Universidad del Azuay

Facultad de administración de empresas

Escuela de ingeniería de sistemas

Integración de cuentas de dominio de Microsoft Windows directorio activo para autenticación en servidor de archivos Linux

Trabajo de graduación previo a la obtención del título de Ingeniero en sistemas

Autores: Marco R. Pino Pinos
Freddy G. Pino Pinos.

Director: Ing. Pablo Pintado

Cuenca, Ecuador
2006

Dedicatoria:

Esta monografía la dedico a mi familia quienes supieron apoyarme a lo largo de toda mi vida y a una persona muy especial que me ayudo a demostrar lo mejor de mí.

Freddy Pino.

Este trabajo va dedicado a mis padres, gracias a su incansable apoyo me han ayudado a alcanzar una meta mas en mi vida.

Rodrigo Pino

Agradecimiento

Un agradecimiento a los profesores de la Escuela de Ingeniería de Sistemas de la Facultad del Azuay por los conocimientos impartidos y de forma muy especial al Ing. Pablo Pintado por todo el tiempo y la ayuda dedicada a este proyecto, además al Ing. Sergio Betancourt por la confianza brindada.

Freddy Pino

Agradezco a todas las personas que me brindaron su confianza, y de una manera muy especial a mis dos hermanos.

Rodrigo Pino

Índice de Contenidos

Índice de ilustraciones y cuadros

Resumen

El proyecto ofrece a los servidores con sistema operativo Linux la posibilidad de establecer una relación de confianza con el Microsoft directorio activo mediante el demonio Kerberos. Una vez establecida esta relación es posible originar consultas al Directorio Activo sobre la información de autenticación de usuarios y pertenecías de grupo. El Servidor Linux se comunicará con Microsoft Directorio Activo utilizando el demonio Winbind.

Al manejar un solo repositorio de información de usuarios estos tienen la posibilidad de realizar un solo proceso de autenticación al arrancar la estación de trabajo y acceder a cualquier tipo de servidor sin importar su sistema operativo en el dominio.

Abstract

This project offer to the server a operating system called Linux to establish a safe connection with Microsoft Active Directory through the daemon Kerberos. Once the connection is established it is possible to make questions to the Microsoft active Directory about the authentication of users and the verification of groups. The Linux servers will communicate with Active directory Microsoft by daemon Winbind. The fact that it will be possible to manage only one storage area of the users will open the possibility of doing only one process of authentication when the system starts, so it makes easy the access to any type of server even if they have a different operative system.

Introducción

El usar equipos computacionales dentro de la red de datos de la organización es una herramienta necesaria para mejorar el desempeño de la misma, lastimosamente las PYMES de nuestro país se ven frenadas en su uso debido al costo de las licencias o su dificultad de instalación y/o administración. Estas dificultades motivaron a realizar una guía práctica para mejorar el ambiente de red computacional, brindando la oportunidad de tener un completo control sobre los usuarios mediante el Microsoft Directorio Activo instalado sobre un servidor Windows y ofreciendo la posibilidad de tener recursos compartidos sobre equipos Linux sin costo de licencias, con un trabajo de administración de red sencillo.

Para realizar esta monografía utilizaremos información sobre Microsoft recopilada de los cursos para MSCE y la información obtenida en el Internet sobre el sistema operativo Linux.

CAPÍTULO I

Red de computadores en una empresa

Introducción

Toda la problemática de esta monografía se centra en el manejo de redes heterogéneas es decir manejar en un mismo ambiente de trabajo varios sistemas operativos de redes cumpliendo diferentes actividades, pero la primera incertidumbre que esto puede generar es: ¿Para que implementar una red de datos en mi empresa?, esta pregunta puede responderse analizando las siguientes necesidades:

- Información compartida y actualizada entre los empleados.- En los actuales momentos se le considera a la información oportuna y actualizada como el bien más importante de una empresa, al no tener una manera optima de compartirla está podría perder su validez por el tiempo en que pasa de un empleado a otro, además de tener el riesgo de extravió o que llegué a las manos equivocadas como un ejemplo podríamos tener el manejo de roles de pago.

- Manejo optimizado de recursos costosos.- No siempre los recursos económicos serán los suficientes para instalar impresoras con altos niveles de desempeño en todos los departamentos de la empresa, unidades de Medios ópticos - magnéticos en todos los equipos o gran posibilidad de almacenamiento en disco duro en todas las máquinas si lo hiciéramos podemos caer en la subutilización de algunos de ellos, es por eso la necesidad de compartir el uso de algunos de ellos entre varias personas llegando así a mejorar el costo – beneficio de los bienes adquiridos.

Los conceptos acerca de las licencias GNU que mencionamos en este capítulo son tomadas del sitio web: <http://www.gnu.org/home.es.html>.

1.1 Problemática en redes heterogéneas

Hoy en día cuando por distintas razones se utiliza dentro de una misma red de área local varios sistemas operativos de red, los administradores de la misma se encuentran con un ambiente en el cual tienen que realizar tareas como la creación, mantenimiento de usuarios y otros objetos en varios lugares, en el caso concreto de coexistir en una misma red de área local los sistemas operativos Microsoft y Linux tendrían que manejar una consola para administrar los usuarios para acceso a las estaciones de trabajo sobre Microsoft y otro ambiente de consola distinto para administrar los mismos usuarios sobre Linux, observándose así los problemas que esto conlleva al tener que duplicar la información de usuarios, esto también aumenta la complejidad para el usuario final al tener que recordar varios inicios de sesión y claves que dependerían su uso del servicio al cual desean acceder.

1.2 ¿Por que utilizar Dominios Microsoft?

Un dominio constituye un límite de seguridad. El directorio incluye uno o más dominios, cada uno de los cuales tiene sus propias directivas de seguridad y relaciones de confianza con otros dominios. Los dominios ofrecen varias ventajas:
Organizar objetos. Al utilizar unidades organizativas en un dominio es más fácil administrar las cuentas y recursos del dominio.

- Las directivas y la configuración de seguridad (como los derechos administrativos y las listas de control de accesos) no pueden pasar de un dominio a otro.
- Al delegar la autoridad administrativa en dominios o unidades organizativas desaparece la necesidad de tener varios administradores con autoridad administrativa global.
- Los dominios ayudan a estructurar la red de forma que refleje mejor la organización.
- Cada dominio almacena solamente la información acerca de los objetos que se encuentran ubicados en ese dominio. Al crear particiones en el directorio

de esa manera, Directorio Activo puede ampliarse y llegar a contener una gran cantidad de objetos.

Los dominios son las unidades de replicación. Todos los controladores de dominio de un dominio determinado pueden recibir cambios y replicarlos a los demás controladores del dominio. Un único dominio puede abarcar varias ubicaciones físicas distintas o sitios. Al utilizar un solo dominio se simplifican mucho las tareas administrativas.

1.3 ¿Como reducir costos en licencias con Linux?

La industria del desarrollo de software es una de las más rentables a nivel mundial debido en gran medida a la popularidad de las PC en los hogares y su gran uso dentro de las empresas, este alto nivel de ganancias es debido a los costos de las licencias, en nuestro país las pequeñas y medianas empresas casi nunca tienen en cuenta estos costos dentro de sus presupuestos anuales, debido en gran parte a la acostumbrada piratería de software, a olvidos involuntarios, o por reducir gastos, cualquiera que fuese las razones ahora es posible reducir estos valores manteniendo software de calidad y siendo legal, esta opción constituye el software GNU, el software GNU tiene como objetivo dar a todos los usuarios la libertad de redistribuir y cambiar software GNU. Si los intermediarios pudieran quitar esa libertad, se tendríamos muchos usuarios, pero esos usuarios no tendrían libertad. Así en vez de poner software GNU en el dominio público, se lo protege con copyleft. “Copyleft dice que cualquiera que redistribuye el software, con o sin cambios, debe dar la libertad de copiarlo y modificarlo más”.

En esta monografía se utiliza Linux con licencias GNU en el servidor de archivos y servidor Proxy, si se quisiese implementar estos servicios sobre servidores Microsoft como primer punto debería considerarse el costo del hardware sobre el cual van a funcionar estos servidores, Microsoft impone requerimientos de hardware con prestaciones altas para sus productos, mientras que Linux podría funcionar inclusive en equipos Pentium II. Como otro punto a considerar está que Microsoft introduce el concepto de licencias CAL (Licencias de acceso) es decir si necesitamos un servidor

Proxy será necesario comprar las licencias CAL para cada uno de los clientes que necesiten este recurso además del costo de la licencia del producto Microsoft Windows 2000 Server que también variará de acuerdo al número de procesadores instalados en el hardware, estos costos sumados terminarán siendo más altos que los obtenidos sobre servidores Linux.

1.4 El trabajo de administración una red en una PYMES

En una red de área local de una PYMES el trabajo de un administrador de red en caso que este cargo existiera dentro de este tipo de organización contempla el manejo de tareas rutinarias como las siguientes:

- Mantenimiento de usuarios.- Creación, modificación, deshabilitar, habilitar cuentas, cambio de claves.
- Manejo de permisos de acceso a recursos.- Establecimiento de políticas, definición de niveles de acceso.
- Acceso a servicios de red.- Configurar acceso a Internet, cuentas de correo electrónico.

1.5 Conclusiones

Es imprescindible tener una red de computadores por los beneficios que esta presenta. Microsoft ofrece una consola potente, completa y simplificada para el manejo de usuarios pero la implementación de otros servicios sobre servidores Microsoft podría llegar a encarecer significativamente el costo de la solución, es posible abaratar estos costos si estos servicios adicionales se instalan sobre la plataforma Linux.

CAPÍTULO II

Microsoft Directorio Activo

Introducción

En este capítulo se le brinda un marco teórico referencial de Directorio Activo, para la comprensión de funcionamiento y ventajas que proporciona la unificación de zonas DNS con el dominio de Microsoft Directorio Activo.
El marco teórico utilizado en este capítulo es tomado en base al libro: "Microsoft Windows 2000 Active Directory Services – Curso oficial de certificación MCSE", Microsoft Press, Capitulo 4.

2.1 ¿Qué es Microsoft Directorio Activo?

Directorio Activo es servicio de Windows Server, que contiene un almacén datos replicados, estructurado de forma lógica jerárquica los objetos la red, que facilita la búsqueda para la utilización de la información por parte de los administradores y usuarios en cualquier punto de la red. Los administradores controlan el acceso y la publicación de los objetos de la organización, mediante directivas facilitando su tarea, y los usuarios autorizados de la red puedan tener acceso a recursos de dicha red. Para publicar los objetos, utilice las *Herramientas administrativas*.

El servicio de directorio de Directorio Active tiene las siguientes características:

- Un Directorio es el almacén de: datos del directorio, datos de configuración, datos de esquema, que se almacena en los controladores de dominio.
    - Datos del directorio, se trata de la información del directorio, por ejemplo: contactos de correo electrónico, atributos de las cuentas de usuarios y equipos

- Datos de configuración, describen la topología del directorio, mediante una lista de los dominios, árboles y bosques así como las ubicaciones de los controladores de dominio y los catálogos globales.
- Datos de esquema, define: las cuentas de usuarios y equipos, grupos, dominios, unidades organizacionales y directivas de seguridad. Sólo los usuarios autorizados puedan modificar el esquema, porque los objetos están protegidos mediante listas de control de acceso.

- Un Esquema, su estructura y contenido se encuentra en controlador de dominio definido como servidor principal de operaciones. Esquema es el conjunto de dos tipos de definiciones: atributos y clases, que se almacenan como objetos para que el directorio activo los pueda administrar.

  Los objetos del esquema describen las clases de objetos, sus restricciones y límites en las instancias de estos objetos, así como el formato en sus nombres. Los atributos almacenan información que describe el objeto, y las clases describen los posibles objetos que se pueden crear en el directorio.
- Un Catálogo global, de forma predeterminada se crea en el controlador de dominio inicial del bosque. Con un sólo controlador de dominio en el dominio, el controlador de dominio y el catálogo global estarán el mismo servidor. Con múltiples controladores de dominio se puede configurar de manera opcional cualquier controlador de dominio para que guarde un catálogo global. Si no hay disponible un catálogo global cuando un usuario inicia el proceso de inicio de sesión en la red, el usuario sólo podrá conectarse al equipo local. Esto permite realizar dos funciones principales:
  - Permitir que una cuenta, que envía la solicitud de inicio de sesión, envié información de pertenencia a grupos universales a un controlador de dominio.
  - Permitir encontrar información del directorio con independencia de cuál sea el dominio que contiene realmente los datos. Una consulta relativa a un objeto puede resolverla un catálogo global del dominio en el que se inició la consulta.
- Un sistema de índices y consultas, permite realizar tareas diarias en una red, que implican la comunicación con otros usuarios y la conexión con recursos publicados. Para encontrar la información del directorio fácilmente con el comando Buscar del menú Inicio, con Mis sitios de red del escritorio, además

se logra mayor eficiencia filtrando los datos recuperados del directorio, si utiliza los cuadros de diálogo avanzados Buscar de Usuarios y equipos del Directorio Activo.

- Un servicio de replicación, hace un seguimiento de cuántos cambios han realizado por las adiciones, modificaciones y eliminaciones de los datos del directorio. Todos los controladores de dominio de un dominio participan en la replicación y contienen una copia completa de toda la información del directorio de sus dominios. El uso de este esquema común permite a los usuarios y los servicios tener acceso a la información del directorio en cualquier momento y desde cualquier equipo del bosque asegurando la integridad y coherencia.
- Integración con el subsistema de seguridad, las principales características, son la autenticación y el control de acceso. La autenticación, para asegurar el proceso de inicio de sesión en el sistema y para tener acceso a los recursos de red. El Control de acceso, permite las consultas, modificaciones de los datos del directorio: Utilizando un descriptor de seguridad se enumera a los usuarios y a los grupos a los que se concede el acceso a un objeto, así como los permisos específicos asignados a dichos usuarios y grupos, a además autentica al usuario con la información almacenada en Directorio Activo, comprobando las propiedades definidas en la lista de control de acceso discrecional (DACL).
- El cliente de Directorio Activo, es el software que se configura en el equipo del cliente de Directorio Activo, para que pueda iniciar la sesión en la red. Si encuentra un controlador de dominio envía una consulta de nombre DNS a sus servidores DNS. La respuesta del servidor DNS contiene los nombres DNS de los controladores de dominio y sus direcciones IP. El primer controlador de dominio que responde es el que se utiliza para el proceso de inicio de sesión.

2.2 Que tener en cuenta al planificar un dominio Microsoft.

La estructura de dominios más fácil de administrar es un dominio único con pocas unidades organizativas y una sola zona en el espacio de nombres DNS. Al planearla,

debe comenzar con un único dominio y agregar dominios adicionales y aumentar zonas en el espacio de nombres sólo cuando el modelo de dominio único ya no se ajuste a sus necesidades.

Dominios

Un dominio puede abarcar varios sitios y contener millones de objetos. La estructura de sitios y la estructura de dominios son independientes y flexibles. Un único dominio puede abarcar varias ubicaciones geográficas y un único sitio puede incluir usuarios y equipos que pertenecen a múltiples dominios. No es necesario crear árboles de dominio independientes sólo para reflejar la organización de la compañía en divisiones y departamentos. Para este propósito, puede utilizar unidades organizativas dentro de un dominio. Se puede asignar configuraciones de Directiva de grupo a esas unidades organizativas y colocar en ellas usuarios, grupos y equipos. Algunas de las razones por las que se debe crear más de un dominio son las siguientes:

- Requisitos de contraseñas distintos en los diversos departamentos y divisiones
- Número muy grande de objetos
- Nombres de dominio de Internet distintos
- Mayor control de la replicación
- Administración descentralizada de la red

El primer dominio de un árbol de dominio se denomina dominio raíz. Los dominios adicionales del mismo árbol de dominio son dominios secundarios. Un dominio que se encuentra inmediatamente encima de otro dominio del mismo árbol se denomina dominio principal del dominio secundario.

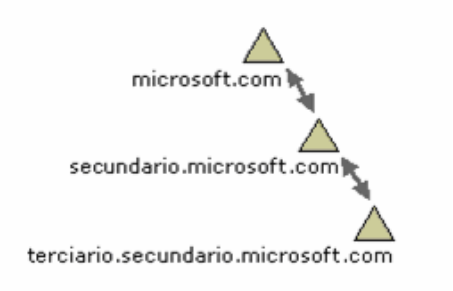

Fig. 2.2.1. Árbol de dominios

Todos los dominios que comparten el mismo dominio raíz forman un espacio de nombres contiguo. Esto significa que el nombre de un dominio secundario consta del nombre de ese dominio secundario más el nombre del dominio principal. En esta ilustración (Fig. 2.2.1), secundario.microsoft.com es un dominio secundario de microsoft.com y es el dominio principal de secundario2.secundario.microsoft.com. El dominio microsoft.com es el dominio principal de secundario.microsoft.com. Además, es el dominio raíz de este árbol de dominio.

Unidades organizativas

Un tipo de objeto de directorio especialmente útil contenido en los dominios es la unidad organizativa. Las unidades organizativas son contenedores de Directorio Activo en los que puede colocar usuarios, grupos, equipos y otras unidades organizativas. Una unidad organizativa no puede contener objetos de otros dominios. Una unidad organizativa es el ámbito o unidad más pequeña a la que se pueden asignar configuraciones de Directiva de grupo o en la que se puede delegar la autoridad administrativa. Con las unidades organizativas, puede crear contenedores dentro de un dominio que representan las estructuras lógicas y jerárquicas existentes dentro de una organización. Esto permite administrar la configuración y el uso de cuentas y recursos en función de su modelo organizativo.

La estructura de DNS inicial.

Dado que Directorio Activo y el espacio de nombres del Sistema de nombres de dominios (DNS, Domain Name System) tienen la misma estructura, un diseño

meticuloso es fundamental para asegurar que la implementación de Directorio Activo se realice sin problemas, al principio se suele utilizar un espacio de nombres único distinto al espacio de nombres externo como por ejemplo: espacio de nombre externo: *suempresa.com* y espacio de nombre interno: *suempresa.int*.

2.3 Requerimientos previos a la implementación de Microsoft Directorio Activo

Previo a la implementación de Microsoft Directorio Activo es necesario conocer sus principales características:

- Relación de confianza
- Unidades organizativas

Relación de confianza

Una confianza de dominio es una relación establecida que tienen lugar entre dos dominios, los controladores de dominio se encargan de determinar la relación de confianza (Fig. 2.3.1) entre el dominio que confía (Recurso) y el dominio en el que se confía (Cuenta, inicio de sesión de usuario).

Fig. 2.3.1. Relaciones de confianza entre dominios

Las relaciones de confianza se establecen automáticamente a través de todos los dominios del bosque, por lo que no es necesario realizar ninguna tarea administrativa, y brindan:

- Al usuario de un dominio autenticarse por un controlador de dominio de otro dominio para utilizar sus recursos.

- Al administrador, poder conceder los derechos y permisos adecuados para la cuenta de usuario en otro dominio que confía (recursos)

Características de una relación de confianza entre dominios:

- Unidireccional (intransitivas).- Las solicitudes de autenticación sólo se pueden transmitir desde el dominio que confía (recursos) al dominio en el que se confía (cuenta). Son intransitivas todas las relaciones de confianzas entre dominios que no pertenecen al mismo bosque. En una confianza unidireccional, el dominio A confía en el dominio B y el dominio B confía en el dominio C, entonces el dominio A no tiene una relación de confianza con el dominio C.

  Un dominio Microsoft establece una confianza unidireccional con:

  - Los dominios de Windows 2000 de un bosque diferente
  - Los territorios de MIT Kerberos V5

- Bidireccional (Transitiva, Intransitiva).- En la transitiva las solicitudes de autenticación se pueden transmitir entre dos dominios en ambas direcciones. Se pueden utilizar para acortar la ruta de confianza en árboles o bosques de dominios grandes y complejos. En cambio las intransitivas son confianzas unidireccionales entre los dominios implicados. El dominio A confía en el dominio B y el dominio B confía en el A.

- Confianza explícitas.- Las confianzas explícitas son relaciones de confianza creadas por los usuarios para crear y administrar confianzas explícitas (se crean en la consola: Dominios y confianzas de Directorio Activo) ya que no se crean automáticamente durante la instalación de un controlador de dominio.

  Existen dos clases de confianzas explícitas: las externas, y las de acceso directo.

  Las confianzas externas: (unidireccional intransitivas)

- Permiten la autenticación de usuarios en un dominio fuera de un bosque.
- Crean relaciones de confianza con dominios que se encuentran fuera del bosque
- La ventaja de crear confianzas externas radica en permitir la autenticación de usuarios en un dominio que no abarcan las rutas de confianza de un bosque
- Puede combinar dos confianzas de un sentido para crear una relación de confianza de dos sentidos.
- Para quitar completamente la confianza, deberá eliminarla de un controlador de dominio de Windows 2000 en el dominio que confía.

Para crear una confianza explícita:

- Se debe conocer los nombres de dominio y una cuenta de usuario con permiso para crear confianzas en cada dominio.
- A cada confianza se le asigna una contraseña que debe conocer el administrador de ambos dominios de la relación.

- Confianzas de acceso directo (confianzas transitivas).- Las confianzas de acceso directo acortan la ruta de una confianza que la seguridad de Windows 2000 utiliza en la autenticación en un bosque complejo, optimizando el rendimiento. Al crear una confianza de acceso directo entre dominios del nivel medio de dos árboles de dominio, se produce su uso más efectivo.

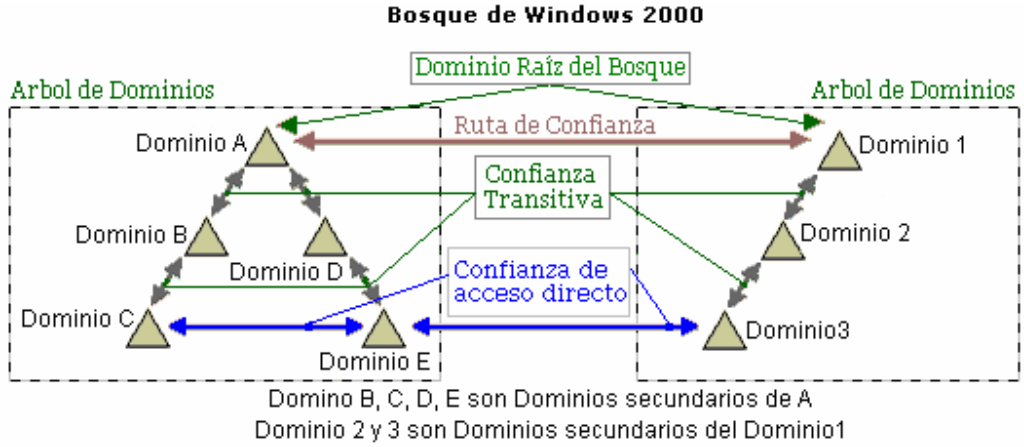

Fig. 2.3.2. Relaciones de confianza entre árboles

Funcionamiento (Fig. 2.3.2):

- Se establecen las relaciones de confianza transitiva y bilateral, dentro de un bosque de dominios en el momento en que se crea el nuevo dominio. O al unir un dominio nuevo al bosque de dominio.
- Se crea un árbol de dominios cuando, se agregan dominios secundarios (Dominio 2, 3) al dominio nuevo (Dominio1).
- Si crea un nuevo árbol de dominios en un bosque (Dominio1), se forma una relación de confianza transitiva bidireccional entre este y el dominio raíz del bosque (Dominio A).
- Una ruta de confianza es la serie de relaciones de confianza de dominio que debe atravesar la seguridad de Windows 2000 para pasar las solicitudes de autenticación entre dos dominios cualesquiera.
- Si es necesario, puede crear varias confianzas de acceso directo entre dominios de un bosque, Para optimizar la autenticación.
- Si no se agrega ningún dominio secundario el dominio nuevo (Dominio1) es solo un dominio raíz, la ruta de confianza está entre este y cualquier otro dominio raíz del bosque.
- Si se crea un nuevo dominio secundario (Dominio 2, 3), se crea automáticamente, una relación de confianza transitiva bidireccional entre este y el dominio principal (Dominio 1).

2.4 Implementando DNS en su red de área local.

Cuando instala Directorio Activo en un equipo servidor, promociona el servidor a la función de un controlador de dominio (DC) para un dominio especificado. Cuando se completa este proceso, se le pide que especifique un nombre de dominio DNS para el dominio de Directorio Activo al que va a unir y promocionar el servidor.

Si, durante este proceso, un servidor DNS autorizado para el dominio que ha especificado no se puede localizar en la red o no admite el protocolo de actualización dinámica de DNS, se le pide que active la opción para instalar un servidor DNS de Windows 2000. Esta opción se proporciona porque se requiere un servidor DNS para

admitir el uso de Directorio Activo y para que los equipos con Windows 2000 localicen este servidor en otros controladores de dominio para el dominio.

2.4.1 Concepto de DNS.

El Sistema de nombres de dominio (DNS, Domain Name System). DNS es un servicio estándar de Internet que traduce nombres legibles de equipos host, como mipc.microsoft.com, a direcciones IP numéricas (Fig. 2.4.1.1). Esto permite que los procesos que se ejecutan en equipos de redes TCP/IP puedan realizar la identificación y conexión.

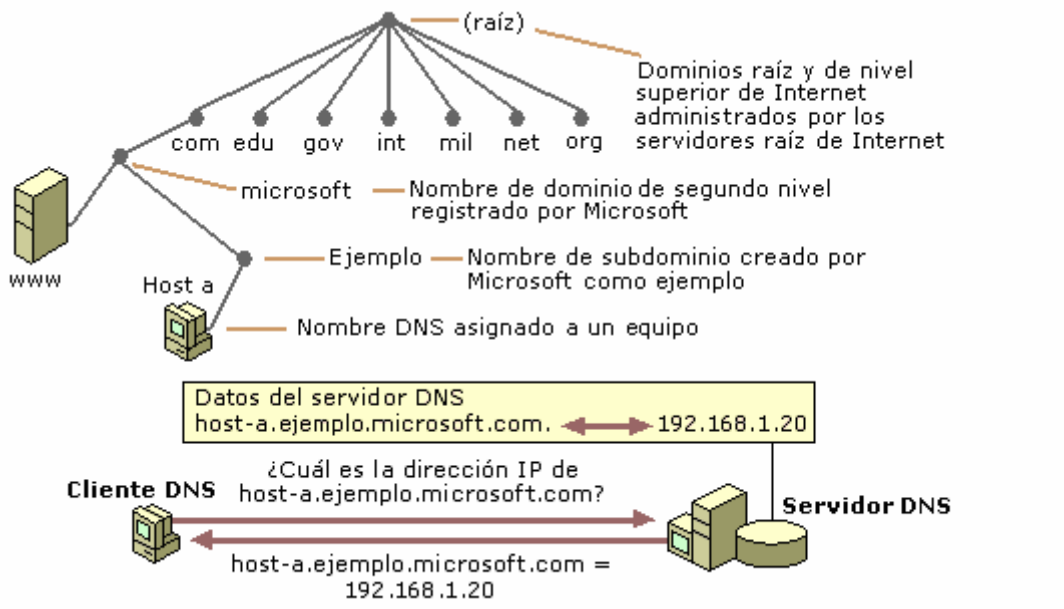

Fig. 2.4.1.1. Estructura DNS.

Los nombres de dominio completos (FQDN Fully Qualified Domain Names) de DNS, cuando se lee de izquierda a derecha, se mueve desde su información más específica (el nombre DNS de un equipo llamado "host-a") a su grupo de información más alto o más general (el punto final (.) que indica la raíz del árbol de nombres DNS). Este ejemplo muestra los niveles de dominio DNS independientes que se dirigen desde la ubicación de host específica del "host-a":

- Nombre de recurso o de host,- Nombres que representan una hoja en el árbol DNS de nombres e identifican un recurso específico. Normalmente, la etiqueta de la izquierda de un nombre de dominio DNS identifica un equipo específico en la red.
  "**host-a**.ejemplo.microsoft.com."
- Subdominio.- El dominio "ejemplo", son nombres adicionales que puede crear una organización y se derivan del nombre de dominio registrado de segundo nivel. Incluyen los nombres agregados para desarrollar el árbol de nombres de DNS en una organización y que la dividen en departamentos o ubicaciones geográficas. Que corresponde a un subdominio donde el nombre de equipo "host-a" está registrado para su uso.
  "host-a.**ejemplo**.microsoft.com."
- Dominio de segundo nivel.- El dominio "microsoft", que corresponde al dominio principal, son nombres de longitud variable registrados que un individuo u organización utiliza en Internet. Estos nombres siempre se basan en un dominio de nivel superior apropiado, según el tipo de organización o ubicación geográfica donde se utiliza el nombre que es la raíz del subdominio "ejemplo".
  "host-a.ejemplo.**microsoft**.com."
- Dominio de nivel superior.- El dominio "com", es un nombre de dos o tres letras que se utilizan para indicar un país o región, o el tipo de organización que usa un nombre y es la raíz del dominio "microsoft".
  "host-a.ejemplo.microsoft.**com**."
- El dominio raíz.- El punto final (.), que es un carácter de separación estándar que se utiliza para calificar el nombre de dominio DNS completo en el nivel raíz del árbol del espacio de nombres DNS.

2.4.2 Instalando DNS.

En primer lugar tenemos que verificar que se tenga disponible en las herramientas administrativas el asistente de instalación de DNS, en caso contrario los pasos a seguir serían:

Diríjase al panel de control desde el menú inicio, seleccione la opción: agregar quitar programas (Fig. 2.4.2.1).

Fig. 2.4.2.1. Panel de Control – Agregar o quitar programas.

En el formulario Agregar o quitar programas (Fig. 2.4.2.2) seleccione la opción Agregar o quitar componentes Windows.

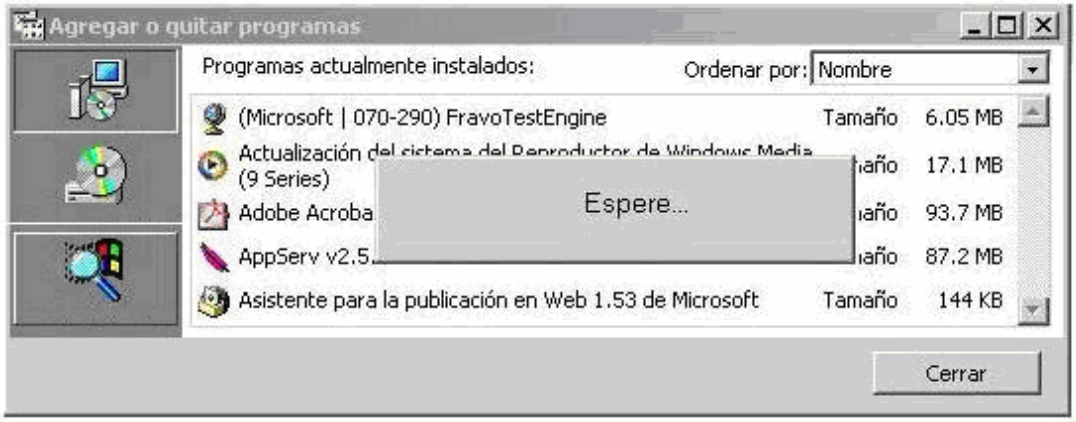

Fig. 2.4.2.2. Agregar o quitar programas – Componentes Windows.

Seleccione la opción Servicios de Red y presione el botón Detalles del formulario Asistente para componentes, se presentará el formulario Servicios de red, aquí busque la opción Sistema de nombres de dominio (DNS) y presione el botón Aceptar (Fig. 2.4.2.3).

Fig. 2.4.2.3. Componentes Windows – Agregando DNS.

Después de instalarse los componentes se presentará un formulario indicando la finalización del proceso.

Para proceder a la configuración del Servidor DNS instalado en los pasos anteriores diríjase como indica la siguiente figura (Fig. 2.4.2.4):

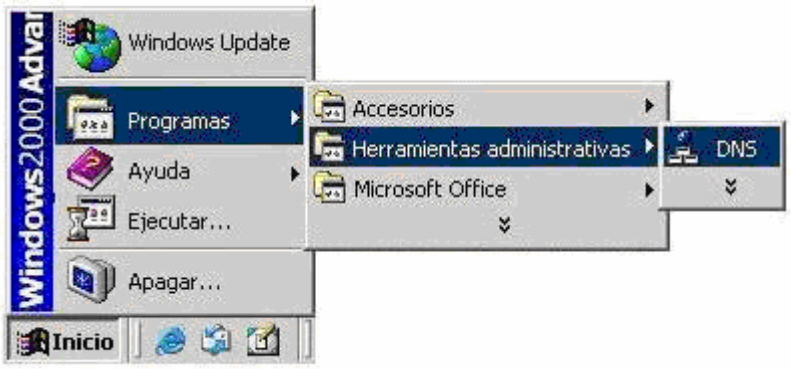

Fig. 2.4.2.4. Ingresando a consola DNS.

2.4.3 Creando y configurando zonas sobre DNS.

La Consola DNS de Microsoft (Fig. 2.4.3.1) muestra la información organizada por zonas de búsqueda directa e inversa:

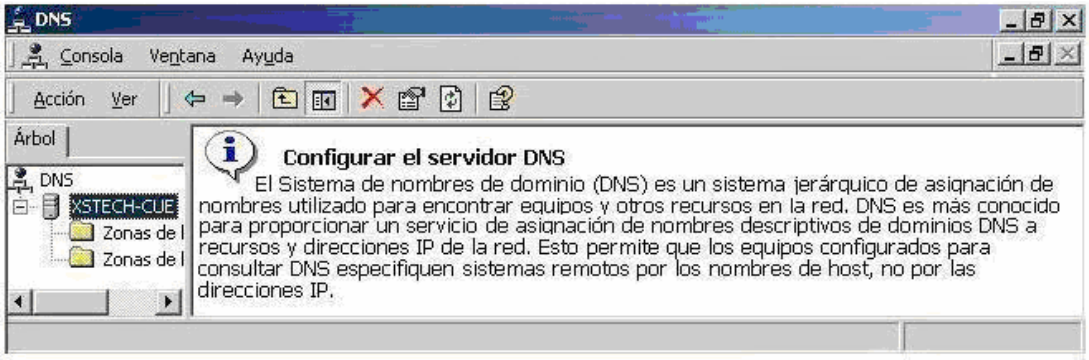

Fig. 2.4.3.1. Consola DNS.

Para implementar una nueva zona de búsqueda de clic derecho sobre el tipo de zona que desea crear y elija la opción Crear una zona nueva… (Fig. 2.4.3.2)

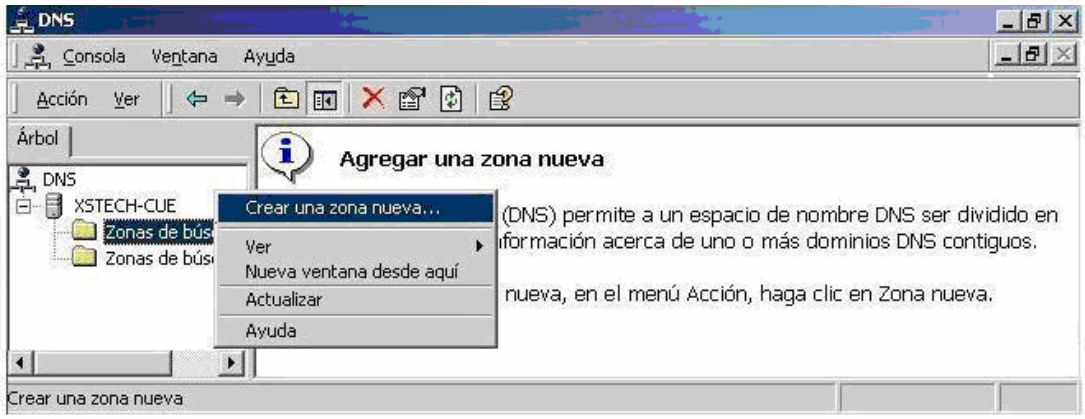

Fig. 2.4.3.2. Creación de zonas DNS directa.

Esta opción iniciara un asistente que le pedirá información concerniente al tipo de zona (Fig. 2.4.3.3), Nombre de la zona (Fig. 2.4.3.4) y Nombre del archivo de zona (Fig. 2.4.3.5), Al momento la zona no está integrada al directorio Activo, posteriormente esta zona la enlazaremos al mismo.

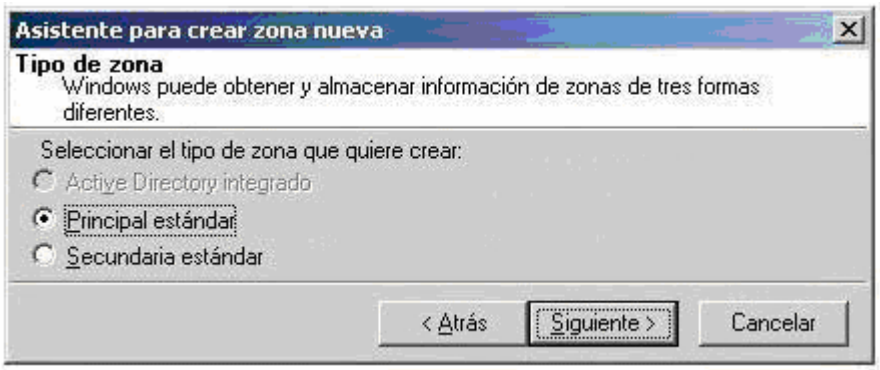

Fig. 2.4.3.3. Tipos de zonas DNS directa.

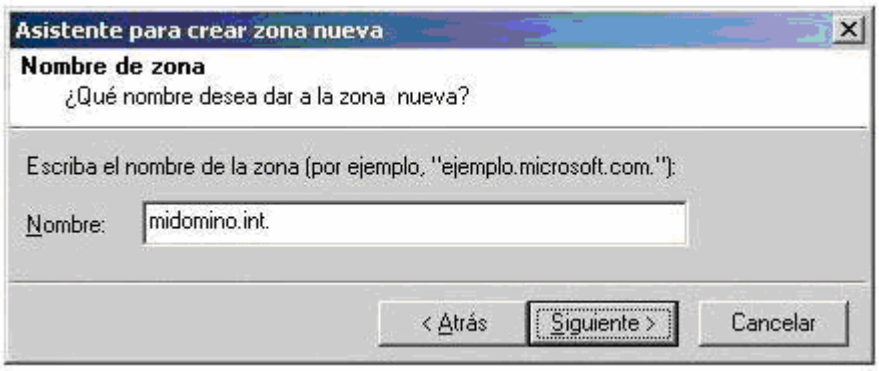

Fig. 2.4.3.4. Nombre de zona DNS directa.

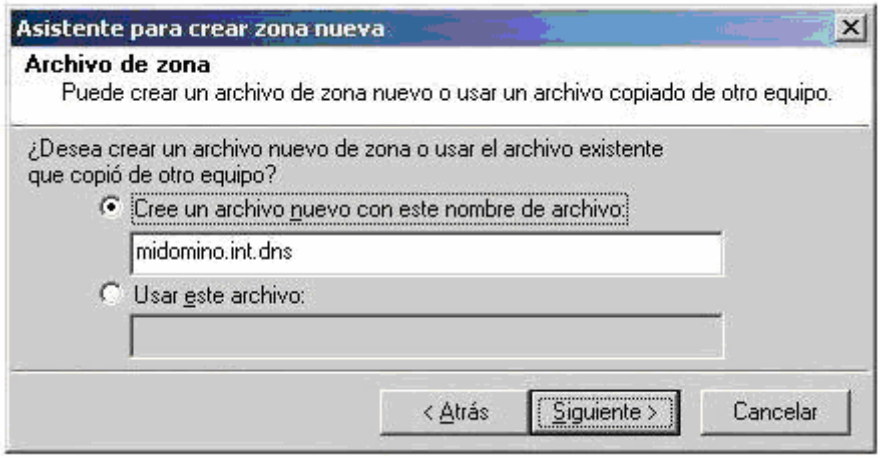

Fig. 2.4.3.5. Archivo de zona DNS directa.

Luego se debe generar la zona de resolución inversa para la zona que implementamos en los pasos anteriores, de igual forma para iniciar el asistente sobre la consola DNS, damos clic derecho sobre zonas de búsqueda inversa (Fig. 2.4.3.6) en el panel izquierdo y seleccionamos la opción Crear una zona nueva, este asistente recopila información acerca del tipo de zona (Fig. 2.4.3.7) y la red IP que resolverá la zona (Fig. 2.4.3.8).

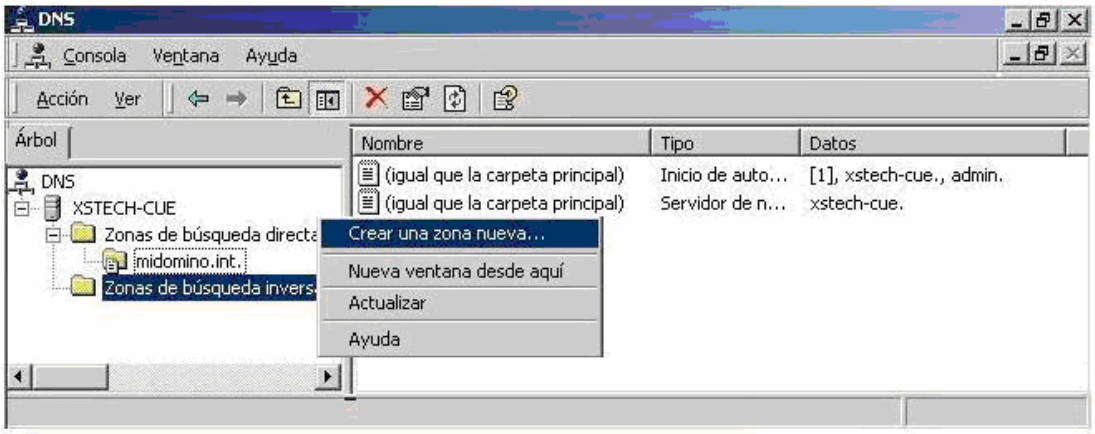

Fig. 2.4.3.6. Creación de zona DNS inversa.

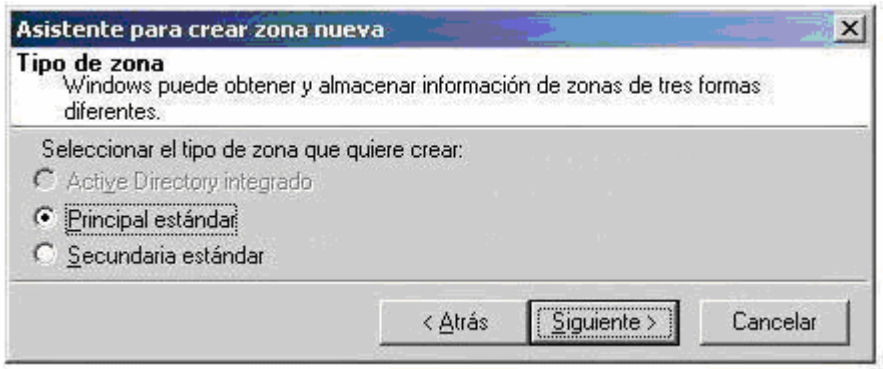

Fig. 2.4.3.7. Tipo de zona DNS inversa.

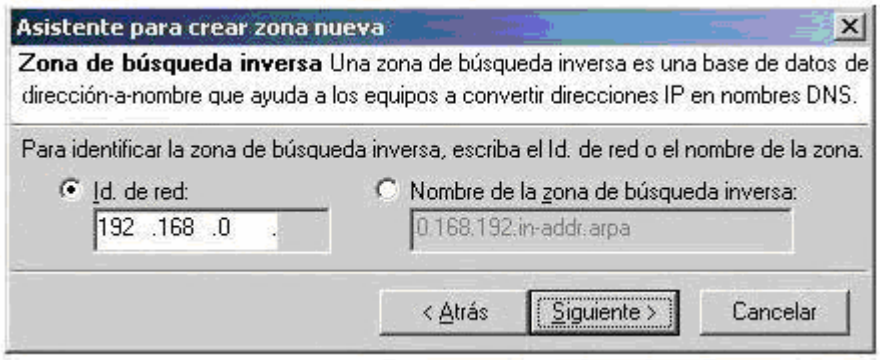

Fig. 2.4.3.8. Red Ip de zona DNS inversa.

Para permitir que otros servidores DNS puedan realizar actualización sobre las entradas de este desde la consola DNS, en las propiedades de las zonas habilitar la opción: ¿Permitir actualizaciones dinámicas? Esta opción se puede habilitar sobre la zona inversa (Fig. 2.4.3.9) y sobre la zona de búsqueda

directa (Fig. 2.4.3.10), al finalizar este proceso las zonas quedaran configuradas y listas para instalar Directorio Activo (Fig. 2.4.3.11).

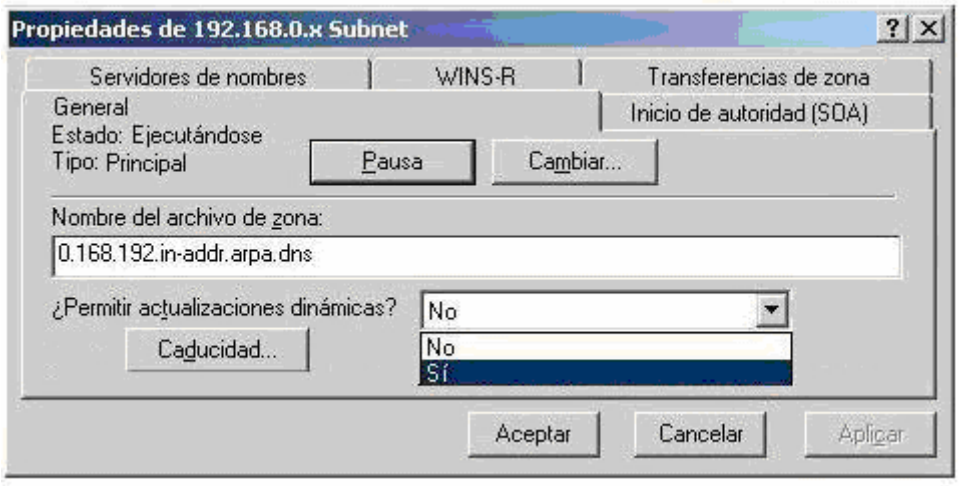

Fig. 2.4.3.9. Habilitar actualizaciones dinámicas en zona DNS inversa.

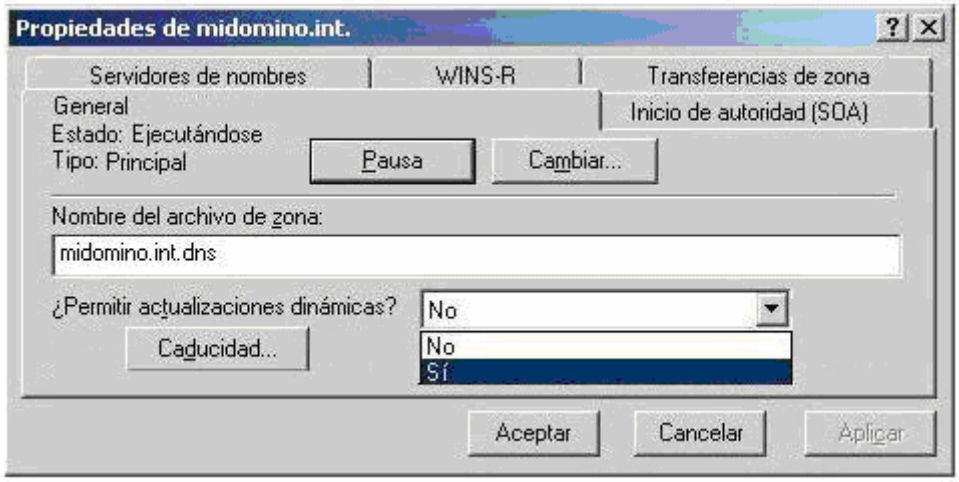

Fig. 2.4.3.10. Habilitar actualizaciones dinámicas en zona DNS directa.

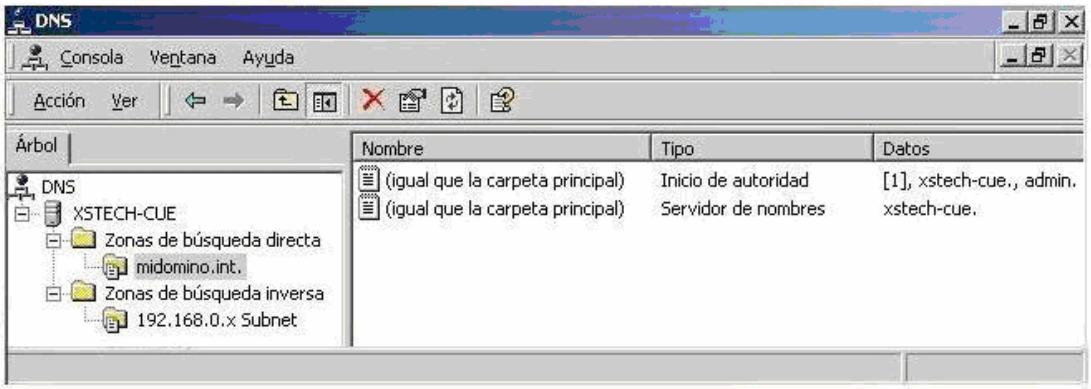

Fig. 2.4.3.11. Revision de zonas creadas.

2.5 Integración de DNS y Microsoft Directorio Activo.

Directorio Activo está integrado con DNS de las siguientes formas:
Los clientes de Directorio Activo utilizan DNS para buscar controladores de dominio.

- Directorio Activo y DNS tienen la misma estructura jerárquica.
  Aunque son independientes y se implementan de forma distinta para propósitos diferentes, el espacio de nombres de una organización para DNS y Directorio Activo tienen una estructura idéntica. Por ejemplo, microsoft.com es un dominio DNS y un dominio de Directorio Activo.
- Las zonas DNS se pueden almacenar en Directorio Activo.
  Si utiliza el servicio DNS de Windows 2000, los archivos de zona primaria se pueden almacenar en Directorio Activo para su replicación en otros controladores de dominio de Directorio Activo.
- Los clientes de Directorio Activo utilizan DNS para buscar controladores de dominio.
  Para localizar un controlador de dominio determinado, los clientes de Directorio Activo envían una consulta al servidor DNS que tienen configurado para obtener determinados registros de recursos.

Dado que Directorio Activo está integrado con DNS y comparte la misma estructura de espacio de nombres, es importante advertir la diferencia entre ellos:

- DNS es un servicio de resolución de nombres.

  Los clientes DNS envían consultas de nombres DNS a su servidor DNS configurado. El servidor DNS recibe la consulta del nombre y, o bien la resuelve mediante los archivos almacenados localmente o consulta otro servidor DNS. DNS no requiere Directorio Activo para funcionar.

- Directorio Activo es un servicio de directorio

  Proporciona un depósito de información y servicios para poner la información a disposición de usuarios y aplicaciones. Los clientes de Directorio Activo envían consultas a los servidores de Directorio Activo por medio del Protocolo Lightweight de acceso a directorios (LDAP, Lightweight Directory Access

Protocol). Un cliente de Directorio Activo consulta DNS con el fin de encontrar un servidor de Directorio Activo. Directorio Activo necesita DNS para funcionar.

Directorio Activo utiliza DNS como un servicio localizador, que resuelve nombres de dominios, sitios y servicios de Directorio Activo en una dirección IP. Para iniciar una sesión en un dominio de Directorio Activo, un cliente de Directorio Activo consulta a sus servidores DNS configurados la dirección IP del servicio LDAP que se ejecuta en un controlador de dominio para un dominio específico.

2.6 Instalación de Microsoft Directorio Activo.

Antes de iniciar la instalación de Microsoft Directorio Activo (Promocionar un servidor a controlados de Dominio) es necesario tener instalado el servidor de DNS, no es necesario tener implementado ningún tipo de zona de resolución, el proceso de promoción determinara la necesidad de generar o no dicha zona de resolución de nombre. Para iniciar el proceso de promoción, desde la opción ejecutar del menú inicio ingrese *dcpromo* y luego presione el boton aceptar (Fig. 2.6.1) este comando iniciara un asistente (Fig. 2.6.2) que le guiara paso a paso en este proceso.

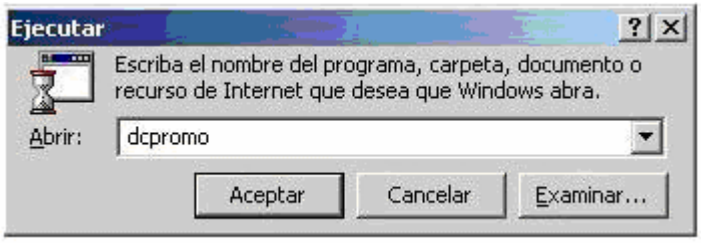

Fig. 2.6.1. Ejecución de asistente para promoción de dominio.

Fig. 2.6.2. Introducción de asistente para promoción de dominio.

Como primer paso se le pedirá que seleccione el tipo de controlador de dominio a promocionar, en nuestro caso este va a ser el primero y único controlador de dominio por lo que seleccionamos la opción Controlador de dominio para un nuevo dominio (Fig. 2.6.3), en el caso que se este agregando un controlador a un dominio existente se debería seleccionar la segunda opción.

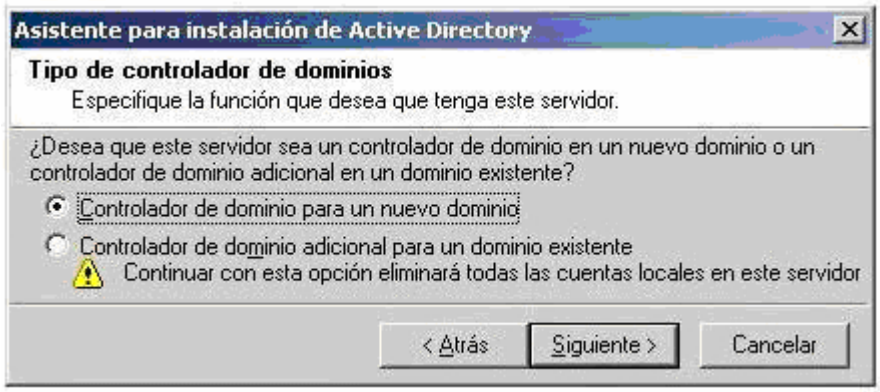

Fig. 2.6.3. Selección de tipo de controlador.

El asistente preguntará acerca de la topología que se generará con este controlador de dominio, respecto a árboles (Fig. 2.6.4) y a los bosques (Fig. 2.6.5) nuestra topología generará un nuevo árbol y bosque en el dominio.

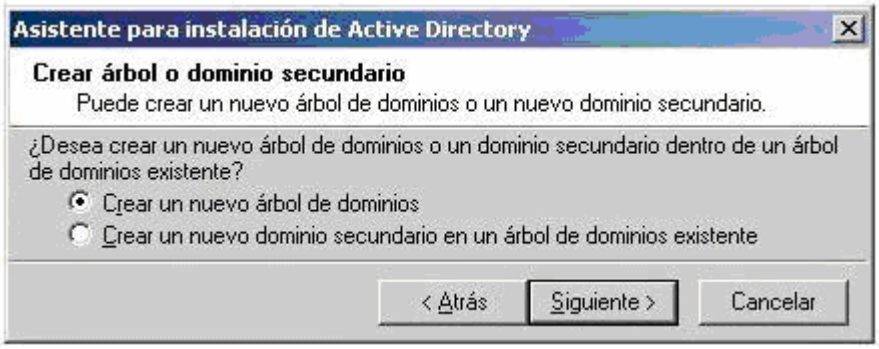

Fig. 2.6.4. Selección de rol de dominio o árbol.

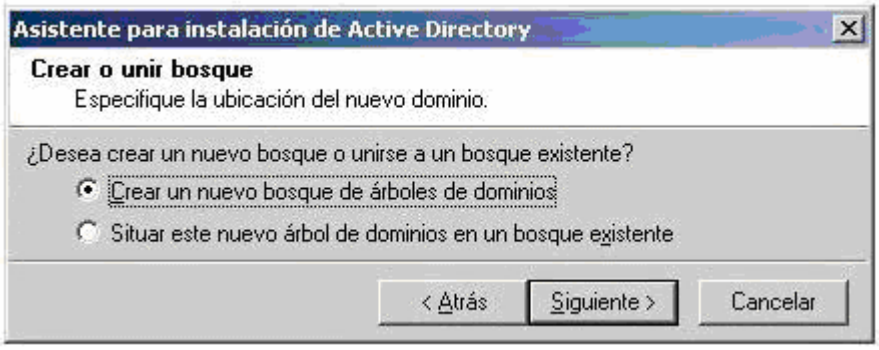

Fig. 2.6.5. Selección de rol en bosque.

El siguiente paso es determinar el nombre del dominio en base al nombre del dominio DNS creado anteriormente (Fig. 2.6.6).

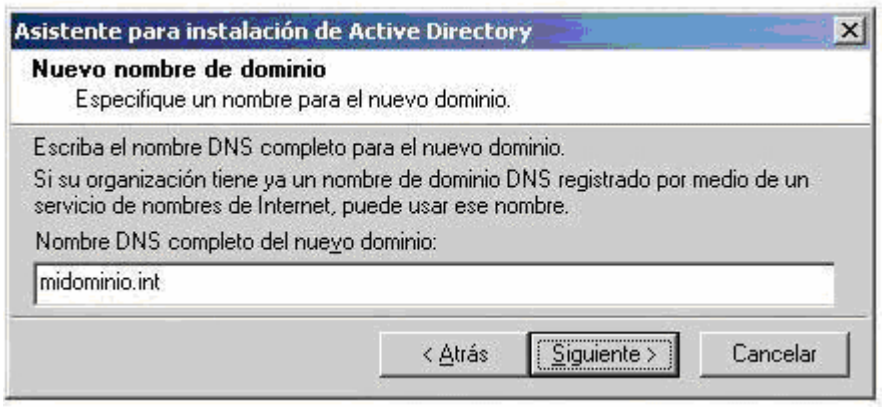

Fig. 2.6.6. Nombre del dominio de acuerdo al dominio DNS.

Los siguientes pasos del asistente recopilan información de la ubicación en el disco de la base de datos del Directorio Activo (Fig. 2.6.7), de la carpeta del volumen del sistema que se compartirá en la red (Fig. 2.6.8) y de la compatibilidad con servidores anteriores a Windows 2000 Server (Fig. 2.6.9).

Fig. 2.6.7. Ubicación de la base de datos del dominio.

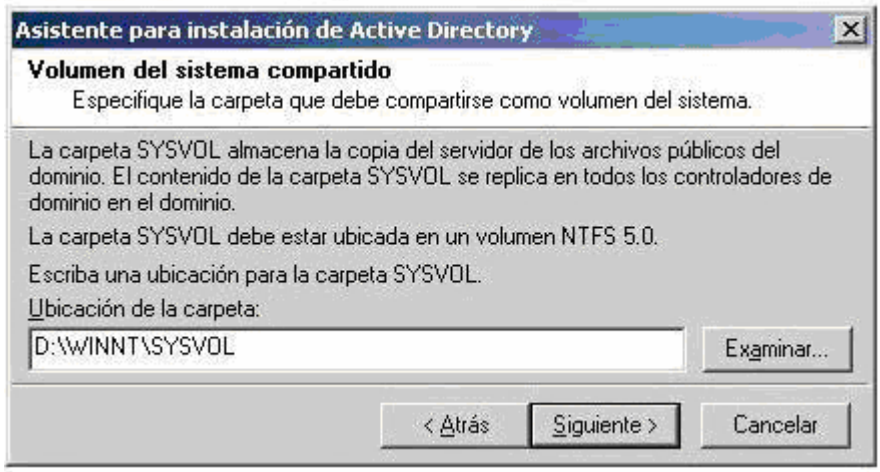

Fig. 2.6.8. Ubicación del volumen del sistema compartido.

Fig. 2.6.9. Selección de compatibilidad con servidores anteriores a Windows 2000.

Para finalizar el asistente y comenzar la instalación se le pide que introduzca la clave del usuario Administrador (Fig. 2.6.10) y se mostrara un resumen de las opciones seleccionadas en el asistente (Fig. 2.6.11).

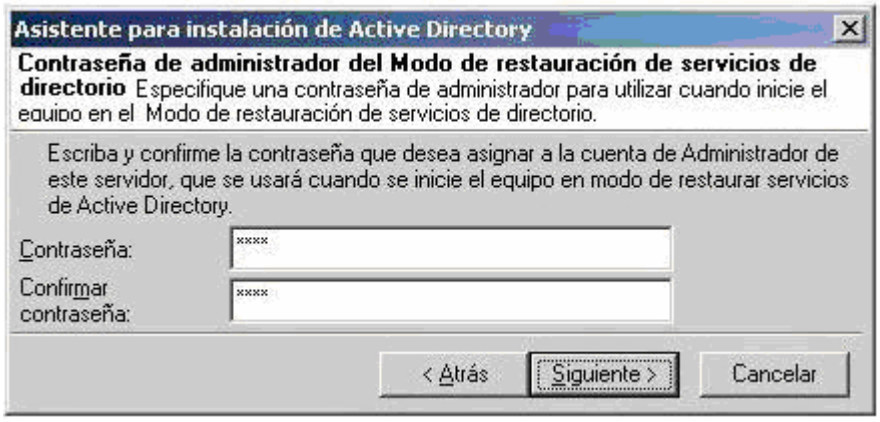

Fig. 2.6.10. Ingreso de contraseña de administrador del dominio.

Fig. 2.6.11. Resumen de opciones seleccionadas.

Al final la instalación se realizara en algunos minutos (Fig. 2.6.12) y se terminara el asistente (Fig. 2.6.13) con lo cual el dominio estará listo para ingresar los objetos al mismo.

Fig. 2.6.12. Proceso de promoción de controlador de dominio.

Fig. 2.6.13. Mensaje de finalización de asistente de promoción de dominio.

2.7 Conclusiones

Con la utilización de las herramientas administrativas de Microsoft se consigue un manejo sencillo y en forma gráfica de los servidores DNS y controladores de dominio. Los controladores de dominio dependen enteramente de las zonas DNS para su funcionamiento.

CAPÍTULO III

Manejo de Objetos sobre Microsoft Directorio Activo

Introducción

La parte que teórica tratada con más énfasis, por su mayor importancia para la comprensión y desarrollo de la aplicación propuesta son: Cuentas de Usuario, equipos. La consola administración usuarios y equipos, de las herramientas administrativas nos permiten el mantenimiento de las cuentas de usuarios que se les debe autenticar, con un único inicio de sesión al dominio para el uso de todos sus recursos.

3.1 Objetos de Microsoft Directorio Activo.

Los recursos que el Directorio Activo considera como objetos administrables (Fig. 3.1.1) son:

- Archivos y Carpetas
- Recursos Compartidos
- Usuarios
- Equipos
- Servicios
- Impresoras

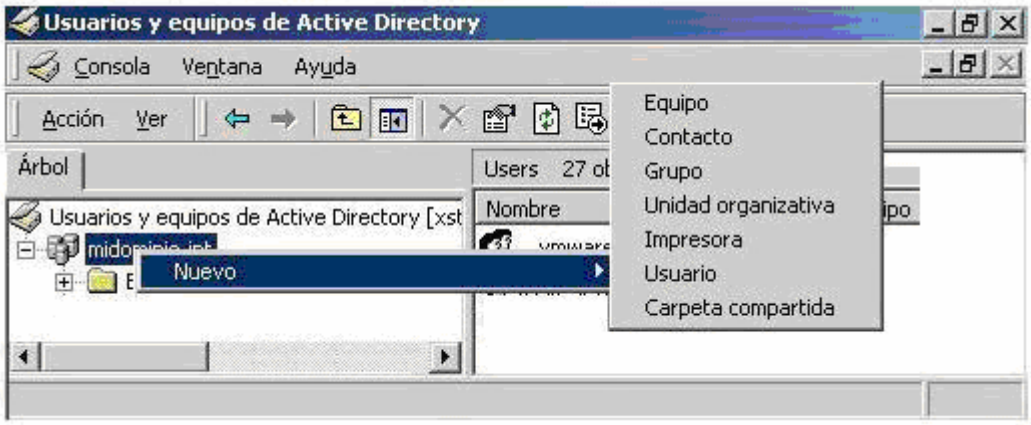

Fig. 3.1.1. Objetos administrables a través de la consola.

Los objetos de mayor importancia para la comprensión y desarrollo de aplicación son:

- Cuentas de Usuario de Directorio Activo permite que un usuario inicie sesiones en equipos y dominios con una identidad que se puede autenticar y autorizar para tener acceso a los recursos del dominio. Cada usuario que se conecta a la red debe tener su propia cuenta de usuario y su propia contraseña única.
- Los equipos donde se ejecuta Windows 2000 o Windows NT que se unen a un dominio tienen una cuenta de equipo. Las cuentas de equipo son similares a las cuentas de usuario y ofrecen un medio para autenticar y auditar el acceso a la red de los equipos y el acceso a los recursos del dominio. Cada equipo conectado a la red debería tener su propia cuenta de equipo única. Las cuentas de equipo también se crean mediante Usuarios y equipos de Directorio Activo.

3.2 Usuarios

3.2.1 Creación de Perfiles de usuarios.

En el Directorio Activo los perfiles de usuario definen la configuración para: Personalizar el entorno del escritorio, conexiones de red y de impresoras, y otras configuraciones especificadas, existen tres tipos de perfiles diferenciados por su objetivo de uso los cuales se crean de forma distinta:

- Perfil de usuario local. Se crea la primera vez que se inicia una sesión, su creación y las modificaciones efectuadas son específicas del equipo en concreto y está almacenado en el disco duro local del equipo.
- Perfil de usuario móvil. Lo crea el administrador del sistema, la creación y sus cambios efectuados se almacenan en un servidor, estando disponible siempre que se inicie una sesión en cualquier equipo de la red.
- Perfil de usuario obligatorio. Son perfiles móviles que se utilizan para especificar configuraciones particulares de usuarios o grupos de

usuarios. Sólo los administradores del sistema pueden realizar cambios en los perfiles de usuario obligatorios.

Los perfiles de usuario ofrecen varias ventajas a los usuarios:

- Varios usuarios pueden utilizar el mismo equipo y cada uno dispone de su configuración de escritorio cuando inicia la sesión.
- Cuando los usuarios inician una sesión en sus estaciones de trabajo, reciben la configuración de escritorio que tenían al terminar la última sesión.
- La personalización del entorno de escritorio efectuada por un usuario no afecta a la configuración del resto de los usuarios.
- Los perfiles de usuario se pueden almacenar en un servidor para que los usuarios puedan utilizarlos en cualquier equipo de la red que ejecute Windows 2000 o superior. Se denominan perfiles de usuario móviles.

3.2.2 Mantenimiento de cuentas de usuario

Cuando cree una cuenta de usuario nueva, o cambie el nombre de una cuenta de usuario.

- Puede escribir una contraseña con hasta 127 caracteres en los equipos Windows 2000 y en los equipos Windows 95 o Windows 98, solo admiten hasta 14 caracteres. Si la es más larga, es posible que no pueda iniciar la sesión en la red desde estos equipos.

Para abrir Administración de equipos, haga clic en Inicio, seleccione Configuración y, a continuación, haga clic en Panel de control. Haga doble clic en Herramientas administrativas y, a continuación, doble clic en Administración de equipos.

1. Abra Administración de equipos.

2. En el árbol de la consola, en Usuarios locales y grupos, haga clic en Usuarios, desde esta consola podrá:

Crear una cuenta de usuario nueva:

Al crear una cuenta de usuario nueva para el dominio se debe considerar que no debe agregar un usuario nuevo al grupo Administradores a menos que el usuario vaya a realizar únicamente tareas administrativas, los pasos para realizar esta tarea son:

1. Haga clic en Acción y después en Usuario nuevo (Fig. 3.2.2.1 – 3.2.2.3).
2. Escriba la información correspondiente al usuario en el cuadro de diálogo:
3. Determine las opciones sobre la contraseña y la forma de creación de la cuenta
4. Realice una de las acciones siguientes:
    - Para crear un usuario adicional, haga clic en Crear y repita los pasos 2 y 3.
    - Para finalizar, haga clic en Crear y después en Cerrar

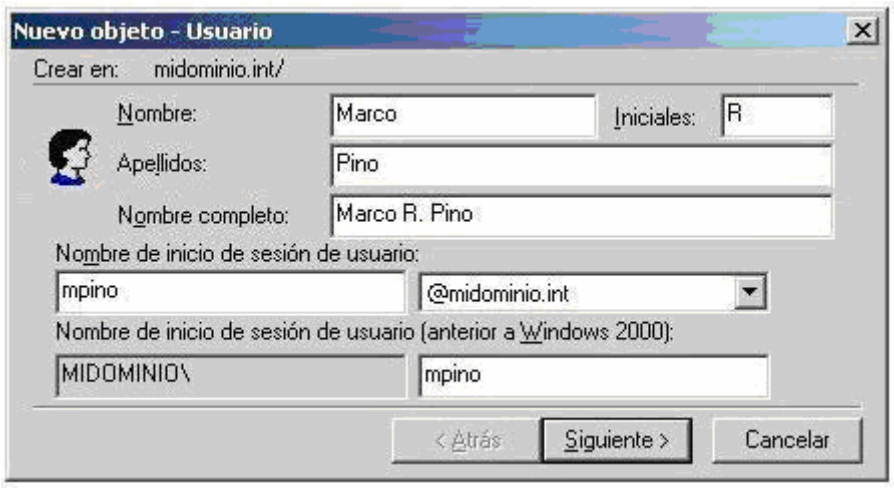

Fig. 3.2.2.1. Ingreso de información de usuario nuevo.

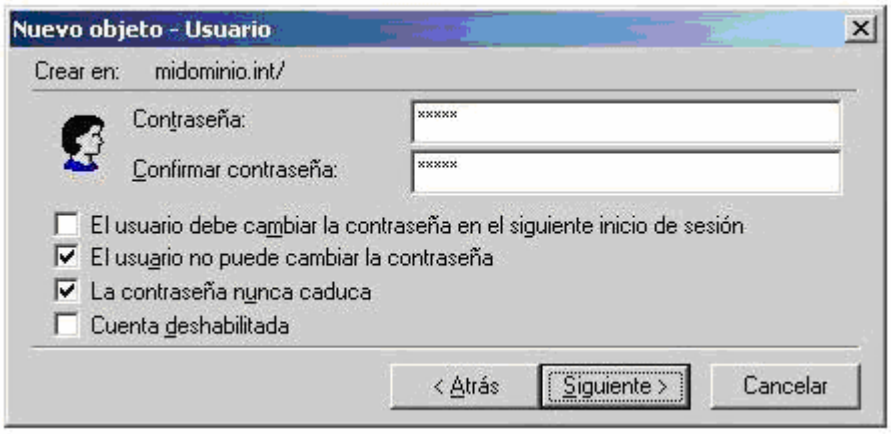

Fig. 3.2.2.2. Estableces contraseña y opciones de cuenta nueva.

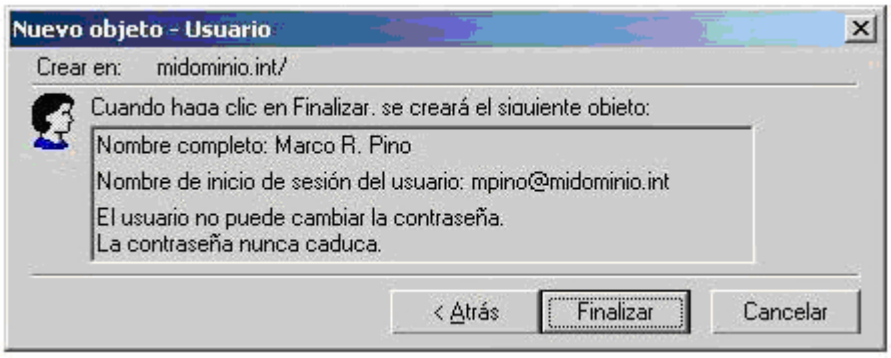

Fig. 3.2.2.3. Confirmación de los datos de cuenta nueva.

Modificar, cambiar la contraseña de un usuario, deshabilitar o habilitar una cuenta:

1. Abra Administración de equipos.
2. En el árbol de la consola, en Usuarios locales y grupos, haga clic en Usuarios
3. Haga clic en la cuenta de usuario a realizarle el mantenimiento.

Para modificar una cuenta de usuario

- Haga clic en Acción y después en Propiedades.
- Realice los cambios que desee y haga clic en Aceptar.

Para cambiar la contraseña de un usuario

- Haga clic en Acción y después en Establecer contraseña.

Para deshabilitar o habilitar una cuenta de usuario

- Haga clic en Acción y después en Propiedades.
- Para deshabilitar la cuenta de usuario seleccionada, active Cuenta deshabilitada.
- Para habilitar la cuenta de usuario seleccionada, desactive Cuenta deshabilitada.

Al realizar esta tarea tenga en cuenta:

- Debe iniciar sesión como administrador o miembro del grupo Administradores para habilitar o deshabilitar la cuenta Invitado.
- Una cuenta deshabilitada todavía existe, pero el usuario no está autorizado a iniciar sesión con ella. Aparece en el panel de detalles, pero el icono de la cuenta está marcado con una X.

- Cuando se habilita una cuenta de usuario, el usuario está autorizado a iniciar sesión con la cuenta de la forma habitual.
- No se puede deshabilitar la cuenta integrada Administrador.

Eliminar una cuenta de usuario:

1. Haga clic en Acción y después en Eliminar.
2. Si aparece un mensaje de confirmación, haga clic en Aceptar.
3. Cuando aparezca el mensaje que le pregunta si desea eliminar la cuenta, haga clic en Sí.

Al realizar esta tarea tenga en cuenta:

- Cuando necesite quitar cuentas de usuario, es recomendable deshabilitar las cuentas en primer lugar. Cuando esté seguro de que al deshabilitar la cuenta no se causa ningún problema, puede eliminarla de forma segura.
- No se puede recuperar una cuenta de usuario eliminada.
- No se pueden eliminar las cuentas integradas Administrador e Invitado.

Cambiar el nombre de una cuenta de usuario

Puesto que una cuenta de usuario con el nombre cambiado conserva su identificador de seguridad (SID), mantiene todas las demás propiedades, como la descripción, la contraseña, la pertenencia a grupos, el perfil de entorno de usuario, la información de cuenta, y todos los permisos y derechos asignados. Las actividades para realizar está tarea son:

1. Haga clic en Acción y después en Cambiar nombre.
2. Escriba el nombre de usuario nuevo y presione ENTRAR.

3.3 Grupos.

3.3.1 Tipos de grupos y su uso.

Los grupos se utilizan para:

- Administrar el acceso de equipos y usuarios a recursos compartidos como los objetos de Directorio Activo y sus propiedades, recursos compartidos de red, archivos, directorios, colas de impresión, etc.
- Filtrar las configuraciones de Directiva de grupo.
- Crear listas de distribución de correo electrónico.

Hay dos tipos de grupos en Windows 2000:

- Grupos de seguridad
- Grupos de distribución

Los grupos de seguridad se muestran en las listas de control de acceso discrecional (DACL, Discretionary Access Control List) en las que están definidos los permisos sobre recursos y objetos. Los grupos de seguridad se pueden utilizar también como entidades de correo electrónico. Al enviar un mensaje de correo electrónico al grupo, el mensaje se envía a todos los miembros del grupo.

En los grupos de distribución no es posible habilitar la seguridad. No pueden aparecer en las listas DACL. Los grupos de distribución sólo se pueden utilizar con aplicaciones de correo electrónico (como Exchange) para enviar correo electrónico a grupos de usuarios. Si no necesita un grupo para propósitos de seguridad, cree un grupo de distribución en lugar de un grupo de seguridad.

Aunque se puede agregar un contacto a un grupo de seguridad o a un grupo de distribución, no se pueden asignar derechos y permisos a los contactos. Se puede enviar correo electrónico a los contactos de un grupo.

Cada grupo de seguridad o de distribución tiene un ámbito que identifica el alcance de aplicación del grupo al árbol o al bosque de dominios. Existen tres ámbitos distintos: universal, global y dominio local.

- Los grupos de ámbito universal pueden tener como miembros grupos y cuentas de cualquier dominio de Windows 2000 en el árbol o el bosque de dominios y se les pueden conceder permisos en cualquier dominio del árbol o el bosque de dominios. Los grupos de ámbito universal se denominan grupos universales.

- Los grupos de ámbito global pueden tener como miembros grupos y cuentas sólo del dominio en el que se ha definido el grupo y se les pueden conceder permisos en cualquier dominio del bosque. Los grupos de ámbito global se denominan grupos globales.
- Los grupos con ámbito local de dominio pueden tener como miembros los grupos y cuentas de un dominio de Windows 2000 o Windows NT, y sólo se pueden utilizar para conceder permisos en un dominio. Los grupos con ámbito local de dominio se denominan grupos locales de dominio.

Si hay varios bosques, los usuarios definidos sólo en uno de ellos no se pueden incluir en los grupos definidos en otro bosque, al igual que no se pueden asignar permisos en un bosque a grupos definidos solamente en otro bosque.

Al instalar un controlador de dominio se instalan también varios grupos predefinidos en las carpetas Usuarios e Integrados de la consola de Usuarios y equipos de Directorio Activo. Estos grupos son grupos de seguridad que representan conjuntos comunes de derechos y permisos que puede utilizar para conceder determinadas funciones, derechos y permisos a las cuentas y grupos que coloca en los grupos predeterminados.

Los grupos predeterminados de ámbito local de dominio se encuentran en la carpeta Integrados. Los grupos predeterminados de ámbito global se encuentran en la carpeta Usuarios. Puede mover los grupos integrados y predefinidos a otros grupos o carpetas de unidades organizativas del dominio, pero no puede moverlos a otros dominios.

Grupos integrados

Los grupos predeterminados existentes en la carpeta Integrados de Usuarios y equipos de Directorio Activo son los siguientes:

- Operadores de cuentas
- Administradores
- Operadores de copia de seguridad

- Invitados
- Operadores de impresión
- Replicador
- Operadores de servidores
- Usuarios

Estos grupos integrados tienen un ámbito local de dominio y se utilizan principalmente para asignar conjuntos predeterminados de permisos a usuarios que van a tener control administrativo en el dominio. Por ejemplo, el grupo Administradores de un dominio tiene un conjunto amplio de capacidades de administración sobre los recursos y cuentas del dominio.

La siguiente tabla muestra los derechos predeterminados que tienen asignados estos grupos:

Derecho de usuario	**Permite**	**Grupos a los que está asignado este derecho de forma predeterminada**
Tener acceso a este equipo desde la red	Conectar con el equipo a través de la red.	Administradores, Todos, Usuarios avanzados
Hacer copias de seguridad de archivos y carpetas	Hacer copias de seguridad de archivos y carpetas. Este derecho prevalece sobre los permisos de los archivos y carpetas.	Administradores, Operadores de copia de seguridad
Saltarse la comprobación de recorrido	Pasar de una carpeta a otra para tener acceso a los archivos, aún en el caso de que el usuario no tenga premiso de acceso a las carpetas de archivos principales.	Todos
Cambiar la hora del sistema	Establecer la fecha y hora del reloj interno del equipo.	Administradores, Usuarios avanzados
Crear un archivo de paginación	Este derecho no tiene ningún efecto.	Administradores
Depurar programas	Depurar diversos objetos de nivel inferior, por ejemplo, subprocesos.	Administradores
Forzar el apagado desde un sistema remoto	Cerrar un equipo remoto.	Administradores

Aumentar la prioridad de una programación	Aumentar la prioridad de ejecución de un proceso.	Administradores, Usuarios avanzados
Cargar y descargar controladores de dispositivo	Instalar y quitar controladores de dispositivo.	Administradores
Inicio de sesión local	Iniciar una sesión en el equipo a través de su teclado.	Administradores, Operadores de copia de seguridad, Todos, Invitados, Usuarios avanzados y Usuarios
Administrar los registros de auditoría y seguridad	Especificar los tipos de acceso a recursos (por ejemplo, acceso a archivos) que deben incluirse en la auditoría, y ver y borrar el registro de seguridad. Este derecho no permite a un usuario establecer la directiva de auditoría del sistema. Los miembros del grupo Administradores siempre pueden ver y borrar el registro de seguridad.	Administradores
Modificar las variables de entorno del firmware	Modificar las variables de entorno del sistema que se almacenan en la memoria RAM no volátil de los equipos que admiten este tipo de configuración.	Administradores
Perfilar el rendimiento de un proceso individual	Realizar un análisis de rendimiento (muestreo de rendimiento) en un proceso.	Administradores, Usuarios avanzados
Perfilar el rendimiento del sistema	Realizar un análisis de rendimiento (muestreo de rendimiento) en el equipo.	Administradores
Restaurar archivos y carpetas	Restaurar copias de seguridad de archivos y carpetas. Este derecho prevalece sobre los permisos de los archivos y directorios.	Administradores, Operadores de copia de seguridad
Apagar el sistema	Cerrar el sistema Windows 2000.	Administradores, Operadores de copia de seguridad, Todos, Usuarios avanzados y Usuarios.
Tomar posesión de archivos y otros objetos	Tomar posesión de archivos, carpetas, impresoras y otros objetos del equipo (o conectados a él). Este derecho prevalece sobre los permisos que protegen esos objetos..	Administradores

Tabla. 3.3.1.1. Derechos por grupos.

Grupos predefinidos

Los grupos predefinidos incluidos en la carpeta Usuarios de Usuarios y equipos de Directorio Activo son los siguientes:

- Nombre de grupo
- Publicadores de certificados
- Administradores del dominio
- Equipos de dominio
- Controladores de dominio
- Invitados de dominio
- Usuarios de dominio
- Administradores de empresa
- Administradores de Directiva de grupo
- Administradores de esquema

Puede utilizar estos grupos de ámbito global para recopilar en varios grupos los diversos tipos de cuentas de usuario existentes en ese dominio (usuarios normales, administradores e invitados). Esos grupos pueden a su vez incluirse en grupos de ámbito local de dominio en ese dominio y en otros.

De forma predeterminada, cualquier cuenta de usuario que cree en un dominio se agrega automáticamente al grupo Usuarios de dominio y cualquier cuenta de equipo que cree se agrega automáticamente al grupo Equipos de dominio. Puede utilizar los grupos Usuarios de dominio y Equipos de dominio para representar todas las cuentas que se han creado en el dominio. Por ejemplo, si desea que todos los usuarios del dominio tengan acceso a una impresora, puede asignar permisos para la impresora al grupo Usuarios de dominio (o puede colocar el grupo Usuarios de dominio en un grupo local de dominio con permisos para la impresora).

De forma predeterminada, el grupo Usuarios de dominio de un dominio es miembro del grupo Usuarios de ese mismo dominio.

El grupo Administradores de dominio puede representar a los usuarios que tienen múltiples derechos administrativos en un dominio. Windows 2000 Server no incluye automáticamente en ese grupo ninguna cuenta, pero si

desea que una cuenta tenga todos los derechos de administrador en un dominio (y posiblemente en otros dominios), puede incluirla en el grupo Administradores de dominio. Como Windows 2000 Server permite delegar la autoridad, no se deben conceder estos múltiples derechos administrativos a muchos usuarios.

De forma predeterminada, el grupo Administradores de dominio en un dominio es miembro del grupo Administradores en el mismo dominio.

De forma predeterminada, el grupo Invitados de dominio es miembro del grupo Invitados en el mismo dominio y contiene automáticamente la cuenta de usuario Invitado predeterminada del dominio.

3.4 Conclusiones

Las tareas de administración de usuarios (creación de una cuenta nueva para los usuarios, deshabilitar, modificar y eliminar), se realizan de forma completamente intuitiva usando la consola Usuarios y Equipos de Directorio Activo mejorando considerablemente la carga administrativa.

CAPÍTULO IV

Directivas de grupo en Microsoft Directorio Activo

Introducción

En el desarrollo del siguiente capítulo se explica que las directivas de grupo son una herramienta muy eficaz para disminuir la carga administrativa de la red, porque de forma selectiva damos configuraciones de una política de grupo, que es la ejecución de un script que se ejecutara después que el usuario realice su autenticación, es decir al inicio de la sesión.

4.1 Concepto de directiva de grupo.

La Directiva de grupo se almacena en los objetos de Directiva de grupo.
Se puede utilizar para:

- Configurar opciones de seguridad,
- Administrar aplicaciones, puede instalar en determinados equipos o que está disponible para ciertos grupos de usuarios.
- Administrar la apariencia del escritorio,
- Asignar secuencias de comandos
- Redirigir carpetas desde equipos locales a ubicaciones de red.

Los objetos de Directiva de grupo constituyen una herramienta administrativa muy eficaz ya que se puede controlar la configuración de forma selectiva a cuentas de usuario, y equipo y se puede aplicar a sitios, dominios, unidades organizativas pero nunca a los grupos, en toda la organización. El complemento Directiva de grupo. Se utiliza para crear o modificar objetos de Directiva de grupo.

4.2 Planificación de directivas de grupo.

Al implementar una directiva de grupo es necesario considerar las necesidades reales del grupo de equipos o usuarios destino, no es posible implementar políticas solo por el hecho de hacerlas, es también necesario considerar establecer políticas con objetivos puntuales, es decir: políticas de respaldo, políticas de instalación de aplicativos, políticas de seguridad y control de acceso. Al no aplicar esta consideración y mantener varias políticas multipropósito asignadas a la misma unidad organizacional podrían llegar estas a contradecirse y con esto podríamos tener resultados inesperados.

4.3 Implementación de directivas de grupo.

Para la implementación de políticas de Grupo diríjase al menú Inicio, Programas, Herramientas Administrativas, Usuarios y Equipos de Active Directory seleccione la unidad Organizacional a la cual quiere aplicar la política y con el clic derecho abra las Propiedades (Fig. 4.3.1).

Fig. 4.3.1. Propiedades de Unidad Organizacional.

Una ves que se encuentre en las Propiedades de la unidad organizacional (Fig. 4.3.2) diríjase a la pestaña Directiva de Grupo presione el botón Nueva para crear una nueva política, ingrese el nombre de la política y presione el botón Modificar para editarla.

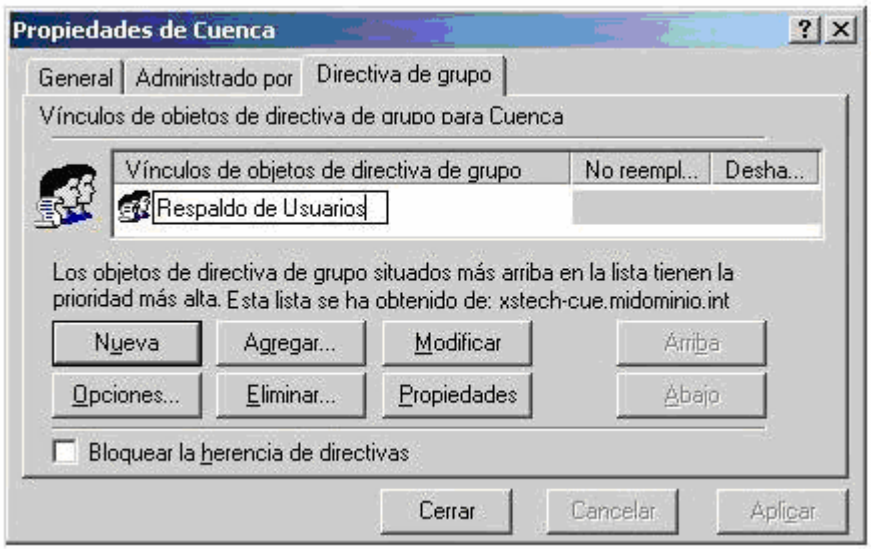

Fig. 4.3.2. Agregando una política a una unidad organizacional.

La consola de edición de Directivas de Grupo o Políticas (Fig. 4.3.3) muestra varias categorías de de directivas que se agrupan en dos principales:

- Configuración de equipo.- Son las políticas que se aplican antes que el sistema operativo muestre la pantalla de ingreso de credenciales para iniciar sesión en un equipo con Windows XP Professional o Windows 2000 Professional.
- Configuración de usuario.- Son las políticas que se aplican después que el usuario haya ingresado sus credenciales para iniciar sesión en el equipo.

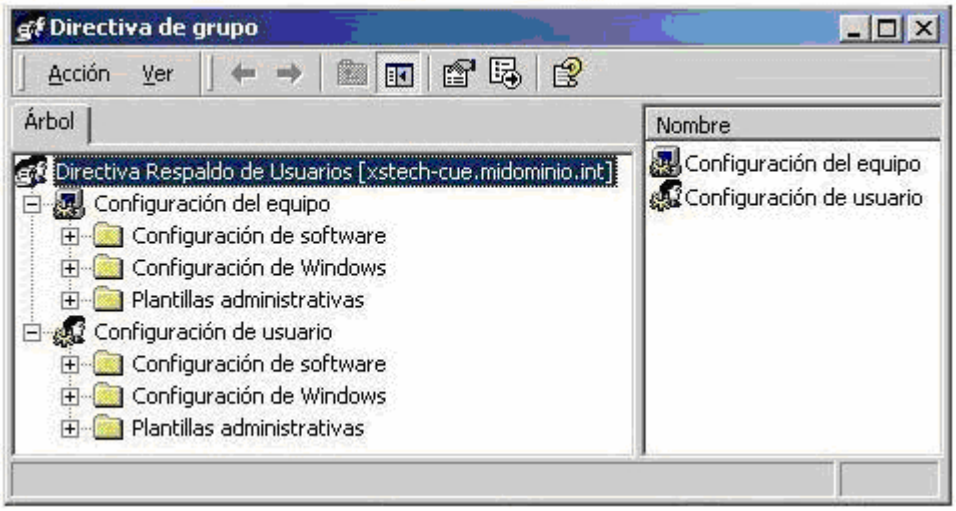

Fig. 4.3.3. Consola de edición de políticas.

Para el desarrollo de nuestro ejemplo de funcionamiento estableceremos una política por usuario (Fig. 4.3.4), en la que ejecutaremos un script escrito en visual Basic que realizará el respaldo del perfil del usuario, para indicar que script se ejecutará tenemos que ir a las Propiedades de Iniciar sesión que se encuentra en la categoría Archivos de Comando en la Configuración de Windows de la Configuración de usuario.

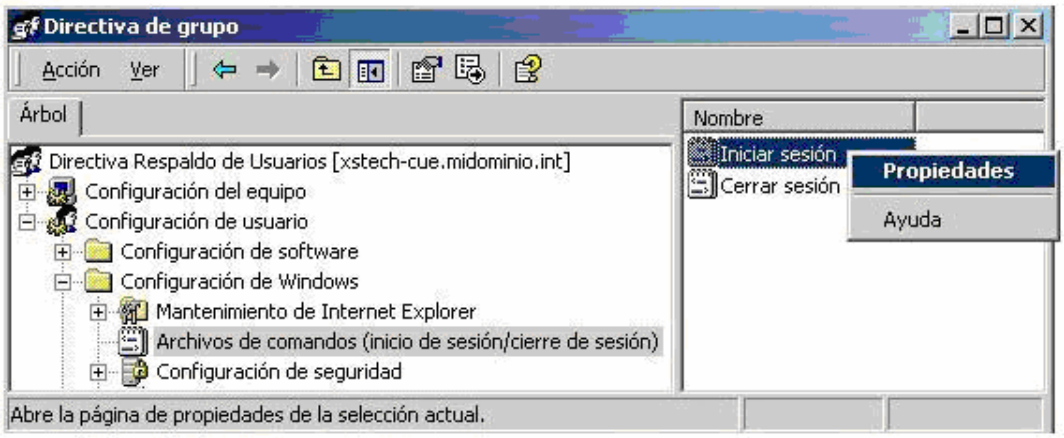

Fig. 4.3.4. Modificando las acciones de inicio de sesión.

Una ves que se encuentre dentro de las Propiedades de Iniciar Sesión (Fig. 4.3.5) presione el botón Agregar, este mostrara un cuadro de dialogo: Agregar un archivo de Comandos (Fig. 4.3.6) mediante el cual seleccionaremos el script (Fig. 4.3.7) que debe encontrarse dentro de la carpeta del Volumen del sistema compartido. Una ves seleccionado el archivo acepte toda la pila de formularios abiertos.

Para probar el correcto funcionamiento de las políticas inicie sesión con un usuario que este dentro de la unidad organizacional a la cual se aplicaron las políticas.

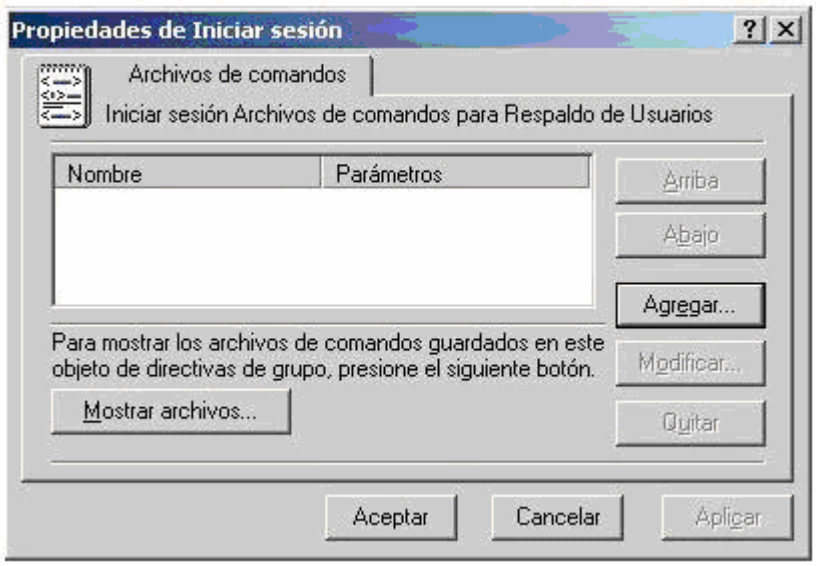

Fig. 4.3.5. Formulario para el ingreso de la ubicación del script.

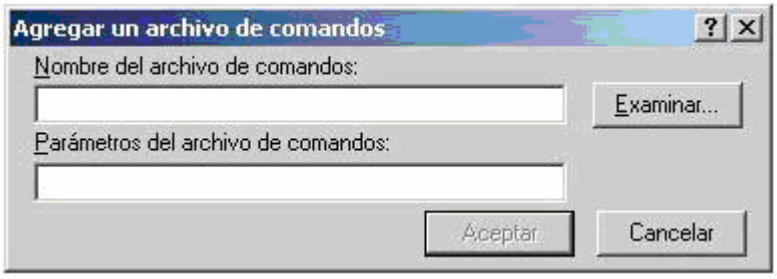

Fig. 4.3.6. Seleccionando el archivo de comandos.

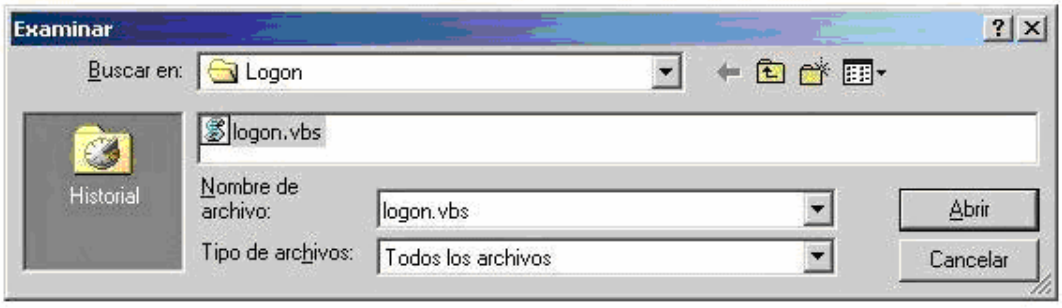

Fig. 4.3.7. Seleccionando el script en visual Basic script.

4.4. Conclusiones

Con el ejemplo se verifica la disminución de la administración de los usuarios ya que la política de grupo planificada de respaldo del perfil de usuario que inicia la sesión

funciona gracias a la ejecución del script que contiene código para la realización de un backup.

CAPÍTULO V

Kerberos sobre sistemas operativos Linux.

Introducción

Para que un servidor pueda ofrecer información a otro debe existir entre estos servidores una relación de confianza establecida, no es posible entregar información concerniente a cuentas de usuario, claves u otro tipo de información a cualquier equipo que lo pida.
Los conceptos aquí utilizados se derivan de los publicados en el sitio Web: <http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node296.html>

5.1 Concepto de Kerberos.

Durante 1983 en el M.I.T. (Massachussetts Institute of Technology) comenzó el proyecto Athena con el objetivo de crear un entorno de trabajo educacional compuesto por estaciones gráficas, redes de alta velocidad y servidores; el sistema operativo para implementar este entorno era Unix 4.3BSD, y el sistema de autenticación utilizado en el proyecto se denominó Kerberos ([MNSS87]) “en honor al perro de tres cabezas que en la mitología griega vigila la puerta de entrada a Hades, el infierno”.

Hasta que se diseñó Kerberos, la autenticación en redes de computadores se realizaba principalmente de dos formas: o bien se aplicaba la autenticación por declaración (Authentication by assertion), en la que el usuario es libre de indicar el servicio al que desea acceder (por ejemplo, mediante el uso de un cliente determinado), o bien se utilizaban contraseñas para cada servicio de red. Evidentemente el primer modelo proporciona un nivel de seguridad muy bajo, ya que se le otorga demasiado poder al cliente sobre el servidor; el segundo modelo tampoco es muy bueno: por un lado se obliga al usuario a ir tecleando contínuamente su clave, de forma que se pierde

demasiado tiempo y además la contraseña está viajando contínuamente por la red. Kerberos trata de mejorar estos esquemas intentando por un lado que un cliente necesite autorización para comunicar con un servidor (y que esa autorización provenga de una máquina confiable), y por otro eliminando la necesidad de demostrar el conocimiento de información privada (la contraseña del usuario) divulgando dicha información.

Kerberos se ha convertido desde entonces en un referente obligatorio a la hora de hablar de seguridad en redes. Se encuentra disponible para la mayoría de sistemas Unix, y viene integrado con OSF/DCE (Distributed Computing Environment). Está especialmente recomendado para sistemas operativos distribuidos, en los que la autenticación es una pieza fundamental para su funcionamiento: si conseguimos que un servidor logre conocer la identidad de un cliente puede decidir sobre la concesión de un servicio o la asignación de privilegios especiales. Sigue vigente en la actualidad (en su versión V a la hora de escribir este trabajo), a pesar del tiempo transcurrido desde su diseño; además fué el pionero de los sistemas de autenticación para sistemas en red, y muchos otros diseñados posteriormente, como KryptoKnight ([MTHZ92], [JTY97]...), SESAME ([PPK93]) o Charon ([Atk93]) se basan en mayor o menor medida en Kerberos.

El uso de Kerberos se produce principalmente en el login, en el acceso a otros servidores (por ejemplo, mediante rlogin) y en el acceso a sistemas de ficheros en red como NFS. Una vez que un cliente está autenticado o bien se asume que todos sus mensajes son fiables, o si se desea mayor seguridad se puede elegir trabajar con mensajes seguros (autenticados) o privados (autenticados y cifrados). Kerberos se puede implementar en un servidor que se ejecute en una máquina segura, mediante un conjunto de bibliotecas que utilizan tanto los clientes como las aplicaciones; se trata de un sistema fácilmente escalable y que admite replicación, por lo que se puede utilizar incluso en sistemas de alta disponibilidad.

Un servidor Kerberos se denomina KDC (Kerberos Distribution Center), y provee de dos servicios fundamentales: el de autenticación (AS, Authentication Service) y el de tickets (TGS, Ticket Granting Service). El primero tiene como función autenticar

inicialmente a los clientes y proporcionarles un ticket para comunicarse con el segundo, el servidor de tickets, que proporcionará a los clientes las credenciales necesarias para comunicarse con un servidor final que es quien realmente ofrece un servicio. Además, el servidor posee una base de datos de sus clientes (usuarios o programas) con sus respectivas claves privadas, conocidas únicamente por dicho servidor y por el cliente que al que pertenece.

Proceso de Autenticación Kerberos:

El proceso de autenticación en Kerberos se realiza en las siguientes etapas:

- Cliente que solicita un servicio
- Servidor que ofrece dicho servicio
- Servidor de autenticación
- Servidor de tickets
- Clave secreta del cliente
- Clave secreta del servidor
- Clave secreta del servidor de tickets
- Clave de sesión entre el cliente y el servidor de tickets
- Clave de sesión entre cliente y servidor

Por que utilizar ticket

Un ticket sirve para un solo servidor y para un solo cliente pero una vez emitido, puede ser utilizado muchas veces por el cliente para tener acceso a ese servidor, hasta que el ticket expira. Como el ticket está encriptado con la clave del servidor no se pierde seguridad al permitir que el usuario le pase el ticket al servidor, ya que no podrá modificarlo.

5.2 Implementación y configuración de Kerberos sobre Linux.

Primero se debe verificar que la instalación de Samba haya sido realizada para soportar Kerberos, normalmente la instalación por defecto lo soporta, pero es necesario estar seguro de esto. El comando smbd tiene algunas opciones para mostrar en pantalla información acerca de esto, con los siguientes comandos se mostraran más líneas de las que se muestran aquí.

```
root@windbag:/usr/sbin# cd /usr/sbin
root@windbag:/usr/sbin# smbd -b | grep KRB
HAVE_KRB5_H
HAVE_ADDRTYPE_IN_KRB5_ADDRESS
HAVE_KRB5
...
root@windbag:/usr/sbin# smbd -b | grep ADS
WITH_ADS
WITH_ADS
...
root@windbag:/usr/sbin# smbd -b | grep WINBIND
WITH_WINBIND
WITH_WINBIND
```

En el caso que el resultado de estos comandos no muestre esta información será necesario recompilar Samba, está tarea casi nunca es necesaria.

Cuando se encuentre seguro que la instalación de Samba soporte Kerberos, es necesario modificar el archivo de configuración /etc/krb5.conf, la mínima configuración para que el equipo Linux se pueda conectar al servidor controlador de dominio llamado xstech-cue en el dominio: midominio.int debe ser:

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
[libdefaults]
 default_realm = MIDOMINIO.INT
 dns_lookup_realm = true
 dns_lookup_kdc = true
[realms]
 EXAMPLE.COM = {
  kdc = kerberos.example.com:88
```

```
 admin_server = kerberos.example.com:749
 default_domain = example.com
}
MIDOMINIO.INT = {
 kdc = xstech-cue.midominio.int:88
 admin_server = xstech-cue.midominio.int:749
}
MIDOMINIO.INT = {
 kdc = xstech-cue.MIDOMINIO.INT
}
[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
[kdc]
 profile = /var/kerberos/krb5kdc/kdc.conf
[appdefaults]
 pam = {
   debug = false
   ticket_lifetime = 36000
   renew_lifetime = 36000
   forwardable = true
   krb4_convert = false
 }
```

Debe utilizarse mayúsculas para ingresar el nombre del dominio en los lugares descritos en la configuración de ejemplo descrita en la parte superior.

5.3 Generando ticket de seguridad.

Una ves que se realice esta configuración es necesario ingresar el siguiente comando para conectarse al servidor de dominio y generar el ticket de seguridad, si la conexión se realiza de forma exitosa se le pedirá el password de el usuario con el que se conecto al dominio.

```
# kinit Administrador@MIDOMINIO.INT
Password for Administrador@MIDOMINIO.INT
```

El comando:

```
root#  klist -e
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrador@MIDOMINIO.INT

Valid starting     Expires            Service principal
02/15/06 23:19:38  02/16/06 09:19:41  krbtgt/MIDOMINIO.INT@MIDOMINIO.INT
        renew until 02/16/06 23:19:38, Etype (skey, tkt): ArcFour with HMAC/md5, ArcFour with
HMAC/md5
02/16/06 00:12:43  02/16/06 09:19:41  xstech-cue$@MIDOMINIO.INT
        renew until 02/16/06 23:19:38, Etype (skey, tkt): ArcFour with HMAC/md5, ArcFour with
HMAC/md5

Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
```

Muestra un listado de todos los ticket almacenados en cache por el sistema.

5.4 Conclusiones

Para que dos o más equipos puedan interactuar libremente compartiendo todo tipo de información debe generarse una relación de confianza. Esta relación de confianza se puede establecer mediante Kerberos, el mismo que no es propietario de ningún sistema operativo ni fabricante.

CAPÍTULO VI

Servicio Samba y Winbind sobre sistemas operativos Linux.

Introducción

Utilizar Winbind como un medio para autenticar los accesos de los usuarios a los recursos compartidos mediante Samba es una forma rentable de compartir y también centralizar información de la organización y usuarios en un solo servidor.
Todos los conceptos aquí utilizados son conclusiones obtenidas de la investigación realizada en la Internet en los sitios:
<http://www.tuxteno.com/contents.php?cid=163>
<http://www.siriusit.co.uk/docs/doc.php?pageID=13&typeID=3>
<http://www.enterprisenetworkingplanet.com/netos/article.php/3487081>

6.1 Concepto de Samba.

Samba es una suite de aplicaciones Unix que habla el protocolo SMB (Server Message Block). Los sistemas operativos Microsoft Windows y OS/2 utilizan SMB para compartir por red archivos e impresoras y para realizar tareas asociadas. Gracias al soporte de este protocolo, Samba permite a las máquinas Unix entrar en el juego, comunicándose con el mismo protocolo de red que Microsoft Windows y aparecer como otro sistema Windows en la red (desde la perspectiva de un cliente Windows).

Con un servidor Samba correctamente configurado sobre cualquier Linux, los clientes Windows pueden conectarse a unidades de red con sistemas de Archivos Linux. De igual forma, los clientes Samba sobre Linux pueden conectarse a recursos compartidos Windows a través de su nombre UNC. Aunque existan algunas limitaciones que radican en las diferencias entre los sistemas operativos como por ejemplo autentificación, nombres de archivos o caracteres de fin de línea, Samba ofrece un mecanismo general para compartir recursos sobre una red heterogénea.

El servicio Samba es también conocido como NetBIOS para UNIX. Samba puede ser utilizado de varias formas, en una intranet o cualquier otra red privada, por ejemplo se puede utilizar Samba para transferir archivos entre un servidor Linux y un cliente Windows. Cualquiera usando Web Server corriendo Apache y Linux puede considerar usar Samba en lugar de utilizar FTP para administrar el contenido del sitio Web de forma remota, de esta manera los clientes SMB pueden realizar actualizaciones de los archivos de forma remota.

Samba brinda mucha ayuda al trabajar con servidores Linux que no sean necesariamente servidores Web. Es posible desarrollar aplicaciones que se ejecuten sobre plataformas Windows que utilicen impresoras sobre Linux. Los usuarios Windows pueden conectarse a unidades de red Linux para compartir archivos con el resto de computadores, Con Samba los usuarios pueden tomar ventaja de algunas de las facilidades para acceder a dichos archivos o impresoras, estas son algunas de las maneras de acceder a los recursos compartidos de Linux desde clientes Windows.

- Usar el explorador de Windows para seleccionar equipos con recursos compartidos a través del nombre de equipo, y mostrarlo con un doble clic.
- Utilizar la función encontrar Equipo del menú inicio para localizar los recursos compartidos.
- Manejar la opción Conectarse a unidad de red del Explorador de Windows para acceder a los recursos compartidos con Samba y mantenerla como una unidad de red cada ves que se inicie sesión en el equipo.

Compartir datos desde clientes Windows funciona de forma similar, los clientes Linux pueden explorar y acceder a recursos compartidos sobre Windows, por ejemplo para conectarse a un recurso compartido de forma oculta como C$ en un equipo que se llame FileCue01, el cliente samba sobre la consola de comandos deberá ingresar: \\\\FileCue01\\c$ -U nombreUsuario donde el nombre de usuario es una cuenta valida de Windows, en caso de ser necesario ingresar un password Samba lo preguntará. Samba utiliza paths UNC (Universal Naming Convention) para hacer referencia a los sitios de red, y debido a que los shells de Linux interpretan al carácter backslash de una forma especial es necesario duplicarlos para hacer referencia a un sitio de red.

Samba es la idea de Andrew Tridgell. El proyecto nació en 1991 mientras Andrew trabajaba con la suite de Digital Equipment Corporation (DEC) llamada Pathworks, creada para conectar ordenadores VAX DEC con los de otras compañías. Sin conocer la trascendencia de lo que estaba haciendo, Andrew creó un programa servidor de archivos para un extraño protocolo que formaba parte de la suite Pathworks. Este protocolo pasó a llamarse más tarde SMB. Unos años más tarde, lo liberó como su servidor SMB particular y lo comenzó a distribuir por Internet bajo el nombre de "SMB Server". Sin embargo, Andrew no pudo mantener ese nombre -este pertenecía a un producto de otra compañía-, así que intentó lo siguiente para buscarle un nuevo nombre desde Unix:

```
$ grep -i '^s.*m.*b' /usr/dict/words
```

Obteniendo como respuesta:

```
salmonberry
samba
sawtimber
scramble
```

De ésta manera nació el nombre de Samba.

6.2 Concepto de Winbind.

Winbind es una ayuda que permite a los usuarios cuya información de autentificación está almacenada en una base de datos de dominio Windows, poder autentificarse en un sistema Unix. El resultado es un entorno unificado de autentificación, en el cual una cuenta de usuario se puede conservar entre un sistema Unix o un controlador de dominio Windows NT/2000/XP. Esto facilita enormemente la administración de cuentas, debido a que los administradores ya no necesitarán mantener los dos sistemas sincronizados, permitiendo a los usuarios cuyas cuentas estén asociadas a un dominio Windows, autentificarse cuando accedan a un recurso compartido por Samba.

Samba realiza la autenticación de usuarios Windows asociado al modulo PAM.
Winbind

Demonios y utilidades:

- winbindd.- Este demonio se utiliza junto con el servicio de nombres para obtener la información de los usuarios y grupos desde un servidor Windows NT y permitir a Samba autorizar a los usuarios dentro de un servidor Windows NT/2000.
- Wbinfo.- Una utilidad utilizada para realizar peticiones al demonio winbind.

6.3 Preparando Linux para la instalación de Samba.

Se debe diferenciar la instalación de un servidor Samba de la instalación de un cliente, en muchas ocasiones un mismo ordenador puede actuar como cliente y servidor Samba, se entenderá por servidor Samba, aquel ordenador que preste servicios (autentificación, compartición de unidades y archivos, etc.), y un cliente será aquel que los utilice (acceso a los recursos compartidos, autentificación, montaje de sistemas de archivos compartidos, etc.).

6.4 Instalando y configurando Samba.

El paquete principal del servidor Samba es "samba", a continuación se muestra la información relativa al mismo:

```
$ /usr/bin/apt-cache show samba
Package: samba
Priority: optional
Section: net
Installed-Size: 5912
Maintainer: Eloy A. Paris <peloy@debian.org>
Architecture: i386
Version: 3.0.4-5
Replaces: samba-common (<= 2.0.5a-2)
Depends: samba-common  (= 3.0.4-5), netbase, logrotate,
```

```
libacl1 (>= 2.2.11-1), libc6 (>= 2.3.2.ds1-4), libcomerr2 (>= 1.33-3),
libcupsys2-gnutls10 (>= 1.1.20final-1), libkrb53 (>= 1.3.2),
libldap2 (>= 2.1.17-1), libpam0g (>= 0.76), libpopt0 (>= 1.7),
debconf (>= 0.5) | debconf-2.0, libpam-runtime (>= 0.76-13.1),
libpam-modules
Suggests: samba-doc
Filename: pool/main/s/samba/samba_3.0.4-5_i386.deb
Size: 2360466
MD5sum: 47bd4f3c91c0c4542c9a1cdb61416516
Description: a LanManager-like file and printer server for Unix
 The Samba software suite is a collection of programs that
 implements the SMB protocol for unix systems, allowing you to serve
 files and printers to Windows, NT, OS/2 and DOS clients. This protocol
 is sometimes also referred to as the LanManager or NetBIOS protocol.
 .
 This package contains all the components necessary to turn your
 Debian GNU/Linux box into a powerful file and printer server.
 .
 Currently, the Samba Debian packages consist of the following:
 .
  samba - LanManager-like file and printer server for Unix.
  samba-common - Samba common files used by both the server and the client.
  smbclient - LanManager-like simple client for Unix.
  swat - Samba Web Administration Tool
  samba-doc - Samba documentation.
  smbfs - Mount and umount commands for the smbfs (kernels 2.2.x and above).
  libpam-smbpass - pluggable authentication module for SMB password database
  libsmbclient - Shared library that allows applications to talk to SMB servers
  libsmbclient-dev - libsmbclient shared libraries
  winbind: Service to resolve user and group information from Windows NT servers
  python2.3-samba: Python bindings that allow access to various aspects of Samba
 .
 It is possible to install a subset of these packages depending on
 your particular needs. For example, to access other SMB servers you
 should only need the smbclient and samba-common packages.
Task: file-server, print-server
```

Una de las dependencias del paquete "samba" es "samba-common"

El paquete "samba" sugiere la instalación de la documentación asociada al mismo. Aun siendo recomendable instalar dicha documentación, será tarea del administrador la elección de su instalación.

Después de instalar el paquete a través de rpm o apt se debe configurar el archivo smb.conf a continuación se muestra una configuración básica del mismo para compartir impresoras y los directorios de los usuarios, solo la sección global cambia cuando se una al Directorio Activo.

```
[global]
   workgroup = MIDOMINIO
   server string = Samba Server
   printcap name = /etc/printcap
   load printers = yes
   cups options = raw
   log level = 1
   log file = /var/log/samba/%m.log
   max log size = 50
   security = ads
   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
   dns proxy = no
   idmap uid = 16777216-33554431
   idmap gid = 10000-33554431
   template shell = /bin/bash
   template homedir = /home/MIDOMINIO/%U
   winbind use default domain = yes
   winbind enum users = yes
   winbind enum groups = yes
   realm = MIDOMINIO.INT
[homes]
   comment = Home Directories
   valid users = %S
   browseable = no
   writable = yes
[printers]
   comment = All Printers
   path = /var/spool/samba
   browseable = no
   guest ok = no
```

```
   writable = no
   printable = yes
[MIDOMINIO]
   comment = Data
   path = /home/MIDOMINIO
   read only = No
```

La opción workgroup es el nombre NETBIOS del dominio Microsoft, La entrada Server string es un comentario para describir al servidor, los niveles para generar entradas en el archivo de log (log level) van desde 0 para no generar nada y 10 para utilizar está opción al máximo.

Para ejecutar una prueba ejecute:

```
$ testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Processing section "[MIDOMINIO]"
Loaded services file OK.
Server role: ROLE_DOMAIN_MEMBER
```

Este comando verifica el archivo smb.conf para determinar si existen errores de sintaxis, cualquier error registrado debe ser corregido para proceder a iniciar el servicio samba.

```
# /etc/init.d/samba start
```

Finalmente, se debe ejecutar el siguiente comando para unir nuestro equipo linux al dominio de Directorio Activo.

```
# net ads join -U Administrador
Administrador's password:
Joined 'SERVER' to realm 'MIDOMINIO.INT.'
```

En el caso que todos los pasos anteriores se realizaron de forma adecuada en la consola Directorio Activo Usuarios y Computadoras de las herramientas administrativas de Windows 2000 Server, dentro de la unidad organizacional Integrada Computadoras deberá aparecer el equipo Linux denominado como server, como se describe en el siguiente gráfico (fig 6.4.1).

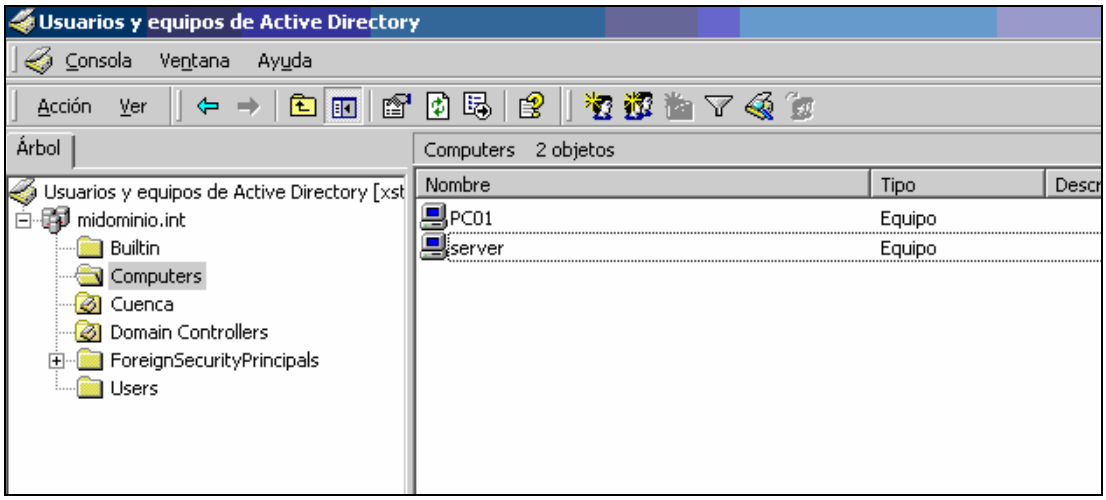

Fig. 6.4.1. Equipo Linux visto desde Microsoft Directorio Activo.

6.5 Configurando Winbind para la integración con Microsoft Directorio Activo.

Para configurar la autenticación sobre Directorio Activo para usuario Linux es necesario editar el archivo de configuración /etc/nsswitch.conf. Las primeras 3 líneas son las más importantes las siguientes líneas variaran de acuerdo a las necesidades del sistema Linux, en este archivo se le indica a Linux donde debe revisar los usuarios cuando hay un requerimiento de autenticación de usuarios.

```
passwd:     files winbind
shadow:     files winbind
group:      files winbind
hosts:      files dnsbootparams: files
ethers:     files
netmasks:   files
networks:   files
protocols:  files winbind
rpc:        files
services:   files winbind
netgroup:   files winbind
```

```
publickey:   files
automount: files winbind
aliases:      files
```

Una ves guardado los cambios se debe iniciar los servicios de Winbind y Samba, como se describe en las siguientes líneas:

```
# /etc/init.d/samba start
# /etc/init.d/winbind start
```

Para verificar el funcionamiento de Winbind utilice los siguientes comandos para mostrar una lista de los usuarios y grupos existentes en el controlador de Dominio:

```
# wbinfo -u
mpino
fpino
__vmware_user__
Administrador
Invitado
TsInternetUser
# wbinfo -g
BUILTIN\System Operators
BUILTIN\Replicators
BUILTIN\Guests
BUILTIN\Power Users
BUILTIN\Print Operators
BUILTIN\Administrators
BUILTIN\Account Operators
```

El siguiente comando verifica que los inicios de sesión y claves se están validando contra el Directorio Activo y no en el equipo local:

```
# getent passwd
administrador:*:16777219:16777225:Administrador:/home/MIDOMINIO/administrador:/bin/ba
sh
```

Finalmente como usuario root ejecute el comando net ads info para Mostar la información del Directorio Activo.

6.6 Demonio Samba.

Hoy en día, la suite Samba gira alrededor de un par de demonios Unix que permiten compartir recursos entre los clientes SMB de una red. Estos demonios son:

- Smbd.- Demonio que permite compartir archivos e impresoras sobre una red SMB y proporciona autentificación y autorización de acceso para clientes SMB.
- nmbd.- Demonio que soporta el servicio de nombres NetBIOS y WINS, que es una implementación de Microsoft del servicio de nombres NetBIOS (NBNS). Este demonio también ayuda añadiendo la posibilidad de navegar por la red.

6.7 Conclusión

La configuración del demonio Winbind y Samba puede resultar una tarea compleja, los errores pueden darse incluso en el mal uso de mayúsculas o minúsculas para determinar el nombre del dominio Microsoft así como también por errores en procesos anteriores como la generación de ticket de seguridad, pero una ves funcional se vuelve una gran herramienta barata y segura al alcance de cualquier empresa o persona.

CAPÍTULO VII

Squid sobre sistemas operativos Linux.

Introducción

Squid es el servidor Proxy más popular y extendido entre los sistemas operativos basados sobre UNIX. Es muy confiable, robusto y versátil. Al ser software libre, además de estar disponible el código fuente, está libre del pago de costosas licencias por uso o con restricción a un uso con determinado número de usuarios.

7.1 Concepto de Squid.

Squid es un Proxy y cache con los protocolos HTTP, FTP, GOPHER y WAIS, Proxy de SSL, cache transparente, WWCP, aceleración HTTP, cache de consultas DNS y más.

Entiéndase por cache almacenar en el disco duro del servidor las páginas más visitadas desde la estaciones de tal manera que se realiza un ahorro significativo del ancho de banda del enlace del centro de acceso cuando se solicita la página nuevamente desde la misma u otra estación.

7.2 Instalando y configurando Squid.

Para la instalación de Squid desde rpm ejecute:

```
# rpm -iv squid-2.3.STABLE4-1.i386.rpm
```

Para instalarlo desde las Fuentes ejecute lo siguiente:

```
# tar zxvf squid-2-3-STABLE3-src.tgz
```

```
# cd squid-2.3.STABLE3
# ./configure
# make
# make install
```

Squid utiliza el fichero de configuración localizado en /etc/squid/squid.conf,. Existen un gran número de parámetros, para su funcionamiento básico se debe configurar los siguientes:

- http_port
- cache_mem
- cache_dir
- Al menos una Lista de Control de Acceso
- Al menos una Regla de Control de Acceso
- cache_mgr
- httpd_accel_host
- httpd_accel_port
- httpd_accel_with_proxy
- Parámetro http_port:

¿Que puerto utilizar para Squid?

Squid por defecto utilizará el puerto 3128 para atender peticiones, sin embargo se puede especificar que lo haga en cualquier otro puerto o bien que lo haga en varios puertos a la vez. En el caso de un Proxy Transparente, regularmente se utilizará el puerto 80 y se valdrá del re-direccionamiento de peticiones de modo tal que no habrá necesidad alguna de modificar la configuración de los navegadores Web para utilizar el servidor Proxy bastará con utilizar como puerta de enlace al servidor. Es importante recordar que los servidores Web, como Apache, también utilizan dicho puerto, por lo que será necesario reconfigurar el servidor Web para utiliza otro puerto disponible, o bien desinstalar o deshabilitar el servidor Web, cabe recalcar que utilizar un Proxy transparente hará que perdamos la característica de autenticación de usuarios para acceso al servicio.

Regularmente algunos programas utilizados comúnmente por los usuarios suelen traer por defecto el puerto 8080 -servicio de cacheo WWW- para utilizarse al configurar que servidor proxy utilizar. Si queremos aprovechar esto en nuestro favor y ahorrarnos el tener que dar explicaciones innecesarias al usuario, podemos especificar que Squid escuche peticiones en dicho puerto también. Siendo así localice la sección de definición de http_port, y especifique:

```
#
#You may specify multiple socket addresses on multiple lines.
#
# Default: http_port 3128
http_port 3128
http_port 8080
```

Parámetro cache_mem

El parámetro cache_mem establece la cantidad ideal de memoria para lo siguiente:

- Objetos en tránsito.
- Objetos Hot.
- Objetos negativamente almacenados en el caché.

Los datos de estos objetos se almacenan en bloques de 4 Kb. El parámetro cache_mem especifica un límite máximo en el tamaño total de bloques acomodados, donde los objetos en tránsito tienen mayor prioridad. Sin embargo los objetos Hot y aquellos negativamente almacenados en el caché podrán utilizar la memoria no utilizada hasta que esta sea requerida. De ser necesario, si un objeto en tránsito es mayor a la cantidad de memoria especificada, Squid excederá lo que sea necesario para satisfacer la petición. Por defecto se establecen 8 MB. Puede especificarse una cantidad mayor si así se considera necesario, dependiendo esto de los hábitos de los usuarios o necesidades establecidas por el administrador.

```
cache_mem 16 MB
```

Parámetro cache_dir:

Este parámetro se utiliza para establecer que tamaño se desea que tenga el cache en el disco duro para Squid. Para entender esto un poco mejor, se debe responder a esta pregunta: ¿Cuanto desea almacenar de Internet en el disco duro? Por defecto Squid utilizará un cache de 100 MB, de modo tal que encontrará la siguiente línea:

```
cache_dir ufs /var/spool/squid 100 16 256
```

Los números 16 y 256 significan que el directorio del cache contendrá 16 subdirectorios con 256 niveles cada uno. No necesidad de modificar estos parámetros.

Es muy importante considerar que si se especifica un determinado tamaño de cache y este excede al espacio real disponible en el disco duro, Squid se bloqueará inevitablemente. Es necesario se cauteloso con el tamaño de cache especificado.

Controles de acceso.

Es necesario establecer Listas de Control de Acceso que definan una red o bien ciertas maquinas en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid.

- Listas de control de acceso.

  Regularmente una lista de control de acceso se establece siguiendo la siguiente sintaxis:

  ```
  acl [nombre de la lista] src [lo que compone a la lista]
  ```

Si uno desea establecer una lista de control de acceso que defina sin mayor trabajo adicional a toda la red local definiendo la IP que corresponde a la red y la máscara de la sub-red. Por ejemplo, si se tienen una red donde las máquinas tienen direcciones IP 192.168.x con máscara de sub-red 255.255.255.0, se puede utilizar lo siguiente:

```
acl REDLOCAL src 192.168.1.0/255.255.255.0
```

- Reglas de Control de Acceso

Estas definen si se permite o no el acceso a Squid. Se aplican a las Listas de Control de Acceso. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador, es decir, a partir de donde se localiza la siguiente leyenda:

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#
```

La sintaxis básica es la siguiente:

```
http_access [deny o allow] [lista de control de acceso]
```

Pueden tambien definirse reglas valiéndose de la expresión !, la cual significa excepción, por ejemplo se puede utilizar lo siguiente:

```
http_access allow REDLOCAL
http_access deny ¡REDLOCAL
```

Parámetro cache_mgr.

Por defecto, si algo ocurre con el Cache, como por ejemplo que muera el procesos, se enviará un mensaje de aviso a la cuenta webmaster del servidor.
Puede especificarse una distinta si acaso se considera conveniente.

```
cache_mgr administrador@midominio.int
```

Cache con aceleración.

Cuando un usuario hace petición hacia un objeto en Internet, este es almacenado en el cache de Squid. Si otro usuario hace petición hacia el mismo objeto, y este no ha sufrido modificación alguna desde que lo accedió el usuario anterior, Squid mostrará el que ya se encuentra en el cache en lugar de volver a descargarlo desde Internet. Esta función permite navegar rápidamente cuando los objetos ya están en el cache de Squid y además optimiza enormemente la utilización del ancho de banda.

En la sección HTTPD-ACCELERATOR OPTIONS deben habilitarse los siguientes parámetros:

```
httpd_accel_host virtual
httpd_accel_port 0
httpd_accel_with_proxy on
```

7.3 Integración con Microsoft Directorio Activo para la validación de usuarios.

Para activar la integración se deben ejecutar las siguientes tareas. Es necesario brindarles los privilegios de lectura a Squid para que le sea factible leer los usuarios de Winbind, está tarea se la realiza de la siguiente forma:

```
root#  chgrp squid /var/cache/samba/winbindd_privileged
root#  chmod 750 /var/cache/samba/winbindd_privileged
```

Se debe configurar correctamente Squid para que pueda interactuar con los componentes de Samba para poder realizar la validación con Directorio Activo. Para realizar esta tarea es necesario modificar los siguientes parámetros en el archivo /etc/squid.conf:

```
[ADMINISTRATIVE PARAMETERS Section]

cache_effective_user squid
cache_effective_group squid

[AUTHENTICATION PARAMETERS Section]

auth_param ntlm program /usr/bin/ntlm_auth / --helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children 5
auth_param ntlm max_challenge_reuses 0
auth_param ntlm max_challenge_lifetime 2 minutes
auth_param basic program /usr/bin/ntlm_auth / --helper-protocol=squid-2.5-basic
auth_param basic children 5
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours
acl AuthorizedUsers proxy_auth REQUIRED
http_access allow all AuthorizedUsers
```

Squid por defecto utiliza el usuario nobody. Se necesita agregar un usuario del sistema y un grupo llamado squid en caso que no se encuentren presentes, normalmente estos se agregaran en las instalaciónes de squid realizadas con rpm. Estos usuarios se agregan en /etc/passwd y /etc/group.

Se debe cambiar los permisos en la carpeta var y log de Squid, para realizar esta tarea ingrese los siguientes comandos:

```
root#  chown -R squid /var/cache/squid
root#  chown -R chown squid:squid /var/log/squid
root#  chmod 770 /var/log/squid
```

Finalmente Squid debe ser capaz de escribir en el cache de disco para realizar esta tarea ejecute:

```
root#  chown -R chown squid:squid /var/cache/squid
root#  chmod 770 /var/cache/squid
```

Para crear el directorio de cache de Squid ejecute:

```
root#  squid –z
```

7.4 Conclusiones.

Squid es fácil de configurar y utilizar no necesita demasiados recursos para su correcto funcionamiento, ofrece varias posibilidades de reportes con la instalación de paquetes adicionales y su forma de manejo de cache aumenta considerablemente la calidad del servicio de Internet para los usuarios de la red de área local, y si todo lo explicado en los capítulos anteriores fue realizado de forma exitosa estaremos asegurando que solo los usuario validados por el Dominio Microsoft puedan acceder a el, evitando así que cualquier intruso pueda utilizarlo.

CAPÍTULO VIII

Aplicación ejemplo sobre redes heterogéneas.

Introducción

Unos de los problemas en la actualidad dentro de las redes de área local es el mantener respaldos de los documentos y correo electrónico de los usuarios, en este capítulo se presentara una solución alternativa utilizando la infraestructura que hemos armado en los capítulos anteriores, manteniendo además la filosofía de que los respaldos son propios de un usuario y no debería permitirse que cualquiera pueda revisarlos.

8.1 Desarrollo

Describamos la infraestructura: Varios usuarios con equipos portátiles y de escritorio con Microsoft Windows 2000 Professional o XP iniciando sesión sobre un servidor de prestaciones medias con Microsoft Windows 2000 Server y teniendo acceso a una carpeta propia del usuario (Fig. 8.1.1) sobre un servidor de prestaciones de hardware bajas con sistema operativo Linux ejecutando Winbind, Samba y Squid para acceso a Internet.

Fig. 8.1.1. Vista de la carpeta compartida sobre el servidor de archivos Linux

Se desarrolla un script sobre visual Basic script que mediante políticas de grupo se establece su ejecución cada ves que un usuario inicia sesión sobre una estación de

trabajo. Este script utilizara el comando ntbackup disponible en los sistemas operativos Microsoft desde la versión 2000, aquí detallaremos la ayuda del archivo transcrita de la ayuda de Windows: “El programa ntbackup o Copia de seguridad le ayuda a proteger los datos de pérdidas accidentales si su sistema tiene un problema de hardware o de medios de almacenamiento. Por ejemplo, puede utilizar Copia de seguridad para crear un duplicado de los datos del disco duro y, a continuación, archivarlos en otros dispositivos de almacenamiento como pueden ser un disco duro, unidad de red o una cinta. Si los datos originales de su disco duro se borran o sobrescriben accidentalmente, o el acceso a ellos es imposible debido a un error de funcionamiento del disco duro, podrá restaurar los datos que estén en la copia archivada.

Puede realizar operaciones de copia de seguridad desde archivos de proceso por lotes utilizando el comando ntbackup seguido de diversos parámetros en la línea de comandos.

Puede realizar operaciones de copia de seguridad en el símbolo del sistema o con un archivo por lotes mediante el comando ntbackup seguido de diversos parámetros.

Sintaxis:

ntbackup backup [systemstate] "nombre del archivo bks " /J {"nombre del trabajo"} [/P {"nombre del grupo"}] [/G {"nombre de guid"}] [/T { "nombre de la cinta"}] [/N {"nombre del medio"}] [/F {"nombre del archivo"}] [/D {"descripción del parámetro"}] [/DS {"nombre del servidor"}] [/IS {"nombre del servidor"}] [/A] [/V:{yes|no}] [/R:{yes|no}] [/L:{f|s|n}] [/M {tipo de copia de seguridad}] [/RS:{yes|no}] [/HC:{on|off}] [/UM] ”

El script forma una línea de comando que contiene información acerca de que se respaldará, donde se respaldara y como se llamara el respaldo, al momento el respaldo se llamara igual que el nombre del usuario que inicio la sesión, nombreusuario.bkf, se almacenara en \\Server\MIDOMINIO\nombreusuario y se respaldara todo el contenido de la variable de sistema %UserProfile% (Fig 8.1.2).

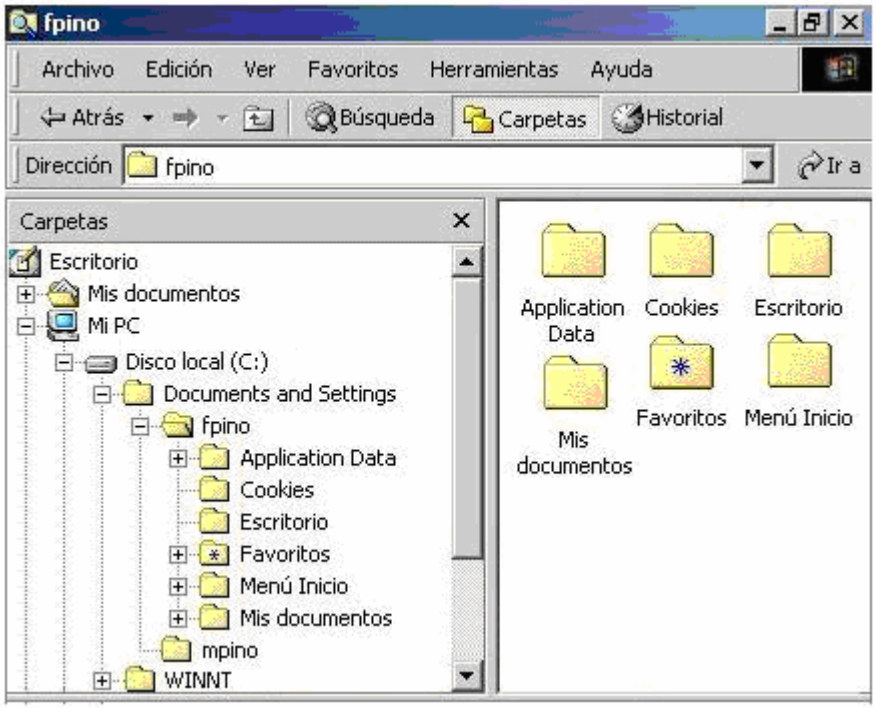

Fig. 8.1.2. Vista de la carpeta de la cual se obtendrá el respaldo.

El código fuente del Script es:

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:" & "{impersonationLevel=impersonate}!\\" &
strComputer & "\root\cimv2")
Set colOperatingSystems = objWMIService.ExecQuery("Select * from
Win32_OperatingSystem")
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set WshShell = WScript.CreateObject("WScript.Shell")
Set WshNetwork = WScript.CreateObject("WScript.Network")
For Each objOperatingSystem in colOperatingSystems
        if objOperatingSystem.Caption = "Microsoft Windows XP Professional" or
objOperatingSystem.Caption = "Microsoft Windows 2000 Professional" then
                lt_UserProfile = WshShell.SpecialFolders("Templates")

                contador = 1
                bandera = 0
                While (bandera <> 3)
                        if (mid(lt_UserProfile,contador,1) = "\") then
                                bandera = bandera + 1
                        end if
```

```
                    contador = contador +1
                wend
                contador = contador - 2
                lt_UserProfile = mid(lt_UserProfile,1,contador)
                Unidad = "\\server\MIDOMINIO\"
                'Proceso de Respaldo
                'Obtencio de Datos
                lt_Cname = "Equipo :     " & WshNetwork.ComputerName
                lt_Uname = "Usuario:     " & WshNetwork.UserName
                lt_Dominio = "Dominio:     " & WshNetwork.UserDomain
                lt_Origen = "Origen :     " & lt_UserProfile
                F = chr(34)
                BackupPath = Unidad & WshNetwork.UserName & "\" &
WshNetwork.UserName & ".bkf"
                lt_Tarea = "ntbackup backup "& F & lt_UserProfile & F & " /j " & F &
"Respaldo de " & WshNetwork.UserName & F & " /f " & F & BackUpPath & F & " /m normal"
                lt_mensaje = "Realizando respaldo total de: "
                WshShell.Exec(lt_tarea)
                'Mensaje final
                lt_destino = "Destino:     " & BackupPath
                WScript.Echo lt_mensaje & Chr(13) & Chr(13) & lt_cname & Chr(13) &
lt_uname & Chr(13) & lt_dominio  & Chr(13) & lt_Origen & Chr(13) & lt_destino & Chr(13) &
Chr(13) & "XStech Corp(r)"
        end if
Next
```

8.2 Proceso de validación de usuarios

El proceso de validación de usuario se realiza de la siguiente forma en este ejemplo (Fig. 8.2.1):

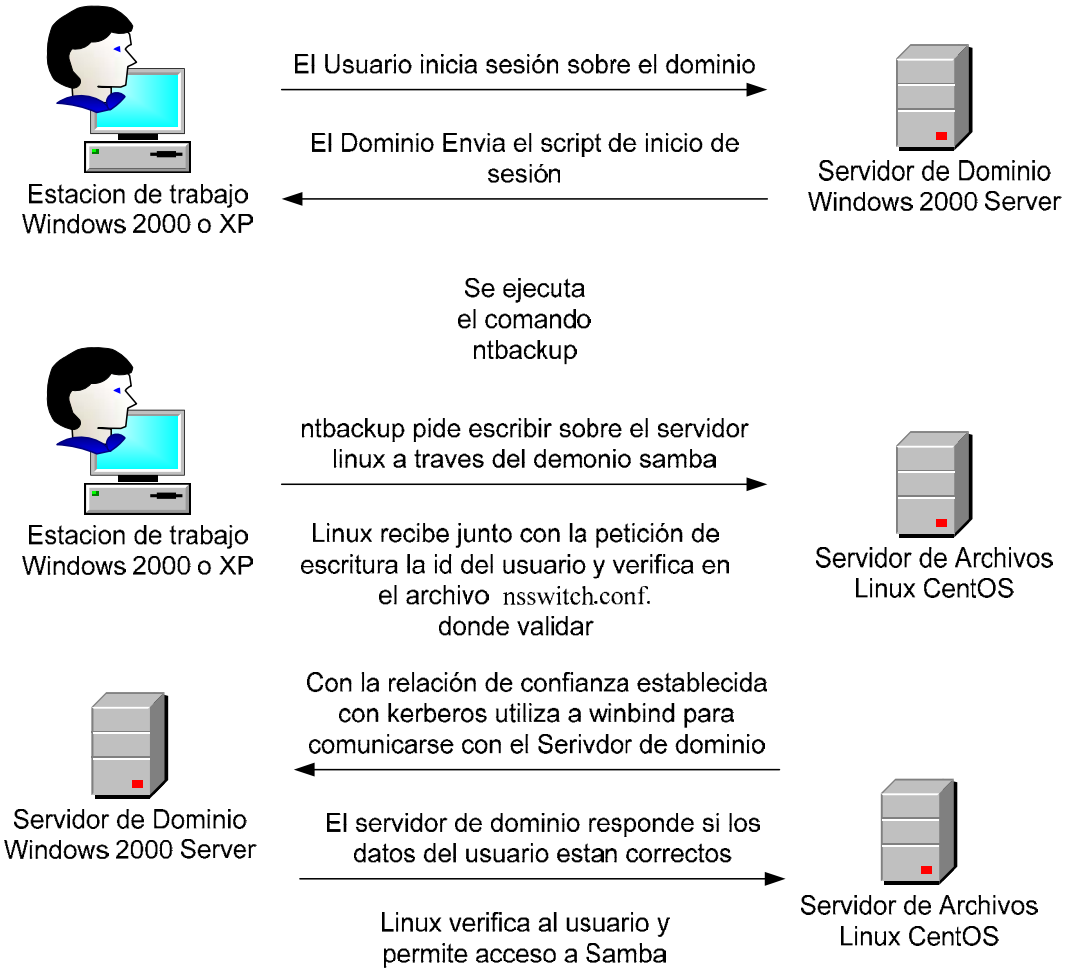

Fig. 8.2.1. Proceso utilizado en el ejemplo.

CAPÍTULO IX

Conclusiones y recomendaciones.

Conclusiones:

- Las redes de computadores son una herramienta indispensable para que una pequeña empresa mejorar su productividad.
- Debido a las: características, funcionalidad, facilidad de uso, instalación y potencial de las políticas de grupo que ofrecen los dominios Microsoft se lo recomienda para cualquier tipo de empresa.
- Al trabajar de forma conjunta Kerberos y Winbind tenemos la posibilidad que cualquier Linux pueda realizar autenticaciones de usuario sobre Microsoft Directorio Activo.
- Es posible abaratar costos teniendo servidores Linux, pero el costo de implementación y mantenimiento de los mismos es alto debido a la poca escasez de personal perito en la materia.
- Tener centralizado el proceso de autenticación de usuarios brinda la posibilidad de brindar más servicios sobre varios Sistemas Operativos, con una única autenticación el usuario puede iniciar sesión en una estación de trabajo con Windows y de forma similar en una con Linux.
- Es posible controlar de mejor forma los accesos a recursos de red al tener un único identificador de usuario sobre toda la red.

Recomendaciones:

Para el desarrollo de esta monografía es muy importante tener en cuenta que los servidores deben estar sincronizados sus relojes, si este punto no se toma en cuenta nunca se podrá conseguir que se establezca una relación de confianza entre ellos.

Cada ves que se realice un cambio en los archivos de configuración realice un respaldo de los mismos, pueden generarse errores difíciles de reparar.

Tenga claro cada uno de los términos utilizados en los archivos de configuraciones pueden ser sumamente importantes en el caso que desconozca uno de ellos investíguelos antes de modificar sus valores.

Se recomienda para el estudiante de la escuela de ingeniería en la universidad ó para el profesional actual la profundización de conocimientos, por la implicación negativa que trae consigo el no estar familiarizado con las tareas de instalación, configuración y otras tareas administrativas que son imprescindibles para el adecuado aprovechamiento o ventajas que brinda los dos sistemas operativos Microsoft Windows server y linux.

Se recomienda además estudio de los sistemas operativos de una manera profunda y adecuada ya que son la base y están íntimamente relacionados con las comunicaciones dentro de todo tipo de red.

Glosario.

AS.- Authentication Service

DACL.- Discretionary Access Control List lista de control de acceso

DC.- Controlador de dominio

DEC.- Digital Equipment Corporation

DNS.- Domain name System

FQDN.- Fully Qualified Domain Names

FTP.- File transfer protocol

IP. - Internet protocol

KDC.- Kerberos Distribution Center

LDAP.- Lightweight Directory Access Protocol

NFS.- Network File System

OSF/DCE.- Distributed Computing Environment

PC.- Personal Computer

PYMES.- Pequeña y mediana empresa

SID.- identificador de seguridad

TGS.- Ticket Granting Service

IT.- Tegnologia de la información

MIT.- Massachussetts Institute of Technology

Bibliografía.

- Sistema operativo GNU - Fundación para el software libre: <http://www.gnu.org/home.es.html>
- Computer Networking: <http://compnetworking.about.com/od/softwareapplicationstools/l/bldef_samba.htm>
- Integración de redes: <http://es.tldp.org/Tutoriales/doc-openldap-samba-cups-python/html/ldap+samba+cups+pykota.html>
- Squid: <http://www.tuxteno.com/contents.php?cid=163> <http://www.siriusit.co.uk/docs/doc.php?pageID=13&typeID=3>
- Join Samba to your Active Directory Domain <http://www.enterprisenetworkingplanet.com/netos/article.php/3487081>
- Samba & Windows 2003 Active Directory <http://lilly.csoft.net/~vdebaere/handleiding/samba-activedirectory/index_en.html>
- Kerberos <http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node296.html>
- Información del directorio activo de Microsoft. <www.microsoft.com/spain/technet/productos/directorioactivo/default.mspx>
- "Microsoft Windows 2000 Active Directory Services – Curso oficial de certificación MCSE", Microsoft Press.