UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Facultad de Estudios Superiores Acatlán

Migración, implementación y estabilización de un dominio bajo la infraestructura tecnológica del servicio de Directorio Activo

TRABAJO PROFESIONAL

Que para obtener el título de:
Licenciado en Matemáticas Aplicadas y Computación

p r e s e n t a :

AMADOR ESPINOZA MARIA LETICIA

Asesor: Ing. Reyes Laurencio García Moncada

México, D.F. Abril 2007

A LA MEMORIA DE MI HERMANA:
NORMA AMADOR ESPINOZA

A MIS PADRES:
DELFINA ESPINOZA ORTEGA
ALFREDO AMADOR ORTIZ
Por lo que representan para mí y por ser parte importante de una hermosa familia.

A MIS AMIGOS:
Por los ratos buenos y malos que compartimos y por los consejos que me otorgaron en los momentos difíciles.

CON ADMIRACIÓN Y RESPETO A MIS MAESTROS Y ASESORES.

A la UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, con gratitud imperecedera.

Mi agradecimiento a todas aquellas personas que directa o indirectamente contribuyeron al logro de una de mis metas...

… Obtener el Título Profesional

Índice:

Introducción

Petróleos Mexicanos (PEMEX) es la empresa más grande de México y una de las 10 compañías petroleras más grandes del mundo, tanto en activos como en ingresos. Cuenta con alrededor de 140 mil empleados para actividades de exploración y producción de hidrocarburos, refinación, gas y petroquímica.

Su tecnología le ha permitido aumentar sus reservas y reconfigurar su plataforma de exportación, vendiendo al exterior crudo de mayor calidad y valor, además de ser autosuficiente en gas natural. Abastece materias primas, productos, servicios y cuenta con una industria petroquímica moderna y en crecimiento.

Debido al tamaño de Petróleos Mexicanos y a la diversidad de usuarios que se comunican y comparten información diariamente, la empresa conformó un grupo de Tecnologías de Información (TI) donde se determinó que todo el esquema de correo electrónico, colaboración y mensajería se tenía que integrar y homologar en una sola plataforma que permitiera comunicar a los usuarios de forma eficiente y transparente, simplificando los procesos administrativos en TI.

Antes de iniciar esta estandarización se contaba con varios productos de correo electrónico, lo que limitaba la posibilidad de una comunicación universal, una integración y flujo de información directo en las labores cotidianas, ocasionando complejidad en la administración de sistemas debido a la diversidad de ambientes.

Luego de diversas pruebas, PEMEX se decidió por las herramientas de comunicación y colaboración de Microsoft, por ser aplicaciones conocidas por los usuarios y la posibilidad de integrar a una empresa de esta magnitud en una sola plataforma.

PEMEX REFINACIÓN inició el proceso de migración de su infraestructura de mensajería y colaboración en el 2003, siendo un proyecto de dos etapas. En la primera etapa se tuvo que estandarizar previamente las plataformas de sistema operativo para que Exchange pudiera interactuar con los datos del servicio de Directorio Activo. Lo que implicó migrar de la plataforma de

Windows Server NT 4 a Windows Server 2003. En la segunda etapa se implantó el servicio de mensajería con Exchange 2003.

Por lo tanto, el objetivo del presente trabajo es: actualizar y estandarizar la plataforma tecnológica de servidores de red basada en la infraestructura de Microsoft Windows Server 2003 integrado con el servicio de Directorio Activo, para ofrecer a los usuarios servicios encaminados a mejorar sus procesos de negocio de manera más segura y confiable. Facilitar la administración integrando toda la plataforma operativa. Acceder a la información de manera segura mediante un servicio de Políticas de Grupo, controlando las reglas de acceso y destino a los datos de los usuarios.

Debido a la complejidad de los dos proyectos, en este trabajo sólo se explicará la parte de migración de Windows Server NT 4 a Windows Server 2003 con la implementación del Servicio de Directorio Activo, definiendo las políticas de los usuarios, su perfil y grupos de trabajo mediante el Servicio de Políticas de Grupo (GPO).

Este proyecto se desarrolló particularmente en una de las Subgerencias de Pemex Refinación, donde me encuentro laborando. Esta área comprende entre sus actividades la parte de administración, monitoreo y soporte a equipos (Windows Server, Unix y Pc´s). Parte importante del trabajo es la administración de cuentas de usuario para acceso al dominio y el servicio de mensajería; además del soporte a usuarios.

El presente trabajo es una recopilación de las actividades que se realizaron al migrar de la plataforma en Windows Server NT 4 a Windows Server 2003. Se encuentra dividido en cuatro capítulos, en el primero se presentan algunos conceptos y términos de uso de las plataformas de Microsoft Windows NT 4.0 y Windows Server 2003.

En el segundo capítulo se explica brevemente la preparación del dominio y la definición de los estándares para los atributos del Directorio Activo; tomando en cuenta la modificación al esquema de atributos que se utilizarán en el proyecto de mensajería.

En el tercer capítulo se explica como se migró de la plataforma Microsoft Windows NT 4.0 a Windows Server 2003. Desde la configuración del

controlador de dominio, hasta la migración de cuentas de usuario, cuentas de equipo, preparación de unidades organizacionales. Así como la introducción de los equipos al nuevo dominio y copia de perfiles de usuarios.

Por último, en el cuarto capítulo se revisa la estabilización del Directorio Activo, verificando puntos de parametrización como: roles de los controladores de dominio, catálogo global, administración de unidades organizaciones y aplicación de políticas de grupo.

Capítulo I. Fundamentos del Servicio de Directorio Activo

En este capítulo se describen algunos conceptos y términos de uso de las plataformas de Microsoft Windows NT 4.0 y Windows Server 2003, para situarnos en el ambiente en el que se desarrollo el presente trabajo.

En el punto uno, se detallan conceptos de la conectividad de redes, como son: tipos de redes, enfoques de conectividad, protocolos de red. En el punto dos, se presenta la introducción a los sistemas operativos, para situar a Windows NT Server y Windows Server 2003, sus principales características y servicios.

1. Generalidades de la conectividad de redes

Una red es un conjunto de computadoras conectadas entre sí para facilitar la comunicación y compartir recursos. Las redes de computadoras tienen reglas básicas que aseguran la entrega confiable de información. Estas se pueden ver de la siguiente forma:

- La información debe entregarse de manera confiable sin ningún daño en los datos.
- La información debe entregarse de manera consistente – la red debe ser capaz de determinar hacia dónde se dirige la información.
- Las computadoras que forman la red deben ser capaces de identificarse entre sí a lo largo de toda la red.
- Debe existir una forma estándar de nombrar e identificar las partes de la red

Si se divide una red en componentes, podríamos dividir en dos partes: una la red física: el cableado, tarjetas de red, servidores, computadoras y demás equipo que utiliza la red para transmitir datos. La otra parte es la disposición lógica de esos componentes o sea las reglas que permiten a los componentes físicos trabajar en conjunto.

La red lógica es lo que los usuarios ven cuando se encuentran trabajando. Las redes lógicas son colecciones de recursos tales como espacio en disco duro, impresoras y aplicaciones a las que su computadora no tendría acceso si no estuviera conectada a una red.

Dentro de los ejemplos de red lógica se incluyen los protocolos de red. Éstos son formas especiales que tienen las computadoras para comunicarse entre sí.

1.1.1 Tipos de redes

Aunque las redes comparten el mismo propósito y concepto general y esencialmente dan los mismos beneficios, la puesta en práctica de las redes puede ser bastante diferente. Las diferentes variedades de redes son:

1.1.1.1 Área Local (LAN)

Una red de área local o *LAN* es la forma menos compleja de las redes de computadoras. Una LAN no es más que un grupo de computadoras enlazadas a través de una red que se encuentra en un solo lugar. Las computadoras conectadas a la red se llaman nodos.

Las LANs tienen las siguientes características:

- Ocupan tan sólo un lugar físico – de aquí la palabra *local* del nombre.
- Pueden ser *redes punto a punto* (o de igual a igual, lo cual significa que no existe una computadora central), o *redes cliente/servidor* (lo que significa que una computadora central, llamada *servidor*, tiene la mayor parte de los recursos de la red y es accesada por los clientes o las computadoras de los usuarios).
- Tienen altas velocidades de transferencia de datos.
- Todos los datos son parte de la red local.

Aunque las LANs son las redes más sencillas, eso no significa que sean necesariamente pequeñas o simples. Las LANs pueden ser grandes y complejas.

1.1.1.2 Área Metropolitana (MAN)

Para el momento en el que una LAN ha crecido a miles de usuarios, es seguro que la red se ha expandido más allá de su ubicación original. Si la expansión es local (es decir, dentro de una región geográfica muy pequeña, como edificios adyacentes), con frecuencia la red se divide en varias redes pequeñas y se enlaza en una MAN (red de área metropolitana), utilizando líneas telefónicas de alta velocidad o hardware especial que permitan la transferencia de datos a toda velocidad de la LAN.

1.1.1.3 Área Amplia (WAN)

Cuando una serie de LANs o MANs se encuentran muy dispersas geográficamente y no es práctico enlazarlas a velocidades de LAN (generalmente separadas por un par de kilómetros), entonces se construye una WAN (red de área amplia). Las WANs son LANs o MANs dispersas geográficamente y conectadas entre sí a través de líneas telefónicas de alta velocidad.

Las WAN casi siempre utilizan ruteadores. Debido a que la mayor parte del tráfico en una WAN se presenta dentro de las LANs y MANs que conforman la WAN, los ruteadores ofrecen una importante función –aseguran que las LANs y MANs obtengan solamente los datos destinados a ellas.

La figura 1.1.1.3 muestra la configuración de una WAN.

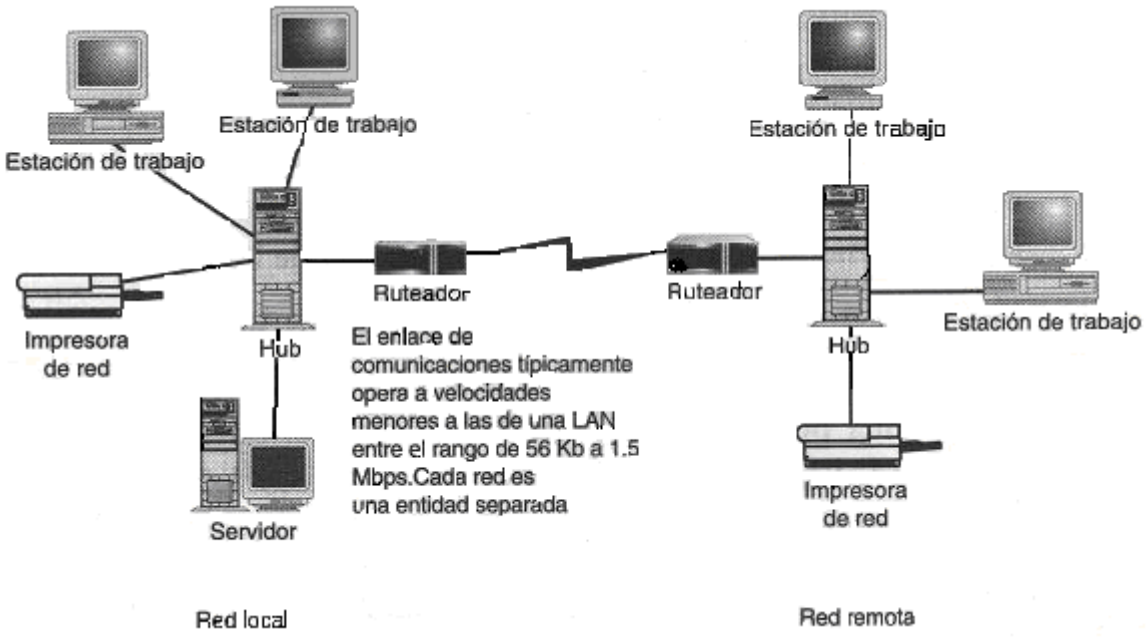


Fig. 1.1.1.3 Configuración de una WAN

1.1.2 Enfoques de conectividad

1.1.2.1 Redes cliente/servidor

Las redes cliente/servidor se usan comúnmente en organizaciones grandes. En este enfoque de la conectividad, la red se compone de uno o más servidores especializados y varios clientes diferentes, como se muestra en la figura 1.1.2.1.

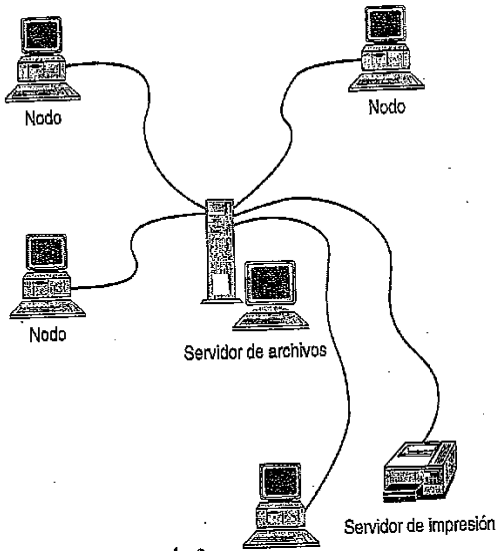


Fig. 1.1.2.1 Red cliente/servidor

Los servidores están diseñados para proporcionar servicios centralizados y los clientes son los diferentes nodos en la red. En un entorno cliente/servidor, las computadoras conectadas a la red se pueden llamar clientes, nodos o estaciones de trabajo.

Diferentes tipos de servidores se pueden usar en una red cliente/servidor. Estos servidores se agregan a la red conforme lo dictan las necesidades de ésta.

Tipos comunes de servidores:

Servidor de archivo. Esta computadora está dedicada a proporcionar almacenamiento y administración centralizados de archivos.
Servidor de impresión. Esta computadora o dispositivo proporciona servicios de impresión centralizados.
Servidor de comunicaciones. Esta computadora está dedicada a proporcionar servicios de módem, fax y correo electrónico.
Servidor de base de datos. Esta computadora está dedicada a ejecutar un programa de base de datos centralizado.

Quizá la mayor desventaja es que si un servidor falla, la red entera falla en relación con ese recurso. Por ejemplo, si un servidor de impresión no está

disponible, no hay forma de imprimir a través de la red hasta que el servicio esté disponible de nuevo. (Puede continuar imprimiendo a través de una impresora local, si hay una disponible.) Debido a que es un asunto crítico mantener en funcionamiento la red, la mayor parte de los entornos que usan un enfoque cliente/servidor confían en una persona exclusiva (o en un departamento entero) para hacer funcionar la red. Esta persona se conoce como administrador de la red. Esta persona debe ser competente en lo relacionado con la conectividad y tener una comprensión de la forma como encajan todas las piezas de la red.

1.1.2.2 Redes punto a punto

En un entorno de conectividad punto a punto no hay servidores centralizados. Esta red resulta idónea para conectar 5 ó 6 nodos. En esta configuración, se usa un dispositivo central de control, denominado hub o switch, para conectar entre sí todas las computadoras. En su lugar, cada nodo en la red proporciona servicios a los que pueden tener acceso otros nodos en la red. Por ejemplo, un nodo puede tener una impresora que pueden usar otros nodos, en tanto que un nodo diferente puede tener archivos de datos a disposición de otros usuarios de la red. Si bien una red punto a punto es una solución sencilla, de bajo costo y fácil de instalar, no es tan eficiente a la hora de buscar, recuperar y almacenar archivos. Una red cliente-servidor es la mejor elección cuando hay que conectar seis o más nodos y se necesita actualizar de forma periódica grandes archivos tales como bases de datos o de información.

La figura 1.1.2.2 muestra un ejemplo de conectividad punto a punto.

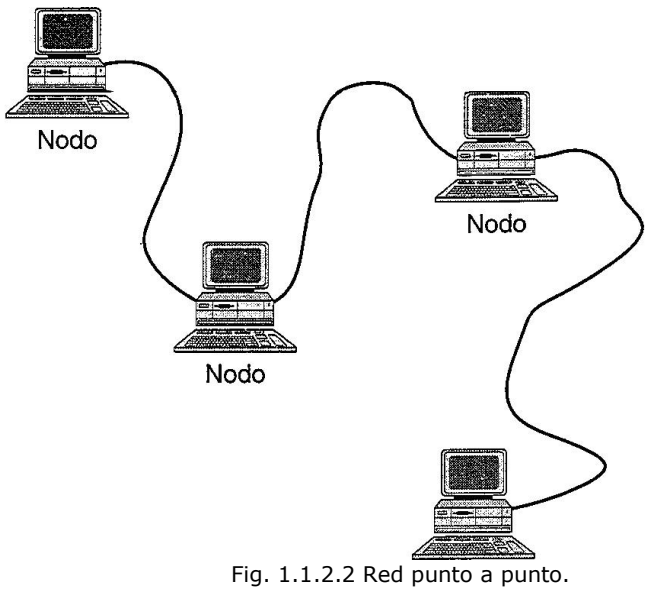


Fig. 1.1.2.2 Red punto a punto.

Como se mencionó, la conectividad punto a punto se usa para redes o grupos de trabajo menores. Por ejemplo: un salón de clase, puede usar este tipo de red. Este enfoque elimina varias de las desventajas del enfoque cliente/servidor. Por ejemplo, si una de las computadoras en la red falla, no se

desactiva la red completa. Por supuesto, los recursos compartidos por ese nodo no están disponibles, pero pueden usarse servicios alternativos por medio de otros nodos en la red. Además, de manera característica no es necesario un administrador de red porque cada persona que usa la red, por lo general mantiene su propia máquina y administra sus propios recursos compartidos.

Ejemplos de redes de punto a punto incluyen Windows 95, Windows para Trabajo en Grupo, LANtastic y 1ONet.

1.1.2.3 Beneficios de la conectividad de redes

La compartición de recursos es más fácil a través de una red; si la red utiliza una configuración punto a punto o cliente/servidor es igual. A continuación se mencionan algunos de estos beneficios:

Espacio compartido en disco

Las computadoras conectadas en red pueden compartir entre sí su espacio de disco duro. A simple vista, esto no parece ser trascendental; después de todo, muchas computadoras tienen discos duros grandes. Sin embargo, no es la capacidad de almacenamiento de archivos lo que es importante en este momento - lo que es importante son las aplicaciones y archivos compartidos.

Aplicaciones compartidas

Aunque la compartición de archivos es una razón importante de la conectividad de redes, la compartición de aplicaciones es otra razón de igual importancia. La compartición de aplicaciones puede ser tan simple como utilizar una copia de Microsoft Word almacenada en otra unidad de usuario o tan compleja como una aplicación groupware que rutea datos de usuario a usuario de acuerdo a un conjunto de reglas preestablecidas.

Impresoras compartidas

Un tercer aspecto de la compartición de recursos son las impresoras compartidas. Como se mencionó anteriormente en el análisis de las desventajas de no tener computadoras en red, las impresoras independientes —es decir, impresoras que se encuentran conectadas a computadoras que no están en red— representan un costo de capital muy significativo. Por lo general, la operación de las impresoras también es muy costosa —consumen tinta o tóner para imprimir y los cartuchos de inyección de tinta y tóner usualmente son muy caros.

Administración centralizada

Una solución para la administración de redes es la de centralizar las funciones de administración. Una vez que las computadoras están en red, existe un gran número de utilerías de software (Systems Management Server de Microsoft,

Saber LAN Manager de McAffe, TME 10 de Tivoli, y Norton Administrator para Redes de Symantec, entre otros) que permiten al administrador de red diagnosticar y reparar problemas, así como instalar y configurar software. Este grupo de utilerías permite al administrador de red reunir y estandarizar configuraciones de computadoras de toda una red —y en el mayor de los casos, instalar software en las computadoras de los usuarios sin tener que abandonar su escritorio.

La instalación inicial y curvas de aprendizaje significan mucho trabajo para el administrador, sin embargo, una vez que se ha terminado la instalación, la vida del administrador de redes es mucho más tranquila. La administración centralizada ahorra tiempo y dinero (dos cosas que los contadores aprecian mucho), así como la conformidad de los usuarios y la credibilidad del administrador (dos cosas que los usuarios y los administradores aprecian). La conectividad de redes justifica totalmente la inversión y el tiempo.

1.1.3 Protocolos de red

Los protocolos son un conjunto de reglas usadas para el envío y recepción de datos a través de una red. Las topologías lógicas le dictan al hardware cómo formar paquetes y transmitir datos a través de la topología física; los protocolos manejan la conversión de datos desde las aplicaciones hasta la topología lógica.

A continuación se presenta una lista de protocolos comunes:

- TCP/IP
- IPX
- NetBIOS/NetBEUI

Para poder entenderlos, se debe entender el modelo OSI, que es el modelo teórico de la conectividad de redes.

1.1.3.1. El modelo OSI

Durante los 1980, un grupo llamado OSI (Interconexión de Sistemas Abiertos), intentó crear una disposición lógica de las diferentes partes que conforman una red. En el largo plazo, sus esfuerzos fueron inútiles (prácticamente nadie opera de acuerdo a los protocolos de OSI), pero crearon un modelo para explicar cómo debe trabajar una red. Al modelo se le llama modelo de las siete capas de OSI, y es la base de la teoría de la conectividad de redes, la fig.1.1.3.1 muestra el modelo OSI.

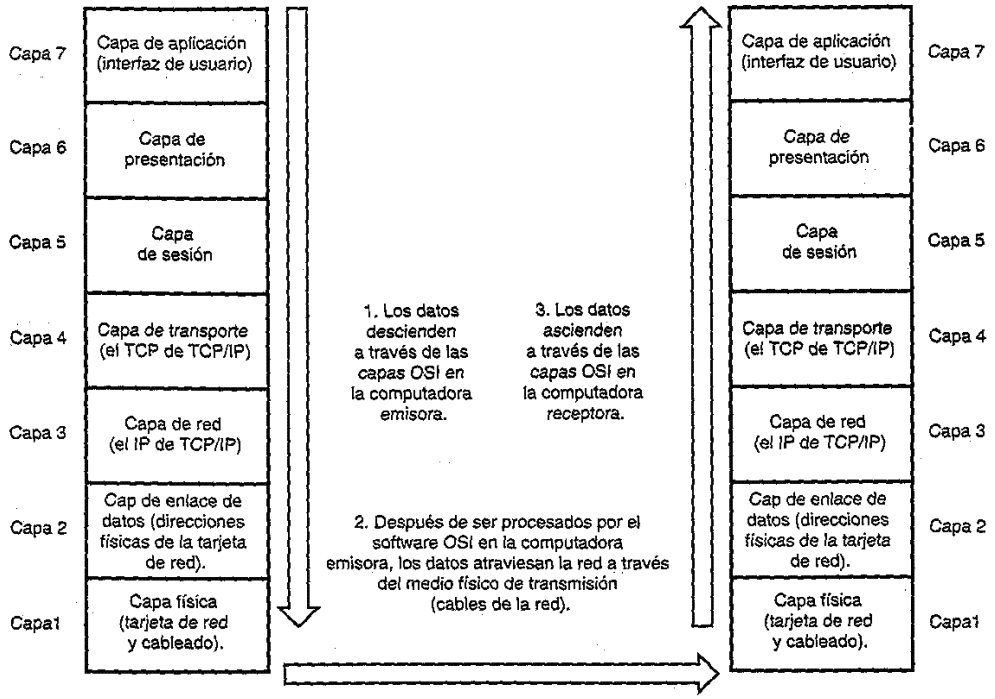


Fig. 1.1.3.1 Modelo OSI

El modelo OSI no es particularmente complicado. El truco consiste en recordar que así como el número de capas OSI aumenta de 1 a 7, el nivel de abstracción también. A medida que la capa está más abajo, es menos abstracta y más concreta. Cada capa se comunica solamente con la capa ubicada directamente arriba o debajo de ella mientras transfiere datos que pueden variar desde impulsos eléctricos en un cable hasta datos en su pantalla. Las siete capas se explican a continuación:

La capa 7 (Aplicación) está conformada por las aplicaciones de software que se utilizan en la pantalla. Tiene que ver con el acceso y transferencia de archivos (aplicaciones FTP o Telnet). Por ejemplo: en el modelo de correo, la capa de aplicación corresponde a la escritura de la carta.

La capa 6 (Presentación) tiene que ver con la forma en que los diferentes sistemas representan los datos. Por ejemplo, la capa 6 define qué pasa cuando trata de desplegar datos en estilo UNIX en una pantalla MS-DOS.

La capa 6 en realidad no tiene una analogía en el modelo del correo, pero si la tuviera sería como reescribir la carta de tal forma que nadie la pudiera leer (lo cual, como usted puede ver, no tiene mucho sentido en un contexto físico). Probablemente, la mejor analogía sería un traductor; utilizando de nuevo el modelo del correo, suponga que su carta está siendo enviada a Estados Unidos. Un traductor (equivalente al software de la capa de presentación) puede traducir al idioma inglés los datos escritos en su sobre. Como en la carta del ejemplo, los datos son alterables y modificables y pueden disponerse de tal forma que se puedan procesar en el tipo de computadora que se requiera.

La capa 5 (Sesión) maneja las conexiones reales entre los sistemas. La capa 5 maneja el ordenamiento de los paquetes de datos y las comunicaciones bidireccionales (de dos vías). En la metáfora del correo, la capa de sesión es similar a la función de fragmentar un solo documento grande en varios documentos pequeños, empaquetarlos y etiquetarlos en el orden en el que deben abrirse.

La capa 4 (Transporte) es como el sistema de correo registrado. La capa 4 se ocupa de asegurar que el correo llegue a su destino. Si un paquete no llega a su destino, la capa 4 se encarga de manejar el proceso de notificación al emisor y solicita el envío de otro paquete. En efecto, la capa 4 asegura que las tres capas debajo de ella (es decir, las capas 1, 2 y 3) estén haciendo sus tareas de una manera eficiente. Si no es así, el software de la capa 4 entra en acción y lleva a cabo la función de corrección de errores. Vale la pena mencionar que aquí es donde hace su trabajo la parte TCP de TCP/IP.

La capa 3 (Red) proporciona un esquema de direccionamiento. Si envía una carta a alguien, tiene que utilizar una dirección que contenga un código postal, ya que es lo que la oficina postal entiende. Cuando una computadora envía un paquete de datos, ésta manda el paquete a una dirección lógica, la cual es como la dirección de una calle.

La capa 3 trabaja en conjunto con la capa 2 para traducir las direcciones de red lógicas de los paquetes de datos (éstas son similares a las direcciones IP, sobre las cuales aprenderá más adelante) a direcciones MAC basadas en hardware (las cuales son similares a los códigos postales) y para transferir los paquetes hacia su destino. La capa 3 es similar a los empleados que ordenan el correo en la oficina postal, quienes no se preocupan por asegurarse que el correo llegue a su destino, por decirlo así. En lugar de eso, la función de estos empleados es clasificar el correo de tal forma que se mantenga lo más cerca posible de su destino. La capa 3 es también la capa más baja. Cuya función no tiene nada que ver con el hardware. La capa 3 es donde entra en juego la parte IP de TCP/IP.

La capa 2 (Enlace de datos), en contraste, no es física. Es un conjunto de reglas acerca de cómo se recibe y entrega el correo. Está involucrada en el proceso de buscar una forma para que los componentes de la capa 1 (las tarjetas, hubs, cable, etcétera) se comuniquen con la capa 3. La capa 2 es donde las direcciones de las tarjetas de red son importantes.

La capa 1 (Física) es similar a los camiones, trenes, aviones y a cualquier cosa que mueve el correo. Desde la perspectiva de una red, esta capa solamente tiene que ver con los aspectos físicos de la red —las tarjetas, cables y concentradores a través de los que viajan los paquetes de información. La capa 1 especifica cuáles son los aspectos físicos, qué deben ser capaces de hacer y (básicamente) cómo llevan a cabo estas funciones.

Si los paquetes de datos se transfieren a través de la red, ésta tiene que llevar a cabo varias tareas de manera exitosa:

Tiene que ser capaz de transmitir datos a través de un medio físico (alambre de cobre, fibra óptica, o —en el caso de las redes inalámbricas— el aire).

- Debe rutear datos al lugar correcto.
- Debe ser capaz de reconocer los datos cuando lleguen a su destino.
- Debe ser capaz de verificar que los datos transmitidos estén correctos.
- Debe ser capaz de interactuar con los usuarios a través de una interfaz que despliegue los datos.

Las diferentes capas del modelo OSI cumplen con estos objetivos de manera frecuente. Sin embargo, el modelo OSI en realidad nunca fue implementado como un protocolo de red; en lugar de eso, los protocolos existentes —principalmente TCP/IP— fueron refinados utilizando el modelo de referencia OSI.

1.1.3.2. TCP/IP

El Protocolo de Control de Transmisión/Protocolo Internet. TCP/IP es el protocolo que transporta el tráfico de datos a través de Internet. La razón por la que TCP/IP gano popularidad es que se trata de un estándar abierto, es decir, que no está controlado por ninguna compañía. En lugar de eso, TCP/IP es parte de un conjunto de estándares creados por un cuerpo llamado IETF (Fuerza de Trabajo de la Ingeniería de Internet). Los estándares IETF son creados por comités y presentados a la comunidad de conectividad de redes a través de un conjunto de documentos llamados RFCs (solicitudes de comentarios).

Las RFCs son documentos en borrador que se encuentran disponibles en Internet y que explican un estándar a la comunidad de la conectividad de redes. Todas las RFCs se consideran documentos en "borrador", ya que cualquier documento puede ser superado por una RFC más reciente. La razón del énfasis en las RFCs, es que forman una gran parte de los fundamentos de los diferentes estándares que conforman la conectividad de Internet actualmente, incluyendo el TCP/IP.

TCP/IP es solamente la notación abreviada de todo un grupo de protocolos que tienen formas estándares de interactuar. TCP e IP comparten el nombre de todo el grupo de protocolos, ya que constituyen los cimientos; son, respectivamente, la capa de transporte (capa 4 de OSI que regula el tráfico) y la capa de red (capa 3 de OSI, que maneja el direccionamiento) del grupo de protocolos TCP/IP. El grupo incluye las formas para transmitir datos a través de redes. En la tabla 1.1.3.2 se describe la función de algunos protocolos.

Tabla 1.1.3.2 Protocolos de red

Nombre	Función
TCP	Protocolo de Control de Transmisión. Asegura que las conexiones se lleven a cabo y se conserven entre computadoras.
IP	Protocolo Internet. Maneja las direcciones del software de la computadora.
ARP	Protocolo de Resolución de direcciones. Compara las direcciones IP con las direcciones (MAC) de hardware.
RIP	Protocolo de información de ruteo. Busca la ruta más rápida entre dos computadoras.
OSPF	Abrir primero la vía más corta. Es un protocolo derivado de RIP que aumenta la velocidad y confiabilidad
ICMP	Protocolo Internet de Mensajes de Control. Maneja los errores y envía mensajes de error de TCP/IP.
SNMP	Protocolo Simple de Administración de Red. Permite que los administradores de red se conecten y administren los dispositivos de red.
PPP	Protocolo punto a Punto. Proporciona conexiones de acceso telefónico hacia redes.
SMTP	Protocolo Simple de Transporte de correo. Maneja la transferencia del correo electrónico entre servidores en una red TCP/IP.
POP3/IMAP4	Versión 3 del Protocolo de Oficina Postal/Versión 4 del Protocolo de Acceso a mensajes de Internet. Ambos establecen formas para que los clientes se conecten a los servidores y colecten correo electrónico.

1.1.3.3 Direcciones IP

TCP/IP tuvo sus comienzos como parte del sistema operativo UNIX a mediados de 1970. Los administradores de redes, quienes previamente habían dependido de UUCP (Programa de Copiado de UNIX a UNIX) para el copiado de archivos y correo entre computadoras, decidieron que debía surgir una mejor y más interactiva forma de transmitir por red, y así nació TCP/IP. Dada la herencia académica de mostrar el material enfrente de la comunidad académica para su revisión crítica y análisis, un paso natural era incluir TCP/IP en el proceso de RFC, donde sus estándares habían sido establecidos desde siempre.

La especificación original de TCP/IP era abierta—o así lo pensaron sus diseñadores. Ellos crearon un espacio de direcciones o una manera estándar de escribir direcciones, la cual establecía 2 a la 32ava potencia de direcciones (es decir: 4,294,967,296 direcciones diferentes), el solo pensar que cuatro mil millones de computadoras pudieran existir, era un poco exagerado.

La razón por la cual las direcciones IP se han agotado tan rápido se debe al diseño del esquema de direccionamiento. Todas las direcciones IP se escriben en notación decimal punteada, con un byte (ocho bits) entre cada punto. Una dirección IP decimal punteada tiene el siguiente formato: 192.168.100.25

Debido a que cada número está descrito por un byte, ya que cada byte tiene 8 bits (1s y0s binarios), cada número puede tener un valor cualquiera entre 0 y 225. Ya que existen 4 números con 8 bits cada uno, se dice que el espacio total de direcciones tiene una longitud de 32 bits (4x8=32).

Las direcciones IP se asignan a organizaciones que las solicitan en lo que se llaman bloques de direcciones. Los bloques de direcciones tienen tres tamaños, basándose en la clase de dirección. El método actual de asignar direcciones IP es ineficiente dada la forma en la que ha crecido internet.

Direcciones clase A

Las direcciones clase A, tienen hasta 16,777,216 direcciones. Utilizan 24 de 32 bits en el espacio de direcciones, leídos de izquierda a derecha. Una dirección clase A tiene el siguiente formato:

x.0.0.0

El número representado por la x es un número cuyo valor debe estar entre 0 y 126. Cuando está escrito en formato binario, el primer bit (el bit que está ubicado más a la izquierda) de la dirección Clase A siempre es 0. Un ejemplo de una dirección IP Clase A es 124.95.44.15. El primer byte, 124, identifica el número de red. Los administradores de la red asignan los valores restantes. Todos los números representados por los 0s pueden variar desde 0 hasta 255.

número red	número equipo	número equipo	número equipo

Direcciones clase B

El siguiente incremento, la clase B, tiene un total de 65,536 direcciones IP por red. Una dirección clase B tiene el siguiente formato:

x.x.0.0

Todas las direcciones clase B comienzan con un 10 binario. Las direcciones clase B componen el 25% del espacio de direcciones IP disponibles. Esto significa que las direcciones clase B hacen un total de 1,073,741,824 de las 4,294,967,296 direcciones IP disponibles.

Los números representados por las x´s son números fijos que varían desde 0 hasta 255. Debido a que los dos números punteados situados más a la derecha se utilizan para crear direcciones IP únicas y debido a que la mitad de 32 es 16, una red clase B tiene un espacio de direcciones de 16 bits.

Un ejemplo de una dirección IP Clase B es 151.10.13.28. Los dos primeros bytes identifican el número de red. Los otros dos bytes son para numerar los equipos de la red. Una manera fácil de reconocer si un dispositivo forma parte de una red Clase B es verificar el primer byte de su dirección IP. Las direcciones IP Clase B siempre tienen valores que van del 128 al 191 en su primer byte.

Direcciones clase C

El incremento más pequeño de direcciones IP disponibles para una organización es clase C. En una red clase C, solamente se puede utilizar el número decimal punteado más a la derecha para formar un total de 256 direcciones IP.

Todas las direcciones clase C comienzan con un 110 binario. Las direcciones clase B forman el 12.5% del espacio de direcciones IP disponible. Esto significa que las direcciones clase B hacen un total de 536,870,912 de las 4,294,967,296 direcciones IP disponibles.

A continuación se muestra un ejemplo de una dirección clase C:

x.x.x.0

Como en los ejemplos de las clases A y B, los números que representan las x´s son números fijos que varían desde 0 hasta 255; el número representado por el 0 puede variar entre 0 y 255.

Un ejemplo de dirección IP Clase C es 201.110.213.28. Los tres primeros bytes identifican el número de red. Una manera fácil de reconocer si un dispositivo

forma parte de una red Clase C es verificar el primer byte de su dirección IP. Las direcciones IP Clase C siempre tienen valores que van del 192 al 223 en su primer byte.

Otras clases de redes

Además de las clases A, B y C, existen otras dos clases de redes:

- Clase D. La dirección más a la izquierda siempre comienza con el 1110 binario, como se muestra en la figura 1.1.3.3.a. Una dirección multidifusión es una dirección exclusiva de red que dirige los paquetes con esa dirección destino hacia grupos predefinidos de direcciones IP. Por lo tanto, una sola estación puede transmitir de forma simultánea una sola corriente de datos a múltiples receptores.

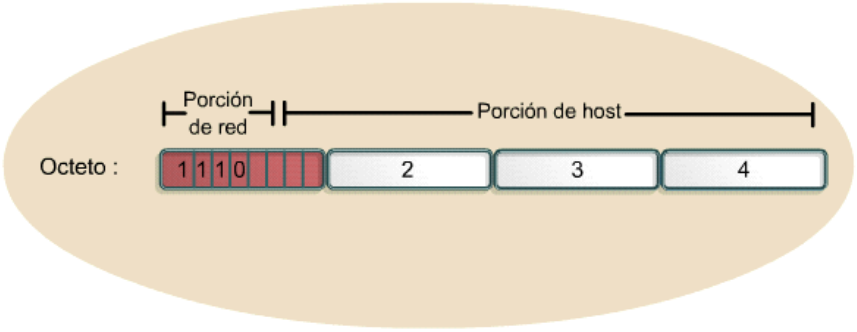


Fig. 1.1.3.3.a Red Clase D

- Clase E. La dirección más a la izquierda siempre comienza con el 1111 binario, como se muestra en la figura 1.1.3.3.b.. Las direcciones clase E están reservadas para propósitos de experimentación. Sin embargo, la Fuerza de tareas de ingeniería de Internet (IETF) ha reservado estas direcciones para su propia investigación. Por lo tanto, no se han emitido direcciones Clase E para ser utilizadas en Internet. Los primeros cuatro bits de una dirección Clase E siempre son 1s. Por lo tanto, el rango del primer octeto para las direcciones Clase E es 11110000 a 11111111, o 240 a 255.

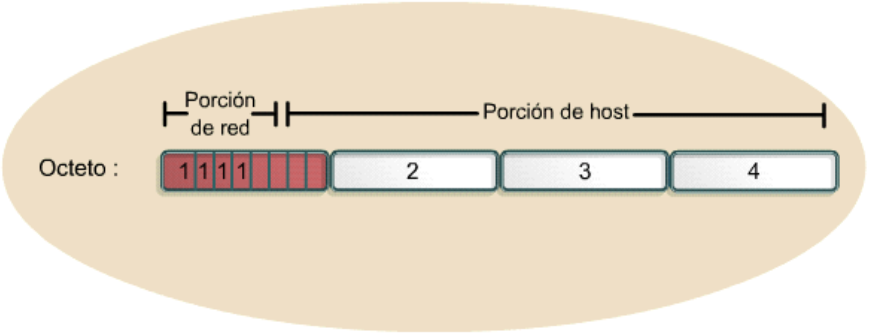


Fig. 1.1.3.3.b Red Clase E

1.2 Sistemas operativos

Un sistema operativo es un conjunto especial de programas de computación que permite que los usuarios y las aplicaciones interactúen con el hardware de la computadora, permitiendo el procesamiento de información en segundo plano y administrando la salida de información hacia el monitor, la impresora u otro dispositivo de salida.

La mayor parte de los sistemas operativos para PC están diseñados para trabajar en un entorno aislado o en redes de punto a punto pequeñas. Un sistema operativo de red (NOS Network Operating System), como Windows NT Server, es responsable no sólo de la administración del servidor, sino también de la administración de las computadoras de esa red.

El sistema operativo es responsable de rastrear que usuarios están conectados a la red y a cuáles recursos se les permite el acceso.

Funciones de los Sistemas Operativos

- Interpreta los comandos que permiten al usuario comunicarse con el ordenador
- Coordina y manipula el hardware de la computadora, como la memoria, las impresoras, las unidades de disco, el teclado o el mouse
- Organiza los archivos en diversos dispositivos de almacenamiento, como discos flexibles, discos duros, discos compactos o cintas magnéticas
- Gestiona los errores de hardware y la pérdida de datos
- Servir de base para la creación del software logrando que equipos de marcas distintas funcionen de manera análoga, salvando las diferencias existentes entre ambos

A continuación se describen los antecedentes de Windows NT Server, así como las características principales.

1.2.1 Historia de Windows

Las primeras computadoras personales fueron introducidas a mediados de la década de 1970. Habiéndose introducido la primera versión del producto en 1985. Desde ese momento, Windows ha desarrollado un gran árbol genealógico que incluye varios sistemas operativos. Es importante señalar que Windows comenzó como un shell gráfico para DOS. La tabla 1.2 muestra las fechas de aparición de diferentes versiones de Windows.

Tabla 1.2 Historia de Windows

Versión	Fecha de aparición
Windows 1.01	**11/85**
Windows 1.03	**8/86**
Windows 1.04	**4/87**
Windows 2.03	**11/87**
Windows 2.1	**5/88**
Windows 2.11	**3/89**
Windows 3.0	**5/90**
Windows 3.1	**4/92**
Windows para Trabajo en Grupo 3.1	**10/92**
Windows NT 3.1	**7/93**
Windows para Trabajo en Grupo 3.11	**11/93**
Windows 3.11	**12/93**
Windows NT 3.5	**10/94**
Windows 95	**8/95**
Windows NT 3.51	**9/95**
Windows NT 4.0	**9/96**
Windows 98	**6/98**
Windows 2000	**2/2000**
Windows Millenium	**6/2000**
Windows XP	**10/2001**
Windows Server 2003	**3/2003**

1.2.2 Windows NT 4.0 Server

Microsoft planeó desarrollar en conjunto con IBM el OS/2 y, de hecho, llevaron a cabo esfuerzos conjuntos hasta la versión 1.03. Sin embargo, a principios de los años 1990, los planes de Microsoft cambiaron y se retiró del modelo OS/2 para crear un sistema operativo para servidores y estaciones de trabajo de clase empresarial que no solamente se ejecutará en computadoras compatibles con Intel. El nombre que Microsoft dio a este sistema operativo fue Windows NT (que se supone significa Windows New Technology).

Windows NT se creó para ofrecer básicamente dos funciones; la primera, que fuera un sistema operativo de clase empresarial para servidores, lo cual significaba que las empresas pudieran ejecutar sus sistemas en él y, a la vez, estar seguros de que trabajaría bien para ellos. Su otra función era servir como sistema operativo para estaciones de trabajo.

La versión inicial de Windows NT salió con varios nombres. El primero fue simplemente ese: Windows NT. Un poco más tarde el producto se renombró como Windows NT 3.1, lo cual puso el número de versión del producto más o menos en sincronía con el producto Windows común, el cual estaba en su versión 3.1. Desde un punto de vista de mercado esto tenía sentido, sobre todo porque la interfaz de usuario tanto en Windows NT como en Windows 3.1 era la misma.

Poco después de salir Windows NT, Microsoft puso a la venta una versión mejorada del producto, la cual fue diseñada para usarse de manera explícita como un servidor. Ésta se llamó Windows NT Advanced Server. Esta disparidad entre los nombres de los productos (Windows NT 3.1 y Windows NT Advanced Server) fue simplificada más adelante cuando los nombres de los productos se volvieron Workstation y Server. Por tanto, siempre que salía una nueva versión, el número de la versión se aplicaba a Windows NT Workstation y a Windows NT Server.

Fue un sistema operativo diseñado para usarlo en servidores de red de área local (LAN). Ofrecía potencia, la manejabilidad y la capacidad de ampliación de Windows NT en una plataforma de servidor e incluía características, como la administración centralizada de la seguridad y tolerancia a fallos avanzada.

Puesto que incorpora funciones de red, las redes de Windows NT Server se integran de forma óptima con el sistema operativo básico, facilitando el uso y la administración de las funciones.

Windows NT Server requiere del uso de al menos un servidor de archivos en la red. Este servidor de archivos ejecuta Windows NT Server como el sistema operativo de red. Los clientes o nodos conectados a la red pueden ejecutar otro tipo de sistemas operativos, como Windows NT Workstation, Windows 95, Windows XP. El único requisito es que los clientes puedan comunicarse con Windows NT Server usando los protocolos que soporta.

A continuación se presentan algunas de las características de Windows NT Server:

- Hardware compartido (ejemplo: impresoras, CD-ROM, unidades de disco)
- Espacio de disco compartido
- Datos compartidos
- Aplicaciones compartidas
- Impresoras en red
- CD-ROM compartidos

1.2.3.1 Descripción general de Windows NT 4.0 Server

Windows NT Server 4.0 proporcionó muchas ventajas sobre versiones anteriores de servidor. A continuación, se abordan algunas de las características más sobresalientes y enfocadas hacia la administración:

- **Administración centralizada de la red**

  Desde el punto de vista de un administrador, una de las características principales de Windows NT Server es que permite la administración centralizada de las cuentas de los usuarios y de problemas relacionados con la seguridad. Esto significa que un administrador puede controlar la configuración y soporte de varios sistemas, desde una ubicación central.

  Windows NT permite establecer *dominios*, los cuales son agrupamientos lógicos de recursos de red. Por tanto, podría tener un dominio que contenga varias redes relacionadas, conectadas con puentes, o puede decidir que su dominio corresponda con su red física. Windows NT le permite administrar el dominio en su conjunto, en lugar de requerir que administre servidores individuales dentro del dominio. El resultado es que se puede establecer la información de usuario una vez y estará disponible para todos los servidores en el dominio.

- **Tolerancia a fallas**

  La tolerancia a fallas es una característica de muchos sistemas operativos; significa tan sólo que el sistema operativo detecta fallas (errores) y los corrige tanto como es posible. Sin embargo, el grado al que un sistema operativo pone en práctica la tolerancia a fallas puede variar. Windows NT ofrece varias características que ayudan a evitar los efectos de los errores del sistema, los cuales son:

  1. **Servicio de directorio**

  Windows NT le permite organizar su red en dominios que pueden administrarse como un conjunto. La raíz de esta característica de diseño se llama Servicio de Directorio de Windows NT. Este servicio se conserva en un servidor llamado controlador principal de dominio (PDC Primary Domain Controller); el cual es una base de datos: de usuarios, grupos e información de recursos para el dominio. También le permite designar controladores de respaldo de dominio (BDC Backup Domain Controller), los cuales son servidores adicionales dentro del dominio.

  El uso de controladores de dominio primario y de respaldo, significa que la tarea de autentificar a los usuarios en una red muy usada no crea un cuello de botella en un servidor. Asimismo, si el PDC no está disponible por alguna razón, puede promover el BDC a la categoría de PDC.

2. Espejeo de disco

El espejeo de disco es una tecnología usada en sistemas seguros o con datos críticos. Cuando se pone en práctica se usan particiones en dos unidades separadas para almacenar información idéntica. La información que se graba en la partición del disco primario también se graba en la partición reflejada en el otro disco, como se muestra en la figura 1.2.3.1. Si un disco falla, el sistema puede usar los datos del otro disco. Windows NT Server soporta el espejeo de disco como una manera de poner en práctica la tolerancia a las fallas. Por tanto, el espejeo de disco es transparente para todos los programas y usuarios en un dominio.

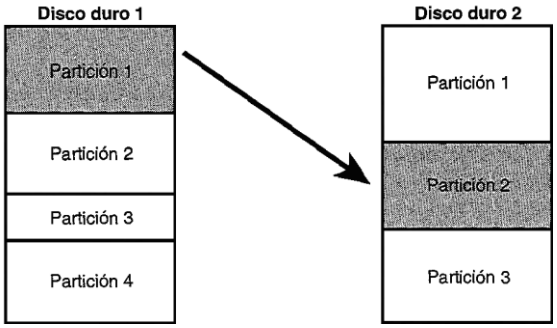


Fig. 1.2.3.1 Espejeo de disco

- **Seguridad**

Windows NT Server 4 es un sistema operativo seguro, lo cual es esencial para usarlo en operaciones críticas o sensibles. Usando las características de seguridad puede lograr cualquiera de lo siguiente:

- Limitar el acceso al dominio a usuarios específicos
- Limitar el acceso al dominio durante ciertas horas
- Limitar el acceso, por usuario ó por grupo, a recursos de red como archivos, directorios e impresoras
- Limitar qué tipo de control tienen los usuarios sobre archivos y directorios

Windows NT Server se evaluó con un nivel de seguridad C2 por el NCSC (National Computer - Security Center; Centro Nacional de Seguridad en Computadoras) de la NSA (National Security Agency; Agencia Nacional de Seguridad), lo cual indica que cumplía con los siguientes criterios particulares, entre otros:

- **Identificación y autentificación**. Cada usuario del sistema debe identificarse de manera única antes de que se le conceda acceso al sistema.

- **Control de acceso discrecional**. El propietario de un recurso de red tiene la capacidad de controlar el acceso al recurso.
- **Reutilización de objetos**. El sistema operativo protege los datos almacenados en memoria de la intrusión por procesos externos. Esto no sólo significa que la memoria usada por un proceso activo está protegida de otros procesos que se están ejecutando en la misma máquina, sino que también, después de que un proceso se ha realizado con la memoria y que ésta se ha regresado a la reserva de memoria disponible, ningún otro proceso puede leer el contenido de esa memoria. Además, la información usada por otros componentes del sistema (disco, monitor, teclado, ratón, etcétera) toda puede protegerse de la misma manera.
- **Auditoría**. El sistema operativo proporciona un medio para auditar las actividades en el sistema, al igual que sucesos relacionados con la seguridad.

- **Administración de las estaciones de trabajo de los usuarios**

Los perfiles de usuario de Windows NT Server le permiten proporcionar mayor facilidad de uso a los usuarios y al mismo tiempo restringir sus actividades en las estaciones de trabajo. Si desea utilizar perfiles para aumentar la productividad de los usuarios, puede guardar en los servidores un perfil con la configuración y las preferencias de los usuarios, tales como las conexiones de red, los grupos de programas e incluso los colores de la pantalla. Este perfil se utilizará cada vez que el usuario inicie una sesión en cualquier computadora con Windows NT, de forma que el entorno definido por el usuario le siga de una estación de trabajo a otra. Si desea utilizar los perfiles de usuario para limitar las actividades de los usuarios, deberá agregar restricciones al perfil, como por ejemplo, impedir que el usuario cambie los grupos y los elementos de programas que usted haya definido, o inhabilitar parte de la interfaz de Windows NT cuando el usuario haya iniciado una sesión.

- **Funcionamiento de la seguridad en la red**

Windows NT Server incorpora diversos métodos de seguridad. Estos métodos proporcionan numerosas formas de controlar la actividad de los usuarios, sin impedirles por ello el acceso a los recursos que necesitan. El fundamento de la seguridad de Windows NT es que todos los recursos y acciones están protegidos por el control de acceso discrecional, que significa que es posible permitir a determinados usuarios acceder a un recurso o realizar una determinada acción, y al mismo tiempo impedírselo a otros usuarios. Además, la seguridad es muy granular

Con Windows NT Server, la seguridad está integrada en el sistema operativo desde el principio, en lugar de incorporarse al mismo como un

componente adicional. Esto significa que los archivos y otros recursos pueden protegerse incluso de los usuarios que trabajan en la misma computadora donde se encuentre el recurso, así como de los usuarios que accedan al recurso a través de la red. Windows NT Server incorpora medidas de seguridad incluso para las funciones básicas del sistema, como el propio reloj de la computadora.

Windows NT Server ofrece asimismo un modelo lógico de administración que permite administrar de un modo eficaz una red de gran tamaño. Cada usuario sólo necesita disponer de una única cuenta, que se almacena de modo centralizado. Esta única cuenta puede proporcionar al usuario el acceso a cualquier recurso de la red, independientemente del lugar donde se encuentre.

Protocolos que soporta:

- NetBEUI
- TCP/IP
- IPX/SPX
- Banyan
- DECnet
- Apple Talk
- Ventajas de NDIS

- **Dominios y relaciones de confianza**

La administración de una red local bajo Windows NT se basa en los dominios y relaciones de confianza.

La unidad básica de la administración centralizada y la seguridad en Windows NT Server es el dominio. Un dominio es un grupo de servidores que ejecutan Windows NT Server y que, en cierto modo, funcionan como un único sistema. Todos los servidores con Windows NT Server de un dominio utilizan el mismo conjunto de cuentas de usuario, por lo que sólo es necesario escribir una vez la información de una cuenta de usuario para que todos los servidores del dominio reconozcan dicha cuenta.

Dentro de los servidores de un dominio existen dos jerarquías: el servidor PDC *(Primary Domain Controller*) y los servidores BDC (*Backup Domain Controller*). Por cada dominio existe sólo un PDC, y varios BDC.

Cuando el administrador del dominio da de alta un nuevo usuario, lo hace sobre el PDC. Los datos de los usuarios se guardan en una base de datos llamada SAM. El PDC se encarga de copiar esa base de datos de usuarios a todos los BDC´s de su dominio de manera periódica (se denomina *replicación)*. Con sólo dar de alta un usuario en el PDC, ese usuario automáticamente puede acceder a cualquier servidor del dominio, usando el mismo nombre de usuario y contraseña.

Los dominios de una red se relacionan mediante el concepto de *Trust o Relación de Confianza*. Se dice que un dominio A confía en otro B, o que hay establecida una relación de confianza desde A hacia B, cuando cualquier usuario autorizado en el dominio B puede entrar sin más en el dominio A. Esta relación de confianza son vínculos entre dominios, que permiten realizar una autenticación transparente, en virtud de la cual un usuario sólo poseerá una cuenta de usuario en un dominio pero podrá acceder a toda la red.

Un *grupo local* es un grupo de usuarios, de manera que cualquier usuario del grupo puede entrar y acceder a los recursos del servidor PDC del dominio al que pertenece el grupo. Un grupo local se define como perteneciente a un dominio.

Un *grupo global* es igual que el anterior excepto en que puede ser visto también por todos los dominios que confían en el dominio al que pertenece el grupo. La diferencia entre local y global es, pues, el ámbito de visibilidad. Si A confía en B, y definimos en B un grupo global, entonces ese grupo también se puede utilizar en A.

Dominios: unidades administrativas básicas

La agrupación de computadoras en dominios proporciona dos grandes ventajas a los usuarios y administradores de la red. Lo que es más importante, los servidores de un dominio constituyen una unidad administrativa única que comparte la información de seguridad y de cuentas de usuario. Cada dominio posee una base de datos que contiene las cuentas de los usuarios y grupos, y las configuraciones del plan de seguridad. Todos los servidores del dominio que funcionen como controlador principal de dominio o como controlador de reserva mantendrán una copia de esta base de datos.

La segunda ventaja de los dominios es la comodidad que brindan al usuario: cuando un usuario examine la red para buscar recursos disponibles, observará que está agrupada en dominios, en lugar de ver los servidores e impresoras de toda la red al mismo tiempo.

Relaciones de confianza: vínculos entre dominios

Estableciendo relaciones de confianza entre los dominios de la red, se permitirá que determinadas cuentas de usuario y grupos globales puedan utilizarse en dominios distintos de aquél en el que estén situadas dichas cuentas. Ello facilita en gran medida la administración, ya que cada cuenta de usuario tiene que crearse una sola vez para toda la red. Además, ofrece la posibilidad de acceder a cualquier computadora de la red y no únicamente a las computadoras de uno de los dominios.

Cuando se establezca una relación de confianza entre dominios, uno de los dominios (el dominio que confía) confiará en el otro (el dominio en el cual se confía). A partir de entonces, el dominio que confía reconocerá a todos los

usuarios y cuentas de grupo globales del dominio en el cual se confía. Estas cuentas podrán utilizarse como se desee dentro del dominio que confía; podrán iniciar sesiones en estaciones de trabajo situadas en el dominio que confía, integrarse en grupos locales dentro de dicho dominio, y recibir permisos y derechos dentro de ese dominio.

Las relaciones de confianza pueden ser unidireccionales o bidireccionales. Una relación de confianza bidireccional es simplemente un par de relaciones unidireccionales, en virtud del cual cada dominio confía en el otro.

El requisito mínimo de un dominio es un servidor con Windows NT Server, que actúa como controlador principal de dominio y que almacena la copia principal de la base de datos de grupos y usuarios del dominio. Si se desea, un dominio puede incluir también otros servidores adicionales que actúen como controladores de reserva.

Controlador principal de dominio (PDC Primary Domain Controller)

El controlador principal de dominio de un dominio de Windows NT Server debe ser un servidor que ejecute Windows NT Server. Cualquier modificación a la base de datos de grupos y usuarios del dominio deberá realizarse en la base de datos que está almacenada en el controlador principal de dominio. El Administrador de usuarios para dominios no permite modificar directamente la base de datos de usuarios de un servidor de dominio que no sea el controlador principal de dominio.

Controladores de reserva (BDC Backup Domain Controller)

Los controladores de reserva que ejecuten Windows NT Server almacenarán también copias de la base de datos de cuentas del dominio. La base de datos de cuentas del dominio estará duplicada en todos los controladores de reserva del dominio.

Todos los controladores de reserva, además del controlador principal de dominio, podrán procesar las peticiones de inicio de sesión por parte de las cuentas de usuario del dominio. Cuando el dominio reciba una petición de inicio de sesión, el controlador principal de dominio o cualquier controlador de reserva podrán autentificar el intento de inicio de sesión. Es conveniente que en un dominio haya uno o varios controladores de reserva, además del controlador principal de dominio. Estos servidores adicionales proporcionan un mecanismo de seguridad: si el controlador principal de dominio no está disponible, un controlador de reserva podrá ser promovido al puesto de controlador principal de dominio, lo cual permitirá al dominio seguir funcionando. La existencia de varios controladores de dominio permite también distribuir la carga de trabajo relacionada con las peticiones de inicio de sesión, lo cual resulta especialmente útil en dominios con un gran número de cuentas de usuario.

Si en un dominio hay varios servidores que ejecutan Windows NT Server, uno de ellos será el controlador principal de dominio. Debe configurar al menos otro servidor como controlador de reserva. Si el dominio tiene servidores situados en distintas ubicaciones físicas conectadas mediante un vínculo de red de área amplia (WAN), cada ubicación deberá tener al menos un controlador de reserva.

Servidores

Además de los controladores principales y de reserva de dominio, existe otro tipo de servidor que ejecuta Windows NT Server. Se trata de servidores designados simplemente como "servidores", no como controladores de dominio. Estos servidores pueden participar en un dominio, si bien no es necesario. Un servidor que participa en un dominio no consigue realmente una copia de la base de datos de usuarios del dominio, pero tiene acceso a todas las ventajas de la base de datos de usuarios y grupos del dominio.

Un servidor que no participa en ningún dominio sólo tiene su propia base de datos de usuarios y procesa por su cuenta las peticiones de inicio de sesión. No comparte la información sobre cuentas con ninguna otra computadora y no puede utilizar cuentas de ningún otro dominio.

Si es posible que el servidor se mueva a otro dominio en el futuro. Es más sencillo mover un servidor de un dominio a otro que mover un controlador de reserva de un dominio a otro.

1.2.3 Windows Server 2003 Enterprise Edition

Desde el punto de vista de Microsoft, Windows es una "familia de productos". Estos sistemas operativos se ejecutarían en diferentes plataformas de hardware, pero compartirían los mismos fundamentos básicos:

- Elementos comunes del sistema operativo
- Interfaz de usuario común
- Plataforma de programación común

Tipos de Productos

La familia de Windows Server 2003 incluye los productos, como se indica en la tabla 1.2.3.

Tabla 1.2.3 Familia de Windows Server 2003

Producto	Descripción
Windows Server 2003, Standard Edition	• Para pequeñas empresas y usos departamentales. • Uso compartido de archivos e impresoras • Conectividad segura a Internet • La implementación centralizada de aplicaciones de escritorio.
Windows Server 2003, Enterprise Edition	• Para empresas de todo tipo, que manejen File Servers, Print Servers, Mensajería, Inventarios.
Windows Server 2003, Datacenter Edition	• Para aplicaciones empresariales críticas, que demandan altos niveles de escalabilidad y disponibilidad.
Windows Server 2003, Web Edition	• Ha sido creado para proporcionar funciones de servidor y alojamiento de Web (páginas Web y servicios Web XML) • Se utiliza principalmente como servidor Web de IIS 6.0.

Para los fines de entender el presente trabajo, se detalla el funcionamiento de los componentes lógicos en la administración del ambiente Windows Server 2003 Enterprise Edition, que es la plataforma usada en Pemex.

A continuación se abordarán los siguientes temas: el servicio de directorio (Directory Service), los diferentes componentes en la estructura del directorio activo (Active Directory) y los diferentes tipos de servidores.

1.2.3.1 Descripción general. Servicio de directorio

El directorio activo es el servicio de directorios de Windows Server 2003. Almacena información acerca de objetos de red, como: usuarios, computadoras y recursos de red. Facilita la búsqueda y utilización de esa información a los usuarios, administradores o aplicaciones, proporcionando una organización lógica y jerárquica de la información de los directorios.

Provee las siguientes funciones:

1. Control centralizado de los recursos de la red
2. Administración centralizada y descentralizada de los recursos
3. Almacenamiento de objetos en una estructura lógica
4. Optimiza el tráfico de la red

1.2.3.2 Estructura lógica del directorio activo

El directorio activo consta de objetos que representan usuarios y recursos como: computadoras e impresoras. Algunos de estos objetos pueden contener otros objetos como es el caso de las unidades organizacionales. En la figura 1.2.3.2, se representan gráficamente los componentes lógicos del directorio activo.

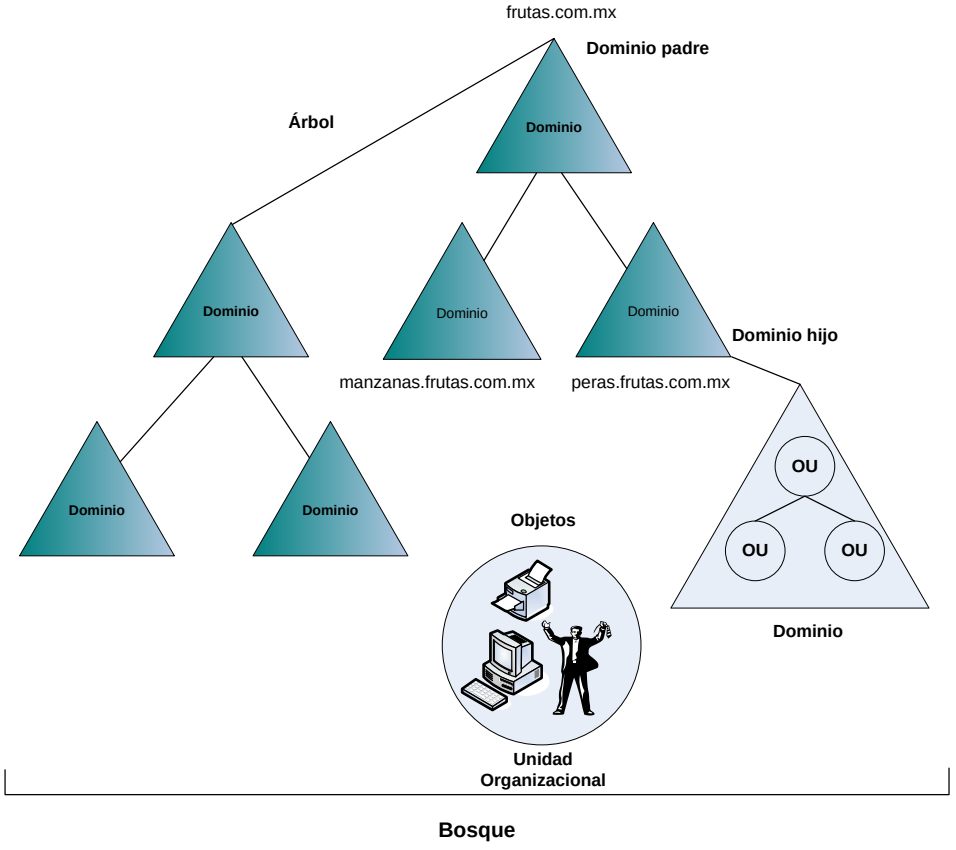


Fig. 1.2.3.2 Estructura lógica del directorio activo

A continuación se describen cada uno de estos componentes:

Objetos

Este es el componente básico del directorio activo. Estos son representados por usuarios y recursos como computadoras e impresoras. Cada objeto en el AD es único y está definido por la combinación única de sus valores de atributos. Las clases de objetos son platillas, para los tipos de objetos que son creados. Por ejemplo: cada objeto que representa a un usuario específico, está basado en una clase de objeto, como se muestra en la tabla 1.2.3.2.

Tabla 1.2.3.2 Clase de objetos

CLASE DE OBJETO	ATRIBUTO
Usuario	Nombre
	Apellido
	Departamento
	Fecha de expiración de la cuenta

Estas clases de objeto se encuentran definidas en el *schema partition* del Directorio Activo.

Usuario

Las cuentas de usuario de dominio se crean en un contenedor, que puede ser un dominio o una unidad organizacional. Cada objeto de usuario dispone de propiedades que contiene valores de configuración personal, de inicio de sesión y de acceso remoto.

Grupos

Al igual que en Windows NT, los grupos de usuarios simplifican en gran medida la administración de los usuarios. Se ofrecen dos tipos de grupos:

1. De distribución
2. De seguridad

La única función de los grupos de distribución es organizar a miembros en un grupo, para enviarles mensajes desde las aplicaciones de correo electrónico. Por ejemplo, si el grupo de distribución CI correo contiene 50 usuarios, y se desea enviarles un mensaje a cada uno de los miembros, en lugar de elegir enviar el mensaje usuario por usuario, sólo se elije el grupo CI correo.

Los grupos de seguridad se utilizan para conceder o denegar el acceso y los permisos a grupos de usuarios, en lugar de hacerlo a usuarios individuales.

El ámbito de un grupo determina las personas que pueden pertenecer a él y dónde se pueden utilizar estos grupos en la red.

Ambos tipos de grupo pueden tener ámbito local, global o universal El ámbito de un grupo también determina los objetos de éste para los que se puede conceder permisos. Las reglas de pertenencia a los grupos de cada ámbito dependen de si el dominio se ejecuta en modo mixto o nativo.

Los grupos locales del dominio pueden contener usuarios y grupos globales de cualquier dominio en modo mixto. Y los globales sólo pueden contener usuarios de su propio dominio. Los grupos universales no están disponibles en el modo mixto.

En el modo nativo, los grupos locales del dominio pueden contener usuarios, grupos globales o grupos universales de cualquier dominio del bosque. Los grupos locales del dominio también pueden contener grupos locales del mismo dominio. Y los grupos globales pueden contener usuarios y grupos globales de su propio dominio. Los grupos universales sólo están disponibles en modo nativo y pueden contente usuarios, grupos globales y otros universales de cualquier dominio del bosque.

Unidad organizacional (OU)

Una unidad organizacional es un tipo de contenedor que se usa para organizar objetos dentro de un dominio. Por ejemplo: se pueden organizar objetos basados en áreas geográficas, en áreas de negocios o en una clase simple, como usuarios, computadoras e impresoras. Una OU, hace más sencillo localizar y administrar objetos. Puede contener objetos como: cuentas de usuario, cuentas de computadora, grupos, impresoras u otras unidades organizacionales anidadas.

Dominio (Domain)

El *Dominio* es el centro del directorio activo. Es una colección de objetos organizados administrativamente, los cuales comparten en común una base de datos, políticas de seguridad y relaciones de confianza con otros dominios. Un dominio tiene un único nombre, y provee el acceso a cuentas de usuario o grupos de cuentas.

Tiene tres funciones:

- Marca el límite administrativo de objetos
- Administra la seguridad de los recursos compartidos.
- Sirve como unidad de replicación de los objetos.

Los objetos de cada dominio son almacenados en la domain partition de la base del Directorio activo (se explica en el punto 1.2.3.3 Estructura física del Directorio Activo. Particiones del directorio activo.)

Las computadoras llamadas *DC a*lmacenan copias o réplicas del domain partition. Estas réplicas se actualizan automáticamente cuando se efectúa un cambio en la información.

Árbol (Domain Tree)

Los dominios están agrupados en estructuras jerárquicas llamadas árboles del dominio. Cuando se añade un segundo dominio al Árbol, este es llamado hijo del dominio raíz*.*

El dominio al cual es unido el *dominio hijo* es llamado *dominio padre*. El nombre del *dominio hijo* es combinado con el nombre del *dominio padre* para formar un nombre único llamado *Domain Name System (DNS)*. De esta manera un árbol tiene un espacio de nombres contiguo. Como se muestra en la figura 1.2.3.2 Estructura lógica del directorio activo.

Bosque (Forest)

Un *bosque* es la instancia más completa. Consiste de uno o más árboles. El primer dominio en el bosque es llamado dominio raíz del bosque*.* El nombre del dominio se refiere al bosque, como *frutas.com.mx.* Por default, la información del directorio activo es compartida dentro del bosque.

1.2.3.3 Estructura física del directorio activo

La estructura física optimiza el tráfico de la red. Define cuando y donde replican la información de la estructura lógica del directorio activo. Consta de sitios físicos de la red (normalmente organizado por ubicación geográfica) y de subredes.

Los elementos de la estructura física del directorio activo son:

Controladores de Dominio (Domain Controller DC)

Los controladores de dominio son las computadoras donde corre el directorio activo en Windows Server 2003. Cada DC replica los elementos lógicos de un dominio o sea las unidades de replicación. Un DC sólo soporta un dominio.

Para asegurar la disponibilidad continua del directorio activo, cada dominio debe contar con más de un DC.

Particiones del directorio activo

Cada DC contiene varias particiones del directorio activo:

- **Domain partition.** Contiene la réplica de todos los objetos del dominio. Estos objetos son replicados sólo a otros DC del mismo dominio.
- **Configuration partition.** Contiene la topología del bosque. Esto es: el registro de todos los DC y las conexiones entre ellos dentro del bosque.
- **Schema partition.** Contiene el esquema del bosque. Cada bosque contiene un esquema que es la definición de las clases de objetos.
- **Application partition.** Contiene objetos que están relacionados con la seguridad y que son usados por una o más aplicaciones. Está partición es replicada a DC específicos del Bosque.

Sitios (Sites)

Un sitio es un conjunto de subredes conectadas entre sí. Después de que los sitios son establecidos, los DC se comunican entre sí frecuentemente. Esta comunicación minimiza la latencia dentro del sitio.

Latencia es el tiempo requerido para que los cambios hechos en un DC sean replicados a otros DC.

Se usan para: optimizar el uso del ancho de banda entre DC separados físicamente. Son usados para controlar cuando y donde replican los DC y donde ocurre el tráfico de logeo.

Los sitios del directorio activo no están relacionados con su espacio de nombres, que está formado por dominios, y los objetos de red no se identifican por el sitio en que se encuentran. O sea que la estructura lógica no debe de coincidir necesariamente con la estructura física.

Un sitio físico puede contener varios dominios, pero un dominio lógico también puede incluir diversos sitios físicos de todo el mundo.

Los sitios constan de una o más subredes del protocolo de internet (IP), conectadas por vínculos rápidos. La velocidad del vínculo viene determinada por el tamaño de la red y por la cantidad de tráfico que ésta procesa.

El administrador asigna subredes a un sitio de Directorio Activo cuando se crea el sitio. La asignación de sitio del DC se establece al crear el Directorio Activo, y permanece igual mientras el administrador no la cambie.

De la ubicación de los controladores de dominio, depende directamente la eficacia de:

- La autenticación del inicio de sesión
- Las consultas de directorio
- Las peticiones de servicios
- El flujo del tráfico de replicación

La replicación es el proceso por el que un controlador de dominio transfiere todos los cambios que se han realizado en él a las bases de datos de los demás controladores de dominio de la red.

Al agregar un controlador de dominio nuevo a un sitio. El directorio activo crea una ruta para la replicación de directorios utilizando el comprobador de coherencia de réplica (KCC).

KCC es un proceso que se realiza en todos los controladores de dominio para crear y modificar la topología de replicación del directorio activo a intervalos establecidos. Ajusta automáticamente la red ante posibles fallos y reconfigura continuamente la topología de replicación para garantizar que este proceso se realice correctamente.

Operaciones maestras (Operations masters)

Cuando se realiza un cambio en el dominio, este cambio es replicado a todos los DC del dominio. Esta replicación es llamada *multimaster replication.*

El directorio activo usa una replicación simple *(single master replicación)* para cambios importantes, como la adición de un nuevo dominio o un cambio hecho al esquema del bosque.

Las operaciones que usa el *single master replication* están dispuestas siempre en un rol específico en el forest o dominio. Estos roles son llamados *operations master roles*. Para cada rol de operación, sólo el DC que tiene ese rol puede asociar y realizar los cambios hechos al directorio. El DC que es responsable de un rol particular es llamado *operations master* para ese rol. El Directorio activo almacena la información acerca de cual DC tiene un rol especifico.

El Directorio Activo tiene definido cinco *Operations Master roles*, cada una de las cuales tiene una localización por default. Roles para el Forest o para el dominio.

Roles definidos para un bosque:

- **Rol de esquema.** Controla todas las actualizaciones al esquema. El esquema contiene la lista de clases de objetos y sus atributos que son usados para crear todos los objetos del AD, como: usuarios, computadoras e impresoras.
- **Rol de Domain Naming**. Controla la adición o remoción de un dominio en el bosque. Cuando se agrega un nuevo dominio al bosque, sólo el DC que tiene este rol puede agregar el nuevo dominio.

Sólo existe un solo servidor con el rol de esquema y dominio de nombres en todo el bosque.

Roles para el Dominio:

- **Emulador del controlador primario de dominio (Primary domain controller emulator PDC).** El PDC es el primer DC que se crea en el nuevo dominio.
- **Maestro de identificador relativo (Relative identifier master RID).** Cuando un nuevo objeto es creado, el DC crea un identificador principal de seguridad (SID), el cual es único para ese objeto en el dominio y un identificador relativo (RID), el cual es único para ese dominio.
- **Maestro de infraestructura (Infraestructure master)**. Cuando los objetos son movidos de un dominio a otro, este rol actualiza las referencias del objeto.

Cada dominio en el bosque tiene su propio PDC, RID y maestro de infraestructura, definidos en un servidor o en varios.

Catálogo Global (Global Catalog GC)

El catálogo global es un repositorio de información el cual contiene información limitada (réplica parcial) de todos y cada uno de los objetos del directorio activo. Una de sus características principales es que realiza búsquedas de recursos entre los dominios y el bosque de manera transparente para el usuario.

El catálogo global contiene:

- Los atributos que son frecuentemente usados en búsquedas. Como: el apellido paterno de un usuario, el apellido materno o el nombre de usuario (logon name).
- La información necesaria para determinar la localización de un objeto en el directorio.
- Un subgrupo de atributos para cada tipo de objeto.
- Los permisos de acceso para cada objeto y sus atributos son almacenados en el catálogo global. Si usted busca un objeto y no tiene los permisos apropiados para verlo, el objeto no aparecerá en los resultados de la búsqueda. Los permisos de acceso aseguran que el usuario pueda buscar sólo objetos para los cuales tiene asignado el acceso.

Un servidor que funciona como catálogo global, es un DC que realiza los procesos de búsqueda del GC. El primer DC que se crea en el AD automáticamente es el catálogo global. Se pueden configurar catálogos globales adicionales para balancear el tráfico de autentificación de logeo y búsquedas.

Funcionalidad de dominios y bosques

La funcionalidad de los dominios y los bosques, introducida en el directorio activo de Windows Server 2003. Tiene a su disposición distintos niveles de funcionalidad de dominios y funcionalidad de bosques según los entornos que se configuren en la totalidad de los servidores del bosque. A continuación se detallan los niveles funcionales, tomando como referencia los niveles funcionales definidos en la tabla 1.2.3.3.

Si todos los controladores del dominio o bosque tiene instalado el sistema operativo Windows Server 2003 y el nivel funcional se establece en Windows Server 2003, se tendrá a disposición todas las funciones completas para los dominios y el bosque.

En cambio, cuando un dominio o bosque con controladores de dominio que ejecutan Windows Server 2003 incluye controladores de dominio de Windows NT 4.0 o Windows 2000, las funciones del directorio activo estarán definidas en un nivel funcional Windows 2000 mixto.

El concepto de habilitar funcionalidades adicionales en el directorio activo es posible en Windows 2000 tanto en modos nativos como mixtos. Los dominios de modo mixto pueden incluir controladores de reserva del dominio de Windows NT 4.0 pero no pueden utilizar grupos de seguridad universales, anidamiento de grupos ni funcionalidad de historial de Id. de seguridad (SID).

Cuando el dominio se establece en modo nativo sí están disponibles los grupos de seguridad universales, el anidamiento de grupos y las capacidades de

historial de SID. Los controladores de dominio que ejecutan Windows 2000 Server no admiten la funcionalidad de dominios y bosques.

Existen tres niveles funcionales de dominio: Windows 2000 mixto (predeterminado), Windows 2000 nativo, Windows Server 2003. De forma predeterminada, los dominios operan al nivel funcional de Windows 2000 mixto.

La tabla 1.2.3.3 incluye los niveles funcionales de dominios y los controladores de dominio compatibles correspondientes.

Tabla 1.2.3.3 Niveles funcionales del dominio

Nivel funcional del dominio	Controladores de dominio compatibles
Windows 2000 mixto (predeterminado)	Windows NT 4.0 Windows 2000 Familia Windows Server 2003
Windows 2000 nativo	Windows 2000 Familia Windows Server 2003
Windows Server 2003	Familia Windows Server 2003

Tras aumentar el nivel funcional del dominio, no podrán incluirse en dicho dominio controladores de dominio que ejecuten sistemas operativos anteriores. Por ejemplo, si aumenta el nivel funcional del dominio a Windows Server 2003, no podrán agregarse a dicho dominio los controladores de dominio que ejecuten Windows 2000 Server.

Tipos de servidores en Windows Server 2003

Servidor miembro

Los equipos que funcionan como servidores en un dominio tienen una de las dos funciones siguientes: **controlador de dominio o servidor miembro.**

Un **servidor miembro** es un equipo que:

- Ejecuta Windows 2000 o 2003 Server
- Es miembro de un dominio
- No es un controlador de dominio

Dado que no es un controlador de dominio, un servidor miembro no se ocupa de los procesos de inicio de sesión de cuentas, no participa en la replicación del

directorio activo ni almacena información de las directivas de seguridad del dominio.

Los servidores miembro operan normalmente como uno de los siguientes tipos de servidores:

- Servidores de archivos
- Servidores de aplicaciones
- Servidores de bases de datos
- Servidores Web
- Servidores de certificados
- Servidores de seguridad
- Servidores de acceso remoto

Estos servidores miembro comparten un conjunto de características relacionadas con la seguridad:

- Los servidores miembro adoptan la configuración de directiva de grupo definida para el sitio, dominio o unidad organizativa.
- Los recursos disponibles en un servidor miembro se configuran para el control de acceso.
- Los usuarios del servidor miembro disponen de los derechos de usuario que se les hayan asignado.
- Los servidores miembro contienen una base de datos local de cuentas de seguridad, el administrador de cuentas de seguridad (SAM, Security Account Manager).

DNS

Los sistemas de resolución de nombres permiten localizar servicios y recursos de red, sus principales características son:

- El DNS se utiliza como servicio primario de resolución de nombres
- Los dominios Windows 2000 y 2003 se asocian directamente a dominios DNS
- Los servidores que sostienen la infraestructura del Directorio Activo son identificados por registros de tipo SRV

Conceptos básicos, que se manejan en un DNS:

- ❖ Registro. Correspondencia en una base de datos entre un nombre y un nombre, o entre un nombre y una dirección I.P.; entre una dirección I.P. y me devuelve un nombre, etc.
- ❖ Nodo. Suma de todos los registros para una misma máquina.
- ❖ Zonas. Suma de todos los registros que comparten cierta parte de su nombre (por ejemplo: todos los registros que terminen en .com pertenecen a la zona com)

Todos los servidores DNS reciben delegación de otros servidores, excepto la zona (.), igualmente delegan a otros servidores los dominios de cada país. No tienen autoridad por si mismos.

Integración del directorio activo con otras aplicaciones

Una vez que se probó el modelo de servicio de directorio, se puede planificar cómo integrar otras aplicaciones basadas en este servicio de directorio, por ejemplo:

- El servicio de mensajería Microsoft Exchange Server 2003
- Las herramientas de administración automática como el Servicio de Actualización de Software de Microsoft y
- La administración de directivas de grupo, que permite utilizar más ampliamente el servicio de Directorio Activo, entre otras.

Capítulo II. Estandarización de la infraestructura

2.1. Introducción

En este capítulo se explican brevemente las tareas de preparación del dominio Windows NT 4.0 hacia la migración de Windows Server 2003, así como: la definición de los estándares de la infraestructura básica del directorio activo en Pemex Refinación.

Se describen las actividades sobre la migración de Windows NT 4.0 a Windows Server 2003, considerando la integración de los atributos del directorio activo con Exchange, tomando en consideración que la arquitectura de Exchange 2003 esta fundamentada en el modelo del directorio activo. Partiendo de la instalación del directorio activo para el dominio ci.ref.pemex.com.

Para el diseño lógico se presentan las definiciones de nomenclatura y estándares utilizados en la Arquitectura de Windows Server 2003, por ejemplo: los estándares de valores y convenciones de nombres que deberán tener los atributos de los usuarios para lograr una sincronización exitosa de la lista de direcciones Inter-Organismo, esta definición aplica para cada uno de los dominios de Pemex Refinación.

Para el diseño físico se exponen los requerimientos de hardware mínimo tanto para un controlador de dominio, como para una estación de trabajo (clientes).

Cabe mencionar, que esta definición se acordó en conjunto y fue aprobada por cada una de las áreas que forman Pemex Refinación.

Además, se debe considerar que el proceso de estandarización a nivel directorio activo se fundamentó en el hecho de tener un modelo único de administración en todo el bosque de Pemex Refinación, logrando:

- Definir los sitios Windows 2003
- Establecer un único modelo de replicación
- Asociar las subnets al sitio Windows 2003 correspondiente
- Identificar para cada dominio los servidores que proporcionarán roles activos del directorio activo en cada uno de los sitios Windows 2003
- Establecer las reglas de utilización de servidores que proporcionan servicios como DC, GC
- Identificar el servidor por dominio que será utilizado para realizar la sincronización con el metadirectorio

2.2 Diseño Lógico

A continuación se describen las definiciones de nomenclatura y estándares que se utilizaron en el diseño de la arquitectura del Directorio Activo para lograr tener un modelo consistente.

Estándares:

1. De los atributos de usuario
2. Nombres de servidores y computadoras
3. De la infraestructura básica del directorio activo (cuentas de administración, políticas, grupos administrativos, unidades organizacionales).
4. De la infraestructura básica del directorio activo en Pemex Refinación.
5. Del modelo de resolución de nombres (DNS)

2.2.1. Estándares de atributos de usuario

Introducción

La estandarización de los atributos de usuario permitirá:

- Mantener una vista homogénea de la lista de direcciones inter-organismo. Los usuarios podrán consultar la lista de direcciones con un formato y estructura similar, independientemente del organismo al que pertenezcan.
- Definir los atributos que serán utilizados para generar la lista de direcciones inter-organismo. La definición de estos atributos permitirá estandarizar la forma en que se realizará la agrupación de usuarios en la lista de direcciones inter-organismo; esto es como se visualizará la lista de usuarios en el servicio de mensajería o correo.
- Establecer una convención de nombres de los valores que podrán ser asignados a cada uno de los atributos. Esta convención de nombres permitirá a los usuarios realizar consultas al directorio y obtener información consistente. Por ejemplo: El atributo "Company" tendrá asignado el nombre del organismo. Con esta convención el usuario podrá identificar con facilidad el organismo de cualquier usuario en el directorio.

Tipos de atributos

Para definir la convención de nombres y valores que deberán ser asignados a cada unos de los atributos, se realizó una clasificación de los atributos de acuerdo al uso que tendrán en la lista de direcciones inter-organismo:

- **Requeridos por Exchange**. Son los atributos necesarios para que un usuario tenga acceso a los servicios del directorio activo y Exchange 2003.
- **Requeridos para lista Inter-Organismo**. Son los atributos que serán utilizados para crear la lista de direcciones inter-organismo. Estos atributos tienen una convención de nombres estandarizada en todos los organismos de Pemex. Si un usuario no tiene asignado un valor en estos atributos, utilizando las convenciones de nombres definidas, el usuario no se sincronizará exitosamente.
- **Opcionales**. Estos atributos serán sincronizados en la lista de direcciones inter-organismo, pero no serán utilizados para crear la lista de direcciones. Si no se tiene un valor asignado en alguno de estos atributos no se tendrá ningún impacto en el proceso de sincronización. Estos atributos tienen una convención de nombres estandarizada en todos los organismos de Pemex Refinación.
- **No homologados**. Estos atributos no serán sincronizados en la lista de direcciones inter-organismo. No tienen una convención de nombres estandarizada. Su uso depende de las necesidades y políticas de cada organismo.

Estándares definidos

Estándares requeridos por Exchange

En la tabla 2.2.1.a se muestran los atributos requeridos por Exchange 2003 para crear una cuenta de usuario, para que funcione con el servicio de mensajería.

Tabla 2.2.1.a Atributos requeridos por Exchange

Sección	Atributo	Convención de Nombres
General	E-mail	Definido por el Organismo
Account	User logon name	
E-mail Addresses	E-mail Addresses	
Exchange General	Mailbox store	
	Alias	

Requeridos para la lista inter-organismo

En la tabla 2.2.1.b se describen los atributos para crear la lista de direcciones inter-organismo. Para asegurar una sincronización exitosa de los directorios, es importante que todos los objetos tengan los valores definidos para estos atributos.

Tabla 2.2.1.b Atributos de usuarios con valores definidos

Sección	Atributo	Convención de Nombres
General	First Name	Nombre(s)
	Last Name	Apellido(s)
	Display Name	Apellidos + Nombre(s)
	Office	Variable de agrupación. Tiene un valor fijo definido por cada Organismo
Organization	Company	Organismo

La tabla 2.2.1.c muestra los valores que deberán tener los atributos de "Company" y "Office" en el directorio activo de cada organismo. Por ejemplo: la definición para el área de Contraloría Interna quedó definida como: "Company" = Refinación y "Office" = Contraloría Interna.

Tabla 2.2.1.c Valores para los atributos "Company" y "Office"

Valores para el atributo " Company "	Valores para el atributo "Office"

Dirección General	Dirección General
Corporativo	DCF DCA CGC
PEP	Sede México Región Norte Región Sur Región Marina Perforación
PGPB	Zona Centro Zona Norte Zona Sur
PTQ	Oficinas Administrativas Cangrejera Coatzacoalcos Escolin Morelos Tula
Refinación	Contraloría Interna Finanzas y Administración Almacenamiento y Distribución Comercial Planeación Producción SASIPA

Se definieron dos niveles para agrupar los objetos en la lista de direcciones inter-organismo. El primer nivel estará definido por el atributo "Company" (define el atributo de organismo) y el segundo nivel estará definido por el atributo "Office" (define el atributo de gerencia).

Opcionales

A continuación se describen los atributos opcionales. Es opcional introducir la información de estos atributos en el directorio activo. Si se ingresa la información de estos atributos al directorio activo, se tiene que realizar de acuerdo a las convenciones de nombres definidas. Como se muestra en la tabla 2.2.1.d.

Tabla 2.2.1.d Atributos opcionales

Sección	Atributo	Convención de Nombres	Ejemplo
General	Telephone Number	Micro-Extensión	811-12345
Address	Street	Calle y número Colonia Municipio Edificio y piso	Av. Marina Nacional No. 329 Col. Huasteca Edificio C 4o piso
	P.O. Box	No utilizar	-
	City	Ciudad	México
	State/province	Estado	D.F.
	Zip/Postal Code	Código Postal	11311
	Country/región	País	México
Telephones	Home	Teléfono particular incluyendo clave lada	(55)12345678
	Mobile	Teléfono celular incluyendo clave lada nacional	(55)12345678
	Fax	Fax incluyendo clave lada nacional	(55)87654321
	Notes	Reservado para uso futuro	-
Organization	Title	Ficha	123456
	Manager	Jefe Inmediato	
	Direct Reports	Se llena con los datos de Manager	

No homologados

En la tabla 2.2.1.e, se describen los atributos no homologados. Estos atributos podrán utilizarse de acuerdo a los requerimientos particulares de cada organismo.

Tabla 2.2.1.e Atributos no homologados

Sección	Atributo
General	Description
	Web page
Telephones	Pager
	IP phone
Organization	Department

2.2.2 Estándares para el alias del usuario

El alias o user logon name del usuario se estructura de la siguiente manera:

a) En el caso de que el usuario cuente con un solo nombre: se toman los dos primeros caracteres, seguido del apellido paterno y el primer carácter del apellido materno.

Ejemplo: Anabel Audelo Rodríguez será: **ANAUDELOR**

b) Para el caso de que el usuario cuente con dos nombres el user logon name, la estructura será la siguiente: las dos primeras letras de cada nombre, seguido del apellido paterno y el primer carácter del apellido materno.

Ejemplo: José Luis Estrada Nuñez será: **JLESTRADAN**

La tabla 2.2.2 muestra un ejemplo de cómo deben llenarse los atributos para un usuario.

Tabla 2.2.2 Ejemplo de atributos para un usuario

Atributo	Ejemplo
First	Juan
Last	Pérez González
Display	Pérez González Juan
Alias	juperezg
Address	Av. Marina Nacional No.329 Col. Huasteca Edificio B2 4o. piso
City	México
State	D.F.
Zip Code	11311
Country	MEXICO
Title	234565
Company	REFINACION
Department	Gerencia de Tecnología y Procesos de Información
Office	Finanzas y Administración
Phone	811-38888
SMTP	juperezg@ref.pemex.com

2.2.3 Estándares para nombres de servidores y computadoras

En la tabla 2.2.3, se describen las definiciones de nomenclatura y estándares que se definieron en el diseño de la arquitectura para los nombres de servidores y nombre de computadoras.

Tabla 2.2.3 Estándares para nombres de servidores y computadoras

Tipo de Estándar	Definición	Ejemplo
Nombre de Servidor	El nombre del servidor se basará en la política establecida desde la implantación de Windows 2003 y el Directorio Activo.	***RFA-OFCW3APP01*** R = Refinación FA = Subdominio OFC = Oficinas Centrales W3 = Windows 2003 APP = Aplicación 01 = No. de Servidor ***RFA-OFCW3COR01*** R = Refinación FA = Subdominio OFC = Oficinas Centrales W3 = Windows 2003 COR = Correo 01 = No. de Servidor
Nombre de computadora	El nombre de computadora se basará en la política establecida desde la implantación de Windows 2003 y el Directorio Activo.	***DGD11APOYO-P01*** DG = Dirección General D = Edificio D 11 = Piso 11 APOYO = Departamento P = PC 01 = No. de Equipo

2.2.4 Estandarización de la infraestructura de administración del directorio activo (cuentas de administración, políticas, grupos administrativos, unidades organizacionales)

En la tabla 2.2.4, se describen las definiciones referentes a las cuentas de administración, identificación de recipientes para aplicación de políticas, la convención de nombres de unidades organizaciones.

Tabla 2.2.4 Definición de la infraestructura de administración

Tipo de Estándar	Definición	Ejemplo
Cuenta de Administración	Se definirá una cuenta de Administración a nivel de dominio CI con los siguientes permisos: • Domain Admin • Local Admin	
Identificación de Políticas de Recipientes	Las Políticas de Recipientes se establecerán para cada dominio (dominio raíz y subdominios). El nombre de la política seguirá una convención en base al sufijo DNS del dominio.	ref.pemex.com ca.dg.ref.pemex.com ci.ref.pemex.com co.ref.pemex.com dg.ref.pemex.com di.ref.pemex.com fa.ref.pemex.com pd.ref.pemex.com pl.ref.pemex.com sp.ref.pemex.com
Identificación de Grupos Administrativos	Se establecerán Grupos Administrativos para cada dominio (subdominio). El Dominio raíz será asociado al Grupo Administrativo predeterminada (First Administrativa Group). El nombre de los grupos seguirá una convención en base al nombre del dominio.	CA - Grupo de Administración Cl - Grupo de Administración CO - Grupo de Administración DI - Grupo de Administración FA - Grupo de Administración PD - Grupo de Administración PL - Grupo de Administración SP - Grupo de Administración
Identificación de Grupos de Ruteo.	Los Grupos de Ruteo seguirán una convención de nombres en base al Nombre de Subdominio + la ubicación del servidor de correo de Exchange 2003	***FAOFC Routíng Group*** FA = Nombre de dominio OFC = Oficinas Centrales
Unidades Organizacionales (Directorio Activo)	En cada Subdominio, se establecerá una Unidad Organizacional en el Directorio Activo para Usuarios y Grupos. La convención de nombres será: "<Subdominio> + Users and Groups	***FA Users and Groups***
Unidades Organizacionales (Anidadas)	Para las OU que se aniden en la OU de Users and Groups, la convención de nombres la establecerá el Administrador de cada Subdominio	

2.2.5 Estandarización de la infraestructura

Comunicaciones:

Para iniciar el proceso de estandarización de la infraestructura fue necesario analizar la información correspondiente a la red de comunicaciones.

En este caso se hace referencia a tener la topología completa de la red de comunicaciones de Pemex Refinación con la finalidad de optimizar el diseño y tener un modelo de servicios eficiente.

Los puntos importantes a considerar fueron:

- establecer entre que localidades había ruteo y cuales no tenían definida una trayectoria de ruteo que les permitiera completar un proceso de replicación
- conocer los anchos de banda con la finalidad de identificar a los usuarios que se encontraran en localidades remotas y con un limitado ancho de banda disponible

El resultado del análisis que se obtuvo de la red de comunicaciones, permitió establecer a nivel directorio activo, los siguientes puntos:

- Un modelo de replicación eficiente
- Se identificó en que localidades se proporcionarían los servicios como DNS, WINS, DC, GC, RID, Infraestructure, etc.
- Permitió establecer que subnets conformarían cada uno de los sitios Windows

Revisión del ambiente de directorio activo

A continuación se describe la situación propuesta de configuración de la arquitectura de servicios implantados del directorio activo y Windows 2003 en Pemex Refinación.

Sobre la Arquitectura del Directorio Activo, los siguientes factores fueron importantes para el diseño de la plataforma, como se muestra en la figura 2.2.5.

- Sistema operativo Microsoft Windows 2003 con service pack 1 instalado en los servidores de dominio.
- Estructura multidominio: 8 subdominios y 1 dominio Raíz ref.pemex.com.
- El domino raíz REF tiene como finalidad agrupar a los demás dominios desde el punto de vista organizacional y se le considera básicamente como un dominio de recursos en donde no se tienen cuentas de usuario ni estaciones de trabajo.
- A excepción de la Subdirección de Distribución (dominio di.ref.pemex.com) y la Subdirección de Producción (dominio

pd.ref.pemex.com), las cuales cuentan con una organización de administración de TI distribuida en unidades regionales, las demás subdirecciones (dominios) cuentan con una organización de administración de TI centralizada. Los centros de soporte se encuentran localizados en la Ciudad de México en las oficinas centrales.

Topología:

La configuración establecida actualmente en Pemex Refinación está sustentada en el modelo de un bosque de 2 niveles con un directorio raíz ref.pemex.com del cual dependen todos los demás dominios al mismo nivel. El directorio raíz representa a todo el organismo Pemex Refinación y del cual dependen los demás dominios con este modelo se mantiene la administración centralizada de TI.

La topología que se muestra en la figura 2.2.5, es la que sustenta el diseño implantado de los servicios del directorio activo en Pemex Refinación actualmente.

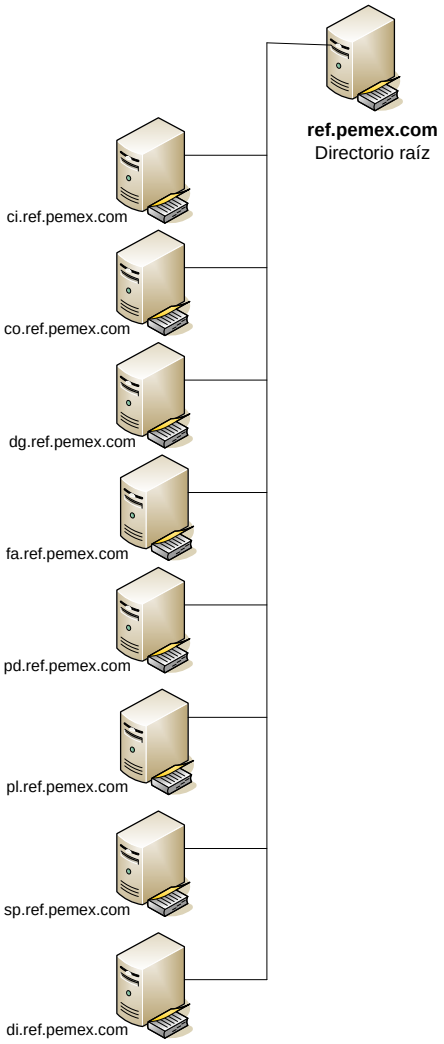


Figura 2.2.5 Topología de directorio Activo en Pemex Refinación

Como se menciona este diseño es de 2 niveles, con el dominio ref.pemex.com como su directorio raíz y a partir de este nivel se generan los dominios que corresponden a cada una de las subdirecciones que conforman Pemex Refinación, se enlistan a continuación:

1. Ci (Contraloría Interna)
2. Co (Comercial)
3. Dg (Dirección General)
4. Di (Distribución)
5. Pd (Producción)
6. Fa (Finanzas y Administración)
7. Pl (Planeación)
8. SP (Seguridad y Protección Ambiental)

Sitios Windows 2003

El diseño de dominios en el directorio activo esta complementado con la creación de sitios Windows 2003, con la finalidad de:

- optimizar la utilización de recursos (utilización del ancho de banda de manera óptima)
- tener servidores que proporcionen servicios eficientes a los usuarios con base a su distribución geográfica

En la tabla 2.2.5, se muestran los sitios definidos:

Tabla 2.2.5 Sitios en Pemex Refinación

SITIOS	
1. Cover	18. Dizplaz
2. Covmx	19. Dizpmag
3. Dimty	20. Dizpmai
4. Dizpaca	21. Dizpmaz
5. Dizpcas	22. Dizpnav
6. Dizpcol	23. Dizpobr
7. Dizpcul	24. Dizpros
8. Dizpens	25. Dizptep
9. Dizpgua	26. Dizpzap
10. Dizpgum	27. Pdcad
11. Dizpmex	28. Pdmad
12. Dizpnog	29. Pdmin
13. Dizppaz	30. Pdsal
14. Dizpsal	31. Pdscz
15. Dizpher	32. Pdtul
16. Dizplaz	33. Refofc
17. Dizpmag	

2.2.6 Estandarización del modelo de resolución de nombres

DNS

El servicio DNS, sirve para realizar la resolución de nombres de máquina a una dirección IP y viceversa. Si el DNS no está bien configurado o tiene problemas, entonces el diseño del AD no funcionará adecuadamente, ya que el directorio activo usa el servicio de DNS para dejar información que después las estaciones de trabajo tendrán que consultar para interactuar correctamente con el servicio de directorio (validación, consultas, búsquedas, etc.).

A nivel DNS, se creo la zona ref.pemex.com y a partir de la misma se delegaron las zonas correspondientes para cada uno de los dominios que conforman el bosque del directorio activo en Pemex Refinación.

Para la estandarización de este servicio, se realizo un estudio por parte Microsoft, recibiendo las siguientes recomendaciones mínimas de configuración:

- Creación de la zona tipo forward lookup zone que corresponde al dominio (ci.ref.pemex.com).
- Establecer cuantos y que servidores se incluirían como name server, los cuales son responsables de la zona de nombres (por seguridad no se permitirá que cualquier servidor pueda solicitar la transferencia de una zona DNS).
- Para las zonas de tipo forward se introducirá en forma manual el registro DNS de estaciones y/o servidores que no tengan la capacidad de registrarse en forma automática (Windows 95/98, Windows NT Workstation, Windows NT Server, UNIX, etc.).
- Establecer en la configuración de la transferencia de zonas DNS de tipo forward y reverse que el proceso de transferencia de zonas solamente se realizará con los servidores que se han incluido como name servers.
- Crear la zona reversa para cada una de las subnets que conforman la zona de nombres (requisito para completar el proceso de registro automático en el directorio activo).
- Cada dominio que conforma el bosque, deberá dar de alta las subnets en la zona reversa DNS integrada al directorio activo para asegurar que se esta completando apropiadamente el proceso de registro de las estaciones de trabajo y servidores en el directorio.
- Establecer la configuración de forwarding que tiene como finalidad establecer la mecánica para resolver nombres que no pertenezcan al espacio de nombres local.
- Definir las alternativas de resolución de nombres en caso de que el directorio raíz este fuera de servicio (configuración de root hints, direccionando la resolución al servidor de la Gerencia de Telecomunicaciones).

Para el caso del dominio ci.ref.pemex.com, se estableció que el controlador de dominio, proporcionaría también el servicio de resolución de nombres

(definiendo al DNS como una zona integrada al directorio activo). Como se muestra en la figura 2.2.6.

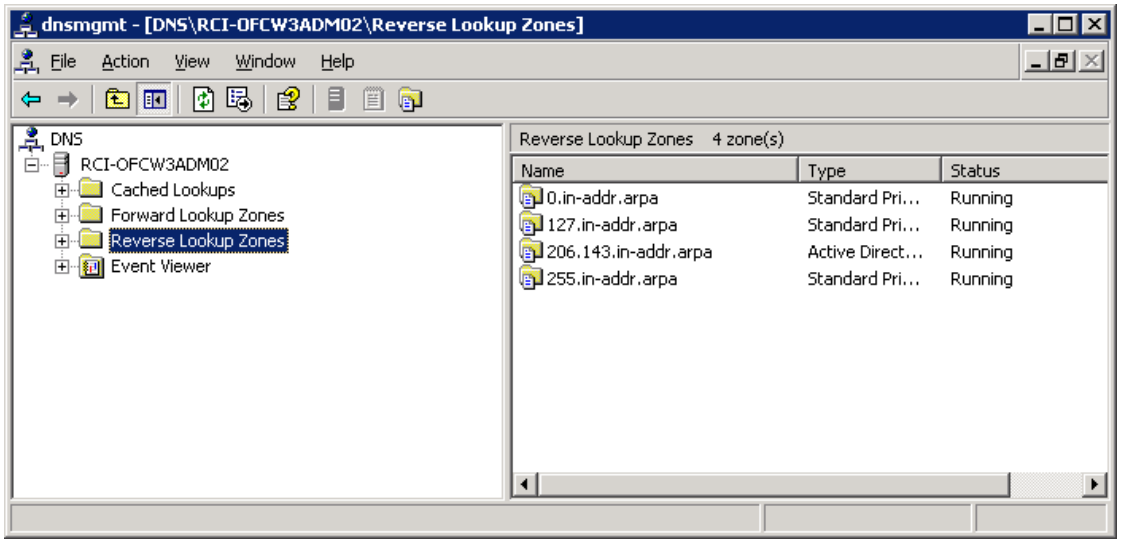


Figura 2.2.6 DNS

2.3 Diseño físico

Una vez establecidos los componentes de la infraestructura del directorio activo, las consideraciones de diseño a nivel general y el diseño específico para Pemex Refinación, a continuación se recomienda la configuración de hardware y software óptima, como se muestra en la tabla 2.3.a.

Tabla 2.3.a Requerimientos

Requerimientos	Recomendado
Hardware	• Procesador Xeón 700 Mhz (2 procesadores) • Memoria: 512 MB • Espacio en Disco Duro: 10 GB como mínimo
Software	• Sistema Operativo Windows 2003 Enterprise Server • Internet Information Server 6.0 • Terminal Services • Antivirus Corporativo para Servidor
Localización	• Oficinas Centrales • Oficinas Regionales

Las tareas que se deben realizar en los controladores de dominio son:

- Actualización de hotfixes
- Configuración de DNS en la configuración de red
- Revisión del servicio de DNS
- Forwarders

La tabla 2.3.b es un ejemplo del formato que se definió, para llevar un control de los cambios y actualizaciones hechas a la configuración del ambiente, por cada controlador de dominio.

Tabla 2.3.b Formato de configuración para un DC

	Configuración Inicial	**Configuración Final**
Nombre		
Oficina		
Fecha		
IP		
Máscara de Red		
Gateway		
DNS		
Sufijo		
Forwarders		
Cambios y Observaciones:		

Capítulo III. Implementación del cambio

En este capítulo, se explica las actividades que se realizaron en el proceso de implementación del Directorio Activo; desde la instalación y configuración del sistema operativo Windows Server 2003, pasando por la instalación de la herramienta de Active Directory Migration Tool (ADMT), la migración de cuentas de usuario, para terminar con la migración de las estaciones de trabajo al nuevo dominio.

Es importante mencionar la infraestructura con la que se trabajó, antes de implementar el Directorio Activo:

- Dos controladores de dominio. Uno con el rol de Primary Domain Controller (PDC) y el otro como Backup Domain Controller (BDC), los cuales tenían instalado el sistema operativo Windows NT 4.0 Server with Service Pack 6.
- Doscientas diez cuentas de usuarios y estaciones de trabajo. El 90% de las estaciones de trabajo, tenía instalado Windows 2000, el 10% restante, tenían instalado Windows NT Workstation with service Pack 6.

3.1 Fases de implementación

El proceso de implementación, se dividió en fases; las cuales se enlistan y describen a continuación:

1. Pre-requisitos del proceso de implementación
2. Instalación del dominio ci.ref.pemex.com
3. Creación de relaciones de confianza entre el dominio RDG-COID11 y CI
4. Instalación de la Herramienta Active Directory Migration Tool (ADMT)
5. Migración de cuentas de usuario
6. Estabilización de las cuentas de usuario
7. Migración de las estaciones de trabajo al dominio CI

3.1.1 Fase 1. Pre-requisitos del proceso de implementación

Antes de poder iniciar el proceso de implementación se realizaron actividades previas, las cuales incluyen algunas consideraciones a tomar en cuenta para el dominio, servidores y usuarios. A continuación se detallan:

1. Configuraciones y consideraciones: son actividades que se realizaron en el dominio raíz; asimismo parametrización de configuraciones en los Controladores de Dominio

1. Previamente fue creado el Dominio DNS: ci.ref.pemex.com; en el dominio raíz: ref.pemex.com.
2. Nombre de dominio NETBIOS: CI
3. Cuenta de servicio: administrator. Se deberá contar con una cuenta que tenga permisos de administración, a nivel del dominio (CI), y que pertenezca a los siguientes grupos de seguridad: Domain Admin, Local Admin, Group Polícy Creator Owners, DnsAdmins.
4. Se deberán de configurar dos servidores, de la siguiente manera:
   - Un controlador principal de dominio con Windows 2003 Server Enterprise Edition, SP1 y la última actualización de hotfixes.
   - Un controlador adicional de dominio con Windows 2003 Server Enterprise Edition, SP1 y la última actualización de hotfixes.

5. El dominio se definió en modo nativo.

6. En todos los casos la configuración regional para los controladores y servidores miembros, se definió de la siguiente manera:
   a) Los parámetros de localidad se definieron como: English (United status).
   b) Los parámetros de configuración de teclado son: ES Spanish (México).
   c) Los parámetros de la zona de tiempo: (GMT -06:00) Central Time (US & Canada).

2. Servidores: se refiere a configuraciones las cuales se considerarón antes de crear las relaciones de confianza entre los dominios.

- Preparar dominios (crear relaciones de confianza entre el dominio origen NT y destino W3K)
- Agregar el grupo global Domain Admins del dominio W3K en el grupo local Administrators del dominio NT
- Verificar que el PDC del dominio NT tenga configurado los siguientes parámetros:

   a. Habilitar la política de auditoría *user and group management.*
   b. Verificar que en el PDC exista un grupo local llamado <DominioNT>$$$
   c. Verificar que en el PDC exista la siguiente llave en el ´registry´: HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/LSA/TcipipClientSupport:REG_DWORD:0x1

- Migrar cada una de las cuentas de usuario del dominio NT a W3K utilizando la herramienta Active Directory Migration Tool.

    a. Homologar cuentas de usuario.
    b. Mapear la unidad donde se encuentra el *.bat (que incluye la ruta antivirus).

Software que se utilizó para realizar la instalación del Sistema Operativo Windows Server 2003:

    a. Windows 2003 Server Enterprise Edition
    b. Windows 2003 Support Tools

3. Usuarios: son verificaciones que se realizarón, antes de migrar las cuentas de usuarios y equipo.

a. Verificar que los nombres de usuario no entren en conflicto con los usuarios existentes en el dominio ref.pemex.com, con base en la homologación acordada en el Grupo de Integración del Directorio Activo.
b. Verificar tamaño del perfil de usuario (en los equipos que tienen instalado los sistemas operativos Windows NT 4.0 Workstation y Windows 2000. Si el perfil excede de 10 MB promedio, reducir su tamaño moviendo los documentos, archivos (mp3, wav, pst, entre otros) y accesos directos del escritorio a una carpeta temporal.
c. Desactivar de las propiedades del usuario, la opción de *User cannot change password* utilizando la herramienta *´User management for domains.*

3.1.2 Instalación del dominio ci.ref.pemex.com

Instalación de Windows Server 2003 – Primer Controlador de Dominio

A continuación se detalla el procedimiento de instalación del sistema operativo Windows Server 2003 Enterprise Edition en el primer controlador de dominio, para el dominio ci.ref.pemex.com. Se inicia la instalación, como se visualiza en la figura 3.1.2.a.

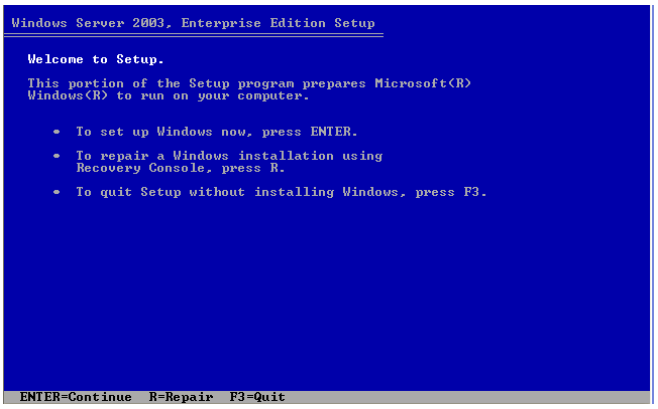


Fig. 3.1.2.a Instalación de Windows Server 2003 Enterprise Edition

Es importante mencionar que el tipo de formato de sistema utilizado para los controladores de dominio es: NTFS, se define en la instalación como se muestra en la figura 3.1.2.b.

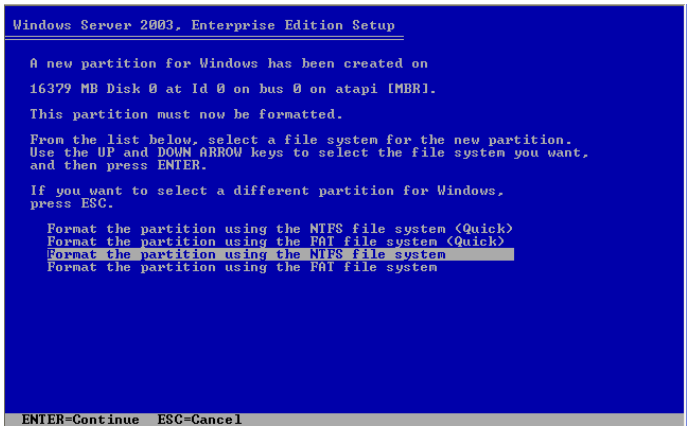


Fig. 3.1.2.b Formato NTFS

A continuación, se inicia el formateo del disco y se empiezan a copiar los archivos de sistema. Después de haberse instalado el sistema operativo, se ingresa al servidor, para configurar el rol de directorio activo.

Configuración del rol de Directorio Activo

Al acceder por primera vez al servidor, se despliega la pantalla de **"Manage Your Server",** este asistente permite asignar roles específicos a un servidor. A través de la opción "**Add or remove a role**" como se muestra en la figura 3.1.2.c.

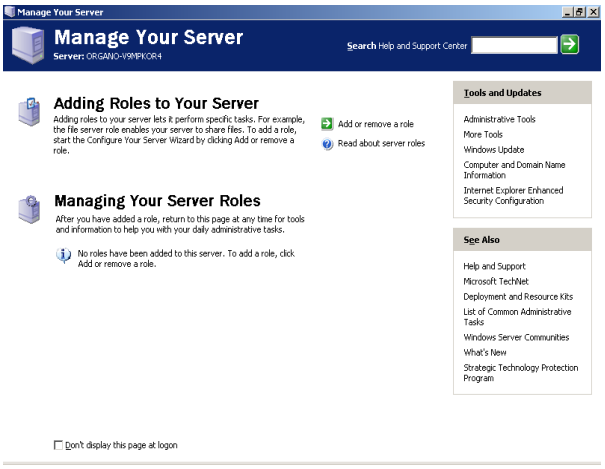


Fig. 3.1.2.c Manage Your Server

A continuación se asignará el rol de "**Domain Controller (Active Directory)"**, desde la pantalla de **"Server Role",** tal como se muestra en la figura 3.1.2.d.

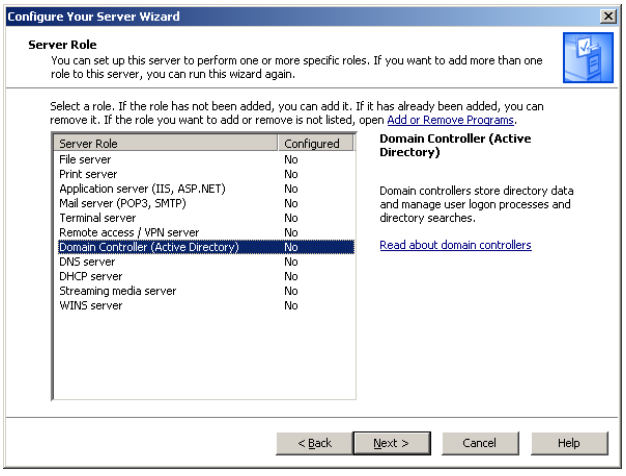


Fig. 3.1.2. d Asignación de rol Domain Controller

Después de haber asignado el rol de controlador de dominio, se muestra el asistente **"Active Directory Installation Wizard"**, en la figura 3.1.2.e "**Domain Controller Type"**, se especifica que el Controlador de Dominio será integrado a un nuevo dominio.

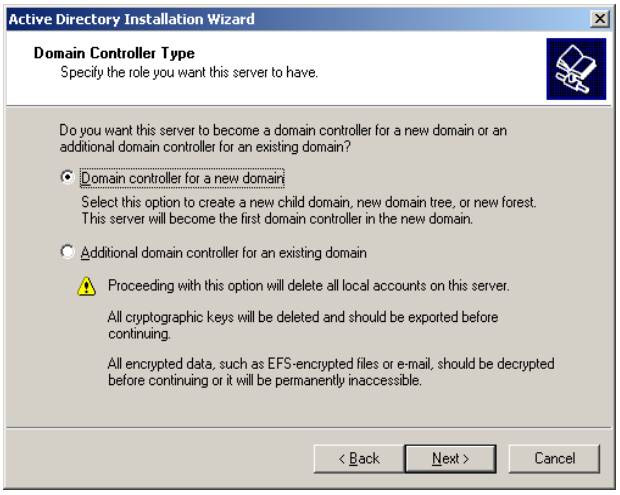


Fig. 3.1.2.e Domain Controller Type

Continuando con el asistente, se configuraron la siguiente información como se muestra en la figura 3.1.2.f "**New Domain Name"**, **"Full DNS name for new domain: ci.**

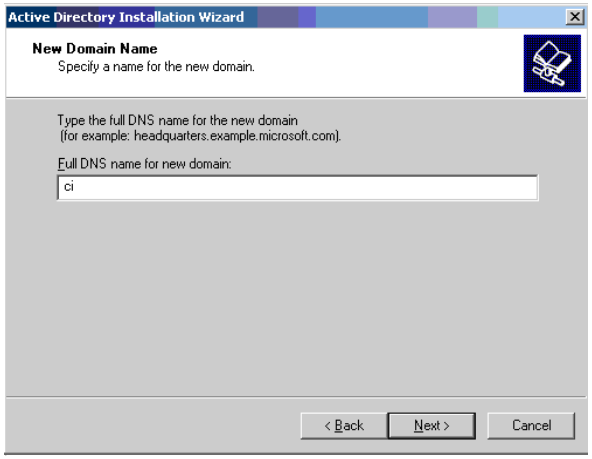


Fig. 3.1.2.f Nombre del nuevo dominio

El siguiente dato es proporcionar el **"Domain NetBIOS Name",** se especifica CI, como se puede visualizar en la figura 3.1.2.g.

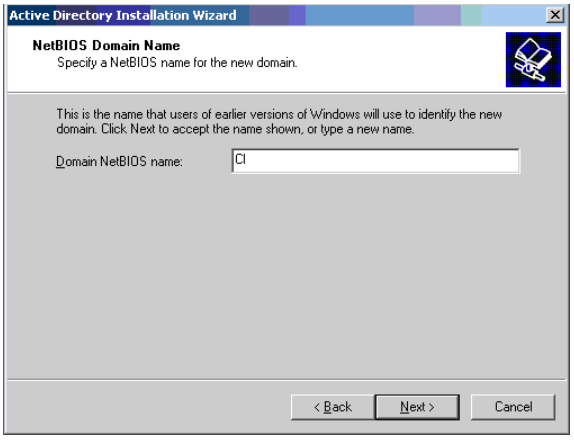


Fig. 3.1.2.g Domain NetBIOS Name

A continuación en la figura 3.1.2.n **"Database and Log Folders"**, se indica la ruta donde se almacenara la base de datos y los logs. La base de datos contiene cada uno de los objetos del directorio activo. Es importante mencionar que estos archivos se tendrán que respaldar de manera periódica.

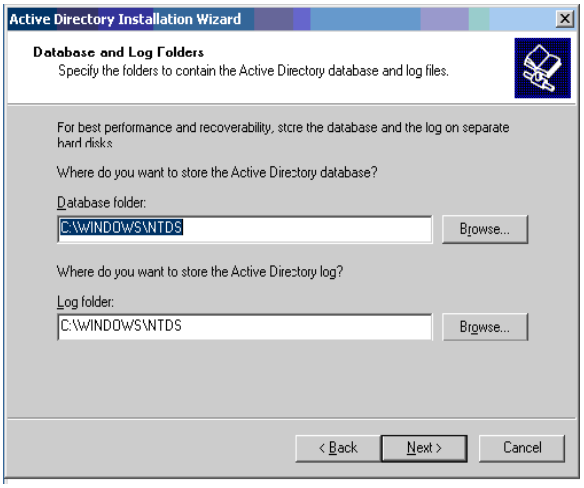


Fig. 3.1.2.h Database and Log Folders

En la pantalla **"Shared System Volume"** se especifica la localización del folder SYSVOL, como se visualiza en la figura 3.1.2.i. Es importante mencionar, que en caso de que se dañe o corrompa el directorio activo, se puede generar la restauración a través de estos archivos: base de datos, logs y SYSVOL.

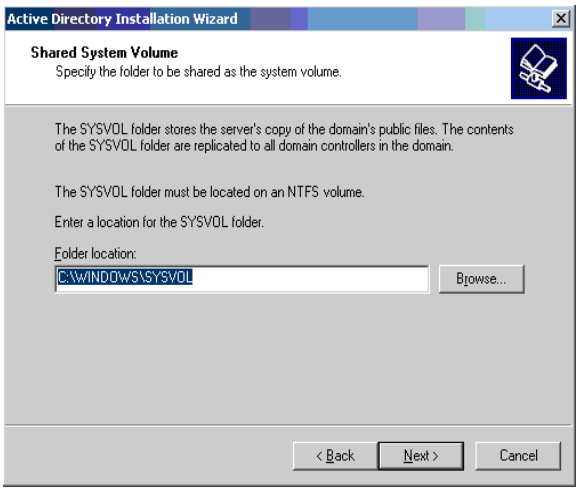


Fig. 3.1.2.i Localización del SYSVOL

En la pantalla **"Permissions"** se definen los permisos de compatibilidad para los objetos de usuarios y grupos. Para el caso que aplica, solo se asignaran permisos de compatibilidad para Windows 2000 y Windows Server 2003, como se muestra en la figura 3.1.2.j.

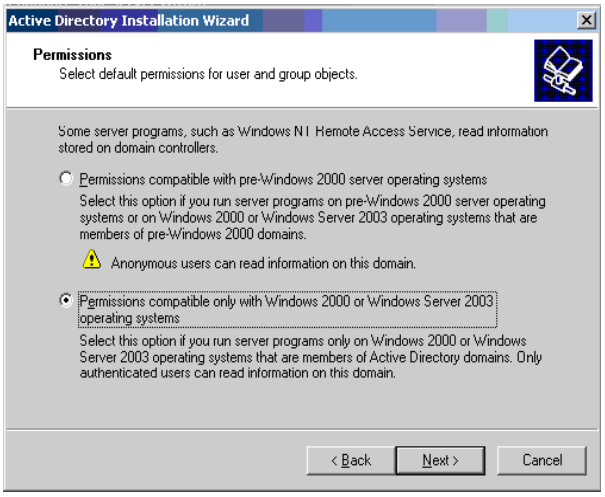


Fig. 3.1.2.i Localización del SYSVOL

Siguiendo con la instalación y configuración del directorio activo, a continuación se nos solicita asignar el password de restauración, desde la pantalla de instalación "**Services Restore Mode Administrator Password".**

Nota: Este password es necesario, en caso de que se necesite restaurar los servicios de directorio a través del Modo de Restauración.

La pantalla **"Summary"**, muestra las configuraciones elegidas para que se verifiquen y confirmen las opciones seleccionadas. Al aceptarse, se realizará la instalación del Directorio Activo.

A continuación, se muestra la pantalla de "**Server Role"**, y se podrán agregar los rol necesarios, tal como se muestra en la figura 3.1.2.k. Para el caso que aplica, se seleccionaron adicionalmente el rol de DNS y DHCP.

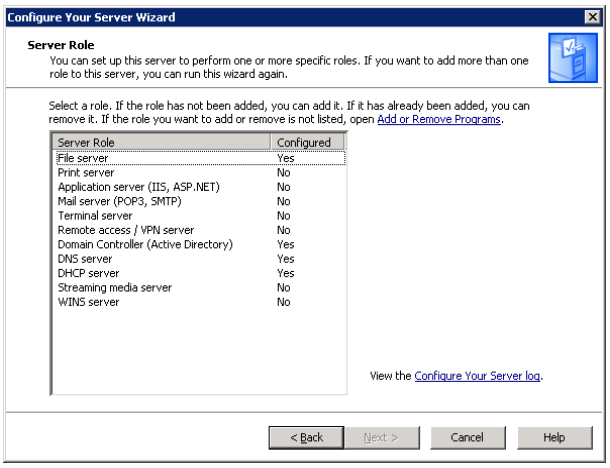


Fig. 3.1.2.k Configuración de roles adicionales

Con estas configuraciones, finaliza la instalación del sistema operativo Windows Server 2003, ha quedado instalado el directorio activo, se especifico la ruta donde se encuentra la base de datos, los logs; así como la ruta del SYSVOL, y el password de restauración; adicionalmente se agregaron los roles de DNS y DHCP para este controlador de dominio.

Para el controlador secundario de dominio, se siguió el mismo procedimiento de instalación. No se agregaron los roles adicionales de DNS y DHCP.

Documentación de las configuraciones iniciales de los controladores de dominio

A continuación se muestra como quedaron documentadas las configuraciones para el controlador principal y secundario, en el formato Consolidado de Controladores de dominio, como se muestra en las tablas 3.1.2.a y 3.1.2.b.

Tabla 3.1.2.a Configuración del Controlador principal de dominio

CONTROLADOR PRINCIPAL DE DOMINIO

	Configuración Inicial	Configuración Final
Nombre	**RCI-OFCW3ADM01**	
Oficina	**CI**	
Fecha	**04/01/2003**	
IP	**143.206.1.**	
Máscara de Red	**255.255.255.0**	
Gateway	**143.206.1.1**	
DNS	**143.206.1.122**	
Sufijo	**ci.ref.pemex.com**	
Forwarders		
Cambios y Observaciones:		

Tabla 3.1.2.b Configuración del Controlador secundario de dominio

CONTROLADOR SECUNDARIO DE DOMINIO

	Configuración Inicial	Configuración Final
Nombre	**RCI-OFCW3ADM02**	
Oficina	**CI**	
Fecha	**10/01/2003**	
IP	**143.206.1.**	
Máscara de Red	**255.255.255.0**	
Gateway	**143.206.1.1**	
DNS	**143.206.1.122**	
Sufijo	**ci.ref.pemex.com**	
Forwarders		
Cambios y Observaciones:		

Roles y Catálogo Global

Finalmente, en la tabla 3.1.2.c, se muestra como quedaron definidas la asignación de roles y el catálogo global, en los controladores de dominio.

Tabla 3.1.2.c Asignación de roles y Catálogo Global

ROL	NOMBRE DEL SERVIDOR
PDC	RCI-OFCW3ADM01
RID	RCI-OFCW3ADM01
INFRAESTRUCTURE	RCI-OFCW3ADM02
Catálogo Global	RCI-OFCW3ADM02

Después de tener asignados los roles en los servidores, el siguiente paso será crear las relaciones de confianza entre los dominios Windows NT 4.0 Server (RDG-COID11) y Windows Server 2003 (ci.ref.pemex.com).

3.1.3. Relaciones de confianza entre el dominio RDG-COID11 y ci.ref.pemex.com

A continuación, se detalla el procedimiento que muestra como fueron creadas las relaciones de confianza, entre el dominio RDG-COID11 de Windows Server NT 4.0 y el dominio ci.ref.pemex.com de Windows Server 2003.

Como primer paso, se genera la relación desde el dominio ci.ref.pemex.com, accesando al **"Active Directory Domains and Trusts"** de la aplicación **"Administrative Tools"**, se elige el dominio ci.ref.pemex.com y se accesa al apartado de **Trust**, como se muestra en la figura 3.1.3.a y 3.1.3.b.

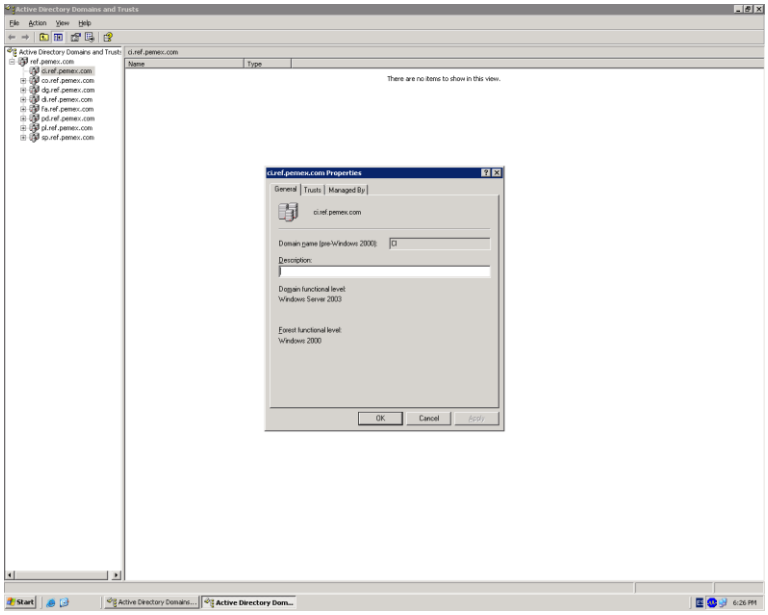


Fig. 3.1.3.a Creación de la relación de confianza en el dominio ci.ref.pemex.com

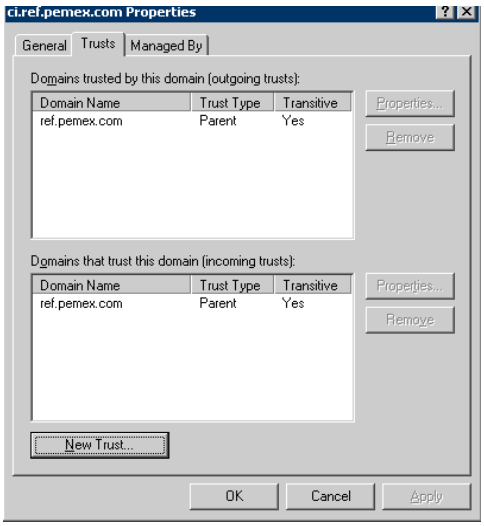


Fig. 3.1.3.b Creación de la relación de confianza con el dominio ref.pemex.com

A continuación, se elige el botón **New Trust,** para definir la nueva relación con el dominio RDG-COID11. Se abre el asistente **"New Trust Wizard".** Como se muestra en la figura 3.1.3.c **"Trust Name"**, se escribe el nombre del dominio con el cuál se quiere generar la relación de confianza. Y en la figura 3.1.3.d "**"Trust Password",** se especifica la contraseña de la relación de confianza.

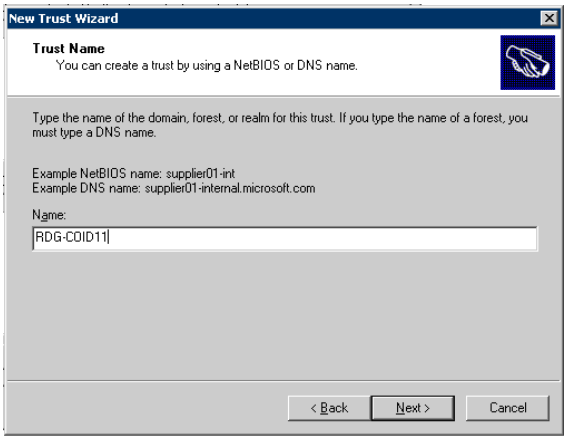


Fig. 3.1.3.c Creación de la relación de confianza con el dominio RDG-COID11

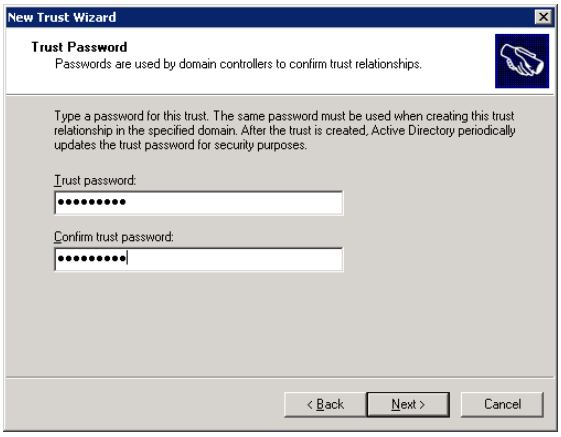


Fig. 3.1.3.d Asignación de contraseña de la relación de confianza

Las siguientes pantallas muestran el resumen de las relaciones creadas, el siguiente paso, será crear la relación de confianza en el servidor del dominio RDG-COID11. Se accesa a la aplicación "**User Manager"**, se elige la opción de **Trusting**, se proporciona el nombre del dominio con el que se creara la relación de confianza, para este caso es CI; y a continuación se proporciona una contraseña para la relación, como se muestra en la figura 3.1.3.e.

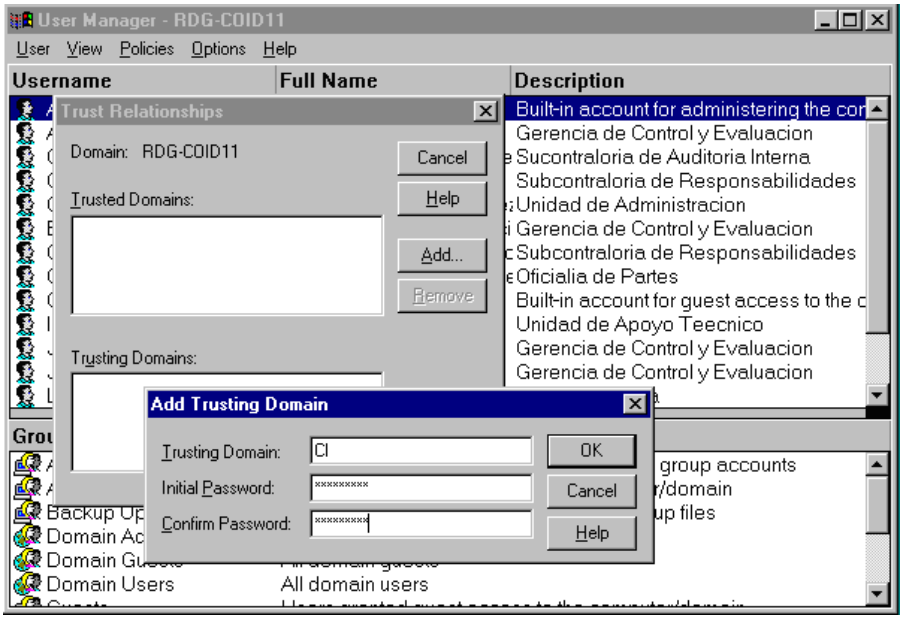


Fig. 3.1.3.e Creación de la relación de confianza en el dominio RDG-COID11

Creadas las relaciones de confianza, entre los dominios. Se tendrán que efectuar los pasos que se definieron en los pre-requisitos del proceso de migración, referente a la parte de servidores. Estas actividades se tendrán que realizar desde la aplicación "**Administrative Tools – User Manager for Domains"** del PDC del dominio RDG-COID11.

1. Agregar el grupo global Domain Admins del dominio ci.ref.pemex.com, en el grupo local Administrators del dominio rdg-coid11. Desde la aplicación **"Local Group Properties - Groups",** como se muestra en la figura 3.1.3.f.

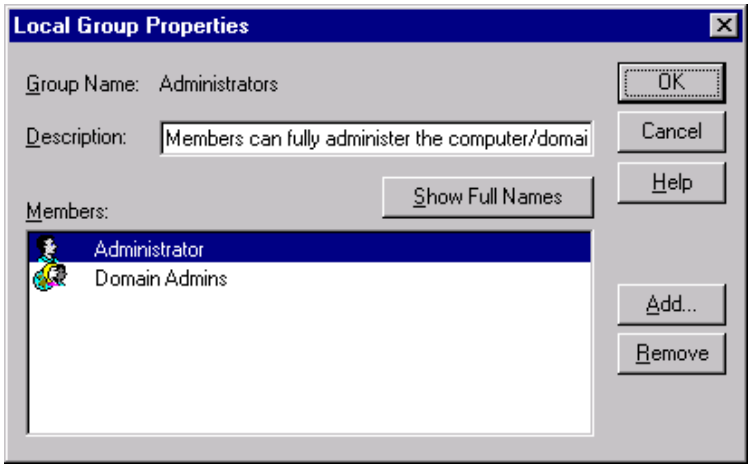


Fig. 3.1.3.f Asignación del grupo Domain Admins

2. Verificar que el PDC del dominio NT tenga configurado los siguientes parámetros:

   a. Habilitar la política de auditoría en el PDC del dominio NT, desde el menú **Policies – Audit Policy,** se habilita la opción de **User and Group** Management, como se muestra en la figura 3.1.3.g a continuación:

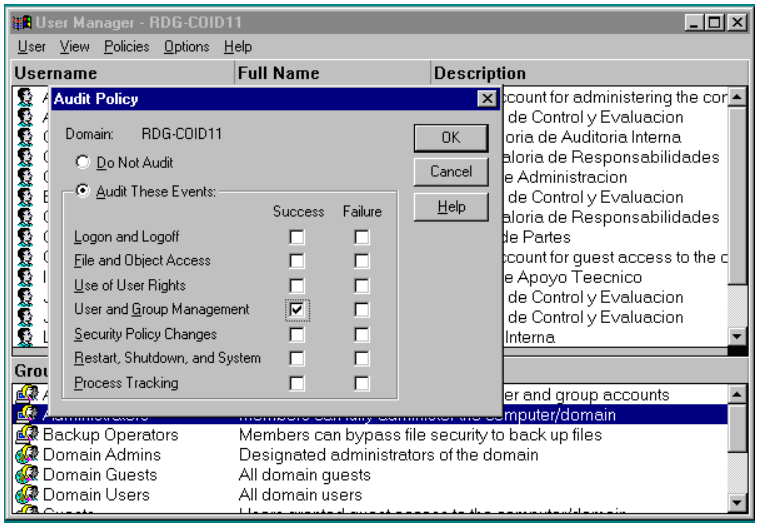


Fig. 3.1.3.g Habilitación de la política de auditoría

b. Verificar que en el PDC exista un grupo local llamado <DominioNT>$$$. Se crea el Grupo Local RDG_COID$$$. Desde el **Menú User – New Local Group**, como se muestra en la figuras 3.1.3.h, 3.1.3.i.

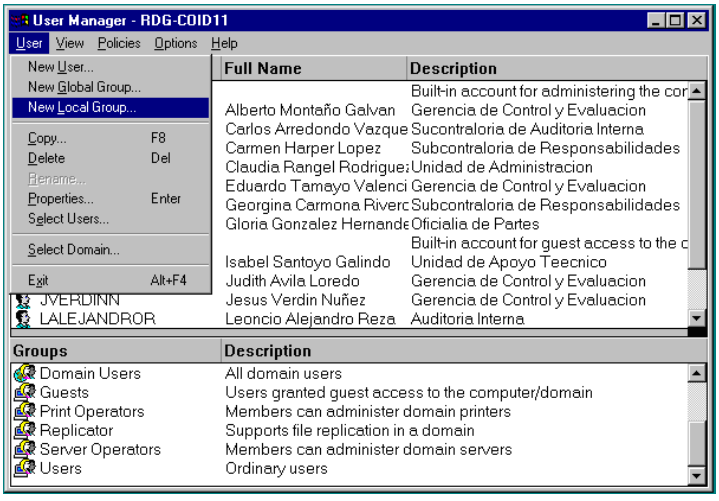


Fig. 3.1.3.h Creación del grupo RDG-COID$$$

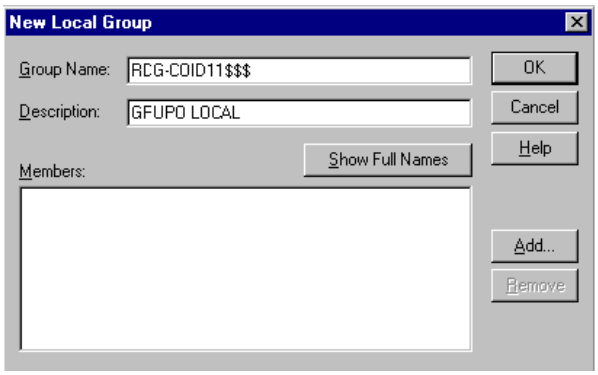


Fig. 3.1.3.i Nuevo grupo local RDG-COID$$$

Ha sido creado el grupo local RDG-COID11$$, como se puede verificar en la figura 3.1.3.j.

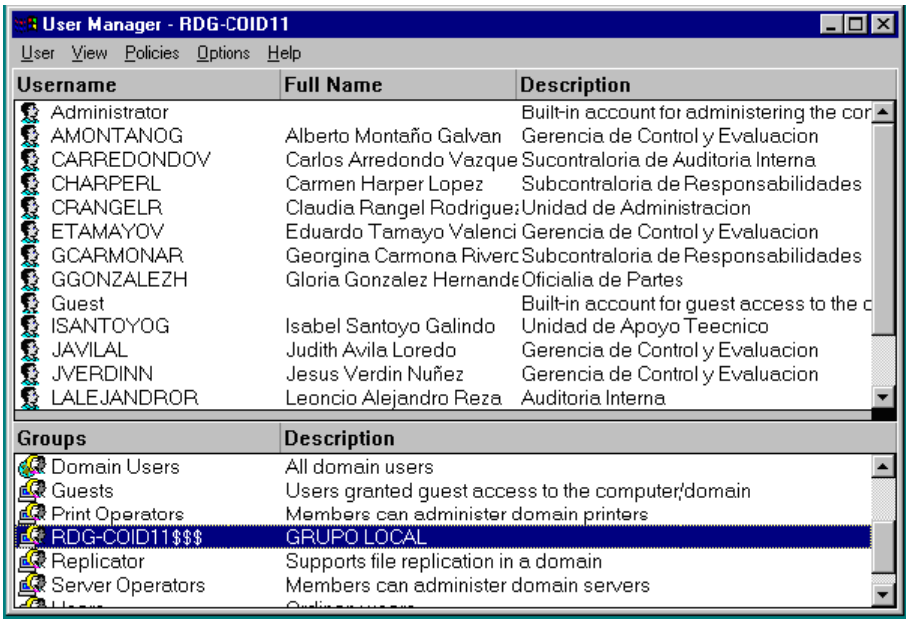


Fig. 3.1.3.j Grupo RDG-COID11$$$

c. Finalmente, habrá que verificar que en el PDC exista la siguiente llave en el ´registry´:

HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/LSA/TcipipClientSupport: REG_DWORD:0x1

Se accesa al registro desde Inicio, ejecutar del sistema operativo, se teclea regedit, visualizándose el Registry Editor, como se puede ver en la figura 3.1.3.k.

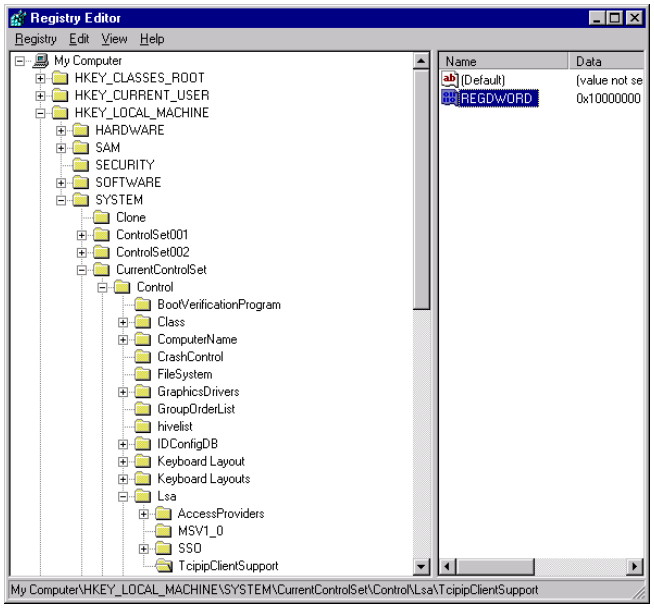


Fig. 3.1.3.k Registry editor

Con estas actividades ha quedado preparado el ambiente. El siguiente paso será instalar la herramienta Active Directory Migration Tool (ADMT), para realizar la migración de las cuentas de usuario.

3.1.4 Instalación de la herramienta Active Directory Migration Tool (ADMT)

A continuación se ejemplifica la instalación de la herramienta Active Directory Migration Tool (ADMT), para realizar la migración de las cuentas de usuario del dominio RDG-COID11 al dominio ci.ref.pemex.com.

Se ejecuta el archivo admt.exe, para iniciar la instalación de esta herramienta, siguiendo las instrucciones del asistente **"Active Directory Migration Tool Setup Wizard"**.

Se indica la ruta de instalación, en la pantalla **"Installation Folder"**, e inicia la instalación, como se muestra en la figura 3.1.4.

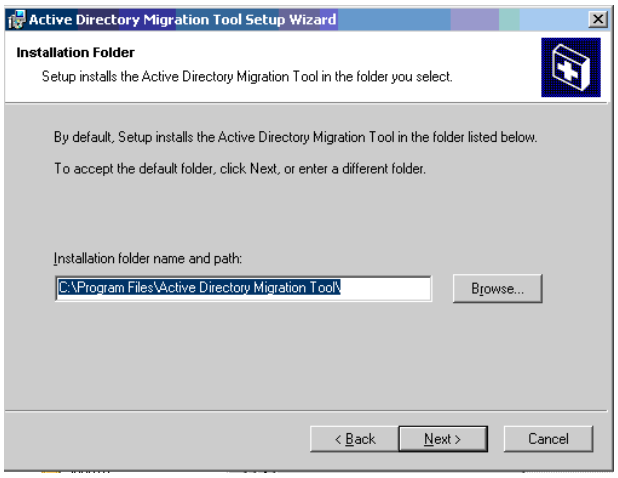


Fig. 3.1.4 Instalación de la herramienta Active Directory Migration Tool

Al tener instalada la herramienta, ya se puede realizar la migración de cuentas de usuario de un dominio a otro.

Antes de realizar la migración de las cuentas de usuario, estas fueron homologadas de acuerdo a lo establecido en el punto 2.2.2 del capítulo dos; que se refiere a los Estándares para el Alias del Usuario.

El alias o User logon name del usuario se compondrá de la siguiente manera:

a. En el caso de que el usuario cuente con un solo nombre: se toman los dos primeros caracteres, seguido del apellido paterno y el primer carácter del apellido materno.

   Ejemplo: Anabel Audelo Rodríguez será: ANAUDELOR

b. Para el caso de que el usuario cuente con dos nombres el **User logon name** se compondrá de las dos primeras letras de cada nombre, seguido del apellido paterno y el primer carácter del apellido materno.

Ejemplo: José Luis Estrada Nuñez será: **JLESTRADAN**

Habiendo realizado las actividades anteriores, hemos preparado los ambientes, en el directorio activo como en las estaciones de trabajo de cada usuario para poder migrar las cuentas de usuario al nuevo dominio.

3.1.5 Migración de cuentas de usuario

A continuación, se ejemplifica la migración de una cuenta a través del uso de la herramienta **Active Directory Migration Tool**, desde el menú **File** se elige la opción "**User Account Migration Wizard**", como se muestra en la figura 3.1.5.a.

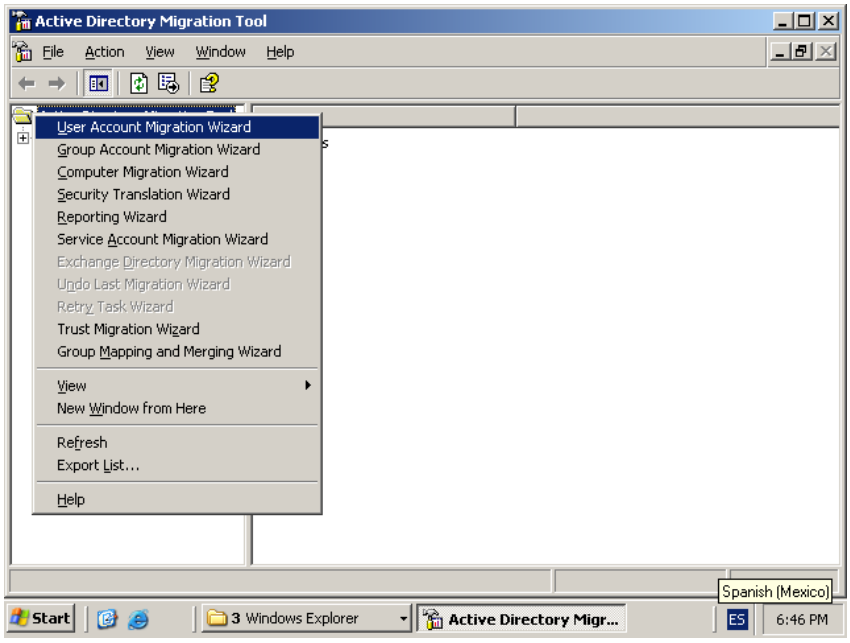


Fig. 3.1.5.a Herramienta Active Directory Migration Tool

Se abre un asistente, a través del cual se migrarán las cuentas de usuario. Como se muestra en la figura 3.1.5.b **"Domain Selection",** se especifica el dominio **origen** (*Source Domain*) y el dominio **fuente** (*Target domain*).

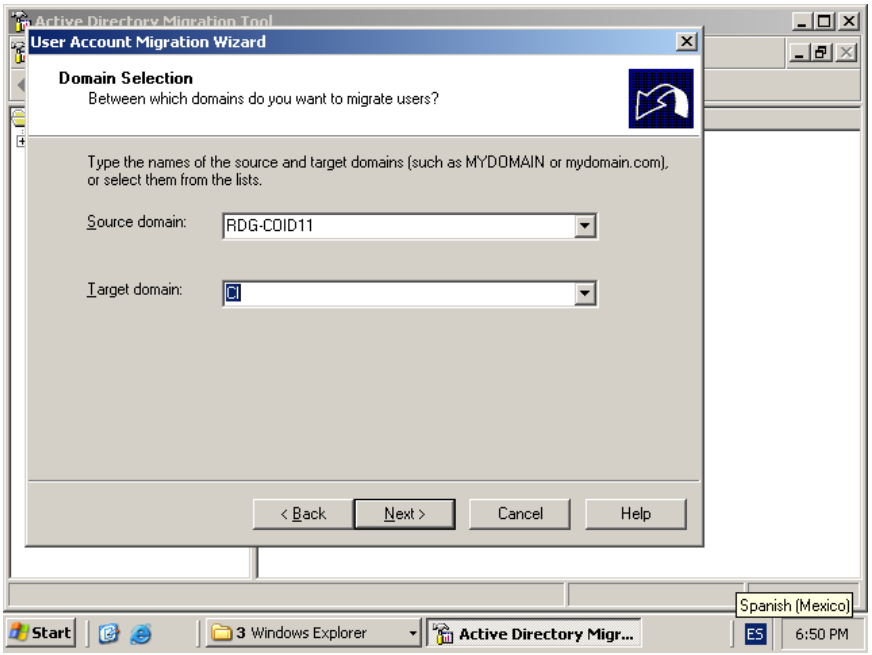


Fig. 3.1.5.b Domain Selection

A continuación, en la pantalla **"User Selection"**, se agregan las cuentas de los usuarios a migrar. Se podrá seleccionar un usuario o grupo de usuarios. Como se muestra en la figura 3.1.5.c, donde se ha seleccionado un usuario.

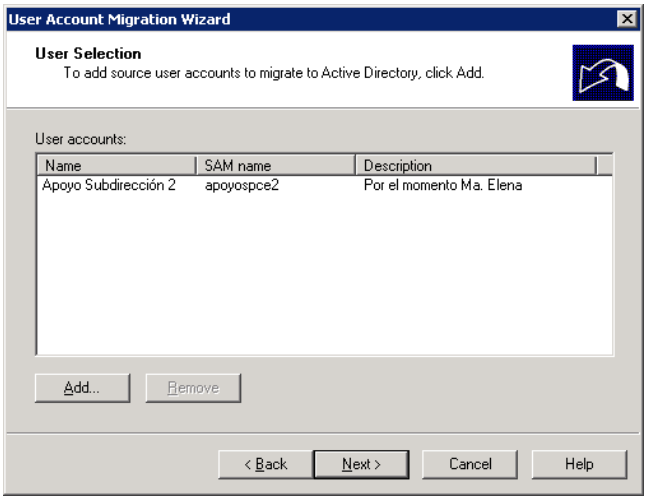


Fig. 3.1.5.c Migración de un usuario

El siguiente paso será indicar en la ventana **"Organizacional Unit Selection"**, la Unidad Organizacional o Target OU, a donde se copiaran las cuentas de usuario, se selecciona la **OU de CI Users,** como se indica en la figura 3.1.5.d. selección de la unidad organizacional.

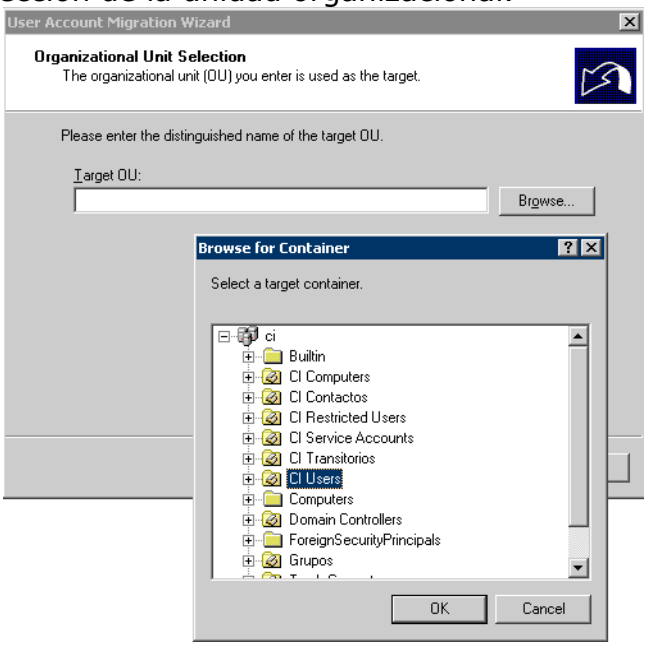


Fig. 3.1.5.d Selección de la unidad organizacional

A continuación, se despliega la ruta LDAP, para el contenedor CI Users, se toman los valores dados por default.

En la figura 3.1.5.e **"User Options",** se muestran algunas opciones de configuración para la migración de cuentas de usuario, para el caso que aplica se toman las predeterminadas por default.

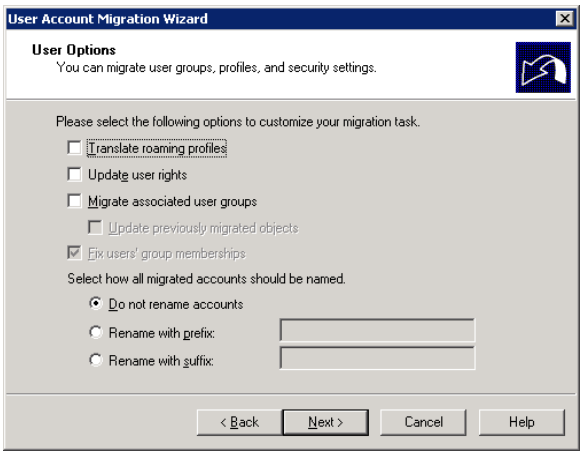


Fig. 3.1.5.e User Options

En la figura 3.1.5.f **"Naming Conflicts",** se selecciona la opción *Ignore conflicting accounts and don´t migrate.* Lo que indica que al migrar una cuenta de usuario, se detecta algún conflicto, no se migrara dicha cuenta.

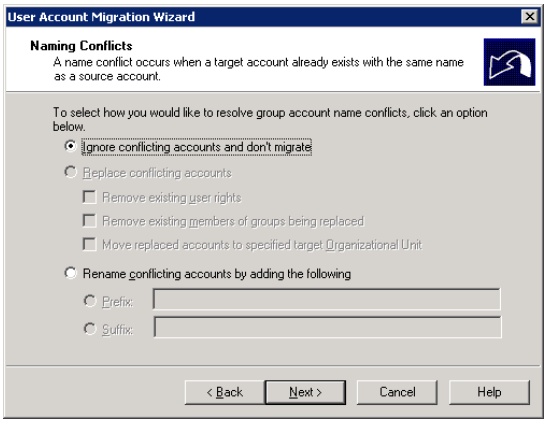


Fig. 3.1.5.f Naming Conflicts

Al finalizar se muestra el resumen de las cuentas migradas. Como se muestra en la figura 3.1.5.g **"Migration Progress"**, donde se muestra el progreso de migración y el detalle del proceso: el número de cuentas de usuario que se copiaron correctamente y las cuentas que generaron error. En caso de que se haya generado un error, se podrá verificar el detalle visualizando el log, en la opción "View Log".

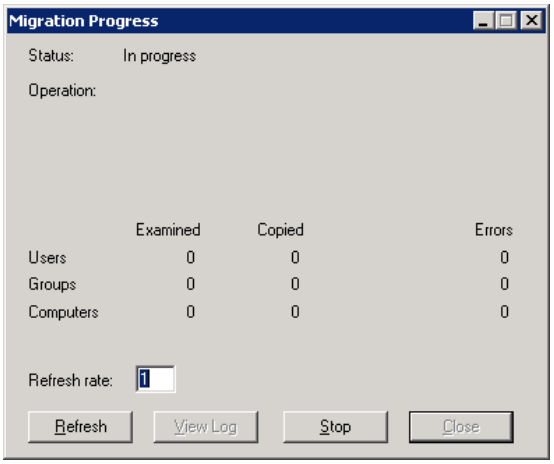


Fig. 3.1.5.g Migration Progress

3.1.6 Estabilización de las cuentas de usuario

Después de haber migrado las cuentas de usuario, se realizaron las siguientes actividades las cuales se detallan a continuación, desde la aplicación **"Active Directory Users and Computers"**.

a. Mapear la unidad donde se encuentra el archivo ofcscan.bat. Donde se especifica la ruta donde se encuentra instalada la aplicación antivirus.
b. Complementar los datos adicionales para cada una de las cuentas de usuario.

a. Mapeo de la ruta de la aplicación Antivirus

Para mapear la ruta de la aplicación antivirus. Se accesa a la cuenta de un usuario desde la aplicación **"Active Directory Users and Computers"**. Y se elige la ficha de **"Profile",** para el caso que aplica se define el archivo **Ofcscan.bat** en el parámetro de Logon script, como se muestra en la figura 3.1.6.a. Este archivo .bat se tendrá que definir para todas las cuentas de usuario existentes en el directorio activo.

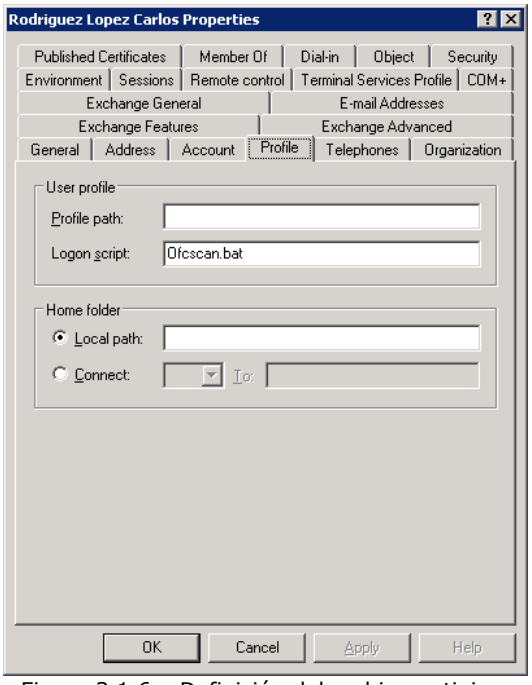


Figura 3.1.6.a Definición del archivo antivirus

Este archivo se colocó previamente en la siguiente ruta: **C:\Windows\Sysvol\Domain\Scripts,** el cual contiene la ruta y el archivo de ejecución, como se muestra en la figura 3.1.6.b.

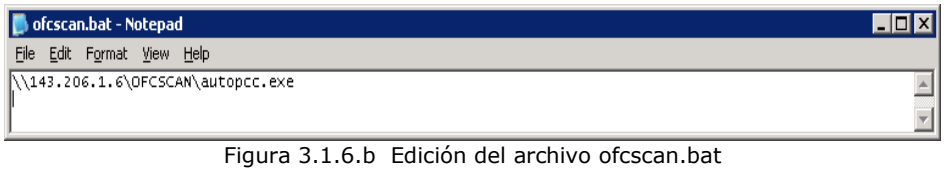


Figura 3.1.6.b Edición del archivo ofcscan.bat

b. Complementar los datos adicionales de la cuenta de usuario

Los datos adicionales a complementar, se agregan de acuerdo a los estándares definidos en el capítulo dos. Como ejemplo, se muestran a continuación las figuras 3.1.6.c, 3.1.6.d y 3.1.6.f referentes a las fichas **"General, Address y Organization"** respectivamente.

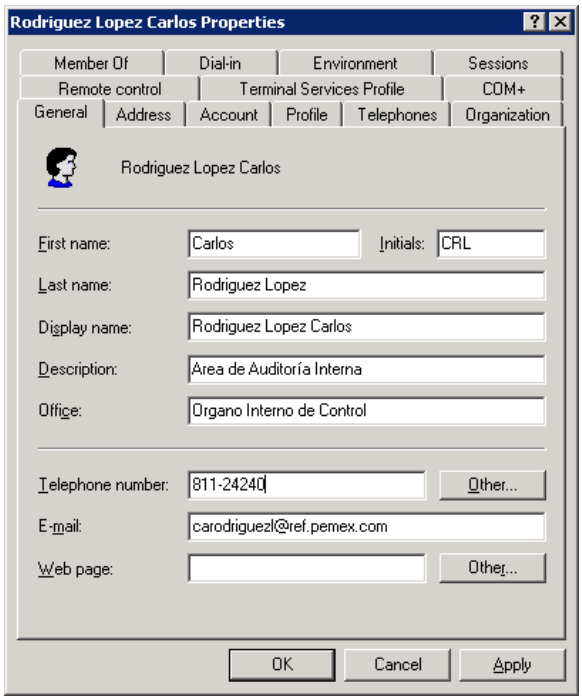


Figura 3.1.6.c Ficha de datos de usuario General

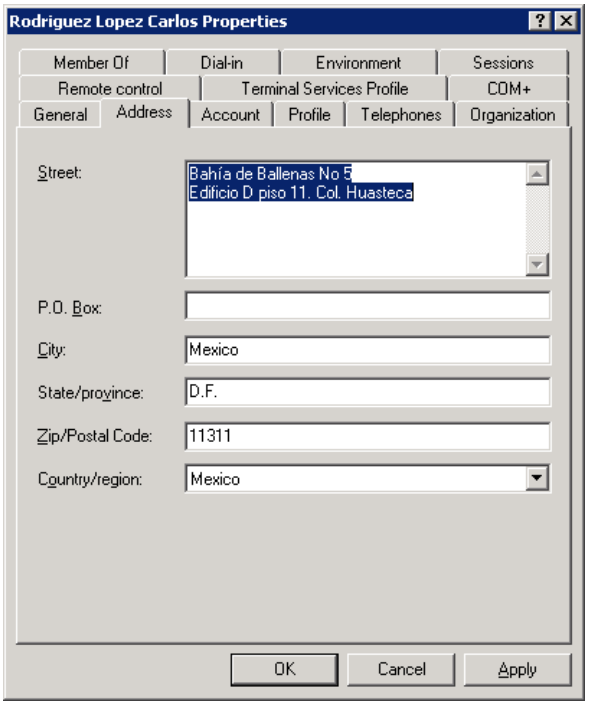


Figura 3.1.6.d Ficha de datos de usuario Address

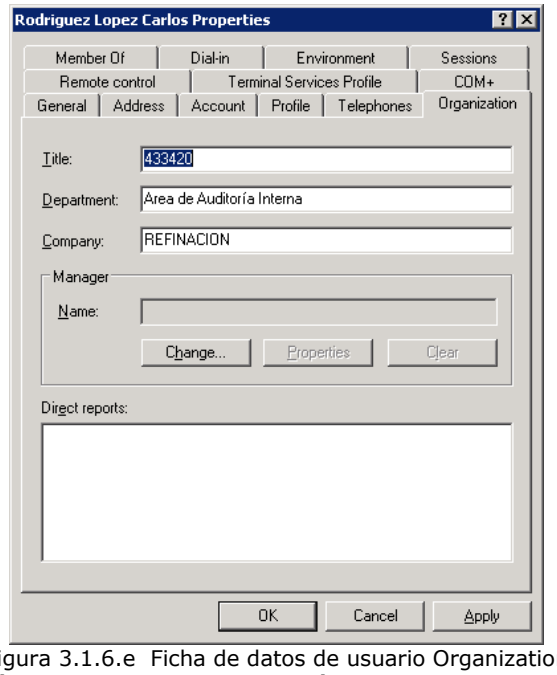


Figura 3.1.6.e Ficha de datos de usuario Organization

El último paso, será realizar la migración de las estaciones de trabajo al dominio CI.

3.1.7. Migración de las estaciones de trabajo al dominio CI

La siguiente actividad, fue migrar cada una de las estaciones de trabajo al nuevo dominio. Se describe a continuación, un ejemplo para un equipo.

1. Iniciar sesión como Administrador local del equipo. Dar clic derecho sobre el icono Mi PC o My Computer y verificar mediante la opción *Administrar o Manage*, lo siguiente:

   a. Que se encuentren los recursos compartidos IPC$ y ADMIN$, como se muestra en la figura 3.1.7.a. desde la opción Recursos compartidos.

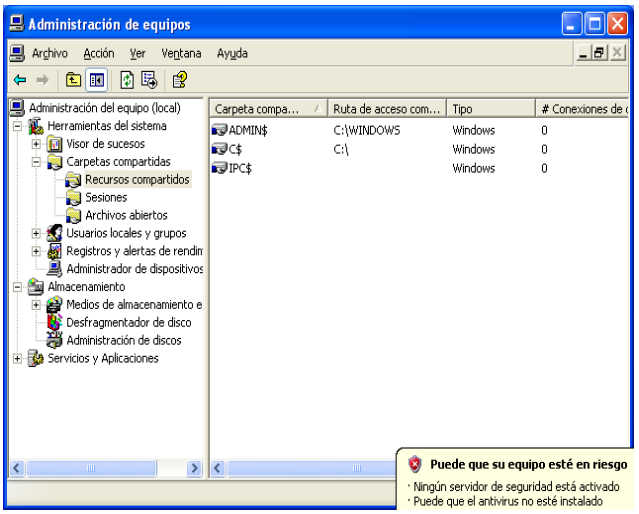


Fig. 3.1.7.a Verificación de recursos compartidos

   b. Que se estén ejecutando los servicios Netlogon, Remote Procedure Call (RPC), Server y Workstation, desde la opción Servicios, como se muestra en la figura 3.1.7.b.

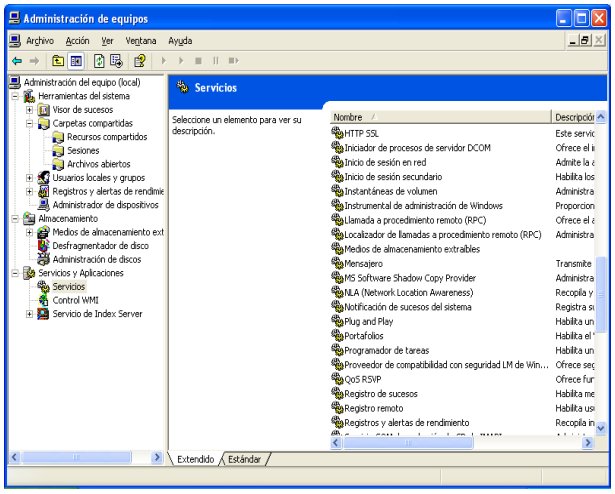


Fig. 3.1.7.b Ejecución de servicios

2. Desde las propiedades de Conexión de área local en Protocolo Internet TCP/IP: Verificar que el DNS y WINS primario sean los respectivos para el dominio, como se visualiza en la figura 3.1.7.c y 3.1.7.d respectivamente.

Si no se encuentran definidas las configuraciones, se realizó lo siguiente:

Desde la pantalla **"Configuración avanzada de TCP/IP"**, en la ficha **DNS**.

1. Habilitar la opción Anexar sufijos DNS principales y de conexiones específicas y activar Anexar sufijos primarios del sufijo DNS principal.
2. Registrar estas direcciones de conexiones en DNS y, utilizar el sufijo ci.ref.pemex.com en el Sufijo DNS para esta conexión.

En la ficha de **WINS**.

1. Agregar la dirección del servidor WINS.
2. Deshabilitar la casilla ´Habilitar la búsqueda de LMHOSTS´.
3. Elegir la opción Predeterminada para la Configuración de NetBIOS.

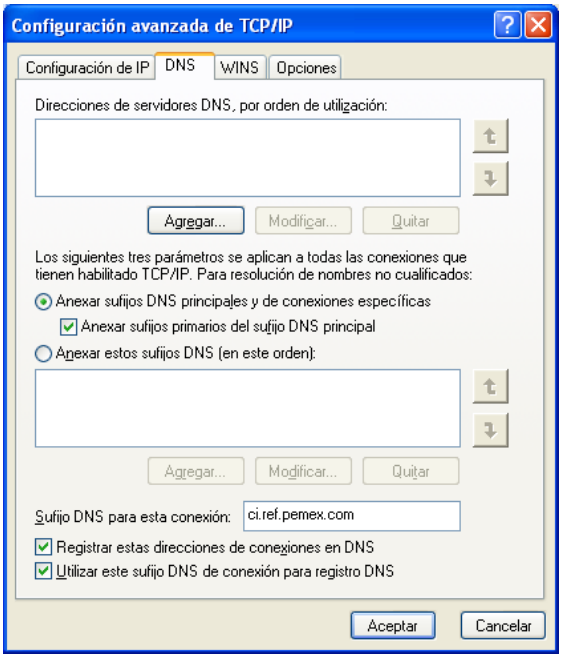


Fig. 3.1.7.c Verificación de DNS

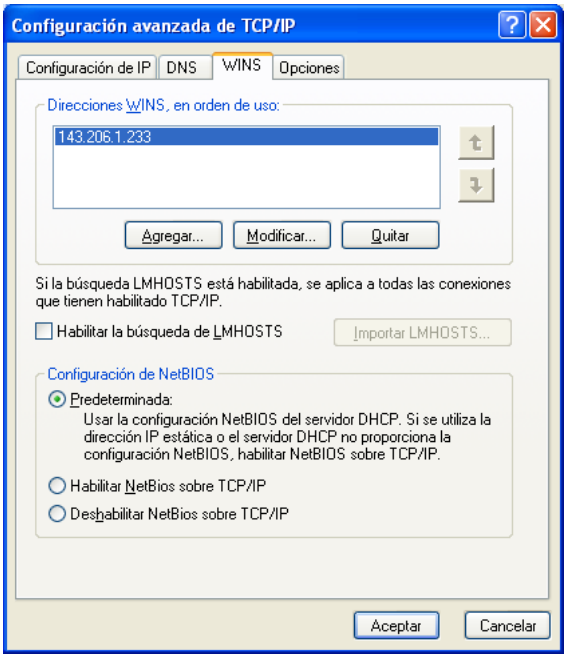


Fig. 3.1.7.d Verificación de WINS

3. Unión al dominio CI. El migrar el equipo al dominio CI, implica una serie de actividades que se explican a continuación:

a. Verificar nombre de equipo homologado
b. Unión del equipo al dominio CI
c. Perfil de usuario homologado
d. Copia de perfil de usuario

Nota: Estas actividades, se realizarán con el usuario de *administrador local*.

a. Verificar nombre de equipo homologado

Desde **Propiedades de mi PC**. Se verificara que el nombre de equipo corresponda a los estándares definidos para nombre de computadora, que se explicó en el punto 2.2.3 del capítulo dos. Como se visualiza en la figura 3.1.7.e.

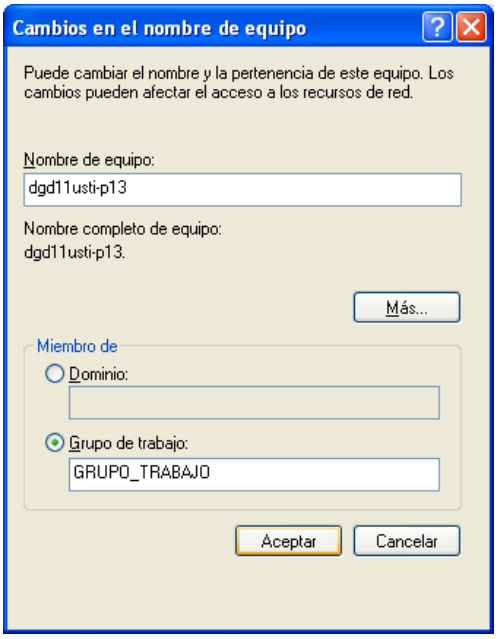


Fig. 3.1.7.e Nombre de equipo

b. Unión del equipo al dominio CI

El siguiente paso, será unir el equipo al dominio CI. Desde **Propiedades de mi PC**. Especificar el dominio CI, en la opción **"Miembro de"**, en **Dominio**, como se muestra en la figura 3.1.7.f.

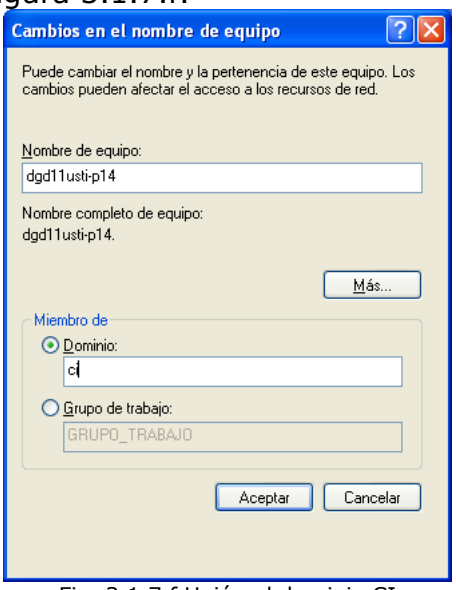


Fig. 3.1.7.f Unión al dominio CI

Al unir el equipo al nuevo dominio ó asignarle un nuevo nombre de equipo, este se reinicia.

c. Perfil de usuario homologado

A continuación se creó el **Perfil de Usuario,** configurándolo de la siguiente manera: desde la ficha **Opciones Avanzadas – Perfiles de Usuario – Configuración,** figura 3.1.7.g.

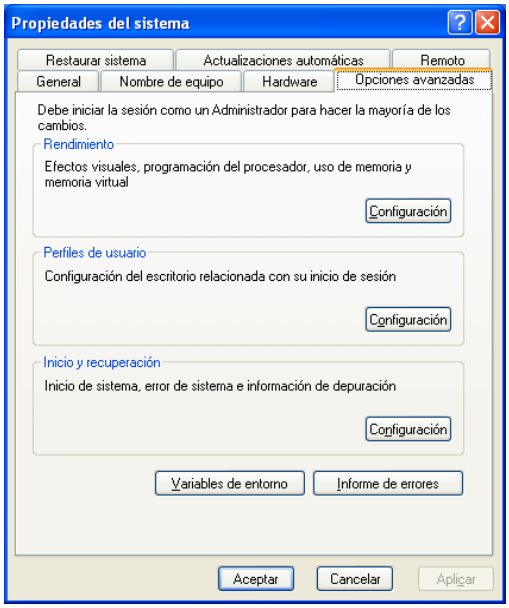


Fig. 3.1.7.g Perfil de usuario

Se elige la opción "**Cuentas de usuario"**, para crear la nueva cuenta, como se indica en la figura 3.1.7.h.

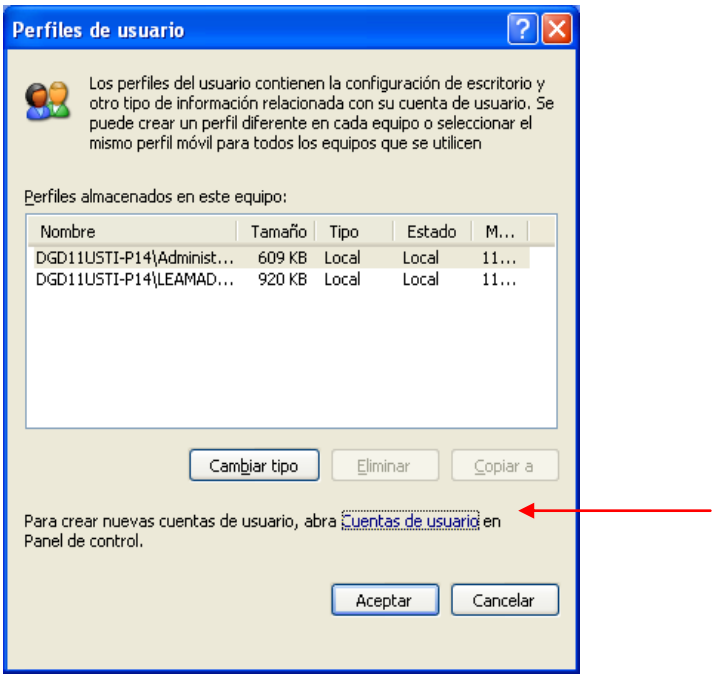


Fig. 3.1.7.h Cuentas de usuario

A continuación se da clic en **Agregar.** Se especifica la nueva cuenta de usuario homologada y en dominio, se especifica CI, como se muestra en la figura 3.1.7.i.

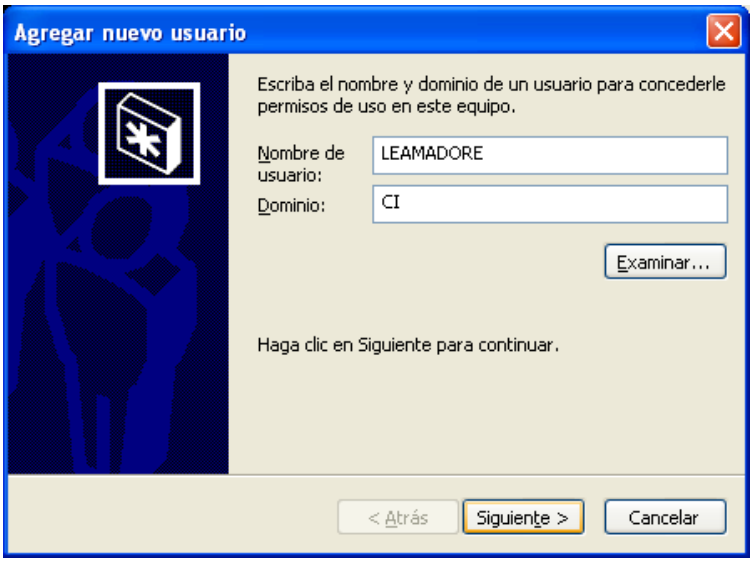


Fig. 3.1.7.i Nombre de usuario y dominio

En la figura 3.1.7.j, se muestra el nivel de acceso definido para el usuario el cual fue: **Otros**, como **Administrador.**

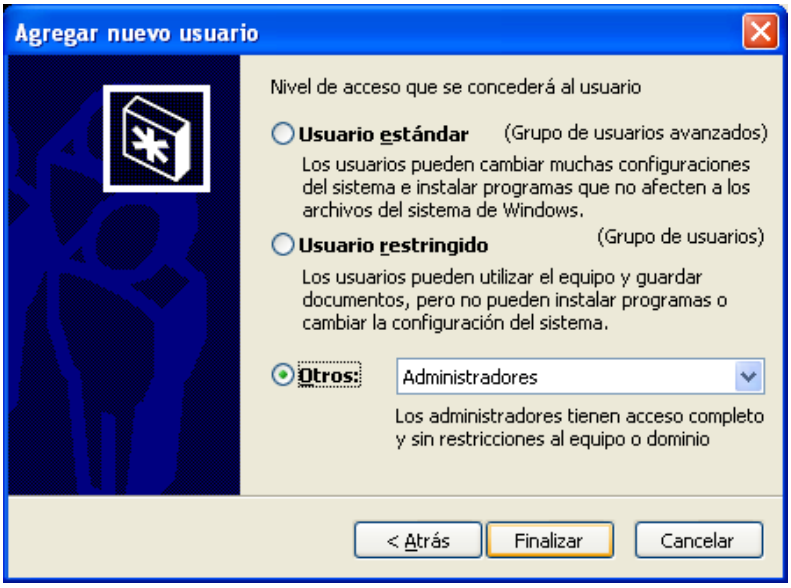


Fig. 3.1.7.j Nivel de acceso

d. Copia del perfil de usuario

Finalmente, se realizó la copia del perfil anterior al nuevo perfil (el perfil de usuario guarda las configuraciones de escritorio y aplicaciones). A continuación se detalla.

La copia se realiza accesando al equipo como Administrador local. Accesando a **Perfiles de usuario**, desde las **Propiedades de Mi PC** Se sombrea el usuario **(Perfil de origen)** y se elige **Copiar a:.** Como se puede ver en la figura 3.1.7.k.

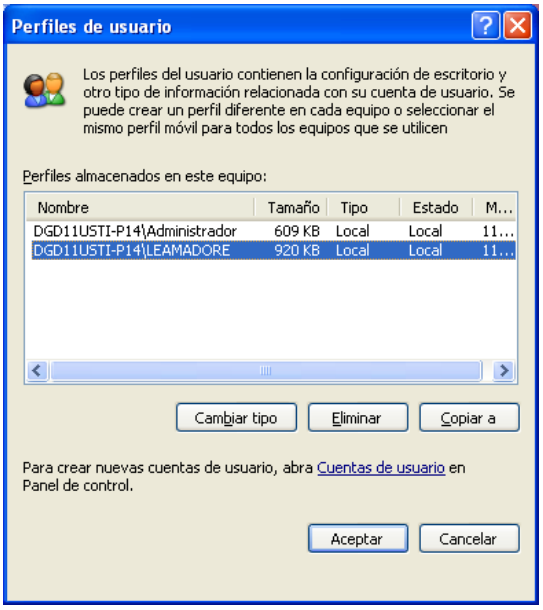


Fig. 3.1.7.k Copia de perfil

Se despliega la pantalla **"Copiar a",** indicando el nuevo perfil de usuario a copiar, que se encuentra dentro de **Documents and Settings**, como se visualiza en la figura 3.1.7.l.

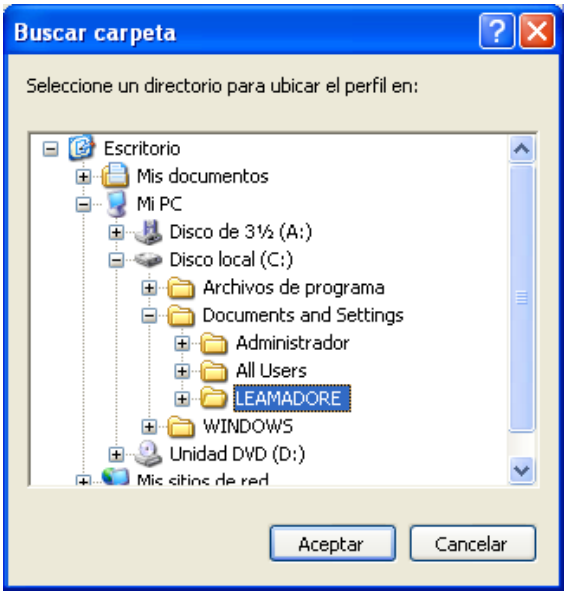


Fig. 3.1.7.l Ruta del perfil de usuario

Indicando la ruta del perfil fuente, a continuación se despliega una pantalla, la cual se confirma.

Por último, se accesara al equipo con el nuevo usuario homologado en el dominio CI. Con lo cual, han quedado realizadas todas las tareas de migración.

Capítulo IV. Estabilización del Servicio de Directorio Activo

4.1 Plan de Estabilización

Una vez que se concreto la migración del directorio activo, se aplicó un plan de estabilización, con la finalidad de: corregir y/o actualizar algunas inconsistencias en la información; las cuales pudieran generar problemas en los servicios que proporciona el directorio activo.

Adicionalmente, se definieron una serie de tareas de revisión periódica del directorio activo. Finalmente, se explican algunas herramientas de diagnóstico para la revisión de un controlador de dominio.

A continuación: se describen las actividades que se llevaran a cabo en el plan de estabilización para el dominio CI.

1. Controladores de dominio actualizados, con el último service pack, actualizaciones críticas y actualizaciones de seguridad
2. Roles de dominio y catálogo global consistentes
3. Configuración de red consistente
4. Atributos consistentes en cuentas de usuario
5. Administración de unidades organizacionales
6. Aplicación de políticas de grupo
7. Consolidación con otras aplicaciones
8. Herramientas de diagnóstico para un controlador de dominio

4.1.1. Controladores de dominio actualizados con el último service pack, actualizaciones críticas y actualizaciones de seguridad

Este punto es importante ya que se debe mantener actualizado el sistema operativo, con el fin de lograr estabilidad y seguridad del mismo. Esta es una tarea que realizar periódicamente.

Al inicio de la implementación del dominio, las actualizaciones se realizaron de manera manual; conectándose al Centro de actualizaciones de Microsoft Windows Update; después se implemento la aplicación WSUS (Windows Service Update Software) a través de las *políticas de grupo* (las cuales se explican en el punto 4.1.6), para realizar dichas actualizaciones tanto en clientes como en servidores. En la figura 4.1.1 se muestran algunas actualizaciones ya instaladas para Windows Server 2003.

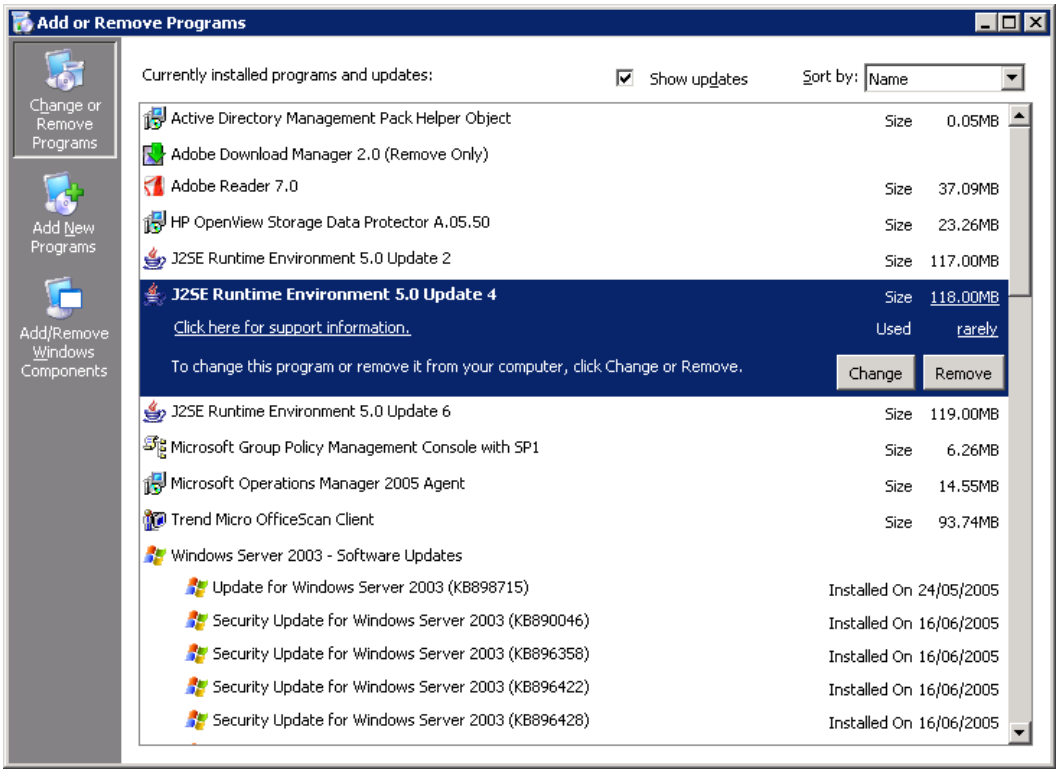
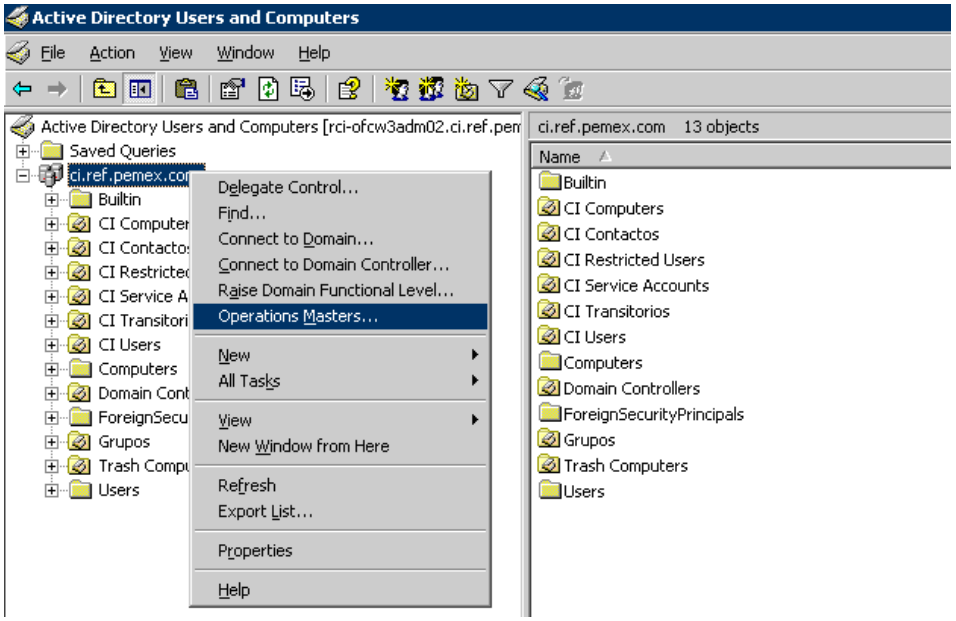


Fig. 4.1.1 Actualizaciones de Windows Server 2003

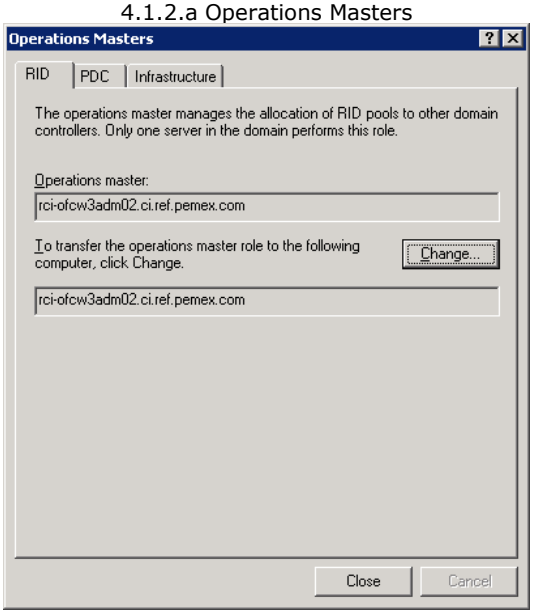
4.1.2. Roles de dominio y catálogo global consistentes

Como se explicó en el capítulo dos, en el apartado 2.3.3 Estructura física del directorio activo, en el punto sobre operaciones maestras del dominio. Cada dominio en el bosque tiene su propio DC con los roles: PDC emulator, RID master e Infraestructure master. Además de la asignación de catálogo global.

A continuación, se muestra como es asignado un rol. Desde la herramienta **"Active Directory Users and Computers",** se elige el dominio y desde **"Operations Masters"**; se asignan los roles a los DC existentes. A continuación se muestra en la figura 4.1.2.a y 4.1.2.b la asignación del rol RID, al DC rci-ofcw3adm02.



4.1.2.a Operations Masters



4.1.2.b Asignación del rol RID

Para el caso, de el GC (catálogo global), este se asigna desde la aplicación **"Active Directory Sites and Services"**. Se elige el site correspondiente, se elige el controlador al cual se asignará la función. Como se muestra en la figura 4.1.2.c.

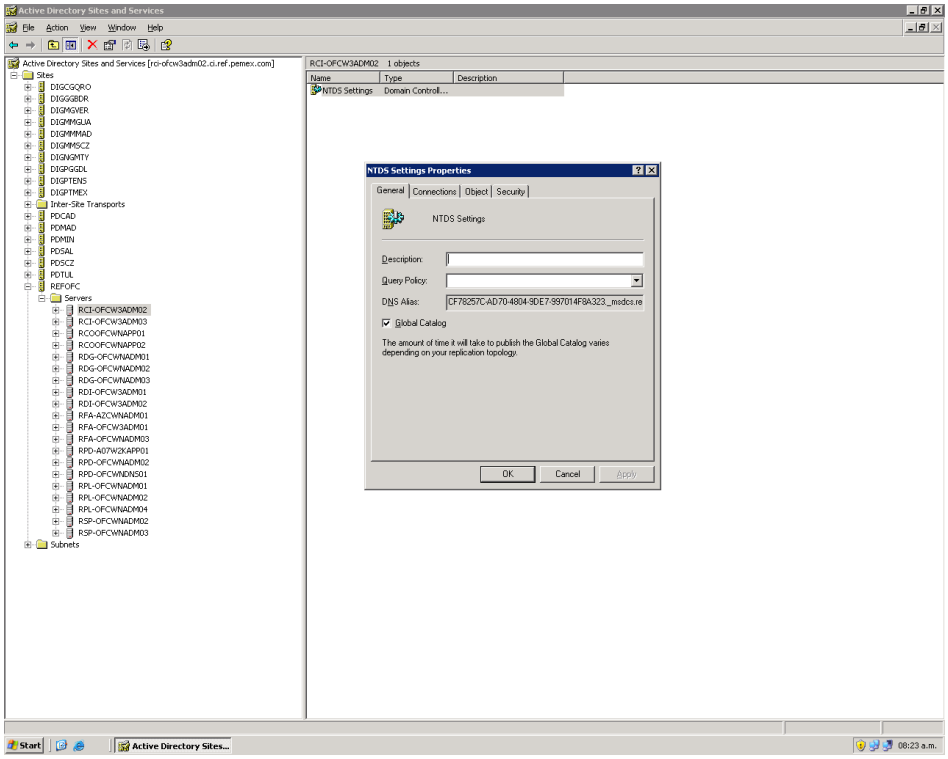


Fig. 4.1.2.c Asignación del catálogo global

4.1.3. Configuración de red consistente – DNS, DHCP

DNS

Como se explicó anteriormente, el servicio DNS es el cimiento del AD; ya que es el encargado de realizar la resolución de nombres de una máquina a una dirección IP y viceversa. Las estaciones de trabajo accesan a esta información para consultar e interactuar con el AD. Se realizan validaciones, búsquedas y consultas.

Para homologar las configuraciones de red en los estaciones de trabajo o clientes, se creó un script .vbs; que se ejecutó en el archivo de inicio de sesión de los clientes. A través de la ejecución del script, se evita, el homologar las configuraciones de red en los clientes de forma manual en cada una de las estaciones de trabajo. A continuación, se muestra en la figura 4.1.3.a parte de este archivo.

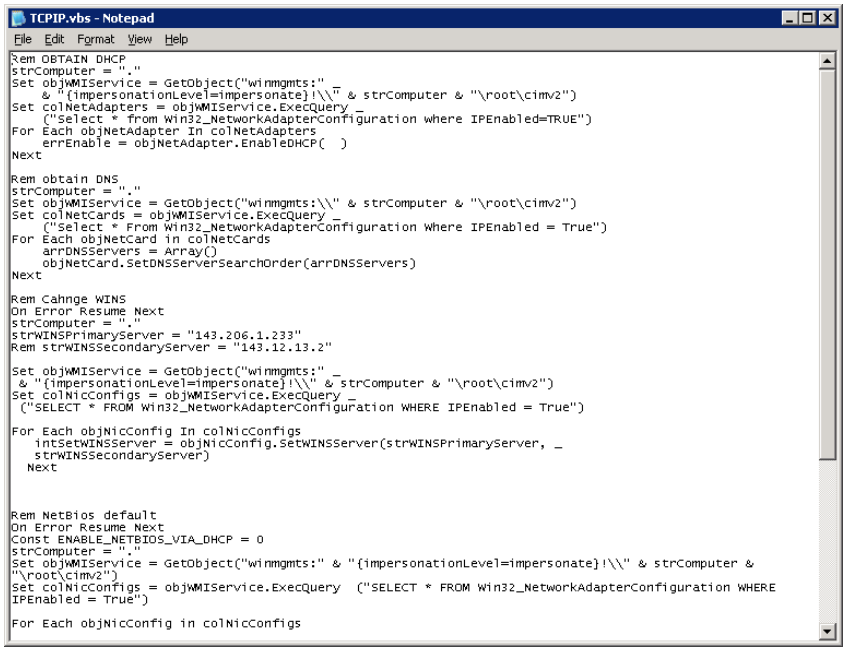


Fig. 4.1.3.a Script para homologar configuraciones de red

DHCP

Inicialmente, las direcciones I.P. eran estáticas, después se implementó el Servicio DHCP, asignando direcciones dinámicas.

Por lo tanto, desde el DHCP, se asignarón los valores para los DNS. Como se muestra en la figura 4.1.3.b.

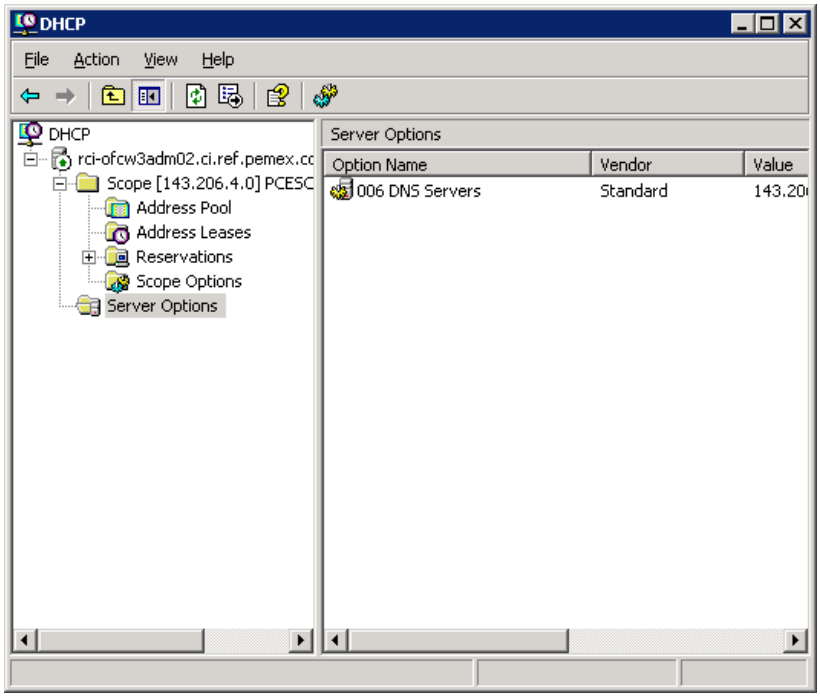


Fig. 4.1.3.b Configuración de DNS en el DHCP

4.1.4 Atributos consistentes en cuentas de usuario

Este punto se refiere a complementar información adicional que no se migró durante la implementación del directorio activo. Sin embargo, dicha información es importante para la implementación de otras aplicaciones; como para el servicio de Mensajería (Microsoft Exchange).

Por ejemplo, la tabla 4.1.4 muestra la homologación del atributo *Company*, el cual tendrá que capturarse como: REFINACIÓN, ya que al inicio de la migración del directorio activo; aunque se encontraba definido el valor como "*refinación"*; este valor no fue homogéneo; esto quiere decir, que podía capturarse como: *Refinación, refinación, Refinación ó REFINACIÓN.*

Tabla 4.1.4 Homologación de atributos

Valores para el atributo "Company"	Valores para el atributo "Office"
REFINACION	Dirección General Contraloría Interna Finanzas y Administración Almacenamiento y Distribución Comercial Planeación Producción SASIPA

La modificación de estos atributos, se realizo a través de scripts. Estas líneas de código se guardaron en un archivo .vbs. El cual se ejecutó desde el controlador de dominio.

El script se ejecuta una sola vez, lo cual da como resultado la modificación para todos los usuarios del dominio; en vez de cambiar los atributos para cada uno de ellos de forma manual.

```
Dim Container
        strPath="OU=CI Users and Groups,DC=ci,DC=ref,DC=pemex,DC=com"
        Set Container=GetObject("LDAP://" & strPath & "")
        ModifyUsers Container
        Set Container = Nothing
        WScript.Echo "Finished"
        Sub ModifyUsers(Object)
        Dim User
        Object.Filter = Array("User")
        For Each User in Object
        User.Put "Company","REFINACION"
        User.Put "physicalDeliveryOfficeName","Órgano Interno de Control"
                User.Put "department", ""
        User.Put "streetAddress","Bahía de Ballenas No. 5, Edificio D, Piso 11, Col. Huasteca"
        User.Put "l","México"
        User.Put "st","D.F."
        User.Put "postalCode","11311"
        User.Put "c","MX"
                User.SetInfo
        Next
```

Por ejemplo, lo que se encuentra marcado en el script en rojo, son atributos que se encuentran homologados, la figura 4.1.4 muestra como se visualizan estos atributos en el directorio activo, después de haberse ejecutado el script.

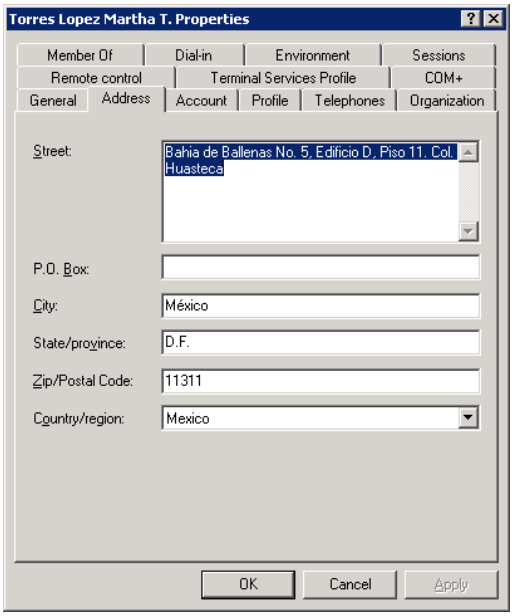


Fig. 4.1.4 Atributos homologados en el directorio activo

4.1.5 Administración de unidades organizacionales

Las unidades organizacionales, sirven para organizar objetos dentro del dominio. Así como, se pueden ordenar objetos en base a su área geográfica, de negocios o en clases simples como: usuarios, computadoras e impresoras. Con el objetivo de hacer más sencillo localizar y administrar objetos.

Para el dominio ci.ref.pemex.com, se crearon seis contenedores, que se muestran a continuación en la figura 4.1.5.a.

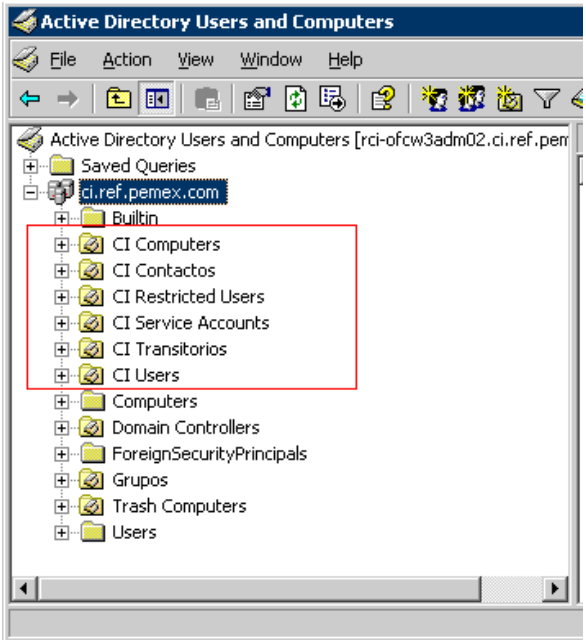


Fig. 4.1.5.a Unidades organizacionales

En la Unidad organizacional CI Computers, se encuentran los objetos referentes a cuentas de computadoras, dentro de este contenedor, se crearon tres contenedores más, para organizar los objetos por tipo de computadora; por ejemplo: desktops, laptops y servers, como se muestra en la figura 4.1.5.b.

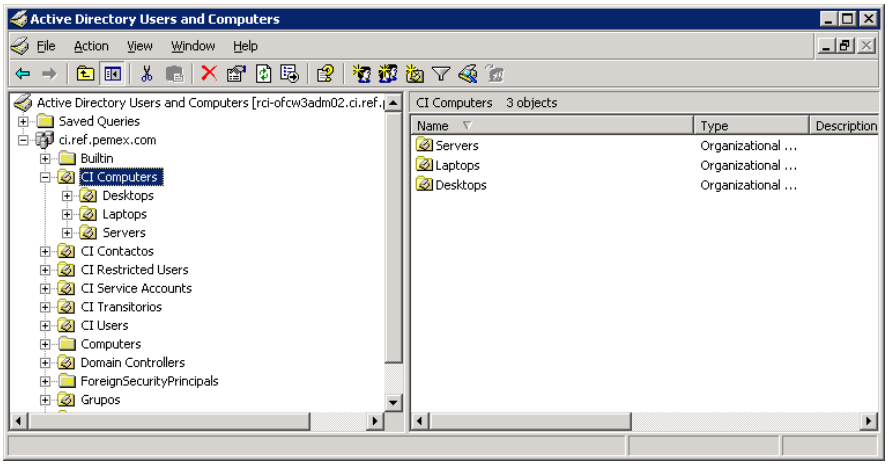


Fig. 4.1.5.b Unidad organización CI Computers

En el caso de las unidades organizacionales relacionadas con las cuentas de usuario, se definieron los contenedores Ci Users y CI Transitorios, la diferencia entre ambos es que en CI Transitorios, únicamente contiene cuentas de usuarios temporales.

Es importante mencionar, que el contenedor CI Users, replica para ser mostrado en la lista global de correo de Pemex. En la figura 4.1.5 se muestran las cuentas de usuario contenidas dentro de la unidad organizacional de CI Users.

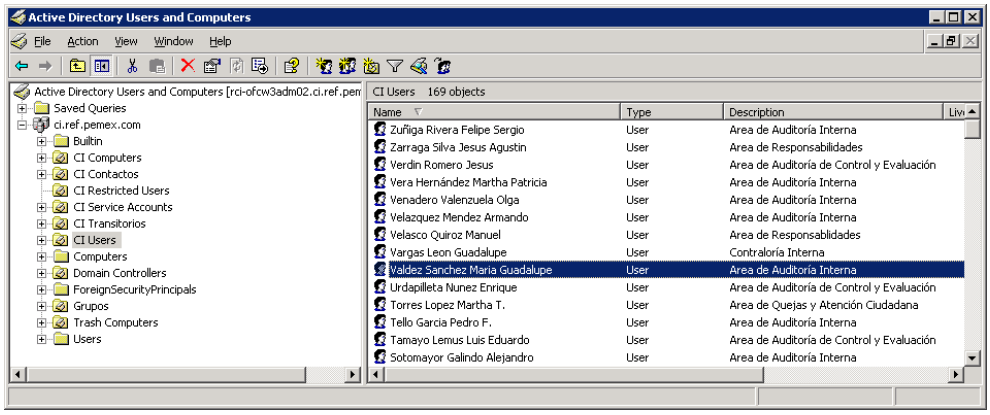


Fig. 4.1.5.c Unidad organizacional CI Users

Trash Computer

Como parte de administración del directorio activo y para evitar que este tenga objetos que no son utilizados mensualmente se ejecuta el archivo moveoldcomputers.vbs; el cual es un script que bloquea aquellas cuentas de equipos que no han sido accesados en 45 días y que pueden ser eliminados definitivamente del directorio activo. Esta actividad permite realizar una depuración de los objetos computadoras y mantener solo los objetos que deben de estar registrados.

A continuación, se presenta el script el cual verifica los objetos computadoras que no han sido utilizados en cuarenta y cinco días, moviéndolos a la unidad organizacional Trash Computers.

moveoldcomputers.vbs - Notepad

File Edit Format View Help

```
' Enumerate all computers and determine which are inactive.
Set objRecordSet = objCommand.Execute
Do Until objRecordSet.EOF
  strComputerDN = objRecordSet.Fields("distinguishedName")
  intTotal = intTotal + 1
  ' Determine date when password last set.
  lngDate = objRecordSet.Fields("pwdLastSet")
  Set objDate = lngDate
  dtmPwdLastSet = Integer8Date(objDate, lngBias)
  ' Check if computer object inactive.
  If DateDiff("d", dtmPwdLastSet, Now) > intDays Then
    ' Computer object inactive.
    intInactive = intInactive + 1
    objFile.WriteLine "Inactive: " & strComputerDN _
      & " - password last set: " & dtmPwdLastSet
    ' Move computer object to the target OU.
    On Error Resume Next
    Set objComputer = objTargetOU.MoveHere("LDAP://" _
      & strComputerDN, vbNullString)
    If Err.Number <> 0 Then
      On Error GoTo 0
      intNotMoved = intNotMoved + 1
      objFile.WriteLine "Cannot move: " & strComputerDN
    End If
    ' Disable the computer account.
    On Error Resume Next
    objComputer.AccountDisabled = True
    ' Save changes to Active Directory.
    objComputer.SetInfo
    If Err.Number <> 0 Then
      On Error GoTo 0
      intNotDisabled = intNotDisabled + 1
      objFile.WriteLine "Cannot disable: " & strComputerDN
    End If
    On Error GoTo 0
  End If
  objRecordSet.MoveNext
Loop

' Write totals to log file.
objFile.WriteLine "Finished: " & Now
objFile.WriteLine "Total computer objects found:   " & intTotal
objFile.WriteLine "Inactive:                       " & intInactive
objFile.WriteLine "Inactive accounts not moved:    " & intNotMoved
objFile.WriteLine "Inactive accounts not disabled: " & intNotDisabled
objFile.WriteLine "-----------------------------------------------"

' Display summary.
Wscript.Echo "Computer objects found:         " & intTotal
Wscript.Echo "Inactive:                       " & intInactive
Wscript.Echo "Inactive accounts not moved:    " & intNotMoved
Wscript.Echo "Inactive accounts not disabled: " & intNotDisabled
Wscript.Echo "See log file: " & strFilePath

' Clean up.
objFile.Close
objConnection.Close
Set objFile = Nothing
Set objFSO = Nothing
Set objShell = Nothing
Set objConnection = Nothing
Set objCommand = Nothing
Set objRootDSE = Nothing
Set objRecordSet = Nothing
Set objComputer = Nothing

Wscript.Echo "Done"

Function Integer8Date(objDate, lngBias)
' Function to convert Integer8 (64-bit) value to a date, adjusted for
' time zone bias.
  Dim lngAdjust, lngDate, lngHigh, lngLow
  lngAdjust = lngBias
  lngHigh = objDate.HighPart
  lngLow = objDate.LowPart
' Account for bug in IADsLargeInteger property methods.
  If (lngHigh = 0) And (lngLow = 0) Then
    lngAdjust = 0
  End If
  lngDate = #1/1/1601# + (((lngHigh * (2 ^ 32)) _
    + lngLow) / 600000000 - lngAdjust) / 1440
  Integer8Date = CDate(lngDate)
End Function
```

Después de ejecutar el script, se revisa la unidad organizacional Trash Computers; todos los equipos que cumplieron con los cuarenta y cinco días de no acceso se encuentran marcados con un círculo rojo, como se visualiza en la figura 4.1.5.d., realizar esta depuración ayuda a no tener almacenada *"basura"* en el directorio activo.

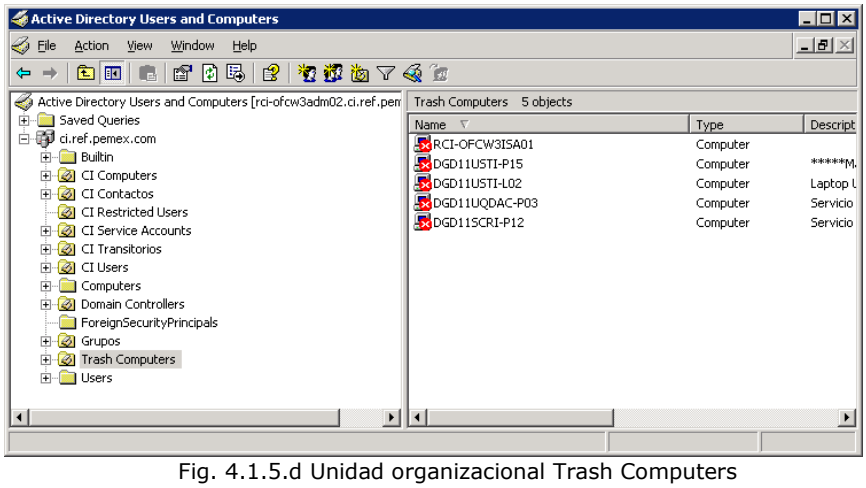


Fig. 4.1.5.d Unidad organizacional Trash Computers

4.1.6 Aplicación de políticas de grupo

Como se explicó anteriormente, el ámbito de un grupo determina las personas que pueden pertenecer a él y dónde se pueden utilizar estos grupos en la red. Existen dos tipos de grupos: de distribución y de seguridad.

La función de los grupos de distribución es: distribuir a todos los miembros del grupo los mensajes con las aplicaciones de correo electrónico.

Los grupos de seguridad se utilizan para conceder o denegar el acceso y los permisos a grupos de usuarios, en lugar de hacerlo a usuarios individuales.

A continuación se explican algunos tipos de grupos, utilizados en el dominio ci.ref.pemex.com, como se muestra en la figura 4.1.6.a

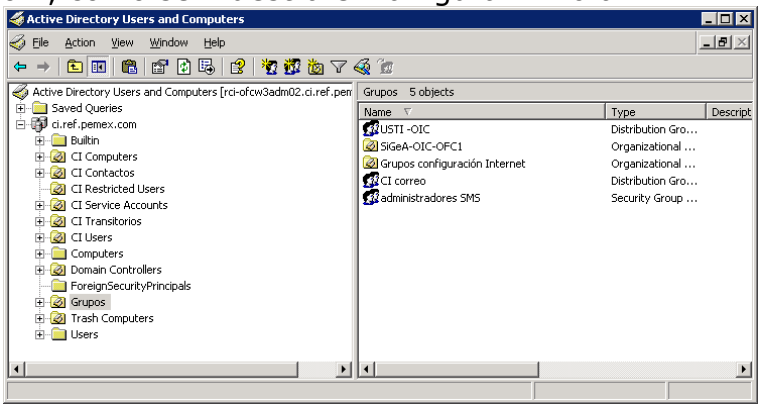


Fig. 4.1.6.a. Grupos en el dominio ci

1.- El grupo USTI-OIC, fue creado como grupo de Distribución – Universal, ver figura 4.1.6.b. Y en la figura 4.1.6.c se muestran las cuentas de usuario que integran a este grupo. Este grupo sirve para enviar correo a todos sus integrantes; esto quiere decir, que si queremos enviar un correo a cada de los integrantes de ese grupo, sólo basta elegir el nombre del grupo USTI-OIC en la lista de correo, y el correo será enviado a todos los integrantes.

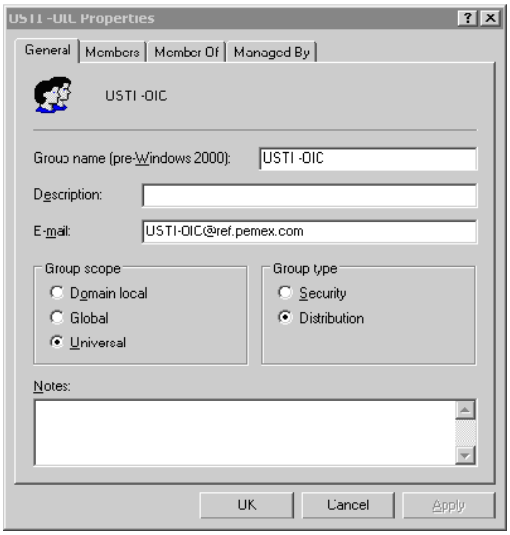


Fig. 4.1.6.b Grupo USTI-OIC

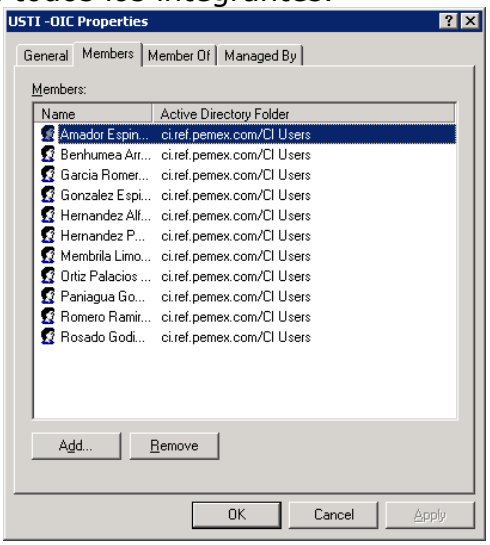


Fig. 4.1.6.c Integrantes del grupo USTI-OIC

2.- Otro ejemplo de unidad organizacional, son las unidades organizacionales que integran las cuentas de usuario que tienen o no salida a Internet, para tal configuración se creo una unidad organizacional llamada: Grupos configuración Internet, la cual contiene dos grupos globales de seguridad:

1. GG_S_Internet (las cuentas de usuario, asignadas a este grupo, no tienen acceso al servicio de Internet). Como se muestra en la figura 4.1.6.d.
2. GG_C_Internet (las cuentas de usuario, asignadas a este grupo, tienen acceso al servicio de Internet). Como se muestra en la figura 4.1.6.e.

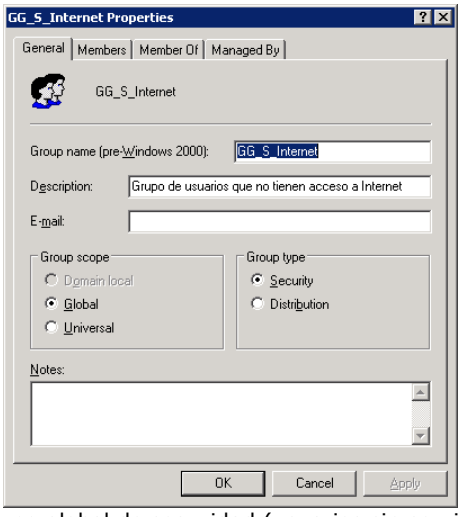


Fig. 4.1.6.d Grupo global de seguridad (usuarios sin servicio de Internet)

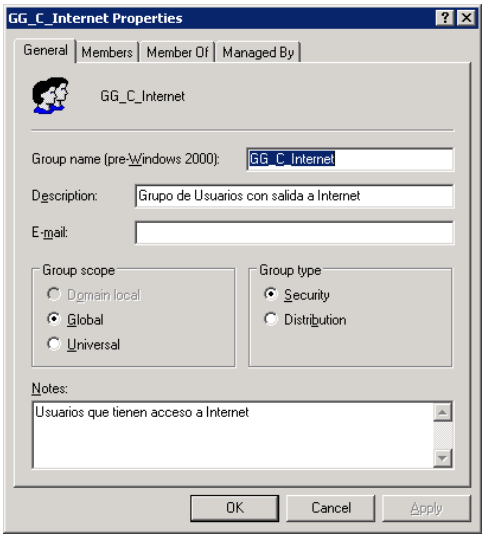


Fig. 4.1.6.e Grupo global de seguridad (usuarios con servicio de Internet)

3.- Este es otro ejemplo de un grupo global de seguridad SIGEA-OIC-OFC1, el cual contiene anidado tres grupos, como se visualiza en la figura 4.1.6.f. Los tres grupos anidados dentro de SIGEA-OIC-OFC1, son:

- SIGEA-OIC-OFC
- SIGEA-OIC-N
- SIGEA-OIC-E

Estos grupos tienen asignados cuentas de usuarios, con diferentes permisos de acceso a un Sistema.

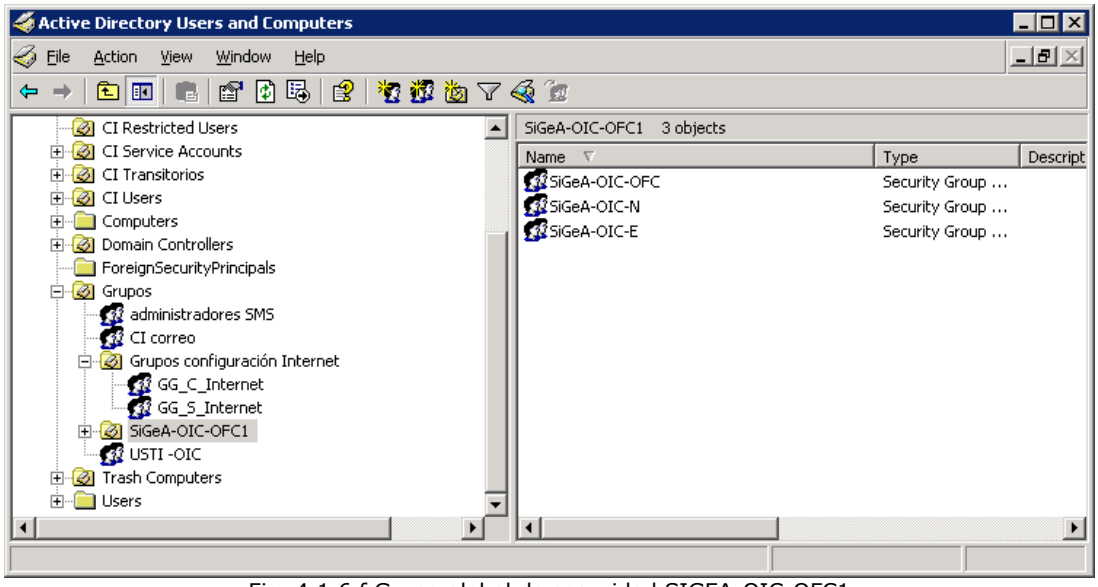


Fig. 4.1.6.f Grupo global de seguridad SIGEA-OIC-OFC1

Group Policy Management (GPO´S)

Las políticas de grupo es una característica de Windows que permite a los administradores aplicar ciertas configuraciones a través de las cuentas de usuario o cuenta de computadora. Se aplican desde la herramienta **Group Policy Management**, en la figura 4.1.6.g se muestra algunas de estas políticas.

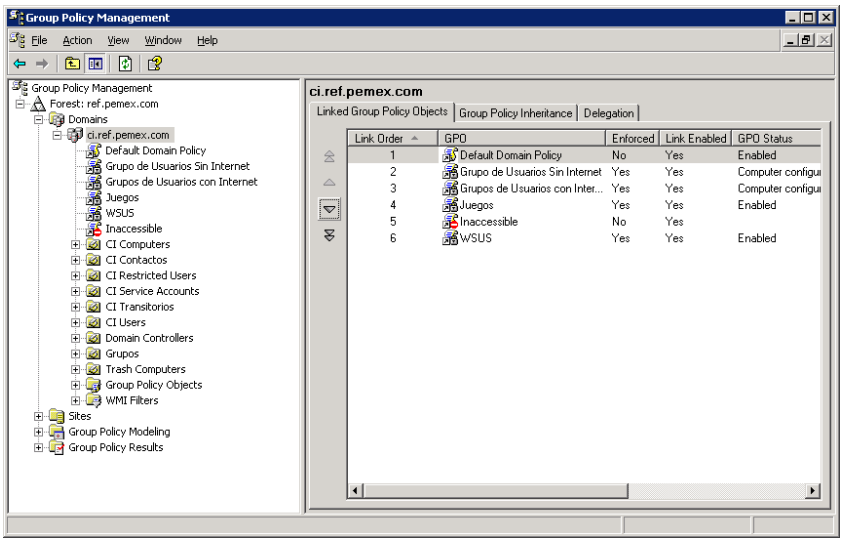


Fig. 4.1.6.g Group Policy Management

1. Política de grupo: Servicio de actualización de software de Windows (WSUS)

La política de actualización de software, se aplica a través de las cuentas de equipo existentes en el directorio activo. Desde la aplicación **WSUS (Servicio de Actualización de Software de Windows)** se mantiene la administración de parches de seguridad y vulnerabilidades para Microsoft Windows, y a través de la política se define los parámetros de envío a las estaciones de trabajo; como por ejemplo, el servidor desde donde se envían los archivos de actualización. Como se puede ver en la figura 4.1.6.h.

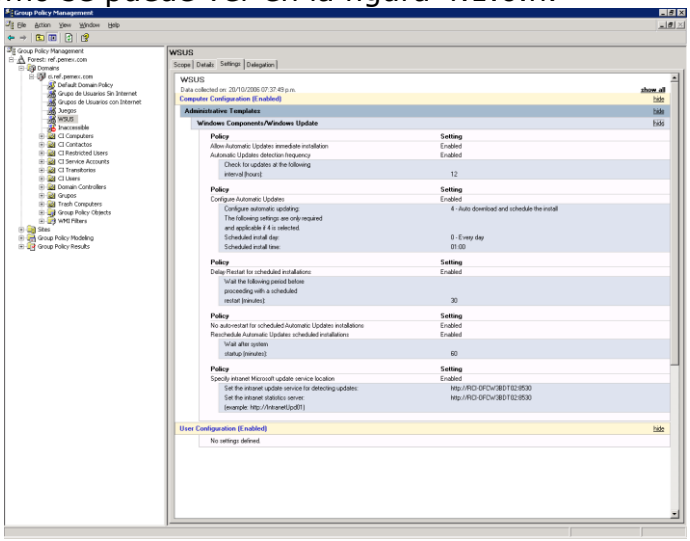


Fig. 4.1.6.g Group Policy Management

2. Política de grupo: Configuraciones para el navegador Internet Explorer

Desde esta política, definimos las configuraciones para el navegador Internet Explorer, las configuraciones de proxies, la página de inicio, etc. Se muestra la definición de estas configuraciones en la figura 4.1.6.h.

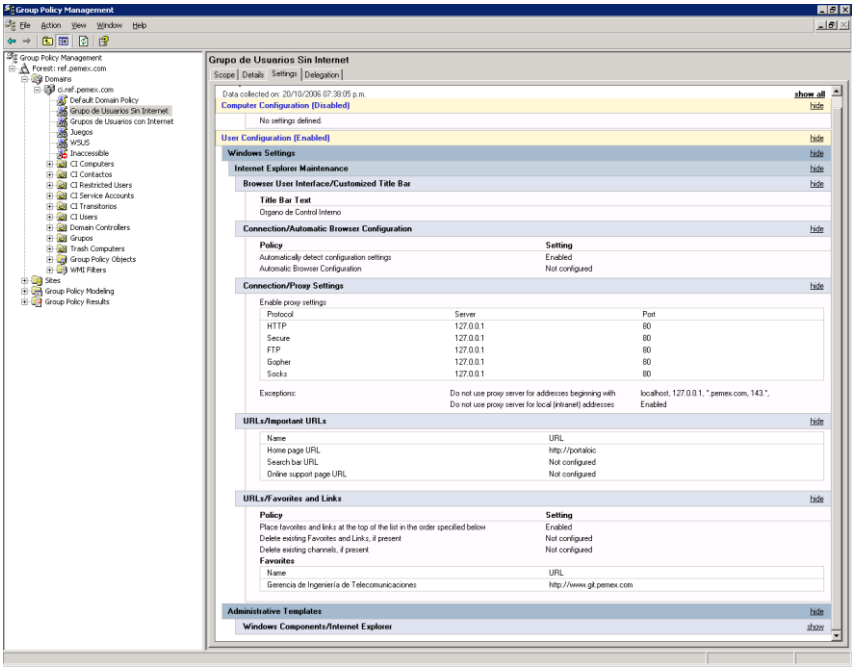


Fig. 4.1.6.h Política configuraciones de Internet Explorer

3. Política de grupo: Deshabilitación de programas de juegos

A través de esta política, se deshabilitan los juegos incluidos con Microsoft Windows, además de algunos archivos especificados por el nombre del archivo. Como se muestra en la figura 4.1.6.i.

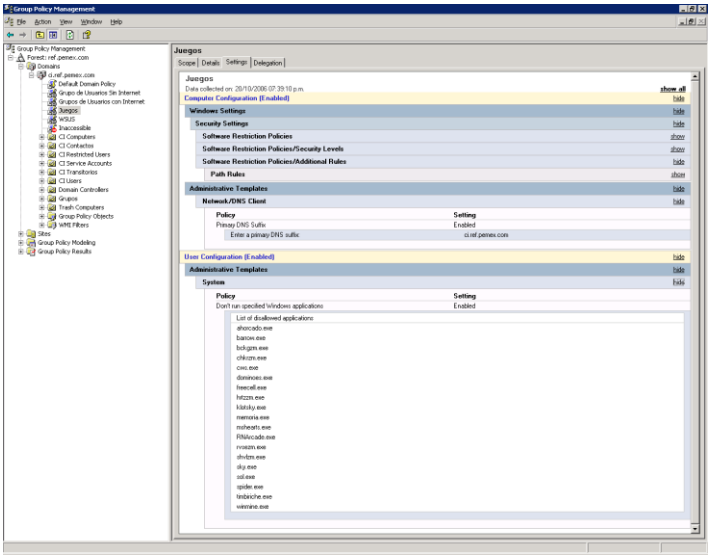


Fig. 4.1.6.i Política de deshabilitación de juegos

4. Política de grupo: Configuración de contraseñas de usuario

También, se encuentran definidos los parámetros de configuración referente a las contraseñas de usuarios: como longitud mínima de caracteres de la contraseña: ocho caracteres, historial de contraseñas: historial de 24 contraseñas, etc. En la figura 4.1.6.j, se muestra las configuraciones aplicadas.

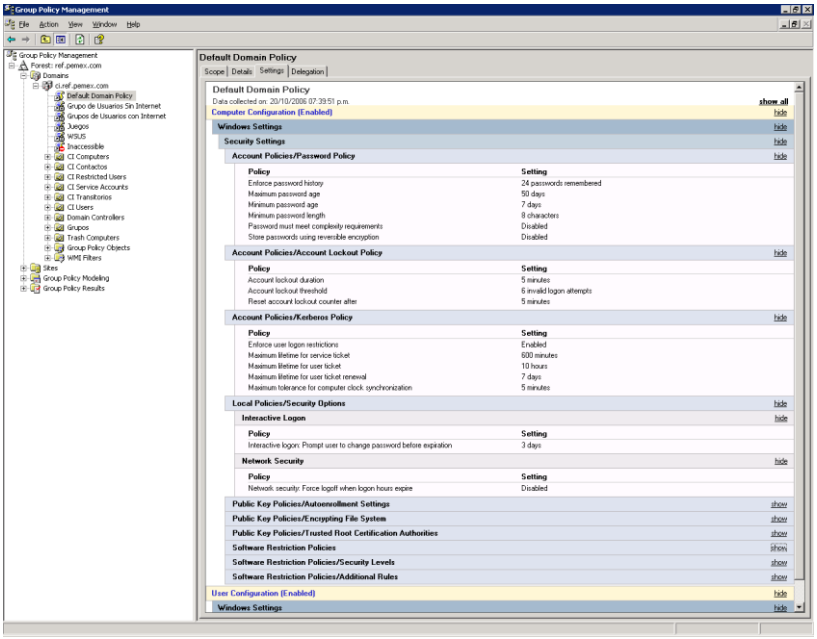


Fig. 4.1.6.j Política para la aplicación de contraseñas de usuario

4.1.7. Consolidación con otras aplicaciones

Al tener estabilizado el directorio activo, se implementarón otras aplicaciones, que toman como base la información contenida en dicho directorio. A continuación se explica el funcionamiento de algunas de estas aplicaciones.

Microsoft Exchange Server

El servicio de mensajería de Microsoft Exchange 2003 hace uso del directorio activo, almacena y comparte información con el sistema operativo Windows Server 2003, de tal forma que la información que se crea y mantiene en el directorio activo, tal como: grupos, unidades organizacionales, etc., puede ser utilizada por Exchange 2003.

Así el directorio activo almacena información del usuario; como su departamento, número telefónico, dirección de e-mail, etc., dicha información es utilizada por Exchange 2003.

Para que dicha información pueda ser almacenada y compartida en el directorio activo, el esquema es modificado para incorporar los atributos de Exchange durante el proceso de preparación del bosque.

La interacción con el directorio activo se lleva a desde la consola de administración (Exchange System Manager ó Active Directory Users and Computes). En la figura 4.1.7. se visualiza la consola Exchange System Manager.

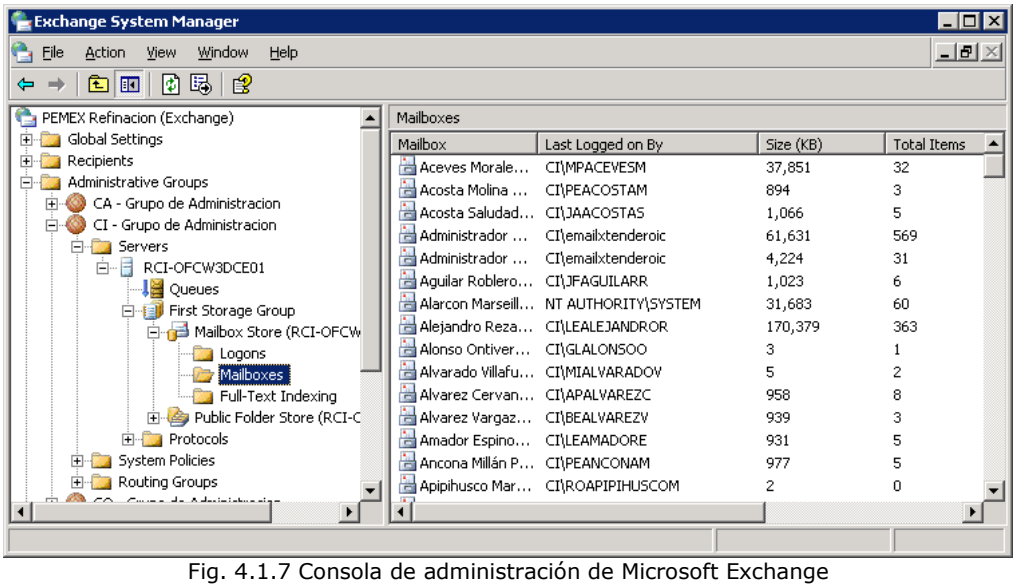


Fig. 4.1.7 Consola de administración de Microsoft Exchange

ES importante mencionar, que se puso especial cuidado en los atributos mostrados en la tabla 4.1.7, para que quedaran estandarizados como se especificó, ya que esta información se visualiza en la lista global de direcciones de Pemex.

Tabla 4.1.7 Atributos homologados para Microsoft Exchange

Sección	Atributo	Convención de Nombres	Ejemplo
Address	Street	Calle y número Colonia Municipio Edificio y piso	Av. Marina Nacional No. 329 Col. Huasteca Edificio C 4o piso
	P.O. Box		-
	City	Ciudad	Mexico
	State/province	Estado	D.F.
	Zip/Postal Code	Código Postal	11311
	Country/región	País	México

Se ejecutó el script, con la finalidad de que dichos atributos quedaran estandarizados para todas las cuentas de usuario.

```
Dim Container
strPath="OU=CI Users,DC=ci,DC=ref,DC=pemex,DC=com"
Set Container=GetObject("LDAP://" & strPath & "")
ModifyUsers Container
Set Container = Nothing
WScript.Echo "Finished"
Sub ModifyUsers(oObject)
Dim User
Object.Filter = Array("User")
For Each User in Object
        User.Put "Company","REFINACION"
        User.Put "physicalDeliveryOfficeName","Organo Interno de Control"
        User.Put "department", "Unidad de Sistemas y Tecnología de Información"
        User.Put "streetAddress","Bahía de Ballenas no. 5, Edificio D, Piso 11, Col. Huasteca"
        User.Put "l","México"
        User.Put "st","D.F."
        User.Put "postalCode","11311"
        User.Put "c","MX"
       User.SetInfo
Next
```

A través de revisiones a la información contenida en el directorio activo, se detectaron ciertas anomalías, dicha información como se mencionó, replica a todos los organismos; por lo cual: se realizaron algunas actividades de revisión y modificación de dichos atributos para ajustarlos a los estándares definidos. La figura 4.1.7.a, muestra un ejemplo para el atributo de teléfono, el cual no se encuentra en el formato especificado.

Problemática:
Revisando la GAL de Refinación, se detecta que en algunos casos los usuarios tienen más de 2 extensiones, un teléfono directo e Intercom en el atributo Telephone Number.

Nombre	Teléfono del trabajo	Oficina	Puesto
Escobedo Corral Samuel Salvador	811-53683; 19448868	Comercial	318572

Solución:

Para dar solución a esto, realizar lo siguiente:
En las propiedades del usuario, en el atributo telephone number, dar click en el botón Other….. y teclear la(s) otra(s) extensión(es) utilizando el mismo formato 811-#####. Si se trata de un número telefónico directo utilizar Dir. ########. Si se trata de Intercom utilizar Intercom. ##
Verificar desde la GAL del cliente Outlook, localizar al usuario y en sus propiedades, <tab> Teléfono y notas se despliegan los datos adicionales de extensión, directo e intercom en el campo Trabajo 2

Fig. 4.1.7.a Anomalías en atributos del directorio activo

En la figura 4.1.7.b, se muestra la ficha **Teléfono y Notas**, en la cual se modifica la información del atributo teléfono.

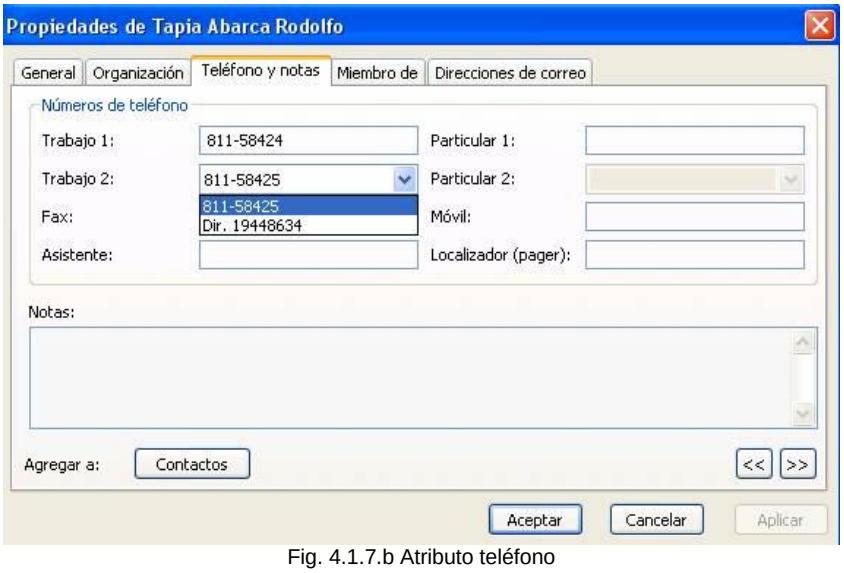


Fig. 4.1.7.b Atributo teléfono

Antivirus

La instalación y/o actualización de la aplicación antivirus, se incluyó dentro del archivo de ejecución; esto es, se ejecuta cuando el usuario inicia sesión en el dominio. En el capítulo tres, apartado 3.1.6; se detalló la ejecución de la aplicación a través del archivo ofcscan.bat.

Es importante mantener todos los equipos actualizados con las últimas versiones de las aplicaciones antivirus; para prevenir posibles infecciones al sistema operativo, archivos y aplicaciones.

Una tarea importante fue: verificar que todos los clientes, así como servidores incluidos los controladores de dominio, tuvieran instalada la aplicación antivirus así como que estuvieran actualizados. Esta tarea de monitoreo, se realiza permanentemente. La figura 4.1.7.c. muestra la consola de administración de la aplicación antivirus.

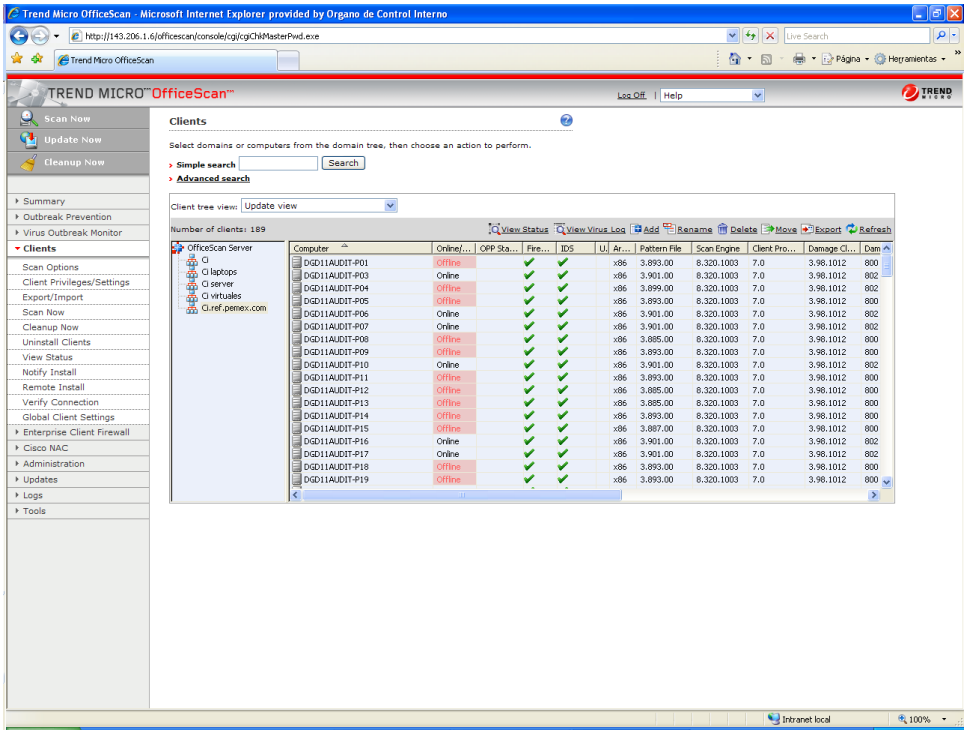


Fig. 4.1.7.c Consola de administración antivirus

Servicio de actualización de software de Windows (WSUS)

Como se explico anteriormente, a través de esta aplicación se envían las actualizaciones como: service pack, parches de seguridad y vulnerabilidades; para el caso que aplica se manejan actualizaciones para los sistemas operativos: Windows Server 2003 y Windows XP.

En dicha aplicación se generó un repositorio de archivos, en un servidor dedicado para tal fin, el cual contiene almacenadas dichas actualizaciones, enviándolas a todos los equipos, a través del directorio activo y las políticas de grupo. La figura 4.1.7.d muestra la consola de administración del servicio de actualización de software, la cual contiene todos los nombres de computadora con el detalle de las actualizaciones.

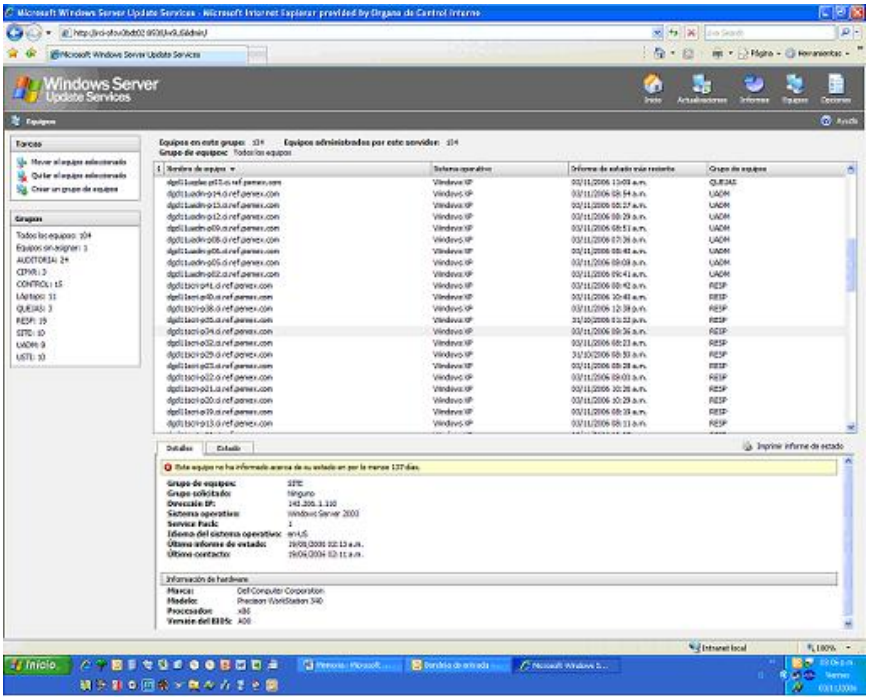


Fig. 4.1.7.d Consola de administración de WSUS

4.1.8 Herramientas de diagnóstico para un DC

En este apartado se describen algunas herramientas de diagnóstico; las cuales son útiles para resolver alguna falla o simplemente para realizar operaciones de mantenimiento y diagnóstico de errores en un controlador de dominio.

Para poder hacer uso de ellas es necesario instalar antes las herramientas Support Tools, incluidas en el CD de Windows Server 2003.

Ante alguna posible falla relacionada con el servicio de directorio activo, se ejecutan algunas de las siguientes herramientas de diagnóstico, las cuales se describen a continuación

LDAP

Esta herramienta, nos ayuda a verificar que el catálogo global del directorio activo se encuentre activo, como se muestra en la figura 4.1.8.a.

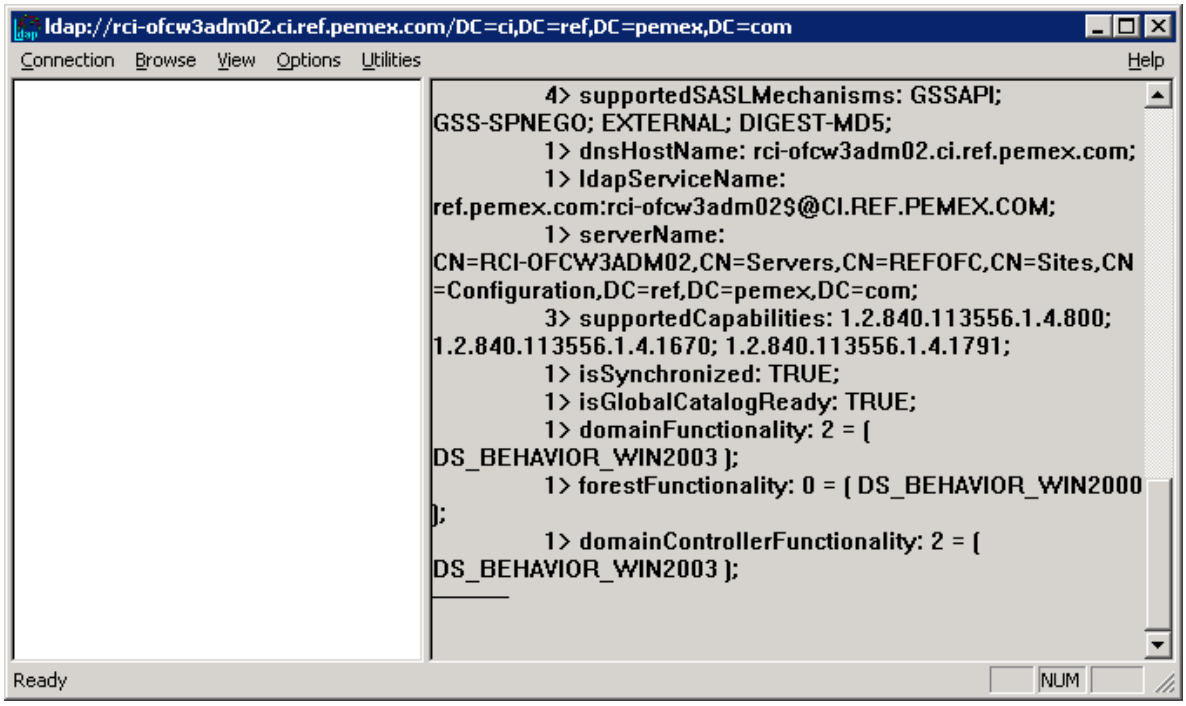


Fig. 4.1.8.a Herramienta LDAP

Dcdiag

Esta herramienta ejecuta una serie de pruebas en los controladores de dominio o bosque con el fin de detectar posibles anomalías referentes a la replicación con otros controladores de dominio, funcionamiento de los roles maestros catálogo global o inconsistencias en la base de datos del servicio de directorio activo. En la figura 4.1.8.b se muestra un ejemplo de ejecución de esta herramienta.

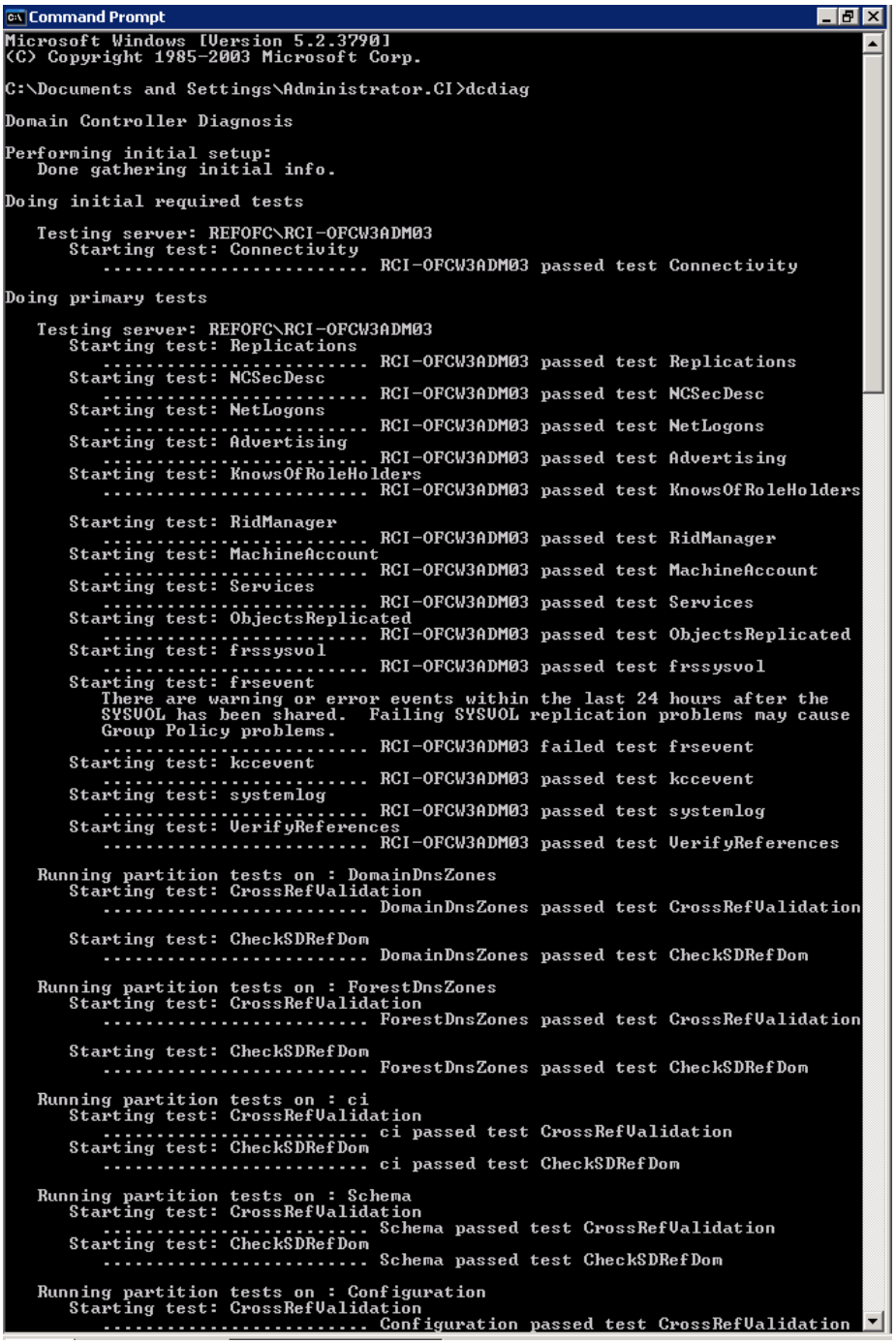


Fig. 4.1.8.b Herramienta Dcdiag

Netdiag

Esta herramienta sirve para hacer una serie de pruebas a nivel de red y conexiones en el controlador de dominio. En la figura 4.1.8.c se muestra la ejecución de esta herramienta, mostrando una lista de los hotfixes instalados en el controlador; además de las configuraciones de red.

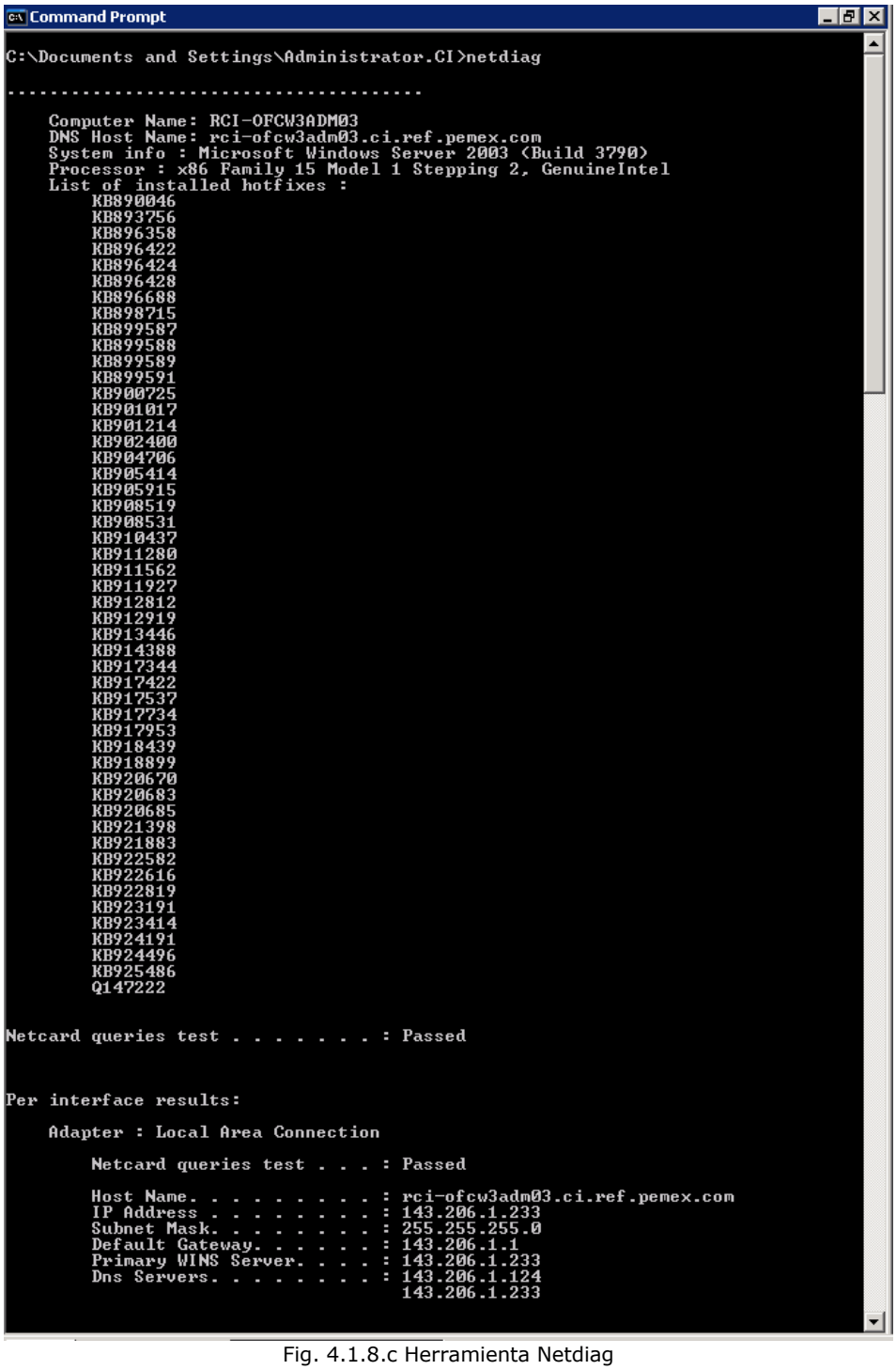


Fig. 4.1.8.c Herramienta Netdiag

Nslookup

Esta herramienta se usa para realizar pruebas de resolución de nombres, verificando si está funcionando correctamente el servicio DNS. En la figura 4.1.8.d se muestra la resolución de nombres para el servidor rci-ofcw3adm02.ci.ref.pemex.com.

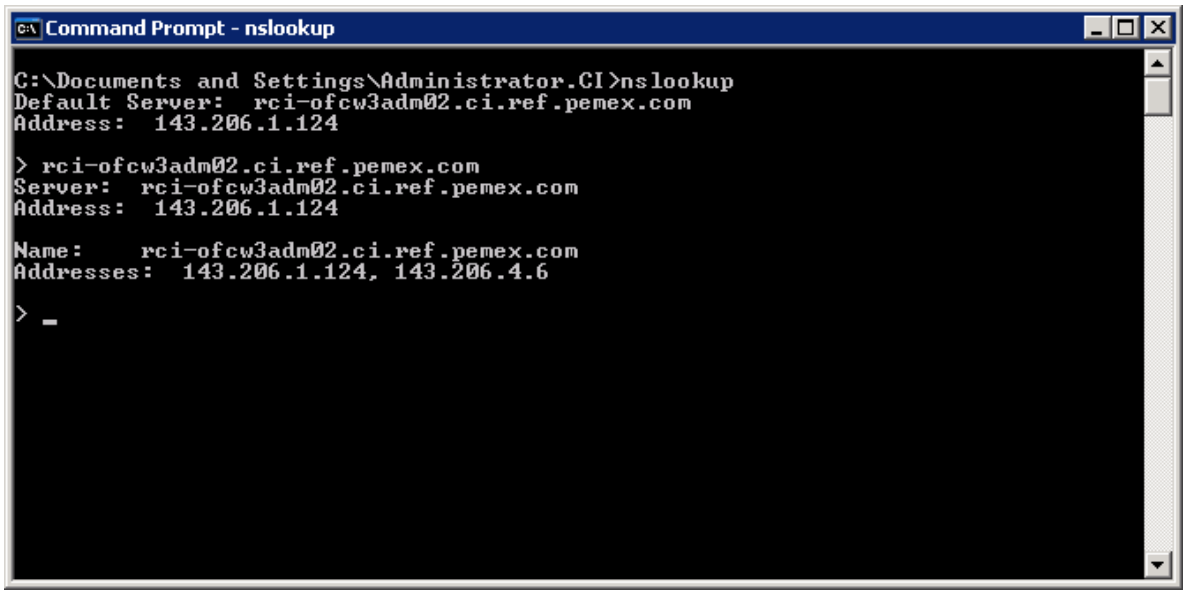


Fig. 4.1.8.d Herramienta Nslookup

Dsastat

Esta herramienta sirve para comparar y detectar diferencias entre las bases de datos del servicio de directorio activo de los controladores de dominio. En las figuras 4.1.8.e y 4.1.8.f se muestra el ejemplo de ejecución y revisión para los controladores de dominio rci-ofcw3adm2 y rci-ofcw3adm03.

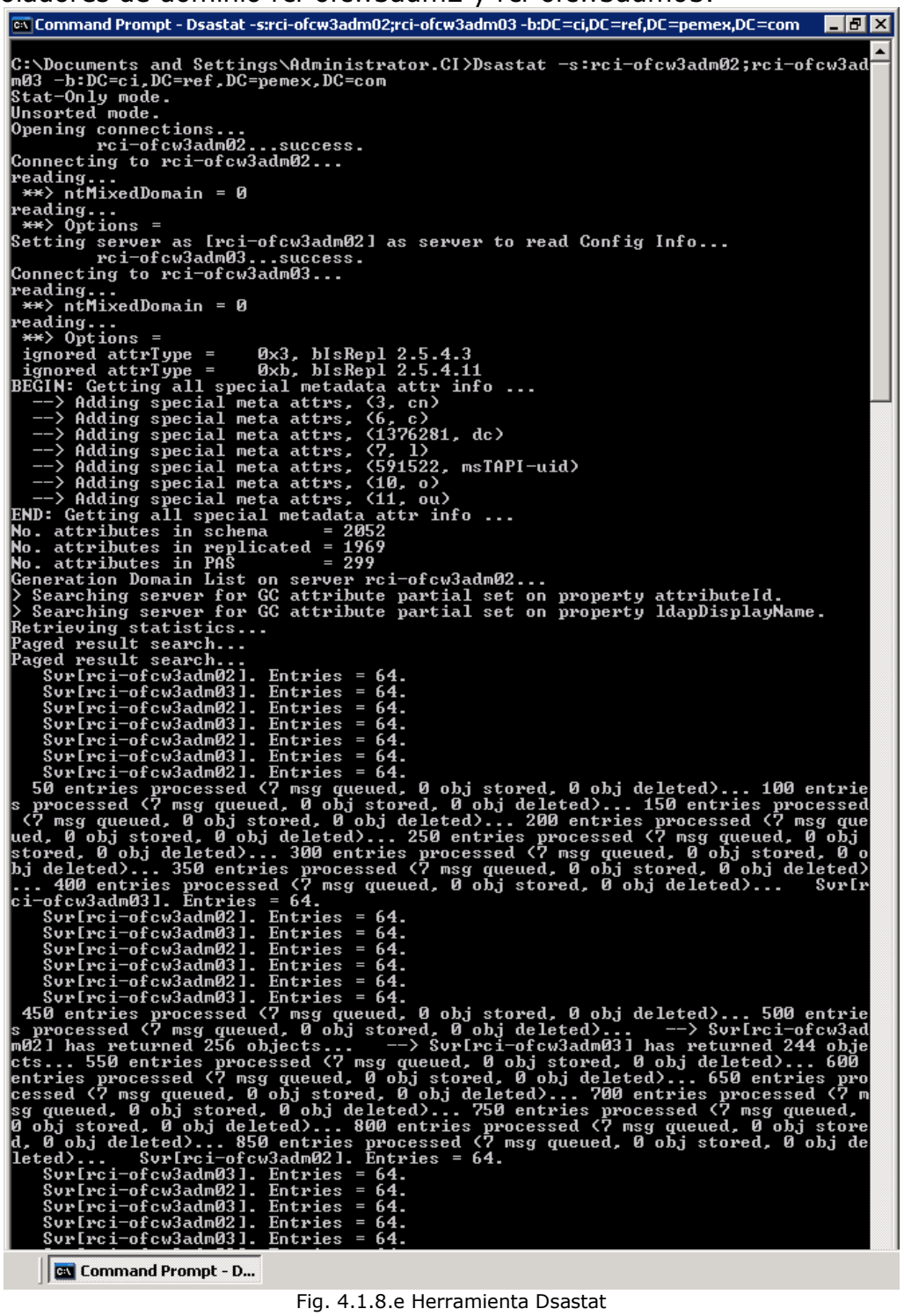


Fig. 4.1.8.e Herramienta Dsastat

Fig. 4.1.8.f Herramienta Dsastat

Repadmin

Esta herramienta comprueba las réplicas entre los servidores asignados del bosque. En la figura 4.1.8.g, se muestra un ejemplo con la información referente al sitio y controlador de dominio, hora y fecha de réplica.

Fig. 4.1.8.g Herramienta repadmin

Replmon

Esta herramienta, realiza las mismas verificaciones que la herramienta repadmin, sólo que de manera gráfica; se puede comprobar el estado de la

réplica entre las diferentes particiones del directorio activo; verificando la replicación entre los diferentes controladores de dominio; se puede forzar la sincronización entre ellos, realizar pruebas de funcionamiento de los roles del servicio de directorio activo. En la figura 4.1.8.h se muestra un ejemplo de la herramienta.

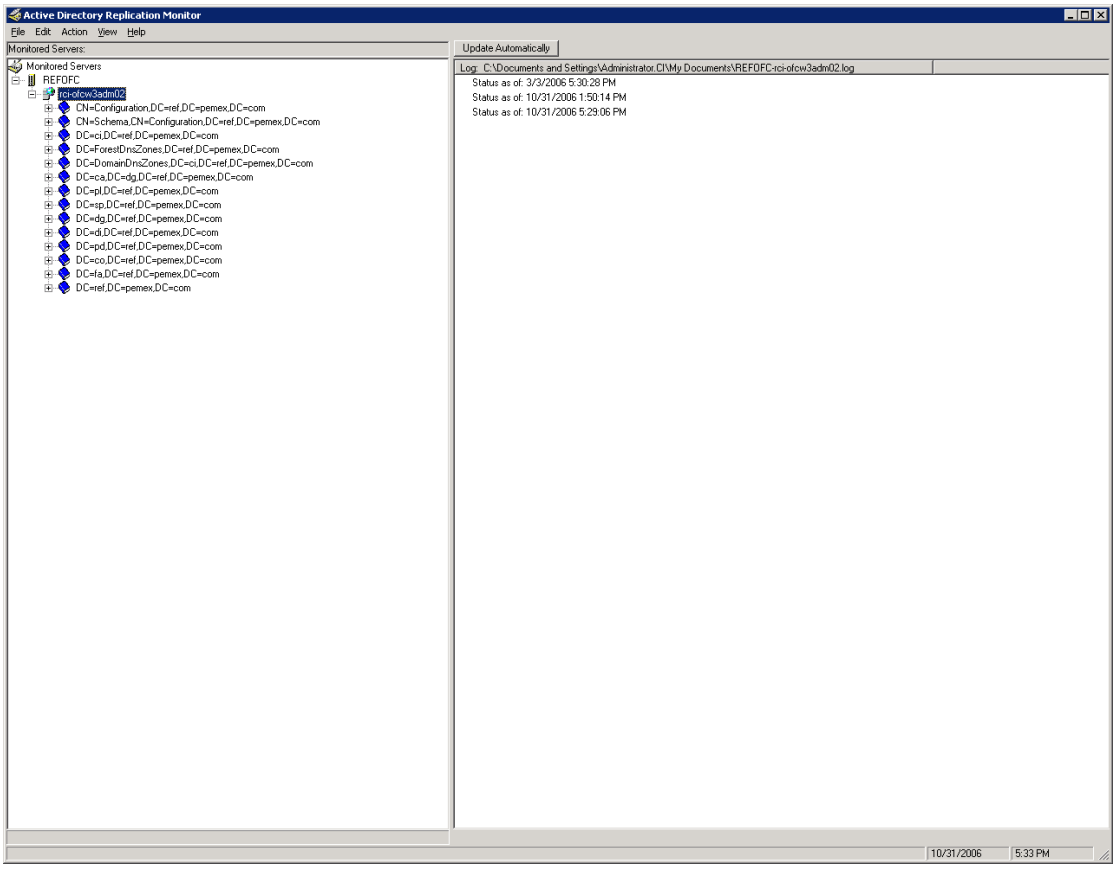


FIg. 4.1.8.h Herramienta Replmon

Conclusiones

Para el desempeño de la actividad laboral la cual desarrollo actualmente como Administrador de un Site, es importante mencionar el aporte que me dio la formación educativa que tuve en la carrera; con gran ayuda de materias como: Sistemas de Información, Arquitectura de computadoras, Base de datos, Sistemas Operativos, Programación Avanzada, Análisis y Diseño de Sistemas, Administración de Centros de Cómputo, entre otras. Las cuales me ayudaron a comprender la lógica y funcionamiento de las computadoras, de los sistemas operativos, aplicaciones y todo el ambiente en el cual esta comprendido el desarrollo de mi actividad laboral.

Así también, se me aportaron las bases para el manejo y la administración de los sistemas operativos y demás aplicaciones para servidor, relacionadas específicamente con el Directorio Activo.

Adicionalmente, es importante comentar la importancia de mantenerse actualizado respecto a los avances en cuanto a tecnología y/o área en la cual estamos laborando; ya que esto traerá como consecuencia además del conocimiento una apertura hacia los mercados de trabajo.
Por otro lado, el aporte que genero a la empresa, el haber implementado este proyecto, fue:

Primero: haber estandarizado la plataforma tecnológica con el sistema operativo Microsoft Windows Server 2003 utilizando la integración con el servicio de directorio activo.

Segundo: el haber logrado actualizar y estandarizar las cuentas de usuario, cuentas de computadora. No permitiendo objetos duplicados, controlando las reglas de acceso y destino a los datos de los usuarios
Tercero: el haber realizado los dos puntos anteriores, se logró pasar a la segunda fase que fue la implementación de Microsoft Exchange y otras aplicaciones.

Todo esto conlleva a facilitar la administración, control y monitoreo de la plataforma operativa, de forma segura, confiable y de manera eficiente. Por lo cual, se logró el objetivo del presente trabajo el cual fue: actualizar y estandarizar la plataforma tecnológica de servidores de red basada en la infraestructura de Microsoft Windows Server 2003 integrado con el Servicio de Directorio Activo, para ofrecer a los usuarios servicios encaminados a mejorar sus procesos de negocio de manera más segura y confiable. Facilitar la administración integrando toda la plataforma operativa. Acceder a la información de manera segura mediante un Servicio de Políticas de Grupo, controlando las reglas de acceso y destino a los datos de los usuarios.

Glosario

Administración de la configuración. Arte (o ciencia) que consiste en asegurarse (desde una consola central) que las estaciones de trabajo de los usuarios tengan instalado el hardware y software correctos y que se configuren de acuerdo con estándares aceptados.

Aplicación. Es un programa que tiene como objetivo llevar a cabo una sola tarea. Por ejemplo, Microsoft Word tiene como objetivo facilitar la preparación de documentos.

Autentificación. Proceso para asegurarse, tanto como sea posible, de que los nombres de inicio de sesión y mensajes provenientes de un usuario (como una contraseña o un correo electrónico) se originan de una fuente autorizada,

Base de datos. Archivo o conjunto de datos estructurados en relaciones lógicas. Por ejemplo, el directorio telefónico es una base de datos en papel con los nombres en una columna y los números telefónicos en otra.

Binario. Que tiene solamente dos estados; se utiliza para describir la aritmética base 2 que utilizan las computadoras. En notación binaria, 1,2,3,4,5 se representa como 1,10,1 1,100,101. El valor del lugar de cada posición en notación binaria se duplica con cada dígito a la izquierda del punto decimal, es decir 16,8,4,2,1. Compare esto con la notación decimal (base 10), en la que cada valor de la posición es igual a diez veces el de la columna a su derecha.

Bit. Porción de información, representada corno un 1 o un 0. Para la computadora, un bit es realmente una diferencia de voltaje: alto voltaje representa un 1, bajo voltaje representa un 0. byte (byte) Ocho bits (también se le llama octeto cuando se analiza TCPIIP). Un byte es igual a un carácter; por ejemplo, la letra e es un byte. Un byte puede representar 256 números (del 0 a! 255) en números binarios.

Cliente. Computadora que utiliza los recursos compartidos por los servidores, cliente/servidor (client/server) Red en la que el procesamiento está distribuido entre un servidor y un cliente, cada uno de ellos con funciones específicas. También se utiliza para describir a las redes que tienen servidores dedicados. Es lo opuesto a de igual a igual

Correo electrónico (e-mail) Es una manera de enviar texto y archivos a través de una red con notificación como la del correo postal.

Cuentas de usuario. Es un objeto almacenado en el Directorio Activo que permite el inicio de sesión único en la red.

Cuentas de equipo. Ofrecen una forma de autenticar a los equipos que acceden a la red y a los recursos del dominio.

Cuentas de grupos. Colección de usuarios, equipos y otros grupos. Su principal objetivo es simplificar la administración.

DHCP. Protocolo de Configuración Dinámica del Host; parte del grupo de protocolos TCP/ IP que maneja la asignación automática de direcciones IP a los clientes.

dirección IP. Secuencia de números asociados con una dirección MAC del adaptador de red. Tiene una longitud de 32 bits y se divide en cuatro grupos de 1 byte que tienen valores de 0 a 255. Ejemplo: 209.61 .64.1.

DNS. Sistema de Nombres de Dominio, son las porciones de los grupos de protocolos TCPIIP que convierten las direcciones IP en nombres. Por ejemplo, DNS convierte 192.168.1.5 en alice.library.net.

dominio. (domain) Grupo de computadoras cuyo inicio de sesión a través de la red se autentifica por medio del servidor NT. En esencia, un dominio le quita la función de autentificación a las estaciones de trabajo individuales y las centraliza en el servidor.

grupo de usuarios.(user group) En los dominios de Windows NT, es una clase de usuarios de dominio agrupados para simplificar la administración. Los grupos se crean y administran en el Administrador de Usuarios para Dominios de Windows NT. Los usuarios pueden tener privilegios específicos asignados y recursos específicos disponibles como resultado de su membresía a un grupo de usuarios. Por ejemplo, el grupo de usuarios de Contabilidad podría tener acceso a los archivos y aplicaciones de contabilidad del sistema. Los usuarios que no pertenezcan al grupo de usuarios de Contabilidad no tienen acceso a dichos recursos.

Internet. Red global de redes que actualmente se utiliza para todo, desde correo electrónico para el comercio hasta la investigación.

LAN. Red de área local, es un grupo de computadoras en una misma área conectadas entre sí sin ruteadores. Todas las computadoras están conectadas hacia el mismo conjunto de hubs o switches en una LAN, y todos los recursos de la red son "locales", corriendo a la máxima velocidad de la red.

Modelo OSI. (OSI model) Modelo de Interconexión de Sistemas Abiertos; modelo de referencia que especifica siete capas para la funcionalidad de redes. El modelo OSI ofrece una forma ideal de comprender la teoría de la conectividad de redes.

navegador. (browser) Programa que ofrece una forma de ver y leer documentos disponibles en World Wide Web. Netscape Navigator y Microsoft Internet Explorer son navegadores.

octeto. (octet) Es el nombre "oficial" de un byte (ocho bits u ocho 1s o Os digitales).

paquete. También se le llama datagrama; es la información colocada dentro de una "envoltura" llamada el encabezado. Los paquetes contienen encabezados (los cuales manejan el direccionamiento), la corrección de errores, las sumas de verificación y (por último) los datos enviados a través de la red.

protocolo. Estándar establecido. En término de conectividad de redes, un protocolo se utiliza para direccionar y asegurar la entrega de paquetes a través de una red.

puerta de enlace (gateway) Un término muy llamativo que describe a un dispositivo que en esencia conecta a dos sistemas. Las puertas de enlace pueden transferir correo, traducir protocolos, enviar paquetes y llevar a cabo otras tareas. El propósito principal de una puerta de enlace es la comunicación.

red. Cualquier grupo de partes que trabajan en conjunto con un orden predecible. En términos de computación, es un grupo de computadoras conectadas por una topología común que permite la transmisión de datos.

respaldo de fallas. (fail over) Extensión lógica de tolerancia a fallas. En un sistema con respaldo de fallas, existen dos (o en ocasiones más) servidores, cada uno con copias idénticas de las unidades y recursos de un servidor maestro. Si el servidor maestro falla, el servidor de respaldo entra en acción de manera dinámica y los usuarios nunca notan la diferencia (excepto por una pequeña baja en velocidad).

ruteador. (router) Dispositivo u (opcionalmente) software que rutea paquetes hacia sus destinos. Los ruteadores deben conectarse con al menos dos redes. Deciden cómo enviar información con base en condiciones de la red.

secuencia de comandos de inicio de sesión. (login script) Archivo de texto almacenado en el servidor que tiene una lista de comandos. Cuando un usuario accesa a la red, el servidor lee el archivo de texto, ejecuta los comandos incluidos en él y a menudo asigna unidades de disco y conecta instantáneamente las impresoras de red de cada usuario. Algunas secuencias de comandos de inicio de sesión contienen líneas que le informan al usuario que está siendo conectado; la secuencia de comandos de inicio de sesión incluye también comandos como net use que establece conexiones de red hacia otras computadoras.

servicios del directorio. (directory services) Conjunto de herramientas que posibilitan a los administradores de red ofrecer a los usuarios acceso a ciertos recursos específicos independientemente del punto donde los usuarios de la red la accesaron. En otras palabras, si Tom en el departamento de mercadotecnia tiene acceso al servidor 1 y al servidor 2, pero no tiene acceso al servidor 3, él solamente puede accesar a los servidores 1 y 2 sin importar si acceso a la red en una computadora perteneciente al departamento de

mercadotecnia, producción o administración. A medida que las redes se han hecho más complejas y han requerido de la administración de un mayor número de usuarios, los servicios del directorio se han convertido en una salvación para los administradores de red que tratan de administran el acceso a través de redes en diferentes sitios con miles de usuarios.

servidor. (server) Computadora de una red que comparte un recurso específico (archivos, impresoras, aplicaciones) con otras computadoras.

servidor proxy. (proxy server) Servidor que maneja las solicitudes de los clientes internos y oculta sus direcciones IP para que no puedan verse en Internet.

sistema operativo. (operating system) Software de una computadora que permite al usuario comunicarse con el hardware y llevar a cabo tareas. Windows 95, Windows NT Workstation, OS/ 2 y UNIR son sistemas operativos.

TCP. Protocolo de Control de Transmisión, es la parte del grupo de protocolos TCP/IP que asegura la entrega confiable de paquetes a sus destinos.

TCP/IP. Protocolo de Control de Transmisión/Protocolo Internet, es un término utilizado para describir los diversos protocolos en los que corre Internet. TCPI/IP es también un estándar abierto; no es propiedad de ninguna compañía. Cualquier persona puede crear una implementación del protocolo TCP/IP si así lo desea.

WAN. Red de área amplia, red compuesta de dos o más LANs conectadas a través de líneas telefónica; generalmente líneas telefónicas digitales.

Bibliografía

Hayden, Matt. Aprendiendo redes en 24 horas, Prentice Hall Hispanoamericana, S.A. México, 1999, págs. 445.

Wyatt, Allen. Aprendiendo Windows NT Server 4, Prentice Hall Hispanoamericana, S.A. México, 2000, págs. 453.

Guía de Administración de Exchange Server 2004
Manual de Active Directory

Microsoft Training & Certification 2274: Managing a Microsoft Windows Server 2003 Enviroment

Microsoft Training & Certification 2275: Maintaining a Microsoft Windows Server 2003 Enviroment

Microsoft Training & Certification 2279: Planning, Maintaning a Microsoft Windows Server 2003 Active Directory Infraestructure

Microsoft Training & Certification 2285: Installing, Configuring and Administering Microsoft Windows XP Professional

Referencias en Internet:

[1] Página principal de Microsoft México
http://www.microsoft.com.mx

[2] Active Directory in Windows Server 2003
http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/default.mspx

[3] HOW TO: Create an Active Directory Server in Windows Server 2003
http://support.microsoft.com/default.aspx?scid=kb;en-us;324753

[4] Windows Server 2003 Active Directory Branch Office Guide
http://www.microsoft.com/downloads/details.aspx?FamilyID=9353a4f6-a8a8-40bb-9fa7-3a95c9540112&displaylang=en

[5] Active Directory Services and Windows 2000 or Windows Server 2003 Domains (Part 1)
http://support.microsoft.com/default.aspx?scid=kb;enus;310996&Product=winsvr2003

[6] Technical Overview of Windows Server 2003 Active Directory
http://www.microsoft.com/windowsserver2003/techinfo/overview/activedirectory.mspx

[7] Frequently Asked Questions About Windows 2000 DNS and Windows Server 2003 DNS
http://support.microsoft.com/default.aspx?scid=kb;en-us;291382

[8] How DNS query Works
http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/WINDOWS2000/en/server/help/sag_DNS_und_HowDnsWorks.htm

[9] Querying DNS Servers
http://www.microsoft.com/resources/documentation/Windows/XP/all/reskit/en-us/Default.asp?url=/resources/documentation/Windows/XP/all/reskit/en-us/prjj_ipa_bsmz.asp

[10] Best practices for DNS client settings in Windows 2000 Server and in Windows Server 2003
http://support.microsoft.com/?kbid=825036

[11] Windows 2000 Active Directory FSMO Roles (Q197132)HHIO
http://support.microsoft.com/default.aspx?scid=kb;ENUS;q197132&GSSNB=1

[12] FSMO Placement and Optimization on Windows 2000 Domain Controllers (Q223346)
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q223346

[13] Directory Replication Basics for Windows 2000 (Q199174)
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q199174

[14] Designing a Site Topology for Active Directory Replication
http://www.microsoft.com/windows2000/techinfo/reskit/deploymentscenarios/scenarios/repl_design_sitetopology_active_directory_repl.asp

[15] Designing a Global Active Directory Domain and Trust Infrastructure
http://www.microsoft.com/windows2000/techinfo/reskit/deploymentscenarios/scenarios/domain_01_sir.asp

[16] How to configure Active Directory diagnostic event logging in Windows Server
http://support.microsoft.com/default.aspx?scid=kb;en-us;314980&sd=tech

[17] Troubleshooting Group Policy in Windows Server 2003
http://www.microsoft.com/downloads/details.aspx?FamilyId=B24BF2D5-0D7A-4FC5-A14D-E91D211C21B2&displaylang=en

[18] HOW TO: Create a System Policy Setting in Microsoft Windows Server 2003
http://support.microsoft.com/default.aspx?scid=kb;en-us;814598

[19] Solución de problemas de la directiva de grupo en Windows 2000:
http://www.microsoft.com/latam/technet/articulos/200110/art06/default.asp

[20] How to remove data in Active Directory after an unsuccessful domain controller demotion
http://support.microsoft.com/default.aspx?scid=kb;enus;216498&Product=win2000

[21] Using Ntdsutil.exe to seize or transfer FSMO roles to a domain controller
http://support.microsoft.com/default.aspx?scid=kb;en-us;255504&Product=win2000

[22] 223787 - Flexible Single Master Operation Transfer and Seizure Process
http://support.microsoft.com/default.aspx?scid=kb;EN-US;223787

[23] 313994 - CÓMO - Crear o mover un catálogo global en Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;es;313994

[24] How to configure Active Directory diagnostic event logging in Windows Server
http://support.microsoft.com/default.aspx?scid=kb;en-us;314980&sd=tech

[25] HOW TO: Use Portqry to Troubleshoot Active Directory Connectivity Issues
http://support.microsoft.com/default.aspx?scid=kb;EN-US;816103

[26] Initial synchronization requirements for Windows 2000 Server and Windows Server 2003 operations master role holders
http://support.microsoft.com/default.aspx?scid=kb;en-us;305476

[27] Desfragmentación de la Base de datos Activa de Directorio
http://support.microsoft.com/?kbid=229602

[28] How do I manually defragment Active Directory?
http://www.winnetmag.com/Article/ArticleID/13400/13400.html

[29] Overview of problems that may occur when administrative shares are missing
http://support.microsoft.com/default.aspx?scid=kb;en-us;842715

[30] 8320 » Troubleshooting - A domain controller is not functioning correctly?
http://www.jsiinc.com/SUBQ/tip8300/rh8320.htm

[31] "Directory Services cannot start" error message when you start your Windows-based or SBS-based domain controller
http://support.microsoft.com/kb/258062/en-us

[32] Active Directory Operations Guide Version 1.5
http://www.microsoft.com/downloads/details.aspx?FamilyID=4a82eccc-76d6-4431-aac4-1ef1ba11dbea&displaylang=en

[33] A List of the Windows 2000 Domain Controller Default Ports (Q289241)
http://support.microsoft.com/search/preview.aspx?scid=kb;en-us;Q289241

[34] Network Ports Used by Key Microsoft Server Products
http://www.microsoft.com/smallbusiness/gtm/securityguidance/articles/ref_net_ports_ms_prod.mspx

[35] Port Requirements for the Microsoft Windows Server System
http://support.microsoft.com/default.aspx?scid=kb;enus;832017&Product=ISAS