen en unidades organizativas que facilitan su manejo y visibilidad.

Las unidades organizativas (OU) son contenedores administrativos dentro de Active Directory que se utilizan para coleccionar objetos que comparten requerimientos comunes de administración, configuración o visibilidad. Como ejemplo podemos suponer una empresa que tiene varias oficinas y se crea una unidad organizativa por cada oficina. Cada unidad organizativa tendrá usuarios, grupos y equipos diferentes pero tendrá algunas características comunes para todos ellos, como puede ser la dirección.

Para crear una unidad organizativa:

1. Abrir el complemento Usuarios y equipos de Active Directory.
2. Seguir pasos de la página 87.

Una vez creada se puede acceder a sus propiedades y modificarlas. La ficha "Administrado por" es mera información, no se le otorga ningún permiso especial al usuario especificado.

Se recomienda activar la opción "Proteger contenedor contra eliminación accidental" que agrega los permisos "Todos::Denegar::Eliminar" y "Todos::Denegar::Eliminar subárbol" a la unidad organizativa. Para borrar dicha unidad deben seguirse los pasos de la página 88.

4.2 Usuarios

Para crear un usuario hay que situarse en la unidad organizativa o contenedor donde se desea crear, que puede ser "Users", y pulsar con el botón derecho (Ver página 89). Al dar de alta al usuario el campo "Nombre completo" se rellena automáticamente y se utiliza para crear diversos atributos del objeto usuario, en particular el nombre común (CN). El nombre común debe ser único dentro del contenedor o unidad organizativa.

El nombre principal del usuario (UPN) está compuesto por el nombre de inicio de sesión seguido del carácter arroba (@) y del sufijo del UPN que suele ser el nombre del dominio. Por ejemplo, santiago@profe.b25.es. Pueden añadirse sufijos por asuntos de seguridad o de simplificación mediante la herramienta "Dominios y confianzas de Active Directory", en las propiedades del elemento que aparece como raíz.

Durante la creación del usuario solamente se introducen unas pocas propiedades del usuario relacionadas con su nombre y su contraseña, posteriormente, a través de sus propiedades pueden incluirse un gran número de ellas, entre las más significativas la pertenencia a grupos.

4.3 Grupos

Los grupos son una clase de objetos que permiten coleccionar usuarios, equipos y otros grupos para generar un único punto de administración. Un ejemplo sencillo consiste en asignar permisos de lectura sobre una carpeta a un grupo; todos los miembros del grupo podrán leer en la carpeta. Para dar el permiso a los usuarios no es necesario darles el permiso de forma individual, basta con hacerles miembros del grupo.

Puede seguirse la creación de un grupo en la pag. 92. Debe tenerse en cuenta:

- El grupo debe crearse en el contenedor adecuado (Users o la unidad organizativa creada al efecto).

- El "Nombre del grupo" debe ser igual al "Nombre del grupo (anterior a Windows 2000)".

- Hay dos tipos de grupos: seguridad, que permiten administrar los permisos de acceso a los recursos y también crear listas de distribución de correos y distribución, que solamente se utilizan para crear listas de distribución de correos.

- El ámbito del grupo puede ser:

  - Local.- se utilizan para asignar permisos sobre los recursos y derechos para realizar tareas. Pueden contener usuarios y grupos globales.

  - Global.- se utilizan para agrupar usuarios de características similares. Contienen usuarios y suelen agregarse a grupos locales para conceder derechos a sus miembros.

  - Universal.- se utilizan para agrupar usuarios y grupos de diferentes dominios. Este tipo de grupos no existían en, por ejemplo, Windows NT.

- En el campo "Descripción" puede exponerse la finalidad del grupo y quién es el responsable de admitir a los miembros. En el campo "Notas" puede ampliarse la información de la descripción.

- La ficha "Administrado por" se utiliza para conocer y ponerse en contacto con el usuario que decide quienes son los miembros del grupo. Si se selecciona "El administrador puede actualizar la lista de suscripciones", a la cuenta especificada en el

cuadro “Nombre” se le asignan permisos para agregar y eliminar miembros del grupo, lo que permite delegar esta función de administración.

4.4 Equipos

Las cuentas de equipo son similares a las de usuario. También deben crearse en el contenedor adecuado, que puede ser Users.

No debe modificarse el campo del nombre para S.O. anterior a Windows 2000.

No debe activarse la casilla de “Asignar la cuenta de este equipo como ...”.

La Descripción debe contener información significativa: a quién se asigna, función …

Algunas de las propiedades se rellenan automáticamente cuando el equipo se une al dominio.

El campo “Administrado por” se suele utilizar como información de la persona que da soporte o de la persona a la que ha sido asignado.

4.5 Encontrar objetos en Active Directory

4.5.1 Vista de objetos del complemento Usuarios y equipos de AD

- Pueden añadirse o eliminarse columnas desde la opción “Ver – Agregar o quitar columnas”.
- Puede cambiarse el orden de las columnas arrastrando sus cabeceras.
- Puede ordenarse la información por el contenido de una determinada columna pulsando sobre la cabecera una o dos veces (ascendente y descendente).

4.5.2 Consultas guardadas

Pueden definirse consultas que permiten filtrar la vista de objetos para que se muestren los usuarios, grupos o equipos que cumplen una determinada característica. Se maneja con botón derecho sobre la carpeta “Consultas guardadas”.

4.5.3 Cuadro de diálogo Seleccionar usuarios, contactos, equipos o grupos

Cuando se agrega un miembro a un grupo, se asigna un permiso o se crea una propiedad vinculada, se presenta el cuadro de diálogo "Seleccionar usuarios, contactos, equipos o grupos, que permite buscar objetos especificando alguno de los datos:

- Tipo de objeto: usuario, grupo, …
- Ubicación o contenedor.
- Parte del nombre (comprobar nombre).
- Propiedades avanzadas (nº de días que no hacen login, …).

4.5.4 El botón Encontrar objetos

En la barra de herramientas del complemento Usuarios y equipos de Active Directory existe un botón (una lupa sobre una carpeta) que activa la herramienta "Encontrar objetos en los servicios de dominio de Active Directory" que permite realizar búsquedas de objetos. Pueden seleccionarse diferentes filtros.

Seleccionando en la lista desplegable Buscar "Búsqueda personalizada", haciendo uso de la ficha "Opciones avanzadas" pueden construirse complejas consultas LDAP. Por ejemplo OU=*main* busca por cualquier unidad organizativa nombres que contengan "main" y devolverá Domain Controlers OU.

4.5.5 La instrucción Dsquery.exe

Puede obtenerse información completa del comando mediante "dsquery /?".

Permite buscar objetos en el Active Directory.

4.6 DN, RDN y CN

Cada objeto del Active Directory tiene un nombre único o nombre distintivo (DN) que lo identifica y que tiene la forma de una ruta del tipo:

CN=Usuario,OU=Users,DC=tiernogalvan,DC=es

Donde CN quiere decir nombre común, OU unidad organizativa y DC componente del dominio.

La ruta parte del objeto y termina en el más alto nivel en el espacio de nombres DNS.

El nombre común del usuario se genera en el momento de su creación y se corresponde con el nombre completo del usuario.

El fragmento del DN anterior al primer OU o contenedor se llama nombre distintivo relativo o RDN. En el ejemplo anterior el RDN sería CN=Usuario. El RDN de un objeto debe ser único dentro del contenedor. En el ejemplo anterior el RDN de la unidad organizativa Users es OU=Users.

5 Delegación y seguridad en Active Directory

En organizaciones amplias las tareas administrativas se distribuyen entre varios administradores. Por ejemplo, el grupo Help Desk o Ayudante de escritorio puede estar habilitado para realizar ciertos cambios en cuentas ya creadas: desbloqueos, cambios de contraseña, …

Todos los objetos de Active Directory se pueden asegurar utilizando una lista de permisos. Los permisos de un objeto se llaman entradas de control de acceso (ACE) y se asignan a usuarios, grupos o equipos. Las ACE's se guardan en la lista de control de acceso discrecional (DACL). La DACL forma parte de la lista de control de acceso del objeto (ACL), que también contiene la lista de control de acceso al sistema (SACL) que incluye configuraciones de auditoría. Los términos y conceptos son idénticos a los permisos en archivos y carpetas.

La delegación del control administrativo, también llamado delegación de control o simplemente delegación, significa asignar permisos que administren el acceso a los objetos y las propiedades en Active Directory. Igual que se puede dar permisos a un grupo para modificar los archivos de una carpeta, también se puede dar a un grupo permisos para restablecer las contraseñas de los objetos usuario.

5.1 Ver la ACL de un objeto

Para ver la ACL de un objeto puede procederse de la forma:

1. Ejecutar la herramienta “Usuarios y equipos de Active Directory”.

2. En el menú “Ver” comprobar que la opción “Características avanzadas” se encuentra activada.

3. Se selecciona el objeto en cuestión, que puede ser un usuario y se accede a sus propiedades (botón derecho), ficha “Seguridad”.

4. Pulsando el botón “Opciones avanzadas” se muestra la ventana de “Configuración de seguridad avanzada para el usuario”. La ficha permisos de esta ventana muestra la lista de control de acceso discrecional (DACL).

5. Cada elemento de la lista puede estar compuesto de varias entradas de control de acceso (ACE's) a las que se accede seleccionando un elemento de la lista y pulsando el botón “Editar”. Aparecerá una ventana con la “Entrada de permiso para el usuario”.

5.2 Objeto, propiedad y derechos de control de acceso

La ACL de un objeto permite asignar permisos a propiedades específicas de un objeto. Se pueden permitir o denegar permisos para modificar, por ejemplo, las opciones de teléfono y correo electrónico.

También se pueden asignar permisos para administrar los derechos de control de acceso, que consiste en poder modificar o restablecer la contraseña. Estos dos derechos son diferentes porque para modificar la contraseña hay que conocer la actual, pero para restablecerla no.

La posibilidad de modificar permisos en un objeto está controlada por la ACE "Permitir: : Modificar permisos". Los permisos de los objetos también controlan si se pueden crear objetos hijo, por ejemplo, para permitir crear objetos equipo asignando la ACE "Permitir: :Crear objetos de equipo" en la OU adecuada.

El tipo y el ámbito de los permisos se determinan usando dos fichas: "Objetos" y "Propiedades", y las listas desplegables "Aplicar a" de cada ficha.

5.3 Asignar un permiso

Vamos a suponer que se quiere permitir al grupo "Help Desk" que pueda modificar la contraseña del usuario James Fine. Esto se puede realizar asignando la ACE correspondiente de la DACL del objeto o utilizando el "Asistente de control de delegación" para la OU completa de usuarios (opción más recomendada que se verá más adelante).

Ver página 120.

En el paso 3 hay que seleccionar el usuario James Fine, que se encuentra en la OU People.

5.4 Permisos con herencia

No es conveniente asignar permisos de forma individual como en el apartado anterior. Lo lógico es asignar permisos a unidades organizativas, que serán heredados por todos los objetos contenidos en las mismas. En el caso del apartado anterior sería más lógico asignar el permiso a la OU que contiene a los usuarios y así Help Desk podrá restablecer la contraseña de todos los usuarios de la OU.

Se dice que un objeto hereda los permisos de su contenedor u OU y a su vez el contenedor hereda los de su contenedor padre, que puede ser otra OU o el dominio completo. Para que la herencia no se propague a un objeto o contenedor habría que deshabilitar la opción "Incluir todos los permisos heredables del objeto primario de este objeto".

Hay permisos que no afectan a cierto tipo de objetos por no disponer del atributo correspondiente; por ejemplo, el permiso para restablecer la contraseña en una OU no afecta a los grupos de la misma por no disponer los grupos del atributo de contraseña.

Puede delimitarse la herencia de permisos haciendo uso de la casilla de verificación "Aplicar a" del cuadro de diálogo "Introducir permiso".

Por otra parte, un permiso explícito prevalece sobre el heredable de tal forma que si un objeto hereda, por ejemplo, un permiso de acceso pero al objeto se le deniega el permiso explicitamente, el resultado es que el objeto no tiene permiso.

Para delimitar la herencia es recomendable, en vez de anular la herencia, otorgar los permisos explícitos oportunos.

5.5 Delegar tareas administrativas con el Asistente

Administrar los permisos manejando las DACL y ACE's no es tarea fácil. Se recomienda hacer uso del "Asistente para delegación de control". Su uso se detalla en la página 122.

Las tareas que muestra el Asistente son más comprensibles y cada una de ellas puede equivaler a una serie de ACE's.

5.6 Información y visualización de permisos

Además de utilizar los métodos de los epígrafes anteriores para poder ver los permisos de la DACL, también puede utilizarse la instrucción "Dsacls.exe". Por ejemplo, para ver un informe de los permisos de la OU People habría que poner:

Dsacls.exe "OU=People,DC=profe,DC=b25,dc=es".

Con "dsacls /?" puede obtenerse más información sobre esta instrucción.

5.7 Eliminar o restablecer los permisos de un objeto

Para eliminar permisos o restablecer los asignados por defecto hay que hacer uso de las ventanas "Configuración de seguridad avanzada" y "Entrada de permisos".

El botón "Restaurar valores predeterminados" de la ventana de "Configuración de seguridad avanzada" permite restaurar los permisos iniciales. Después de restaurar los permisos pueden volver a reconfigurarse los permisos explícitos que se desee asignar a la DACL.

La instrucción Dsacls.exe tiene dos parámetros interesantes:

- /s para restablecer los permisos por defecto.
- /t para que la modificación afecte al objeto y a todos los hijos.

Otra opción para restablecer los permisos de la unidad organizativa People y todas sus unidades organizativas hijo y objetose es la que se utiliza en el ejemplo:

Dsacls.exe "OU=People,DC=profe,DC=b25,DC=es" /resetDefaultDACL

5.8 Permisos efectivos

Los permisos efectivos para un usuario o grupo son los permisos resultantes del efecto acumulativo de cada ACE explícito y heredado. Los permisos efectivos se pueden complicar si se considera que los permisos se pueden permitir o denegar, las ACE's explícitas y heredadas y el hecho de pertenecer a diversos grupos que pueden tener asignados permisos diferentes.

Los permisos asignados a una cuenta de usuario son equivalentes a los asignados a un grupo al que se pertenece.

Los permisos que permiten acceso son acumulativos. Los permisos que niegan un acceso anulan un equivalente de permiso permitir. Si se pertenece a un grupo al que se le permite restablecer contraseñas y a otro grupo al que se le niega los permisos para restablecer contraseñas, la negación del permiso evitará que el usuario pueda restablecer contraseñas.

Generalmente es innecesario asignar la negación de permisos, basta con no asignar el permiso para que los usuarios no puedan realizar la tarea. Debe intentarse evitar el uso de permisos denegar.

Los permisos explícitos pueden anular los permisos heredables. Un permiso explícito permitir anulará un permiso heredable denegar.

La compleja interacción de usuario, grupo, explícito, heredado, permitir y denegar permisos puede conllevar un cierto trabajo para evaluar los permisos efectivos. Para poder comprobar los permisos efectivos existen dos herramientas de ayuda:

- La ficha "Permisos efectivos" de la ventana "Configuración de seguridad avanzada" de un objeto.
- La instrucción Dsacls.exe.

5.9 Diseño de una unidad organizativa

Las OU son contenedores administrativos que deben contener objetos que compartan requerimientos similares de administración, configuración y visibilidad. Los objetos que se administran de la misma forma y por los mismos administradores deben estar dentro de una única OU.

Las cuentas administrativas se administran de forma diferente a las demás cuentas y deben estar en una OU diferente. Si la organización dispone de un equipo de personas que ayudan y dan soporte software y otro equipo que da soporte hardware deberán existir las correspondientes OU que los incluyan. Los primeros realizarán tareas de restablecer contraseñas, desbloquear cuentas, etc. Los segundos podrán incluir equipos en la OU adecuada, cambiar los nombres de los equipos, etc.

Si, por ejemplo, el soporte de equipos no se halla centralizado por la existencia de oficinas ubicadas en distintas localizaciones geográficas, puede existir una unidad organizativa Clients dividida en diferentes subunidades organizativas que representarán cada ubicación geográfica. Cada equipo de soporte local podrá añadir equipos a la subunidad local correspondiente.

Una vez diseñadas las unidades organizativas de forma que permitan una delegación eficaz de las tareas administrativas, deberá refinarse el diseño para facilitar la configuración de equipos y usuarios mediante las Directivas de grupo.

6 AUTOMATIZAR LA CREACIÓN DE CUENTAS DE USUARIO

Ya se ha visto una forma de crear cuentas de usuario en una unidad organizativa. Cuando se debe agregar un gran número de cuentas es conveniente utilizar técnicas avanzadas que permitan la automatización de la tarea.

6.1 Crear usuarios con plantillas

Frecuentemente los usuarios de un dominio comparten propiedades similares. Para automatizar la creación de este tipo de cuentas de usuario apareció la plantilla de cuentas de usuario. Una plantilla de cuenta de usuario es una cuenta de usuario a la que se le han asignado las propiedades comunes a un cierto número de usuarios: pertenencia a grupos de seguridad, horas de inicio de sesión, carpetas de trabajo, perfiles, etc.

Para crear usuarios basados en la plantilla basta seleccionar la misma y elegir la opción Copiar del menú contextual. A continuación se elige “Copiar objeto – Usuario”.

Con las plantillas de creación de cuentas no debe iniciarse una sesión por lo que se recomienda que sean desactivadas.

6.2 Herramientas de linea de comandos

Algunos de los comandos soportados por Active Directory son:

- Dsadd.- crea un objeto.
- Dsget.- muestra los atributos específicos de un objeto.
- Dsmod.- modifica los atributos específicos de un objeto.
- Dsmove.- mueve un objeto a un nuevo contenedor o unidad organizativa.
- Dsrm.- elimina un objeto, todos los objetos en el subárbol bajo un objeto contenedor o ambos.
- Dsquery.- permite realizar consultas aplicando el filtro que se especifique.

Un ejemplo de utilización de estos comandos puede ser:

dsadd user “cn=Santiago Alonso,ou=People,dc=profe,dc=b25,dc=es”

En la página 140 pueden encontrarse más ejemplos.

6.3 Importar usuarios con CSVDE

CSVDE es una herramienta de línea de comandos que permite importar o exportar objetos de Active Directory desde o hacia un fichero de texto cuyos campos se separan con comas. El archivo tendrá extensión ".csv". Este tipo de archivos se puede editar y modificar con un editor de textos, como puede ser el Bloc de notas.

Si se dispone de información de usuarios en una hoja de cálculo o base de datos no es complicado realizar la creación de los correspondientes usuarios en Active Directory de forma automatizada.

La sintaxis básica del comando csvde tiene la forma:

csvde [-i] [-f fichero] [-k]

donde "-i" indica importar (por omisión se entiende exportar), "-f" permite especificar el nombre del fichero desde/donde importar/exportar y "-k" se utiliza en las importaciones para ignorar los errores de "Infracción de restricción" y "El objeto ya existe".

El archivo importado deberá ser un archivo de texto con extensión .txt o .csv que contendrá la información de los usuarios a razón de una línea por cada usuario, a excepción de la primera línea cuyo contenido será los nombres de los atributos que serán especificados de cada usuario. Un ejemplo de contenido del fichero puede ser el siguiente:

DN,objectClass,sAMAccountName,sn,givenName,userPrincipalName
"cn=Lisa Adrews,ou=People,dc=profe,dc=b25,dc=es",user,lisa.andrews,Lisa,
Andrews,lisa.andrews@profe.b25.es

No se puede utilizar CSVDE para importar contraseñas y, sin una contraseña, una cuenta de usuario se encontrará inicialmente deshabilitada. Después de restablecer la contraseña podrá habilitarse el objeto.

6.4 Importar usuarios con LDIFDE

El comando ldifde.exe también permite importar o exportar objetos a/desde un fichero. La sintaxis del comando es similar a la de csvde. Un ejemplo podría ser:

ldifde -i -f fichero.ldf -k

donde el significado de cada parámetro también se corresponde con el comando csvde.

El fichero de importación/exportación difiere fundamentalmente en que cada atributo de cada objeto se especifica en una línea y para separar los atributos de un objeto de los del

siguiente se interpone una línea en blanco. Un ejemplo de fichero podría ser el de las páginas 142 y 143.

7 Dar soporte a los objetos de usuario y cuentas

Una vez creado un usuario hay que configurar los atributos que definen las propiedades de seguridad principal (la cuenta) y las propiedades que administran al usuario.

7.1 Administración con Usuarios y equipos de Active Directory

Desde esta herramienta, a través de las propiedades del menú contextual de un usuario, se accede a los atributos del mismo, que se encuentran recogidos en las diferentes fichas. Pero un usuario tiene más propiedades que las que se muestran en el cuadro de dialogo "Propiedades". Algunas de ellas se llaman propiedades ocultas y pueden ser útiles para la empresa.

Para descubrir los atributos ocultos hay que activar el "Editor de atributos" a través de las opciones "Ver – Características avanzadas". Activando las características avanzadas aparecerá en las propiedades la ficha "Editor de atributos", que muestra todos los atributos del sistema del objeto seleccionado. El botón filtro permite seleccionar algunos atributos más para ver, incluyendo enlaces de referencia y atributos construidos.

Los enlaces de referencia son atributos que son el resultado de referencias a objetos desde otros objetos. Por ejemplo, el atributo "memberOf" de un usuario; cuando un usuario se agrega a un grupo es el atributo "member" del grupo el que se modifica y el que contiene los valores (usuarios miembros); el atributo "memberOf" del usuario se mantiene y actualiza automáticamente.

Un atributo construido es el resultado de un cálculo realizado por Active Directory; por ejemplo el atributo "tokenGroups" que corresponde al número de grupos a los que pertenece el usuario y que es calculado en cada momento (ni se guarda ni se mantiene). Estos atributos no se pueden utilizar en consultas LDAP.

Pueden modificarse los atributos de varios usuarios a la vez, basta con seleccionarlos manteniendo pulsada la tecla <Ctrl> y pulsando sobre cada uno de los usuarios, o utilizando cualquier otro método, y accediendo después a las propiedades del menú contextual; quedarán disponibles un subconjunto del total de las propiedades.

7.2 Atributos de nombre y cuenta

Muchos atributos se relacionan con el nombre de un objeto de usuario y de una cuenta y deben comprenderse ciertas diferencias:

- El atributo de usuario "sAMAccountName", o nombre de inicio anterior a Windows 2000, debe ser único en el dominio.

- El atributo "userPrincipalName" (UPN), consiste en un nombre de inicio de sesión y un sufijo UPN que, por defecto, es el nombre DNS del dominio donde se ha creado el objeto. El UPN debe ser único en el bosque completo.

- El RDN debe ser único dentro de la unidad organizativa, es decir, el atributo cn debe ser único para los usuarios dentro de la OU.

- El atributo "displayName" aparece en la lista de direcciones globales Exchange (GAL) que en muchas ocasiones tiene la sintaxis "Apellido, Nombre".

7.3 Propiedades de cuenta

Algunas de las propiedades que permiten implementar la seguridad de las cuentas de usuario son:

- Horas de inicio de sesión.
- Iniciar sesión en.- permite especificar las estaciones de trabajo del usuario.
- El usuario debe cambiar la contraseña en el siguiente inicio de sesión.
- El usuario no puede cambiar la contraseña.
- La contraseña nunca caduca.
- Cuenta deshabilitada.
- Almacenar contraseña utilizando cifrado reversible.- para el funcionamiento de algunas aplicaciones.
- La tarjeta inteligente es necesaria para un inicio de sesión.- es un componente adicional de identificación física para el proceso de autenticación.
- La cuenta es importante y no se puede delegar.
- La cuenta caduca.

7.4 Administrar atributos de usuario con Dsmod y Dsget

Dsmod modifica los atributos de uno o más objetos existentes. Su sintaxis básica es:

Dsmod user DNusuario … parámetros

donde "DNusuario especifica el nombre distintivo del usuario a modificar. El resto de parámetros indican el atributo a cambiar y el valor. Por ejemplo, el siguiente comando modifica el atributo "Office" de Santiago Alonso:

```
dsmod user "cn=Santiago Alonso,ou=People,dc=profe,dc=b25,dc=es"
       -office "Tordillos"
```

Dsmod user puede modificar solamente un subconjunto de los atributos del usuario. La instrucción "dsmod user /?" muestra una lista de los parámetros soportados.

Para modificar con dsmod los atributos de varios usuarios pueden utilizarse dos procedimientos:

- No especificar los usuarios en la línea de comando, es decir, usando una instrucción del tipo:

  dsmod user -office "Tordillos"

  Así, al ejecutar la instrucción, podremos introducir los DN de los usuarios, encerrados entre comillas, a razón de un DN por línea, pulsando <Intro> al finalizar cada línea y <Ctrl>+<Z> e <Intro> para finalizar la lista de usuarios (en una línea nueva).

- Canalizando o filtrando hacia dsmod el resultado de un comando dsquery. Dsquery permite buscar en Active Directory por criterios especificados y devuelve los DNS de los nombres coincidentes. Por ejemplo, para cambiar el atributo "office" a los usuarios Jesus Alonso y Santiago Alonso puede utilizarse el comando:

  dsquery user -name "* Alonso" | dsmod user -office "Macotera"

  Otro ejemplo, que modifica la unidad y directorio de trabajo de los usuarios es:

```
dsquery user "ou=People,dc=profe,dc=b25,dc=es" | dsmod user
              -hmdir "\\Serv\users\%username%\documents" -hmdrv "U:"
```

La variable %username% contiene el valor sAMAccountName de los objetos de usuario y puede utilizarse para configurar los parámetros -email, -hmdir, -profile y -webpg.

Dsget muestra los atributos seleccionados de uno o más objetos. Su sintaxis es similar a la de dsmod:

Dsget usuario DNusuario … parametros

Ejemplos de utilización pueden ser los siguientes:

dsget user "cn=Santiago Alonso,ou=People,dc=profe,dc=b25,dc=es" -samid

dsquery -office "Tordillos" | dsget user -samid

7.5 Administrar cuentas de usuario

Las tareas administrativas más comunes relacionadas con las cuentas de usuario son: restablecer contraseñas, desbloquear cuentas, deshabilitar, habilitar, mover y renombrar objetos de usuario. Cada una de estas tareas requiere los permisos adecuados para su realización.

- Restablecer la contraseña del usuario.- se realiza cuando un usuario olvida la contraseña. Se restablece pulsando el botón derecho sobre el usuario y eligiendo la opción "Restablecer contraseña". El sistema pedirá la nueva contraseña sin necesidad de conocer la anterior. En el mismo cuadro de diálogo se recomienda activar el cuadro de verificación "El usuario debe cambiar la contraseña en el siguiente inicio de sesión".

  Para restablecer la contraseña desde la línea de comandos usaríamos:

  dsmod user UserDN -pwd Nuevacontraseña -mustchpwd yes

- Desbloquear una cuenta de usuario.- configurando la directiva de bloqueo adecuada se consigue bloquear una cuenta cuando intenta el inicio de sesión repetidas veces sin éxito. Puede desbloquearse desde la ficha "Cuenta" de las propiedades del usuario o desde el cuadro de diálogo que permite restablecer la contraseña.

  No existe un comando que permita desbloquear una cuenta.

- Deshabilitar y habilitar una cuenta.- estas operaciones se realizan cuando se crea una cuenta antes de ser necesitada o cuando un usuario se ausenta durante un periodo largo de tiempo. La operación se puede realizar desde el menú contextual desde Usuarios y equipos de Active Directory o mediante una instrucción de la forma:

  dsmod user UserDN -disabled yes

- Eliminar una cuenta de usuario.- conlleva que se perderán las propiedades del usuario. Active Directory conserva durante un periodo de latencia (60 días) algunas de las propiedades del usuario como sus SID por si se vuelve a necesitar la cuenta. Puede ser interesante mantener la cuenta deshabilitada por un tiempo antes de su eliminación definitiva.

  También se puede considerar el reciclado de cuentas para cuando un usuario puede ocupar la de otro por ocupar su mismo puesto o tener similares características en cuanto a permisos, pertenencia a grupos, etc. En este caso con renombrar la cuenta para que se ajuste al nombre del nuevo usuario puede valer.

  Una cuenta se puede eliminar eligiendo la opción correspondiente de su menú contextual o mediante la instrucción:

  ```
  Dsrm  DNusuario
  ```

- Mover una cuenta.- para mover una cuenta de usuario puede hacerse uso de la operación arrastrar y soltar o, más recomendable, eligiendo la opción "Mover" de su menú contextual. Hay que tener en cuenta que cuando se mueve un usuario hay que cambiar los objetos de directiva de grupo (GPO) que se aplican a ese usuario.

  Tambien puede hacerse uso de la instrucción:

  ```
  Dsmove  DNusuario  -newparent  OUDNdestino
  ```

  donde OUDNdestino es el nombre distintivo de la nueva unidad organizativa.

- Renombrar una cuenta de usuario.- con la opción "Cambiar nombre de usuario" se abre un cuadro de diálogo que permite modificar el nombre común (CN), nombre completo (que mapea los atributos cn y name), nombre, apellido, nombre para mostrar, nombre de inicio de sesión de usuario y nombre de inicio de sesión anterior a Windows 2000.

  También puede utilizarse la instrucción :

  ```
  Dsmod user  DNUsuario  [-upn  UPN] [-fn  Nombre] [-mi  Inicial]
                  [-ln Apellidos] [-dn nombreParaMostrar] [-email  correoElectronico]
  ```

  Con dsmod no se puede modificar los atributos samAccountName ni CN.

8 CREAR Y ADMINISTRAR GRUPOS

De forma general puede decirse que no es práctico ni aconsejable asignar derechos y permisos a usuarios individuales, equipos o identidades de servicio. Las tareas administrativas se asociarán a grupos que además identificarán a los usuarios, filtrarán Directivas de grupos, tendrán asignadas directivas de contraseñas, etc.

8.1 Concepto de grupo

La función de los grupos es coleccionar elementos para administrarlos como una única entidad. Los grupos son seguridades principales con un identificador de seguridad (SID) que a través de su atributo "member" agrupan otras seguridades principales (usuarios, equipos, contactos y otros grupos) para facilitar su administración.

Si, por ejemplo, se conceden permisos sobre una carpeta a un usuario, cuando se borra el usuario deberían eliminarse las correspondientes entradas de la ACL de la carpeta. Si los permisos se asignan a un grupo en el que se incluyen los usuarios adecuados, cuando se elimina una cuenta de usuario, ésta se elimina automáticamente del grupo y no quedarán SID sin resolver en las ACL's. Además, cuando se modifica la ACL de una carpeta, ésta se propaga a sus subcarpetas y ficheros, el indicador de copia de seguridad se modifica y por tanto la carpeta con todo su contenido se copiará en el siguiente backup, aunque los datos no hayan sufrido modificación.

Del análisis exhaustivo de la administración de los recursos de una red se puede llegar a la conclusión de la necesidad de que existan dos tipos de colecciones o grupos: los que congregan usuarios con funciones similares (vendedores, directivos, alumnos de 1º de bachillerato, profesores, …) y los que administran recursos del dominio (impresores, administradores de impresora, lectores en carpeta X, …). Un ejemplo que nos ayude a comprender los distintos tipos de grupos puede ser el siguiente:

En la red de un aula de informática de un colegio se crea un dominio con un controlador de dominio que va a ser el equipo de la mesa del profesor y los servidores miembro que serán los equipos de las mesas de los alumnos. Se va a poner a disposición de todos los usuarios la impresora y una carpeta cuyo contenido serán ficheros con apuntes de las asignaturas.

Teniendo en cuenta los recursos, sin pensar qué usuarios van a utilizarlos, pueden crearse los siguientes grupos (locales):

- gl_impresores.- con permiso para imprimir.
- gl_admin_impre.- con permiso para administrar los trabajos de impresión.
- gl_lectores.- con permiso para leer de la carpeta que contiene los apuntes.
- gl_escritores.- con permiso para leer y escribir en la carpeta de apuntes.

Teniendo en cuenta los usuarios del aula, sin pensar en los recursos existentes, pueden crearse los siguientes grupos (globales):

- gg_profesores.- cuyos miembros serán las cuentas de los profesores.
- gg_bach.- cuyos miembros serán las cuentas de los alumnos de bachillerato.
- gg_asir.- cuyos miembros serán las cuentas de los alumnos del ASIR.

Para administrar el acceso de los usuarios a los recursos basta con establecer la siguiente correspondencia entre los grupos globales y los locales:

- gg_profesores miembro de gl_impresores
- gg_profesores miembro de gl_admin_impre
- gg_profesores miembro de gl_escritores
- gg_bach miembro de gl_impresores
- gg_bach miembro de gl_lectores
- gg_asir miembro de gl_impresores
- gg_asir miembro de gl_admin_impre
- gg_asir miembro de gl_lectores

Así, los profesores pueden realizar todas las operaciones, los alumnos de bachillerato pueden imprimir y leer los apuntes y los alumnos del ASIR pueden imprimir, administrar la impresora y leer los apuntes.

Puede observarse que los grupos locales son utilizados para administrar los recursos y los globales para coleccionar usuarios con funciones o características similares.

8.2 Crear y nombrar grupos

Una forma de crear grupos es seleccionar la unidad organizativa adecuada y pulsando con el botón derecho elegir las opciones “Nuevo – Grupo”.

El cuadro de diálogo que se abre solicita los diferentes nombres para el grupo. El primer “Nombre de grupo” corresponde a los atributos cn y name del objeto y debe ser único en el contenedor. El segundo, el “Nombre de grupo (anterior a Windows 2000)” es el atributo sAMAccountName utilizado por Windows NT y otros sistemas operativos y debe ser único en todo el dominio. Una práctica aconsejable para evitar problemas de duplicidad es utilizar nombres que sean distintos en todo el dominio (tanto para cn, name y sAMAccountName).

Es recomendable utilizar una convención de nombres que identifique el tipo de grupo y su función. Puede recomendarse que no se utilicen prefijos en los nombres de grupos globales puesto que frecuentemente son utilizados por usuarios no técnicos. Así, en el ejemplo anterior los grupos globales podrían ser: profesores, bachillerato y asir.

8.3 Tipos y ámbitos de los grupos

Hay dos tipos de grupos: seguridad y distribución. Los grupos de distribución se utilizan principalmente por aplicaciones de correo electrónico. Estos grupos no tienen habilitada seguridad (SID) y no se les puede asignar permisos o recursos. Si se envía un mensaje a un grupo de distribución el mensaje se envía a todos los usuarios del grupo. Los grupos de seguridad son seguridades principales con SID pudiéndose utilizar en las ACL's como entradas de permiso para controlar la seguridad del acceso a los recursos. Estos grupos también pueden utilizarse para la distribución de correo.

El ámbito de los grupos afecta a lo que contienen, a dónde puede pertenecer y dónde puede ser utilizado. Existen cuatro ámbitos de grupo: global, dominio local, local y universal. Las características que definen cada ámbito se engloban en las siguientes categorías:

- Replicación.- dónde se define y en qué sistemas se duplican.

- Pertenencia.- quienes pueden ser sus miembros y si puede contener seguridades principales de dominios confiables.

- Disponibilidad.- dónde se puede utilizar y si puede agregarse a otros grupos o a ACL's.

8.3.1 Grupos locales

- Replicación.- se definen en la base de datos local (SAM) de un servidor miembro del dominio. El grupo y sus miembros no se duplican en ningún otro sistema.
- Pertenencia.- puede incluir como miembros:

  - Cualquier seguridad principal del dominio: usuarios, equipos, grupos globales y grupos locales de dominio.
  - Usuarios, equipos y grupos globales de cualquier dominio en el bosque.
  - Usuarios, equipos y grupos globales de dominios confiables.
  - Grupos universales de cualquier dominio del bosque.

- Disponibilidad.- tiene ámbito en el equipo local solamente, en las ACL's de ese equipo y no puede pertenecer a ningún otro grupo.

Prácticamente no se utilizan. Los grupos locales Usuarios y Administradores pueden ser suficientes para administrar los equipos locales.

8.3.2 Grupos locales de dominio

Se utilizan fundamentalmente para administrar los permisos de los recursos del dominio. Sus características son:

- Replicación.- se define en el contexto del dominio y tanto él como sus miembros se replican en todos los controladores del dominio.

- Pertenencia.- puede incluir como miembros:

  - Cualquier seguridad principal del dominio: usuarios, equipos, grupos globales y grupos locales de dominio.
  - Usuarios, equipos y grupos globales de cualquier dominio en el bosque.
  - Usuarios, equipos y grupos globales de dominios confiables.
  - Grupos universales de cualquier dominio del bosque.

- Disponibilidad.- se puede agregar a las ACL's de cualquier recurso de cualquier miembro del dominio. Puede ser miembro de otros grupos locales de dominio y grupos locales de equipo.

La diferencia fundamental con los grupos locales es que su replicación y disponibilidad para todo el dominio lo hacen más útil.

8.3.3 Grupos globales

Su función fundamental es agrupar usuarios de características o funciones similares. Sus características principales son:

- Replicación.- se define en el contexto del dominio y tanto él como sus miembros se replican en todos los controladores del dominio.

- Pertenencia.- puede incluir como miembros a usuarios, equipos y otros grupos globales del mismo dominio.

- Disponibilidad.- se encuentra disponible para su uso para todos los miembros del dominio, para todos los otros dominios del bosque y para los dominios externos fiables. Puede ser miembro de cualquier grupo local o universal en el dominio o en el bosque. También puede ser miembro de un grupo local en un dominio de confianza. Finalmente a un grupo local se le pueden agregar ACL's en el dominio, en el bosque o en un dominio de confianza.

  Como se puede ver, tienen una pertenencia limitada pero una disponibilidad muy alta.

8.3.4 Grupos universales

Son útiles en bosques con múltiples dominios. Permiten definir funciones o administrar recursos que abarcan más de un dominio. Tienen las siguientes características:

- Replicación.- se definen en el contexto de un único dominio en el bosque pero se duplican en el catálogo global.

- Pertenencia.- puede incluir como miembros a usuarios, grupos globales y otros grupos universales de cualquier dominio en el bosque.

- Disponibilidad.- pueden ser miembros de un grupo universal o de un grupo local de dominio en cualquier lugar en el bosque. Puede ser utilizado para administrar recursos en cualquier lugar en el bosque.

8.4 Convertir el tipo y el ámbito del grupo

A través de las propiedades del grupo puede modificarse el tipo y ámbito, en la ficha General. Los únicos cambios directos no permitidos son los de grupo global a grupo local de dominio y viceversa. Estos cambios se pueden hacer de forma indirecta cambiando en primer lugar a grupo universal y posteriormente al deseado.

Hay que tener en cuenta que el ámbito de un grupo determina el tipo de objetos que puede contener. Si se intenta cambiar el ámbito de un grupo puede ocurrir que tenga miembros que impidan que el cambio se realice por mera incompatibilidad. En este caso el sistema mostrará el mensaje de error adecuado.

El comando dsmod permite cambiar el ámbito y tipo de un grupo con la sintaxis:

Dsmod grupo DNGrupo -secgrp {yes | no} -scope {l | g | u}

donde DNGrupo es el nombre distintivo del grupo y los dos siguientes parámetros definen el tipo y el ámbito.

8.5 Administrar la pertenencia a grupos

Pueden utilizarse diferentes métodos para incluir los miembros de un grupo: mediante la ficha “Miembros” de las propiedades del grupo, mediante la ficha “Miembro de” del elemento a incluir o seleccionando varios elementos y eligiendo la opción “Agregar a un grupo” del menú contextual.

Cuando se agrega un usuario a un grupo los cambios completos no se realizan hasta que el usuario inicia una sesión.

8.6 Estrategia para la administración de grupos

Las directrices generales a seguir como estrategia de administración pueden ser:

- Organizar lógicamente a los usuarios según las necesidades comunes.
- Crear grupos globales y agregar cuentas de usuario.
- Crear grupos locales de dominio basados en las necesidades de acceso a los recursos.
- Agregar grupos globales a grupos locales de dominio.

En un bosque con múltiples dominios, también hay grupos universales, que encajan en el dominio local y global. Los grupos globales de múltiples dominios son miembros de un único grupo universal. Ese grupo universal es un miembro de grupos locales de dominio en múltiples dominios.

9 AUTOMATIZAR LA CREACIÓN Y ADMINISTRACIÓN DE GRUPOS

Las mismas herramientas que permitían la creación y administración de grupos pueden utilizarse para los grupos: Dsadd, CSVDE, LDIFDE, Windows PowerShell y VBScript.

9.1 Dsadd

Este comando permite agregar grupos al Active Directory usándolo de la forma:

dsadd group "CN=Bachillerato,OU=Groups,DC=profe,DC=b25,DC=es"
-samid bachillerato -secgrp yes -scope g

También puede proporcionarse el nombre del grupo (DNGrupo) de alguna de las formas:

- Canalizando (filtrando) una lista de DN desde otro comando tal como Dsquery.
- Especificando una lista de DN desde la linea de comandos, separados por espacios.
- Dejando el DN vacío para que el comando los solicite, especificando un DN por línea, pulsando <Intro> después de cada nombre, y finalizando con <Ctrl>+<Z> e <Intro>.

Entre los parámetros más utilizados se encuentran

-secgrp {yes | no}.- yes = grupo de seguridad; no = grupo de distribución.

-scope {g | l | u}.- para asignar el ámbito del grupo.

-samid nombre.- nombre SAM.

-desc descripción.- descripción.

-members DNMiembro.- si hay varios miembros deberán separarse por espacios.

-memberof DNGrupo.- miembro de otros grupos existentes (separados con espacios).

9.2 Importar grupos con CSVDE

El método es similar al utilizado con los usuarios. Un ejemplo de fichero .csv sería:

objectClass,sAMAccountName,DN,member

group,Bachillerato,"CN=Bachillerato,OU=Groups,DC=profe,DC=b25,DC=es", "CN=Pedro Perez,OU=Groups,DC=profe,DC=b25,DC=es;CN=Antonio Alonso, OU=Groups,DC=profe,DC=b25,DC=es"

El formato de la instrucción podría ser:

csvde -i -f "fichero" [-k]

9.3 Administrar grupos con LDIFDE

LDIFDE es una herramienta que permite importar y exportar archivos en formato LDIF. El método es similar a CSVDE.

La página 228 tiene un ejemplo.

LDIFDE también permite modificar la pertenencia a los grupos.

9.4 Mostrar los miembros de grupo con Dsget

Desde la herramienta Usuarios y equipos de Active Directory pueden verse los miembros directos de un grupo en la ficha Miembros pero no muestra los miembros anidados. Tampoco muestra los grupos anidados a los que pertenece un usuario o equipo.

El comando dsget muestra la lista completa de pertenencia de un grupo, incluyendo los miembros anidados, con la sintaxis:

dsget group "DNGrupo" -members [-expand]

La opción "-expand" permite mostrar los miembros anidados.

De forma similar, para ver los grupos a los que pertenece un usuario o equipo puede utilizarse:

dsget user "DNUsuario" -memberof [-expand]

dsget computer "Dnequipo" -memberof [-expand]

9.5 Dsmod, dsmove y dsrm

Dsmod permite modificar los atributos de los grupos. Su sintaxis básica es:

dsmod group "DNGrupo" [opciones]

Entre las opciones se encuentran samid y desc pero más útiles pueden ser las que permiten modificar la pertenencia a un grupo:

-addmbr "DNMiembro".- para agregar un miembro al grupo.

-rmmbr "DNMiembro".- para eliminar un miembro del grupo.

Pueden incluirse múltiples entradas DN separadas por espacios.

Puede utilizarse dsget en combinación con dsmod para copiar la pertenencia a un grupo, como en el ejemplo siguiente:

```
dsget group "DN=Ventas,OU=Grupos,DC=profe,DC=b25,DC=es" -members |
   dsmod group "DN=Proyecto,OU=Grupos,DC=profe,DC=b25,DC=es" -addmbr
```

que añade los miembros del grupo Ventas al grupo Proyecto.

Dsmove permite mover o cambiar de nombre a un objeto dentro del dominio. No permite mover objetos entre dominios. Su sintaxis básica es:

```
Dsmove DNObjeto [-newname nuevoNombre] [-newparent DNOUDestino]
```

Por ejemplo para cambiar el nombre del grupo Vendedores por Comerciales sería:

```
dsmove "CN=Vendedores,OU=Grupos,DC=profe,DC=b25,DC=es"
                -newname Comerciales
```

Para mover el nuevo grupo a la OU Marketing se usaría:

```
dsmove "CN=Comerciales,OU=Grupos,DC=profe,DC=b25,DC=es"
                -newparent "OU=Marketing,DC=profe,DC=b25,DC=es"
```

Puede eliminarse un grupo o cualquier otro objeto con la instrucción Dsrm cuya sintaxis es:

```
Dsrm DNObjeto … [-subtree] [-exclude] [-nsprompt] [-c]
```

La opción "-noprompt" hace que el comando no pida conformidad y "-c" permite que el comando se siga ejecutando cuando ocurra algún error.

10 Administrar grupos en una empresa

10.1 Documentar el grupo a través de sus atributos

Para facilitar la correcta administración y uso de los grupos es conveniente documentar su propósito. De esta forma se ayudará a los administradores a conocer cuándo y cómo utilizar cada grupo. Se recomienda hacer uso de las siguientes prácticas:

- Establecer y seguir una estricta convención de nombres.- utilizar prefijos delimitados puede ayudar a ubicar el grupo correcto para un propósito particular.

- Resumir el propósito del grupo en su atributo Descripción.

- Detallar el propósito del grupo en sus Notas.- se pueden especificar, por ejemplo, las carpetas sobre las que se le conceden permisos.

10.2 Proteger contra eliminación accidental

Cuando se borra un grupo accidentalmente, si se crea otro con el mismo nombre su SID no coincidirá con lo cual no se conseguirán los objetivos deseados. En tal caso se deberá realizar la recuperación del grupo antes de que se alcance el periodo de latencia (60 días por defecto). Cuando se recupera un objeto hay que volver a introducir la mayoría de sus atributos, incluyendo el atributo miembro de los objetos de grupo.

Para prevenir la eliminación accidental y sus efectos devastadores pueden seguirse los pasos:

1. Activar la opción “Características avanzadas” del menú Ver de Usuarios y equipos de Active Directory.

2. Seleccionar la casilla de verificación “Proteger objeto contra eliminación accidental” en la ficha Objeto de las propiedades del grupo.

3. Pulsar el botón Aceptar.

Así, se aplica una entrada de control de acceso (ACE) a la ACL del objeto, que explícitamente niega los permisos Delete y Delete Subtree al grupo Everyone.

10.3 Delegar la administración de la pertenencia a un grupo

Para delegar la administración de la pertenencia a un grupo, debe asignarse el permiso "Permitir: : Escribir miembro" para el grupo. Hay muchas formas de delegar el permiso "Escribir miembro".

10.3.1 Ficha "Administrado por"

Esta ficha se encuentra en las propiedades del grupo y tiene dos propósitos: informar de quién administra el grupo y delegar el atributo "member".

Para delegar el atributo "member" hay que:

1. Seleccionar un usuario o grupo a través del botón "Cambiar". Si se introduce el nombre de un grupo se produce un error. Para que admita nombres de grupos hay que marcar la casilla de verificación correspondiente de la lista "Tipos de objetos".

2. Marcar el cuadro de verificación "El administrador puede actualizar la lista de suscripciones".

3. Pulsar sobre el botón "Aceptar". NO SIRVE EL BOTÓN APLICAR.

Cuando se especifica un grupo en la ficha "Administrado por" no se muestra información de contacto por no ser un atributo de los grupos.

10.3.2 Configuración de seguridad avanzada

Puede utilizarse el cuadro de diálogo "Configuración de seguridad avanzada" para asignar directamente el permiso "Escribir miembro", pudiéndose asignar el permiso para un grupo individual o para todos los grupos de la unidad organizativa.

Para realizar esta operación deben estar activadas las Características avanzadas de la opción Ver y seguir los pasos:

1. Seleccionar la opción Propiedades del menú contextual de la OU.

2. En la ficha Seguridad pulsar el botón "Avanzadas".

3. En el cuadro de diálogo Configuración de seguridad avanzada pulsar sobre el botón Agregar. Si no está visible pulsar sobre "Editar – Agregar".

4. En el cuadro de diálogo "Seleccionar" hay que introducir (o buscar) el nombre del

grupo al que se desea otorgar el permiso. Al finalizar pulsar sobre Aceptar.

5. En la ficha Propiedades, en la lista desplegable Aplicar a, hay que seleccionar Este objeto y todos los descendientes.

6. En la lista de permisos hay que seleccionar Permitir: : Leer miembros y Permitir: : Escribir miembros.

7. Aceptar todos los cuadros de diálogo.

10.3.3 Administrar todos los grupos de la OU

El procedimiento sería similar al anterior:

1. Seleccionar la opción Propiedades del menú contextual de la OU.

2. En la ficha Seguridad pulsar el botón “Avanzadas”.

3. En el cuadro de diálogo Configuración de seguridad avanzada pulsar sobre el botón Agregar. Si no está visible pulsar sobre “Editar – Agregar”.

4. En el cuadro de diálogo “Seleccionar” hay que introducir (o buscar) el nombre del grupo al que se desea otorgar el permiso. Al finalizar pulsar sobre Aceptar.

5. En la ficha Propiedades, en la lista desplegable Aplicar a, hay que seleccionar Todos los objetos descendientes.

6. En la lista de permisos hay que seleccionar Permitir: : Leer miembros y Permitir: : Escribir miembros.

7. Aceptar todos los cuadros de diálogo.

10.4 Grupos ocultos

La mayor parte de la gestión de una empresa está implementada por grupos. A los grupos se les conceden permisos, filtran directivas, etc.etc.

Las OU, sin embargo, no se utilizan para gestionar la empresa y, en algunos casos, simplemente no se utilizan; su función es ofrecer un ámbito de gestión para la delegación de permisos administrativos para los objetos de la OU. Por ejemplo, a las OU no se les puede asignar permisos a los recursos, no se les puede asignar directivas de contraseñas, etc. etc.

Las OU no tienen la misma flexibilidad que los grupos; por ejemplo, un usuario o equipo solo puede existir en el contexto de una única OU mientras que una seguridad principal puede pertenecer a muchos grupos. No se puede, por ejemplo, dar permiso de acceso a una carpeta o asignar una única directiva de contraseña a los usuarios de una OU. Estas operaciones pueden realizarse mediante el uso de los llamados grupos ocultos.

Un grupo oculto es un grupo que contiene los mismos usuarios que una OU, más exactamente los usuarios que cumplen un determinado criterio.

Una forma simple de crear un grupo oculto consiste en crear un grupo y a continuación, en la OU que contiene los usuarios, pulsar <Ctrl>+<A> para seleccionar todos los usuarios, pulsar con el botón derecho sobre cualquier usuario seleccionado y elegir "Agregar a grupo". Se selecciona el grupo creado y se pulsa Aceptar.

Hay que tener en cuenta que al agregar/eliminar un usuario en la OU, no se actualiza automáticamente la pertenencia al grupo oculto y hay que agregarlo/eliminarlo manualmente.

10.5 Grupos predeterminados

De forma predeterminada se crean ciertos grupos que ofrecen cierta ayuda a la hora de realizar tareas administrativas:

- Administradores de empresas (en Users del bosque o dominio).- grupo universal miembro del grupo local Administradores en cada dominio en el bosque que le da acceso completo a la configuración de todos los controladores de dominio.

- Administradores de esquema (en Users del dominio raíz del bosque).- grupo universal con control completo del esquema de Active Directory.

- Administradores (en Builtin de cada dominio).- grupo de seguridad local de dominio que tiene control completo sobre todos los controladores de dominio y datos en el contexto de nombres de dominio. El grupo Administradores en el dominio raíz del bosque es el grupo más poderoso de administración de servicios en el bosque; puede modificar la pertenencia de los grupos Administradores de empresas, Administradores de esquema y Administradores de dominio.

- Admins. del dominio (en Users de cada dominio).- grupo de seguridad global miembro del grupo Administradores de su dominio. También se agrega al grupo de Administradores locales de cada equipo miembro del dominio, obteniendo así la posesión de todos los equipos del dominio.

- Operadores de servidores (en Builtin de cada dominio).- grupo local del dominio con capacidad para realizar tareas de mantenimiento en los controladores del dominio. Tiene derecho para iniciar sesión localmente, iniciar y detener servicios, realizar

copias de seguridad y restauraciones de datos, dar formato a discos, crear y eliminar recursos compartidos y detener los controladores de dominio.

- Operadores de cuentas (en Builtin de cada dominio).- grupo local del dominio que puede crear, modificar y eliminar cuentas de usuario, grupo y equipo ubicadas en cualquier OU del dominio (a excepción de la OU Controladores de dominio), así como en los contenedores Usuarios y Computers.

  No puede modificar las cuentas de los miembros de los grupos Administradores ni Administradores del dominio, ni los grupos. Puede iniciar sesión localmente en los controladores de dominio.

- Operadores de copia de seguridad (en Builtin de cada dominio).- grupo local del dominio que puede realizar copias de seguridad y restauración de datos en los controladores de dominio. Puede iniciar sesión localmente y detener los controladores de dominio.

- Operadores de impresión (en Builtin de cada dominio).- grupo local del dominio que puede mantener las colas de impresión en los controladores de dominio. También puede iniciar sesión localmente y detener los controladores de dominio.

Los grupos administrativos anteriores están protegidos por el sistema operativo y no se pueden desproteger. Sus miembros también estarán protegidos de tal forma que sus ACL's se modifican para no heredar permisos de su OU y, además, reciben una copia de ACL bastante restrictiva.

10.6 Identidades especiales

Existen identidades especiales o grupos cuya pertenencia está controlada por el sistema operativo. Los grupos, de este tipo, más significativos son:

- Inicio de sesión anónimo.- representa las conexiones a un equipo y sus recursos que se realizan sin autenticación.

- Usuarios autenticados.- representa identidades que han sido autenticadas.

- Todos.- incluye a los usuarios autenticados y al Invitado.

- Interactivo.- usuarios que inician la sesión localmente.

- Red.- usuarios que acceden a un equipo desde la red (de forma remota).

11 EQUIPOS

Los equipos de un dominio son directrices de seguridad como los usuarios. Tienen una cuenta con un nombre de inicio de sesión y una contraseña que Windows actualiza automáticamente cada treinta días aproximadamente.

Se autentican en el dominio, pueden pertenecer a grupos, tienen acceso a recursos y se configuran con las Directivas de grupo. Y, al igual que los usuarios, algunas veces pierden su contraseña, requieren restablecerlas, o tienen cuentas que necesitan ser habilitadas o deshabilitadas.

A veces, el mantenimiento de las cuentas de equipo tiende a quedar relegado en segundo plano frente a las cuentas de usuario, perjudicando la gestión global el dominio.

Antes de poder iniciar sesión en un equipo con una cuenta de dominio, el equipo debe pertenecer al dominio. Para unirlo al dominio, el equipo debe tener una cuenta en el dominio, con su nombre de inicio de sesión (sAMAccountName), una contraseña y un identificador de seguridad (SID) que representan de forma única al equipo como seguridad principal del dominio. Estas credenciales le permiten al equipo autenticarse contra el dominio y crear una relación de seguridad que luego les permite a los usuarios iniciar sesión en el sistema con las cuentas de dominio.

11.1 Grupos de trabajo, dominios y confianzas

Un equipo individual, o que forma parte de un grupo de trabajo, guarda la información de autenticación de los usuarios y grupos en una base de datos local llamada SAM. Cuando el usuario se conecta a un recurso compartido de otro equipo del grupo de trabajo, deberá volver a autenticarse contra la identidad del equipo remoto.

Cuando un equipo se une a un dominio, delega la tarea de autenticación de usuarios en el dominio. Aunque el equipo continua manteniendo su base de datos SAM para dar soporte a los usuarios locales, las cuentas de usuario serán creadas en la base de datos o directorio central del dominio. Cuando un usuario inicia sesión en el equipo con una cuenta de dominio, es un controlador de dominio quien lo autentica. El equipo ahora confía en otra autoridad para validar la identidad del usuario. Cuando un equipo se une a un dominio, se establece una confianza entre el equipo y el dominio.

11.2 Requerimientos para unir un equipo al dominio

Para unir un equipo a un dominio se necesita:

- Crear un objeto de equipo en Active Directory.
- Tener permisos apropiados para el objeto de equipo que permitan unir un equipo con el mismo nombre que el objeto al dominio.
- Ser miembro del grupo local Administradores en el equipo para modificar su dominio o pertenencia al grupo de trabajo.

11.2.1 Unidades organizativas para los equipos

Antes de crear un objeto de equipo debe existir un lugar donde colocarlo. Cuando se crea un dominio, se crea por defecto un contenedor Computers. Este contenedor no es una unidad organizativa (OU) sino un objeto de la clase "container". Existen diferencias importantes con una OU, por ejemplo, dentro del contenedor no se puede crear una OU, por lo tanto no se puede subdividir. Tampoco se puede vincular un objeto de Directiva de grupo a un contenedor. Por lo tanto, es muy recomendable crear unidades organizativas personalizadas para alojar objetos de equipo en vez de utilizar el contenedor Computers.

La mayoría de organizaciones crean al menos dos OU para los objetos de equipo: una para alojar cuentas de equipos para los clientes, ordenadores portátiles y otros sistemas de usuarios y otra para los servidores. Además, durante la instalación de Active Directory se crea la unidad organizativa "Domain Controllers". Las dos OU se crean separadas para ofrecer ámbitos únicos (diferentes) de administración.

Las organizaciones distribuidas geográficamente con equipos de soporte local, frecuentemente dividen la OU padre en subunidades organizativas, una para cada sitio.

Posteriormente se aplicarán directivas de grupo (GPO) a las OU que afectarán a todos los equipos contenidos.

11.2.2 Delegar permisos para crear equipos

Por defecto los grupos Administradores de empresas, Administradores del dominio, Administradores y Operadores de cuentas tienen permisos para crear objetos de equipo en cualquier OU nueva. Es recomendable restringir completamente la pertenencia a los tres primeros grupos y no agregar usuarios al grupo Operadores de cuentas.

Se recomienda delegar los permisos para crear objetos de equipo a los administradores apropiados o al personal de soporte. El permiso que se requiere es Crear objetos de equipo, que se puede asignar a un grupo para una determinada OU.

Con los permisos adecuados, la creación de un objeto de equipo consiste en situarse sobre la OU adecuada, botón derecho y elegir Nuevo – Equipo. El cuadro de diálogo Nuevo objeto – Equipo solicitará el nombre del equipo y el usuario o grupo que podrá unir el equipo al dominio con la cuenta creada.

El proceso de crear una cuenta de equipo antes de unir el equipo al dominio tiene la ventaja de situar el equipo en la OU correcta y es, por lo tanto, delegada de acuerdo a las directivas de seguridad definidas por la ACL de la OU y está dentro del ámbito de las GPO vinculada a la OU antes de unir los equipos al dominio.

11.2.3 Unir un equipo al dominio

Una vez que se cumplen los dos primeros requerimientos para unir un equipo a un dominio: el objeto de equipo existe y se ha especificado quien tiene permisos para unir un equipo con el mismo nombre al dominio, queda que un Administrador local del equipo modifique la pertenencia de dominio del equipo e introduzca las credenciales de dominio especificadas. Los pasos a seguir pueden ser:

1. Iniciar en el equipo una sesión con credenciales de Administrador local del equipo.

2. Acceder a las propiedades del sistema pulsando con el botón derecho sobre “Mi PC” o “Equipo” y eligiendo Propiedades.

3. Seguir las opciones: Ficha Nombre de equipo – Cambiar – en “Miembro de” seleccionar Dominio – especificar el nombre del dominio.

   Si el equipo no tiene configurado como **DNS1 la dirección IP del servidor de dominio** puede que se produzca un error.

4. Se pulsa Aceptar. Windows solicitará las credenciales de su cuenta de usuario en el dominio y realiza las operación solicitada. El equipo se une al dominio asumiendo la identidad de su objeto de Active Directory. Éste configura su SID para coincidir con el SID de la cuenta de equipo del dominio y establecer una contraseña inicial con el dominio. Además, el equipo agrega el grupo de Administradores del dominio al grupo local Administradores y el grupo Usuarios del dominio al grupo local Usuarios.

5. Se solicita reiniciar el equipo. Debe salirse aceptando los diferentes cuadros de diálogo y se reinicia el equipo.

   Ahora ya se puede iniciar una sesión utilizando las credenciales del dominio.

También puede unirse un equipo al dominio mediante la instrucción Netdom.exe. Utilizar el comando permite el uso de scripts, permite su ejecución desde un equipo remoto, permite especificar la OU para el objeto de equipo, etc. Su sintaxis básica es:

```
netdom  join  Equipo  /domain:Dominio  [/OU:"Ruta de OU"]
              [/User0:Usuario] [/Password0:{Contraseña | *}]
              [/UserD:Usuario del dominio] [/PasswordD:{Contraseña del dom. | *}]
              [/SecurePasswordPrompt] [/REBoot:tiempo en segundos]
```

El significado de las opciones se intuye. SecurePasswordPrompt se utiliza cuando se especifica como contraseña un asterisco (*) y muestra un cuadro de diálogo para introducir la contraseña.

11.2.4 Importancia de crear previamente los objetos de equipo

Es conveniente crear una cuenta de equipo antes de unir el equipo al dominio, aunque por compatibilidad con Windows anteriores se permite unir un equipo al dominio desde el equipo sin que exista previamente una cuenta para el equipo. En este caso Windows crea un objeto de equipo automáticamente en el contenedor de equipos predeterminado, da permiso para unir un equipo a ese objeto y une el sistema al dominio. Este comportamiento de Windows presenta tres problemas:

- El objeto se crea en el contenedor predeterminado, que no es lo más recomendable.
- Si se quiere colocar el equipo en la OU adecuada hay que realizar la operación adicional de moverlo, que frecuentemente se olvida.
- Cualquier usuario puede unir un equipo al dominio, no se requieren permisos administrativos a nivel del dominio, lo que representa una vulnerabilidad de la seguridad por permitir que un usuario sea propietario de un objeto de seguridad principal que puede modificar sus propiedades.

11.3 Configurar el contenedor de equipos predeterminado

Cuando se une un equipo al dominio y no existe previamente un objeto de equipo en el Active Directory, Windows crea una cuenta de equipo en el contenedor predeterminado que por defecto es CN=Computers,DC=domain (como dominio el que corresponda). A continuación no hay que olvidar mover la cuenta a la OU correcta, que tendrá los permisos de administración delegados convenientemente, tendrá vinculadas las GPO que permitan administrar la configuración de los objetos de equipo y permitirá la herencia o propagará los permisos adecuados.

Para reducir el impacto que supone la creación de cuentas de equipo en el contenedor predeterminado puede establecerse como contenedor predeterminado una unidad organizativa sujeta a la delegación y configuración adecuadas. El comando Redircmp.exe, disponible en los controladores de dominio, permite establecer cual será el contenedor predeterminado con la sintaxis:

redircmp "DN de la OU para nuevos objetos de equipo"

De forma similar puede establecerse el contenedor predeterminado de usuarios, que por defecto es CN=Users,DC=domain (dominio el que corresponda) para cuando no se especifica una OU concreta, haciendo uso del comando Redirusr.exe, cuya sintaxis es similar a la de redircmp.

11.4 Restringir la posibilidad de los usuarios de crear cuentas de equipo

Windows permite a cualquier usuario autenticado crear hasta diez objetos de equipo en el contenedor de equipos predeterminado, sin que tenga ningún permiso explícito para hacerlo. Esto es problemático desde una perspectiva de seguridad, ya que los equipos son directrices de seguridad y el creador de una seguridad principal tiene permisos para gestionar las propiedades del equipo.

La cuota de diez equipos se establece por el atributo ms-DS-MachineAccountQuota del dominio y permite a cualquier usuario crear diez cuentas de equipo sin control. Para resolver esta cuestión y que los usuarios no administradores no puedan unir equipos al dominio, puede modificarse el atributo especificado de la siguiente forma:

1. Desde Herramientas administrativas abrir el "Editor ADSI.

2. Botón derecho sobre Editor ADSI y elegir Conectar a.

3. En la sección Punto de conexión elegir Seleccione un contexto de nomenclatura conocido y, desde la lista desplegable, seleccionar Contexto de nomenclatura predeterminado.

4. Aceptar.

5. Ampliar Contexto de nomenclatura predeterminado.

6. Botón derecho sobre la carpeta del dominio y seleccionar Propiedades.

7. Seleccionar ms-DS-MachineAccountQuota y pulsar sobre Editar.

8. Introducir 0 y Aceptar.

Así, aunque el grupo Usuarios autenticados tiene derecho para agregar estaciones al dominio, no podrá hacerlo. Ahora, solamente pueden unir equipos al dominio los usuarios a los que se les ha delegado permisos específicos para unir objetos de equipo organizados previamente o para crear nuevos objetos de equipo.

12 AUTOMATIZAR LA CREACIÓN DE OBJETOS DE EQUIPO

Cuando se necesita crear un número considerable de cuentas de equipo puede hacerse uso de los comandos CSVDE, LDIFDE y Dsadd, así como de VBScript y Windows PowerShell.

12.1 Crear equipos con CSVDE, LDIFDE y Dsadd

CSVDE funciona de forma similar que para importar usuarios o grupos. La sintaxis básica del comando es:

csvde [-i] [-f "archivo"] [-k]

El archivo puede generarse, por ejemplo, con el Bloc de notas o con Microsoft Office Excel. Un ejemplo de fichero puede ser el siguiente:

DN,objectClass,CN,userAccountControl,sAMAccountName
"CN=ordenador01,OU=clientes,DC=profe,DC=b25,DC=es",computer,ordenador01,
4096,ordenador01$
"CN=ordenador02,OU=clientes,DC=profe,DC=b25,DC=es",computer,ordenador02,
4096,ordenador02$

Al importar equipos no se debe olvidar incluir el atributo "userAccountControl" con valor 4049 para asegurar que el equipo será capaz de unirse a la cuenta. También debe incluirse sAMAccountName (nombre anterior a Windows 2000) y los valores deben ser los nombres de los equipos seguidos del carácter $.

LDIFDE se utiliza de forma similar a como se hacía con los usuarios o grupos. Los objetos en este fichero se separan con una línea en blanco y los atributos de cada fichero se especifican a razón de un atributo en cada línea, debiendo ser el primero el atributo DN del objeto a importar.

La página 283 muestra un ejemplo.

La sintaxis básica del comando es:

ldifde [-i] [-f "fichero"] [-k]

El comando Dsadd también permite crear cuentas de equipo. Su sintaxis básica es:

Dsadd computer DNEquipo

Con dsadd pueden crearse varias cuentas de una sola vez, de la forma:

- Introduciendo varios DN en la misma línea, separados por espacios.

- Canalizando una lista de DN desde otro comando como dsquery.

- Dejando el parámetro DN vacío e introduciéndolos después a razón de uno por línea, terminando la lista con <Ctrl>+<Z> e <Intro>.

Dsadd computer puede tener los parámetros adicionales: -samid:SAMNombre, -desc:Descripción y -loc:Localización.

12.2 Crear equipos con Netdom

Netdom permite realizar ciertas tareas de administración de seguridad y cuentas de dominio, entre las que se encuentran unir un equipo a un dominio y crear una cuenta de equipo. Para esta última la sintaxis sería:

```
netdom add nombreEquipo /domain:nombreDominio [/ou:DNOU]
          [/userd:usuario /passwordd:contraseña]
```

Las opciones son obvias. Si no se utiliza la opción /ou:DNOU la cuenta se creará en el contenedor de equipos predeterminado.

13 Dar soporte a objetos de equipo y cuenta

13.1 Configurar propiedades de equipo

Cuando se crea una cuenta de equipo se configuran solamente los atributos fundamentales, incluyendo el nombre del equipo y la delegación para unir el equipo al dominio. A continuación deben configurarse las demás propiedades como parte del proceso de los pasos previos para dar de alta la cuenta de equipo.

A través de las propiedades puede establecerse su ubicación, descripción, pertenencia a grupos, permisos de marcado, y se puede vincular a un objeto de usuario del usuario a quien se le asignará el equipo. La ficha Sistema operativo es de solo lectura. La información estará en blanco hasta que un equipo se una al dominio utilizando esa cuenta, momento en el que el cliente publica la información de su cuenta.

El atributo de enlace “manageBy” mostrado en la ficha “Administrado por” crea una referencia cruzada a un objeto de usuario.

En la ficha Miembro de puede agregarse el equipo a los grupos y asignar así permisos de acceso a los recursos para el equipo (para el grupo) o filtrar la aplicación de un GPO.

Seleccionando varios equipos, pueden modificarse ciertos atributos de forma conjunta.

Con el comando Dsmod solamente se pueden modificar los atributos description y location. Su sintaxis es:

Dsmod computer “DNEquipo” [-desc Descripcion] [-loc ubicación]

13.2 Mover un equipo

Se puede mover un equipo desde la herramienta Usuarios y equipos de Active Directory mediante la técnica de arrastrar y soltar o a través de la opción Mover del menú contextual del equipo.

Los permisos predeterminados de los operadores de cuentas les permiten mover objetos de equipo entre contenedores, incluido el contenedor Computers, excepto en la OU Controladores de dominio. Los Administradores no tienen esta última restricción.

No hay una forma de delegar las tareas específicas para mover un objeto de equipo en Active Directory. El permiso se deriva del permiso para eliminar objetos en el contenedor origen y del permiso para crearlos en el destino.

El comando Dsmove permite mover equipos. Su sintaxis es:

Dsmove DNObjeto [-newname NuevoNombre] [-newparent OUDestino]

-newname permite cambiar el nombre y -newparent especifica la OU destino. Por ejemplo:

```
dsmove "CN=Ordenador15,OU=Computers,DC=profe,DC=b25,DC=es"
       -newparent "OU=Clients,DC=profe,DC=b25,DC=es"
```

13.3 Administrar un equipo desde Usuarios y equipos de Active Directory

Una herramienta poco utilizada en la administración de equipos se encuentra en Usuarios y equipos de AD, en el menú contextual del equipo, opción Administrar. Ofrece acceso inmediato a los eventos registrados del equipo, usuarios y grupos locales, configuración de carpetas compartidas y otras extensiones de administración. Debe ejecutarse como miembro del grupo Administradores del equipo remoto.

13.4 Inicio de sesión de un equipo

Cada equipo miembro del dominio de Active Directory mantiene una cuenta de equipo con un nombre de usuario (sAMAccountName) y una contraseña, tal como la cuenta de un usuario. El equipo almacena su contraseña en la forma de un secreto de autoridad de seguridad local (LSA) y modifica su contraseña en el dominio cada 30 días aproximadamente. El servicio Netlogon utiliza las credenciales para iniciar sesión en el dominio, que establece el canal de seguridad con un miembro del dominio.

13.5 Problemas con las cuentas de equipo

En algunos escenarios los equipos no pueden autenticarse con el dominio:

- Después de reinstalar el sistema operativo en un equipo por haber cambiado su SID.
- Después de una restauración de datos por haber cambiado su clave con el dominio.
- Dessincronización de la clave del equipo con respecto a la del dominio.

Los signos más comunes de problemas con las cuentas de equipo son:

- Mensajes en el inicio de sesión indicando que el controlador de dominio no se puede contactar, que se ha perdido la cuenta de equipo, que la contraseña en la cuenta de

equipo es incorrecta, que la confianza entre el equipo y el dominio se ha perdido, etc.

- Mensajes de error o eventos en el registro de eventos indicando problemas similares.

- Una cuenta de equipo se pierde en Active Directory.

13.6 Restablecer una cuenta de equipo

Cuando falla el canal de seguridad hay que restablecerlo. Muchos administradores realizan esto eliminando el equipo del dominio, colocándolo en un grupo de trabajo y luego uniéndolo nuevamente al dominio. Esto no es una buena práctica porque se pierde su SID y la pertenencia a los grupos.

Lo que hay que hacer es restablecer el canal de seguridad. Para ello puede utilizarse la Herramienta Usuarios y equipos de AD, Dsmod.exe, Netdom.exe o Nltest.exe. Restableciendo la cuenta, el SID del equipo permanece igual y mantiene la pertenencia a los grupos.

- En Usuarios y equipos de AD hay que elegir la opción Restablecer cuenta del menú contextual del equipo. El equipo necesitará volver a unirse al dominio y reiniciarse.

- Con el comando "dsmod computer "DNEquipo" -rest". Habrá que volver a unir el equipo al dominio y reiniciarlo.

- Con el comando "Netdom reset NombreEquipo /domain NombreDominio /user NombreUsuario /password0 {contraseña | *} donde las credenciales corresponden al grupo local de Administradores del equipo. El comando intenta restaurar el canal seguro restableciendo la contraseña en el equipo y en el dominio, por lo tanto, no requiere volver a unirse al dominio o reiniciar.

- En el equipo que ha perdido la confianza, con el comando "nltest /server: NombreServidor sc_reset:DOMINIO\ControladorDominio" que también intentará restaurar el canal seguro restableciendo la contraseña y no se requiera volver a unirse al dominio o reiniciar.

Evidentemente, en primer lugar debe intentarse restablecer la contraseña con los dos últimos comandos para no tener que volver a unir el equipo al dominio ni reiniciar.

13.7 Cambio de nombre a un equipo

Hay que tener en cuenta que para que no se pierda la sincronía debe cambiarse el nombre de forma que se cambie tanto al objeto del dominio como al equipo.

Desde el entorno gráfico puede cambiarse iniciando una sesión en el equipo, ya sea a nivel local o con una sesión remota. Se abren las propiedades del Sistema desde el Panel de control y, en la sección Configuración de nombre de equipo, dominio y grupo de trabajo, se pulsa en Cambiar configuración, se pulsa si es necesario sobre Continuar, y se pulsa sobre Cambiar en la ficha Nombre de equipo.

Desde la linea de comandos puede hacerse con el comando Netdom con la sintaxis:

```
netdom renamecomputer NombreEquipo /newname:NombreNuevo
      [/user0:usuario] [/password0:{contraseña | *}
      [/userD:usuario] [/passwordD:{contraseña | *}
      [/SecurePasswordPrompt] [/Reboot[:segundos]]
```

Para ejecutar el comando deben tenerse las credenciales de un miembro del grupo local Administradores y las credenciales con permisos para cambiar el nombre del objeto de equipo en el dominio.

13.8 Deshabilitar y habilitar cuentas de equipo

Cuando un equipo está fuera de línea o no se va a utilizar por un periodo largo de tiempo puede, y debe, deshabilitarse su cuenta de equipo. El menú contextual del equipo ofrece las opciones Deshabilitar y Habilitar cuenta que permiten realizar estas operaciones.

Mientras una cuenta está deshabilitada, el equipo no puede crear un canal seguro con el dominio. Los usuarios que no hayan iniciado sesión previamente en el equipo no podrán iniciar sesión.

Para deshabilitar/habilitar un equipo desde la linea de comandos puede utilizarse el comando dsmod con las sintaxis:

```
dsmod computer DNEquipo -disabled yes
dsmod computer DNEquipo -disabled no
```

13.9 Eliminar cuentas de equipo

Cuando se elimina una cuenta de equipo se pierde su SID y su pertenencia a los grupos. La operación se puede realizar mediante la opción Eliminar de su menú contextual.

La instrucción “dsrm DNEquipo” también elimina un equipo.

13.10 Reciclar equipos

Cuando se sustituye un equipo por otro, por ejemplo por razones de actualización de hardware, se presenta el escenario típico para restablecer la cuenta de equipo.

Al restablecer la cuenta se restablece la contraseña pero se mantienen todas las demás propiedades del objeto de equipo.

14 Directivas de grupo

Las directivas de grupo ofrecen una infraestructura en la que se definen centralizadamente las configuraciones para ser implementadas a usuarios y equipos de la empresa. En un entorno administrado por una infraestructura de Directiva de grupo bien implementada, poca o ninguna configuración se debe realizar directa y localmente sobre un equipo de escritorio. Todas las configuraciones se definen, se refuerzan y se actualizan configurando los objetos de la Directiva de Grupo (GPO) que afectan a una parte de la empresa tan amplia como la totalidad de un sitio o dominio o tan limitada como una unidad organizativa o un grupo.

Para hacerse una idea de las propiedades o configuraciones manejadas por las directivas, puede echarse un vistazo a las directivas locales.

14.1 Configuración y ámbito de las directivas

El componente más elemental de la Directiva de grupo es una configuración de directiva individual, o simplemente una directiva. Por ejemplo, una configuración de directiva que impide a un usuario acceder a herramientas de edición del registro. Si se define esa configuración de directiva y se aplica a un usuario, el usuario no podrá ejecutar programas como Regedit.exe. Otra configuración de directiva permite deshabilitar la cuenta de Administrador local, que puede utilizarse para deshabilitar la cuenta de Administrador en todos los equipos de escritorio y portátiles.

Como se puede ver, algunas configuraciones de directiva afectan a los usuarios, sin tener en cuenta los equipos, y otras a los equipos, sin tener en cuenta a los usuarios. Unas directivas de grupo son parámetros de configuración de los usuarios y otras de configuración de equipos.

Las configuraciones de directiva se definen y existen dentro de un objeto de Directiva de grupo (GPO). Un GPO es un objeto que contiene una o más configuraciones de directiva.

Los GPO se pueden administrar en Active Directory utilizando la consola Administración de directivas de grupo. Los GPO se muestran en un contenedor llamado Objetos de directiva de grupo. Para crear un GPO nuevo puede utilizarse la opción Nuevo del menú contextual de dicho contenedor.

Para editar un GPO basta con seleccionar la opción Editar de su menú contextual. El GPO se abrirá en el Editor de administración de directivas de grupo (GPME). El GPME muestra las configuraciones de directivas disponibles en una jerarquía organizada que comienza con la división entre la configuración de equipos y la de usuarios. Estas divisiones se descomponen en las carpetas Directivas y Preferencias, estas en otras subcarpetas, y así sucesivamente hasta el nivel más bajo donde se encuentran las directivas.

Para definir una configuración de directiva hay que hacer doble click sobre la directiva y configurarla en el cuadro de dialogo de Propiedades. La configuración puede tener tres estados: No configurada, habilitada y deshabilitada.

El significado de cada uno de los estados es el siguiente:

- No configurada.- el GPO no modificará la configuración existente de esa directiva particular para el usuario o equipo.

- Habilitada.- se aplica el cambio a los usuarios o equipos a los que afecte el GPO.

- Deshabilitada.- se aplica pero de forma inversa a la anterior.

Hay que tener en cuenta que algunas directivas conllevan la negación de un permiso, por ejemplo, denegar el inicio de sesión localmente. En este caso habilitar la directiva supone negar el permiso de inicio de sesión local y deshabilitarla conlleva obtener el permiso.

Algunas configuraciones de directivas agrupan varias configuraciones y pueden requerir parámetros opcionales.

La configuración de un GPO no afecta a los usuarios o equipos hasta que se delimita el GPO, es decir, hasta que se especifica a qué usuarios y equipos se aplica. Hay varios métodos para determinar el alcance del GPO. Uno consiste en vincular el GPO al sitio, dominio u OU de Active Directory y afectará a todos los objetos contenidos. Un único GPO puede vincularse a varios sitios o unidades organizativas.

También puede limitarse el alcance del GPO utilizando un filtro de seguridad, en el que se especifican los grupos de seguridad globales a los que se aplica, o un filtro del Instrumental de administración de Windows (WMI), que utiliza características del sistema como pueden ser la versión del S.O. o el espacio libre del disco.

Un usuario o equipo individual puede estar dentro del ámbito de múltiples GPO's vinculados a sitios, dominios y OU en los que el usuario o equipo existen. El conjunto resultante de directivas también se denomina RSoP.

Las configuraciones de directiva de la rama “Configuración del equipo” se aplican cuando se inicia el sistema y posteriormente cada 90 a 120 minutos; las de la rama “Configuración de usuario” cuando inicia la sesión el usuario y posteriormente cada 90 a 120 minutos. La aplicación de directivas se conoce como actualización de la Directiva de grupo.

Para hacer una actualización manual puede utilizarse el comando Gpupdate.exe; para limitar la actuación del comando a un equipo o usuario pueden utilizarse los parámetros: “/target:equipo o /target:usuario. La actualización automática (en segundo plano) solamente se efectúa si el GPO ha sido actualizado. El parámetro /force fuerza a que se realice una actualización. Las opciones /logoff y /boot originan un cierre de sesión o reinicio

respectivamente si las configuraciones que se aplican lo requieren.

14.2 Procesos que ejecutan las directivas en los equipos cliente

Cuando se inicia la actualización de la Directiva de grupo, un servicio que se ejecuta en todos los sistemas Windows determina los GPO's que se aplicarán al equipo o al usuario. Este servicio descarga cualquier GPO que no esté almacenado en la caché. Después, una serie de procesos llamados extensiones por el lado cliente (CSE) interpretan las configuraciones de los GPO's y hacen los cambios apropiados al equipo local o al usuario que ha iniciado recientemente la sesión. Hay procesos para cada categoría principal de configuración de directiva: un proceso aplica cambios de seguridad, otro ejecuta scripts de inicio y registro de sesión, otro instala software, … Cada versión de Windows ha agregado procesos (CSE) para ampliar el alcance de las Directivas de grupo.

Estos procesos funcionan como clientes dirigidos desde el dominio. La Directiva de grupo cliente extrae los GPO's del dominio provocando que los procesos (CSE) apliquen las configuraciones localmente. Incluso el comportamiento de los procesos se puede configurar a través e las Directivas de grupo. La mayoría de CSE (procesos) aplica la configuración de un GPO solamente si el GPO ha cambiado.

La mayoría de directivas se aplican de tal manera que los usuarios estándar no pueden cambiar la configuración en sus sistemas, siempre están sujetos a la configuración forzada por la Directiva de grupo. Únicamente si el usuario es un Administrador de ese sistema podrá cambiar algunas configuraciones. Si un Administrador modifica una configuración de tal forma que no sigue las normas de la directiva, la configuración se restablecerá a su estado anterior a la modificación en la siguiente actualización de la Directiva de grupo.

Pueden configurarse los CSE para aplicar la configuración de directiva, incluso si el GPO no ha cambiado, en una actualización en segundo plano.

Existen ciertas configuraciones de seguridad que se vuelven a aplicar cada 16 horas, aunque no haya cambiado el GPO.

Para que las directivas se actualicen adecuadamente es conveniente habilitar la configuración de directiva “Esperar siempre la detección de red al inicio del equipo y de sesión”, de lo contrario un cliente puede iniciar el equipo y un usuario puede iniciar sesión sin recibir las últimas directivas desde la red.

Las conexiones lentas y los sistemas desconectados influyen en la forma en que se actualizan las directivas. Más información en la página 321.

14.3 GPO's locales y de dominio

Cada equipo tiene muchos GPO's almacenados localmente en el sistema, los GPO's locales, y pueden estar dentro del ámbito de cualquier número de GPO's de dominio.

Cuando un equipo pertenece a un dominio las configuraciones de los GPO's vinculados al sitio, dominio o OU anulan la configuración de los GPO's locales.

14.3.1 GPO's locales

El GPO local, que existe aunque el equipo no pertenezca a ningún dominio o grupo, afectan solamente al equipo en el que se almacenan. Se almacenan en el directorio %SystemRoot%\System32\GroupPolicy.

En el elemento Configuración del equipo se configuran todos los parámetros relacionados con el equipo. En el elemento Configuración de usuarios se configuran los parámetros que afectan a todos los usuarios. Las configuraciones de usuarios pueden verse modificadas por las configuraciones de los GPO's locales de Administradores y no administradores. Puede concretarse más la configuración con GPO's aplicadas a cuentas de usuario particulares.

La prioridad de las configuraciones es la siguiente:

- GPO locales.
- GPO local de Administradores y no administradores.
- GPO local de usuario.

Así, las GPO's de usuario anulan las de Administradores y no administradores, y estas a las locales.

Para crear y editar GPO's locales se puede ejecutar el comando mmc.exe y añadir el complemento Editor de objetos de directiva de grupos.

14.3.2 GPO's de dominios

Los GPO's basados en dominio se crean en Active Directory y se almacenan en los controladores de dominio. Se utilizan para administrar de forma centralizada la configuración de los usuarios y equipos del dominio.

Cuando se instala AD se crean de forma predeterminada dos GPO's:

- Directiva predeterminada de dominio.- está vinculado al dominio y no tiene ningún grupo de seguridad o filtros WMI asignado, afectando así a todos los usuarios y equipos del dominio.

  Se recomienda modificar según las necesidades la configuración de las directivas relacionadas con este GPO pero no incluir otras nuevas. Si se necesita establecer otras configuraciones deben crearse GPO's adicionales y vincularse al dominio.

- Directiva predeterminada de controladores de dominio.- Está vinculado a la OU Controladores de dominio. Esta OU debe contener únicamente controladores de dominio. Este GPO debe modificarse para implementar directivas de auditoría y derechos de usuario requeridos en los controladores de dominio.

14.4 Crear, editar y vincular GPO's de dominio

Para crear un GPO se puede utilizar la opción Nuevo del menú contextual del contenedor Objetos de Directiva de grupo.

Por defecto, tienen permiso para crear GPO's el grupo Admins. del dominio y el grupo Propietarios del creador de directivas de grupo. Para delegar permisos a otros grupos hay que seleccionar el contenedor Objetos de directiva de grupo, seleccionar la ficha Delegación y añadir los usuarios o grupos adecuados.

Después de crear el GPO hay que establecer su ámbito vinculándolo a un sitio, dominio u OU. Una forma de vincular un GPO es pulsar con el botón derecho sobre el contenedor y elegir la opción Vincular un GPO existente. También se puede crear un vínculo a un GPO desde un sitio si se elige de su menú contextual la opción Crear un GPO en este dominio y vincularlo aquí (se crea y se vincula).

Puede delegarse el permiso para vincular GPO's a un contenedor seleccionando el mismo, eligiendo la ficha Delegación y añadiendo los usuarios o grupos oportunos.

Para editar un GPO basta elegir la opción Editar de su menú contextual.

14.5 Configuración de directivas

Las dos divisiones principales de configuración de directiva son: Configuración del equipo y Configuración el usuario, que a su vez se dividen en Directivas, que se comportan como en las versiones anteriores de Windows, y Preferencias, con opciones nuevas de Windows 2008. Dentro de estas últimas divisiones, las Directivas se encuentran agrupadas en categorías:

- Configuración de software.- ayuda a especificar cómo se instalarán y mantendrán las aplicaciones. También permite agregar configuraciones para los proveedores de software.

- Configuración de Windows.- contiene a su vez los elementos:

  - Scripts.- permite especificar los scripts de encendido/apagado del equipo o inicio/cierre de sesión del usuario.

  - Configuración de seguridad.- permite configurar la seguridad y se puede realizar después, o en vez de, utilizar una plantilla de seguridad. El tema 7 contiene una discusión de tallada.

  - QoS basada en directiva.- define las directivas que administran el tráfico en la red.

- Plantillas administrativas.- contiene las configuraciones basadas en el registro. La descripción de cada configuración se puede ver en la ficha Explicación de las propiedades de cada directiva y en la ficha Extendido del Editor de directivas, que aparece en la parte inferior del panel de detalles.

Las Preferencias permiten administrar configuraciones adicionales y constan de las agrupaciones:

- Configuración de Windows.

- Configuración del panel de control.

14.6 Almacén central

En entornos complejos, los ficheros relativos a los GPO's pueden ubicarse en un almacén central, en una carpeta única de SYSVOL. Una vez establecido el almacén central, el editor de directivas lo reconoce y carga todas las plantillas administrativas desde dicho almacén en vez de desde el equipo local.

14.7 Filtros para las plantillas administrativas

Para la configuración de las plantillas administrativas, pueden crearse filtros para ubicar configuraciones de directivas específicas.

Para crear un filtro hay que pulsar con el botón derecho sobre Plantillas administrativas y seleccionar Opciones de filtro. Para ubicar una directiva específica hay que seleccionar Habilitar filtros de palabra clave, se introducen las palabras que se desea utilizar

como filtro y se seleccionan los campos dentro de los que se realizará la búsqueda. El cuadro de diálogo Opciones de filtro permite filtrar la vista para mostrar solamente las directivas que han sido configuradas, lo que ayuda a ubicar y modificar configuraciones que ya están especificadas en el GPO.

14.8 Otras consideraciones

Es aconsejable documentar las configuraciones de directivas en el elemento Plantillas administrativas especificando el efecto deseado. La ficha Comentarios permite realizar dicha configuración. Los comentarios podrán ser utilizados posteriormente en las búsquedas y filtros.

Otra característica de las Directivas de grupo son los GPO's de inicio que funcionan a modo de Plantillas para crear otros GPO's similares. Puede crearse un nuevo GPO a partir de otro de inicio del que se copiarán las configuraciones.

Cuando se crea un nuevo GPO se puede seleccionar: iniciar con un GPO vacío, iniciar con uno de los GPO's de inicio existentes o iniciar con un GPO de inicio personalizado. Los GPO de inicio se usan a modo de plantillas; su configuración se copia al GPO nuevo.

Cuando un usuario o equipo deja de estar en el ámbito de un GPO, su configuración vuelve a su estado original en la siguiente actualización de directivas. Este comportamiento no es así para las llamadas directivas no administradas, cuya configuración persiste en el registro sin volver a su estado original.

14.9 Resumen

Un sitio puede definirse como un grupo lógico de dominios.

Directiva de grupo.- regla que define algún tipo de permiso, derecho o configuración de alguno de los múltiples aspectos configurables del sistema operativo.

GPO.- conjunto de directivas que puede aplicarse a un sitio, dominio o unidad organizativa.

Hay varios tipos de Directivas:

- Locales.- afectan únicamente al equipo local. Se definen en el equipo y se pueden desactivar. Existen tres niveles, que se aplican en el siguiente orden:

  - Directiva de grupo local.
  - Directiva de grupo local para administradores y no administradores.
  - Directiva de grupo local para usuarios.

- De dominio.- afectan al dominio y se definen en el Active Directory. Tienen preferencia (anulan) sobre las locales. Se dividen en dos grandes grupos:

    - Configuración del equipo.
    - Configuración de usuario.

Orden de aplicación:

- Directiva de grupo local.
- Directiva de grupo de sitio.
- Directiva de grupo de dominio.
- Directiva de grupo de unidad organizativa.
- Directiva de grupo de unidad organizativa hija o de subunidad organizativa.

Orden en la ejecución de directivas:

- La red se pone en funcionamiento y se aplican las directivas de grupo de los equipos.
- Se ejecutan los scripts de arranque.
- El usuario pulsa <Ctrl>+<Alt>+<Supr> e inicia sesión.
- Se ejecutan las directivas de usuario.
- Se ejecutan los scripts de inicio de sesión del usuario.

15 AUDITORÍAS

La auditoría se encarga de registrar las actividades especificadas para su posterior revisión e identificación de comportamientos. Puede registrar actividades correctas o intentos maliciosos de acceso a los recursos. Involucra tres herramientas de administración: la directiva de auditoría, la configuración de auditoría de los objetos y el registro de seguridad.

15.1 Directiva de auditoría

La directiva de auditoría configura un sistema para inspeccionar categorías de actividades. Para configurar la auditoría hay que definir la configuración de la directiva pulsando dos veces en cualquier configuración de directiva y seleccionando la casilla de verificación Definir esta configuración de directiva. A continuación se selecciona si la auditoría se efectúa sobre eventos correctos, eventos erróneos o ambos.

DIRECTIVAS DE AUDITORÍA		
Directiva	**Explicación**	**Configuración predeterminada para controladores de dominio**
Auditar el acceso a objetos	Acceso a carpetas, ficheros, claves de registro e impresoras que tienen sus propios SACL. Hay que configurar las entradas de las SACL de los objetos.	Se auditan eventos correctos de acceso a objetos.
Auditar el acceso del servicio de directorio	Similar a la anterior pero aplicada a objetos de Active directory.	Se auditan eventos correctos de acceso al servicio de directorio.
Auditar el cambio de directivas	Cambios a la directiva de asignación de derechos de usuario, de auditoría o de confianza.	Se auditan los cambios de directiva correctos.
Auditar el seguimiento de procesos	Activación de programas y éxito de procesos.	Se auditan eventos de seguimiento de procesos correctos.
Auditar el uso de privilegios	Uso de privilegios o derechos de usuario.	No se audita.
Auditar eventos de inicio de sesión	Inicios de sesión de los usuarios.	Se auditan los inicios de sesión correctos o erronéos.
Auditar eventos de inicio de sesión de cuenta	Inicio de sesión de usuarios o equipos de Active Directory.	Se audita el inicio de sesión correcto o erróneo.

Auditar eventos del sistema	Inicio y apagado del sistema o modificaciones que afectan al sistema o al registro de seguridad.	Se auditan eventos del sistema correctos o incorrectos.
Auditar la adminis-tración de cuentas	Creación, eliminación o modificación de cuentas de usuario, grupo o equipo, y el restablecimiento de contraseñas.	Se auditan las actividades correctas de administración de cuentas.

Como se puede comprobar, la mayoría de los principales eventos de Active Directory son auditados por los controladores de dominio (cuando los eventos son correctos). Sin embargo, pocos eventos fallidos son auditados y a veces, puede ser interesante auditar los intentos fallidos de hacer login o de hacerse miembro de algún grupo.

15.2 Auditar el acceso a archivos y carpetas

Para realizar una auditoría de acceso a archivos o carpetas hay que realizar tres pasos:

- Activar la directiva de auditoría "Auditar el acceso a objetos".- se selecciona la opción Editar del menú contextual del GPO que corresponda, se expande Configuración del equipo, carpeta Directivas, carpeta Configuración de Windows, Configuración de Seguridad, Directivas locales, Directiva de auditoría, se hace doble clic sobre la directiva "Editar el acceso a objetos" y se activan los cuadros de verificación oportunos (e intuitivos). La configuración de la directiva debe realizarse en el equipo que contiene el objeto a auditar, en el GPO local o en un GPO que afecte (vinculado) al equipo.

- Agregar las entradas de auditoría a la lista SACL del objeto.- a través del menú contextual del fichero o carpeta, opción Propiedades, ficha Seguridad, botón Opciones avanzadas, ficha Auditoría, botón Editar, botón Agregar, se selecciona el usuario, equipo o grupo, se acepta y aparecerá el cuadro de diálogo que permite elegir los accesos correctos o incorrectos al objeto que se quieren auditar. Se sale confirmando (aceptando) todas las ventanas abiertas.

- Ver en el registro de seguridad del servidor el resultado de los eventos.- puede realizarse desde Herramientas administrativas – Visor de eventos – Registros de Windows – Seguridad.

15.3 Auditar los cambios en el servicio de directorio

El procedimiento es similar al caso anterior, teniendo en cuenta que la directiva a configurar ahora es: "Auditar el acceso del servicio de directorio". Los dos últimos pasos, modificar la SACL del objeto y comprobar el registro de seguridad del servidor, también deben efectuarse.

Puede incorporarse una directiva más, que además de auditar el cambio en el servicio de directorio, guarda el valor anterior y el nuevo. Esta auditoría no se instala por defecto; para instalarla hay que ejecutar:

auditpol /set /subcategory:"directory service changes" /success:enable

Así, en la mayoría de los casos, las entradas del registro de eventos mostrarán el valor anterior y actual del atributo modificado.

16 AUTENTICACIÓN

16.1 Configurar las directivas de contraseñas y bloqueo de cuentas

En un dominio de Windows Server 2008, los usuarios deben cambiar sus contraseñas cada 42 días, una contraseña debe tener al menos 7 caracteres de longitud y cumplir requerimientos de complejidad que incluyan tres de cuatro tipos de caracteres: mayúsculas, minúsculas, numéricos y no alfanuméricos. Tres directivas de contraseñas: vigencia máxima de la contraseña, longitud de la contraseña y complejidad de la contraseña, están entre las primeras directivas encontradas por los administradores y usuarios de un Active Directory.

Para mejorar la seguridad de un dominio, pueden establecerse requerimientos de contraseñas más restrictivos para los usuarios administradores o usuarios con mayores privilegios de acceso. En versiones anteriores de Windows esto no era posible, una única directiva de contraseña se aplicaba a todas las cuentas del dominio.

16.2 Directiva de contraseñas

Las directivas de contraseñas se encuentran configuradas en un GPO vinculado al dominio. Para establecer los requerimientos adecuados hay que acceder al GPO, al elemento "Configuración de equipo – Directivas – Configuración de Windows – Configuración de seguridad – Directivas de cuenta – Directivas de contraseñas".

Las directivas de contraseñas existentes son:

- Almacenar contraseñas con cifrado reversible.
- Exigir historial de contraseñas.
- La contraseña debe cumplir los requisitos de complejidad.
- Longitud mínima de la contraseña.
- Vigencia máxima de la contraseña.
- Vigencia mínima de la contraseña.

Cada una de estas directivas afecta al usuario que modifica su contraseña pero no afectan al Administrador al utilizar el comando "Restablecer contraseña" para modificar la contraseña de otro usuario.

16.3 Directivas de bloqueo de cuentas

Dado que los nombres de usuario suelen ser relativamente fáciles de identificar, los intrusos pueden intentar determinar la contraseña a base de introducir combinaciones de caracteres hasta que consiguen realizar el inicio de sesión. Este tipo de ataque puede

prevenirse limitando el número de intentos de inicio de sesión erróneos, a través de las Directivas de bloqueo de cuentas. Estas directivas están accesibles editando el GPO correspondiente, en Configuración del equipo – Directivas – Configuración de Windows – Configuración de seguridad – Directivas de cuenta – Directiva de bloqueo de cuenta. Las tres configuraciones permitidas son:

- Duración del bloqueo de cuentas.
- Restablecer el bloqueo de cuenta después de.
- Umbral de bloqueo de cuenta.- número de intentos de inicio de sesión incorrectos.

16.4 Configurar la directiva de bloqueo y contraseña del dominio

Las directivas de bloqueo y contraseñas del dominio se encuentran configuradas de forma predeterminada en el GPO Default Domain Policy, vinculado al dominio. Hay que tener en cuenta que algunas de estas directivas pueden ser anuladas a través de las propiedades de cada usuario concreto. Por ejemplo, la directiva a nivel de dominio "Vigencia máxima de la contraseña" queda anulada para un usuario que tenga configurada la propiedad "La contraseña nunca caduca" (ficha Cuenta).

También se puede anular la directiva de bloqueo de cuenta y contraseña de dominio utilizando la directiva de bloqueo y contraseña refinada, también llamada directiva de contraseña refinada. Esta directiva permite una configuración aplicable a uno o varios usuarios o grupos del dominio (solo en Windows 2008). Así, es posible aplicar a usuarios con mayor responsabilidad (cuentas administrativas) ciertos requerimientos de contraseñas más estrictos: mayor longitud, mayor frecuencia de modificación, etc..

Las configuraciones administradas por la Directiva de contraseñas refinadas son idénticas a las Directivas de contraseñas y Directivas de cuenta de un GPO con la particularidad de que no son implementadas como parte de la Directiva de grupo, ni se aplican como componentes de un GPO. Forman parte de una clase de objetos de configuración de contraseña de Active Directory llamados PSO (Password Setting Object).

Los PSO pueden administrarse (configurarse) mediante la herramienta administrativa "Editor ADSI".

Pueden crearse más de un PSO dentro del dominio y cada uno contendrá un conjunto completo de configuraciones de directivas de bloqueo y contraseñas. Para aplicar un PSO deberá vincularse a los usuarios o grupos de seguridad globales que se desee. De forma similar a como un usuario puede hacerse miembro de un grupo a través del atributo "MemberOf" del usuario o del atributo "Member" del grupo, un PSO puede vincularse a través de su atributo "msDS-PSOAppliesTo" o a través del atributo "msDS-PSOApplied" del usuario o grupo. Este atributo puede manipularse a través de las Propiedades – Ficha Editor de atributos.

16.5 Prioridad de los PSO's y PSO resultante

Un PSO se puede vincular a más de un grupo o usuario, un grupo o usuario puede tener vinculados más de un PSO y un usuario puede pertenecer a varios grupos. Pero un y solo un PSO determina las configuraciones de bloqueo de cuenta y contraseña de un usuario; es el llamado PSO resultante.

Cada PSO tiene un atributo que determina su prioridad o precedencia. El valor de este atributo es un número entero mayor de 0, siendo el de mayor prioridad el que tiene asignado el valor 1 y el de menor prioridad el que tiene asignado un valor más alto. Cuando un usuario está afectado por múltiples PSO's, será el de mayor prioridad (valor más cercano a 1) el PSO resultante y el que se aplique al usuario.

Las reglas que determinan la prioridad y en consecuencia el PSO resultante son:

- Si múltiples PSO's se aplican a grupos a los que pertenece el usuario, prevalece el PSO con prioridad más alta (valor más próximo a 0).

- Si uno o más PSO's están vinculados directamente al usuario, se ignoran los PSO's vinculados a los grupos, independientemente de su prioridad. Prevalece el PSO vinculado al usuario con la prioridad más alta.

- Si uno o más PSO's tienen el mismo valor de prioridad, Active Directory selecciona el PSO con el identificador único global (GUID) más bajo, que es una selección totalmente arbitraria. Es conveniente establecer las prioridades de los PSO's de forma que se evite este escenario.

Active Directory muestra el PSO resultante en un atributo del objeto de usuario permitiendo identificarlo fácilmente. El atributo en cuestión, msDS-ResultantPSO, puede encontrarse a través de las propiedades del usuario, ficha Editor de atributos. Los PSO's contienen todas las configuraciones de bloqueo y contraseña, no existe la herencia o combinación de configuraciones. El PSO resultante es el PSO autorizado.

Los PSO's no se pueden vincular a unidades organizativas (OU). Para que un PSO afecte a todos los usuarios de una OU deberá crearse un grupo de seguridad global que incluya a todos los usuarios de la OU (un grupo oculto).

El apartado 11 de la práctica 2 es erróneo. En el cuadro "Seleccionar una propiedad para ver" hay que elegir "msDS-PSOAppliesTo", en el cuadro "Editar atributo" se introduce "CN=Admins. del dominio,CN=Users,DC= ...", Agregar, Aceptar y Finalizar.

17 AUDITAR LA AUTENTICACIÓN

Puede auditarse el inicio de sesión correcto o incorrecto para detectar cuándo o dónde se utiliza una cuenta de forma anormal o se intenta realizar un inicio de sesión.

17.1 Directivas relativas a la autenticación

Es importante distinguir entre las directivas "Auditoría de eventos de inicio de sesión de cuentas" y "Auditoría de eventos de inicio de sesión". Cuando un usuario inicia sesión en cualquier equipo en el dominio utilizando su cuenta de usuario de dominio, un controlador de dominio autentifica el intento del inicio de sesión con la cuenta del dominio, lo que genera un evento de inicio de sesión de cuenta en el controlador de dominio. Además, en el equipo donde el usuario inicia la sesión se genera un evento de inicio de sesión.

Cuando un usuario se conecta a una carpeta en un servidor en el dominio, ese servidor autoriza al usuario un tipo de inicio de sesión llamado inicio de sesión de red. En este caso el servidor no autentifica al usuario sino que confía en la validación realizada por el controlador de dominio, pero la conexión del usuario genera un evento de inicio de sesión en el servidor.

Las configuraciones que administran la auditoría de los eventos de inicio de sesión de cuenta y de inicio de sesión se encuentran en los GPO's, en Configuración de equipo – Directivas – Configuración de Windows – Configuración de seguridad – Directivas locales – Directiva de auditoría.

17.2 Delimitar las directivas de auditoría

Es importante delimitar las directivas de auditoría para que afecten únicamente a los sistemas u objetos deseados. Dos ejemplos prácticos pueden ser los siguientes:

- Para auditar los intentos de los usuarios por conectarse a un servidor de archivos puede configurarse la auditoría del evento de inicio de sesión en un GPO vinculado a la OU que contenga a los servidores de archivos.

- Para auditar los inicios de sesión de los usuarios en los equipos de escritorio de un determinado departamento puede configurarse la auditoría del evento de inicio de sesión en un GPO vinculado a la OU que contenga los objetos de equipo del departamento en cuestión.

Hay que tener en cuenta que el inicio de sesión de los usuarios en el dominio en un equipo cliente o al conectarse a un servidor generará un evento de inicio de sesión en ese sistema, no un evento de inicio de sesión de cuenta.

Solamente los controladores de dominio generan eventos de inicio de sesión de cuenta para los usuarios del dominio. Un evento de inicio de sesión de cuenta ocurre en el controlador de dominio que autentifica al usuario del dominio, independientemente del equipo en el que haya iniciado la sesión. Si se desea auditar los inicios de sesión de las cuentas del dominio se debe delimitar la auditoría del evento de inicio de sesión de cuenta para que afecte solamente a los controladores de dominio. El GPO Default Domain Controlers puede ser ideal para este caso.

De forma predeterminada Windows 2008 audita los inicios de sesión e inicios de sesión de cuenta correctos. Para auditar los errores o desactivar la auditoría, hay que definir la configuración adecuada en la directiva de auditoría.

17.3 Visualización de eventos de inicio de sesión

Los eventos de inicio de sesión de cuenta y de inicio de sesión, si son auditados, se graban en el registro de seguridad del sistema que genera el evento. Si se realiza una auditoría de inicio e sesión en los equipos de un determinado departamento, los eventos se registran en el registro de seguridad de cada equipo. Si se auditan los inicios de sesión de cuenta correctos, los eventos se registran en el registro de seguridad de los controladores de dominio; esto significa que para conseguir un cuadro completo de los inicios de sesión de cuenta en el dominio será necesario examinar los registros de seguridad de todos los controladores de dominio.

Es aconsejable equilibrar el registro de eventos en función de la seguridad requerida y los recursos dedicados a analizar los eventos registrados.

17.4 Actividades (ampliación)

En un dominio con un controlador de dominio y un equipo miembro provocar la generación de al menos dos eventos de inicio de sesión:

- Uno al conectarse un usuario del dominio desde el equipo miembro.
- Otro al conectarse desde el controlador del dominio a una carpeta compartida del equipo miembro.

No es necesario crear un GPO ni una OU adicionales puesto que por defecto se auditan los inicios de sesión correctos.

18 DNS

El sistema de nombres de dominio (DNS) se encarga de trasladar los nombres de dominio a direcciones IP y viceversa. El puerto asignado a este protocolo es el 53.

La estructura de nombres soportada por DNS es una estructura jerárquica que comienza en la raiz o ".".

Anexo 1.- Selección de temas

Se han realizado las siguientes agrupaciones:

- Temas incluidos en este documento procedentes de diversas fuentes:

  - Tema 1.- Introducción

- Temas seleccionados para impartir en 1º de ASIR y resumidos en este documento:

  - Capítulo 1 – Lección 1 --- Tema 2.- Instalación
  - Capítulo 2 – Lección 1 --- Tema 3.- Ventanas de administración …
  - Capítulo 2 – Lección 2 --- Tema 4.- Creación de objetos …
  - Capítulo 2 – Lección 3 --- Tema 5.- Delegación y seguridad …
  - Capítulo 3 – Lección 1 --- Tema 6.- Automatizar la creación de …
  - Capítulo 3 – Lección 3 --- Tema 7.- Dar soporte a los objetos de …
  - Capítulo 4 – Lección 1 --- Tema 8.- Administrar grupos
  - Capítulo 4 – Lección 2 --- Tema 9.- Automatizar la creación y …
  - Capítulo 4 – Lección 3 --- Tema 10.- Administrar grupos en una empresa
  - Capítulo 5 – Lección 1 --- Tema 11.- Equipos
  - Capítulo 5 – Lección 2 --- Tema 12.- Automatizar la creación de …
  - Capítulo 5 – Lección 3 --- Tema 13.- Dar soporte a objetos de …
  - Capítulo 6 – Lección 1, 2, 3 --- Tema 14.- Directivas de grupo
  - Capítulo 7 – Lección 4 --- Tema 15.- Auditorías
  - Capítulo 8 – Lección 1 --- Tema 16.- Autenticación
  - Capítulo 8 – Lección 2 --- Tema 17.- Auditar la autenticación
  - Capítulo 9 – Lección 1, 2 --- Tema 18.- DNS

- Temas seleccionados para impartir en 2º de ASIR y excluidos de este documento:

  - Capítulo 3 – Lección 2.- Creación de usuarios con Windows PowerShell y …
  - Capítulos 10, 11, 12, 13, 14, 15, 16 y 17

- Temas que no se imparten:

  - Capítulo 1 – Lección 2.- SD de AD en el Server Core
  - Capítulo 7 – Lección 1, 2, 3.- Configuración de la directiva de grupo
  - Capítulo 8 – Lección 3.- Configurar controladores de dominio de solo lectura


MAX v.6.0
Edición Servidor
DUCAMADRID
Comunidad de Madrid
CONSEJERÍA DE EDUCACIÓN