



INSTALACIÓN DE ACTIVE DIRECTORY

1 OBJETIVO

El objetivo de la esta clase es la presentación de la estructura de Active Directory, ver cuales son sus componentes y la funcionalidad de cada un de ellas.

Al finalizar la clase el alumno podrá:

- Saber que es y para que sirve Active Directory.
- Cuales son los elementos que componen su estructura lógica.
- Que relaciones existen entre cada uno de ellos.
- Como instalar y configurar adecuadamente Active Directory.

2 ¿QUÉ ES ACTIVE DIRECTORY?

Active Directory es el servicio de directorio de Windows 2003 Server Standard Edition, Enterprise Edition y Datacenter Edition. Se encarga de almacenar la información sobre objetos en la red y facilita a administradores y usuarios la búsqueda y el uso de esta información. El servicio de Active Directory utiliza un tipo de almacenamiento de datos estructurado, como punto de partida para la organización jerárquica y lógica de la información del directorio.

Dentro de un directorio podemos encontrar una gran cantidad de objetos como pueden ser servidores de archivos, impresoras, bases de datos, usuarios, etc., por lo cual es imprescindible contar con un mecanismo centralizado que permita a los usuarios localizar tales objetos para su utilización.

Este directorio funciona como la autoridad que se encarga de administrar identidades y mantener las relaciones entre todos los recursos distribuidos. Como funciona a la par del sistema operativo debe estar integrado con el mismo, para posibilitar una correcta administración de los recursos y poseer los niveles de seguridad adecuados, hecho relevante ya que el directorio centraliza todo el trafico de la red, manteniendo la integridad y la privacidad de la misma.

Otras funciones del servicio de directorios son:

- Obligar a proteger los objetos y sus bases de datos de intrusos externos o de usuarios internos que no tengan permiso de acceso a esos objetos.
- Distribuir el directorio a través de muchos equipos en una red.
- Replicar un directorio para hacerlo disponible a más usuarios y para hacerlo más tolerante a fallos.
- Particionar un directorio en muchos recipientes que estén localizados en equipos diferentes distribuidos a través de la red. Esto proporciona más espacio disponible al directorio en conjunto y permite el almacenamiento de un mayor número de objetos.



Las características principales de Active Directory de Windows 2003 son:

Administración simplificada y centralizada.

Windows 2003 organiza los recursos de forma jerárquica en Dominios, estos son agrupaciones lógicas de recursos como pueden ser equipos, servidores, impresoras, etc. Un dominio es la unidad básica de replicación y seguridad en Windows 2003.

Cada conjunto de dominios (denominado árbol), posee uno o más controladores de dominio, que se encargan de almacenar y autenticar usuarios y de administrar permisos de acceso a los recursos. Por cuestiones de simplificación todos los controladores son iguales, por lo tanto se pueden replicar tales actualizaciones a los demás controladores, permitiendo a un administrador iniciar sesión en cualquier equipo del dominio y administrar de forma centralizada objetos de cualquier lugar del mismo.

Escalabilidad

La estructura jerárquica de Active Directory en secciones contenedoras de objetos, permite que el directorio sea expandible a medida que aumenta la red, posibilitando albergar gran cantidad de objetos.

Compatibilidad con estándares abiertos.

Active Directory integra el concepto de nombres de Internet en el servicio de directorio.

Esto permite unificar y gestionar muchos espacios de nombres que existen en la actualidad en entornos heterogéneos de software y hardware en las redes corporativas. Active Directory utiliza DNS para su sistema de nombres y puede intercambiar información con cualquier aplicación o directorio que utilice LDAP (protocolo compacto de acceso a directorios) o el Protocolo de transferencia de hipertextos (HTTP).

También comparte información con otros servicios de directorio como por ejemplo NDS (Novell Directory Service)

Compatibilidad con formatos de nombres estándar

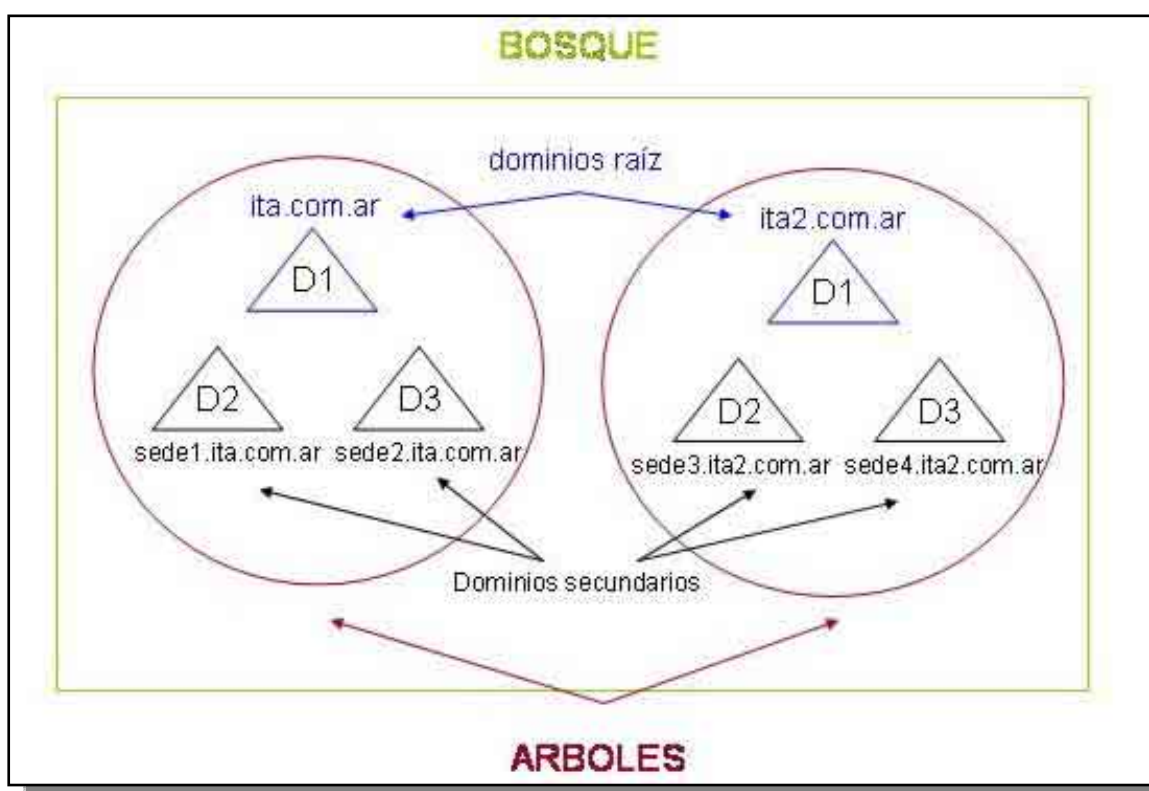
Active Directory admite algunos formatos comunes de nombres. De esta manera, los usuarios y las aplicaciones pueden acceder a Active Directory utilizando el formato con el que estén más familiarizados. Por ejemplo el formato RFC 822 que admite nombres de la forma nombre@dominio.com, formato HTTP (URL) <http://dominio/recurso> y UNC (Universal Naming Convention) [\\dominio.com\equipo\documento.doc](http://dominio.com/equipo/documento.doc).



2.1 CONCEPTO DE DOMINIO, ÁRBOL Y BOSQUE

Debido a la estructura centralizada y jerárquica de Active Directory en Windows 2003 se introduce el concepto de árbol y bosque. Esta estructura jerárquica se organiza de forma triangular, cuando se instala un primer servidor este será el controlador de dominio, y se encargará de administrar la seguridad del mismo. A este primer servidor de la estructura se lo denomina Dominio raíz. (Ej.: ita.com.ar). Si fuera necesario y se agregaran nuevos dominios secundarios, estos se irán encadenando agrupándose en estructuras más complejas llamadas Árboles. Cabe destacar que los dominios secundarios tienen el nombre del dominio raíz más el nombre propio (Ej.: sede.ita.com.ar). De esta forma los diferentes grupos de árboles que se irán formando se agruparan en una nueva unidad llamada bosque.

- Un grupo de dominios constituye un árbol
- Un grupo de árboles constituye un bosque.



Es relevante aclarar que existirá o uno o varios controladores de dominio según sea necesario, en base a las necesidades de la red.



2.2 RELACIONES DE CONFIANZA.

Una relación de confianza es la propiedad que posee un dominio para relacionarse con otro, y poder autenticar usuarios de este. Por lo tanto va a existir un dominio que confía (pondrá a disposición de otro un recurso) y otro dominio en el que se confía, el cual podrá autenticar en el primero y utilizar tal recurso. La administración de la seguridad quedara en manos de este último.

Relación de confianza transitiva.

Transitiva es la relación que se da cuando se genera un nuevo dominio secundario, a partir de un dominio ya existente. Cuando esto sucede, se genera automáticamente una relación de confianza con el dominio precedente. Si se generara un nuevo dominio de tercer orden colgado de este último, tendrá relación de confianza con los anteriores de forma que, obteniendo los permisos necesarios, podrá tener acceso a los recursos del servidor anterior y través de este, a la raíz del árbol.

Si se creara un nuevo dominio raíz de un nuevo árbol, los dominios que se generen a partir de este, tendrán relación transitiva y bi-direccional entre si, pero no con los dominios del otro árbol. Solo los dominios raíz tendrán relación directa, por lo cual si se desea utilizar un recurso del otro árbol habrá que subir escalonadamente hasta el dominio raíz y de allí bajar por el otro árbol hasta el dominio buscado.

Relación Intransitiva.

Una relación intransitiva debe generarse manualmente, ya que en Active Directory se generan relaciones de confianza transitivas de forma predeterminada. Este tipo de relación esta limitada por los dos dominios relacionados y no se transmite a los demás dominios del árbol. Toda relación de confianza generada entre dominios pertenecientes a bosques diferentes es intransitiva. Del mismo modo relaciones entre servidores NT y un dominio Windows 2003 también es intransitiva.

Relación de confianza bi-direccional

Una relación bi-direccional refiere al hecho por el cual el dominio A confía en el dominio B y a su vez B confía en A, por lo tanto los usuarios de ambos pueden autenticarse en cualquiera de los dos dominios.

Relación Unidireccional

Una relación de confianza será unidireccional cuando un dominio A confía en otro B, pudiendo sus usuarios autenticar sobre el dominio A, pero los usuarios de A no podrán autenticar en B. Las relaciones de confianza que se generan en Windows 2003 de forma predeterminada, son transitivas y bi-direccionales.

2.3 CONFIGURACIONES PREVIAS

Una vez finalizada la instalación de Windows 2003, en el primer inicio aparecerá el asistente para Administrar el servidor. Sobre esta ventana tildaremos la opción *Configuraré este No mostrar esta página al iniciar sesión* y cerramos la ventana.



Instituto Tecnológico Argentino Técnico en Redes Informáticas

Plan TRI2A05A

Reservados los Derechos de Propiedad Intelectual

Archivo: CAP2A05ATRI0120

ROG: VCG

RCE: RPB

RDC: VCG

Tema: Instalación de Active Directory

Clase Nº: 20

Versión: 1.2

Fecha: 21/6/05

ESTUDIO



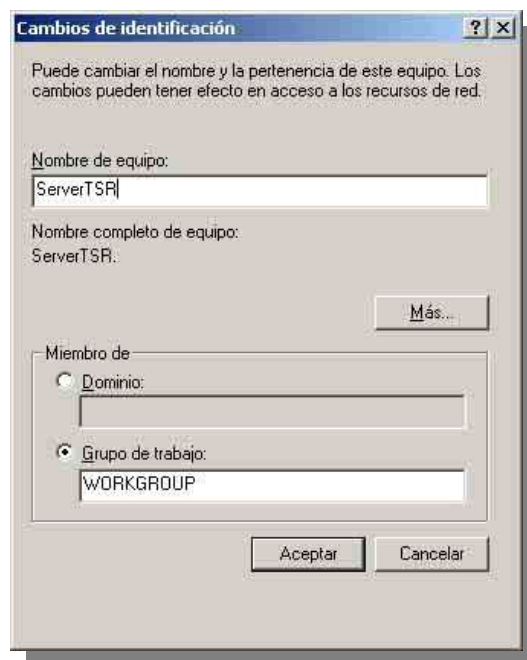
Para comenzar lo primero que debemos hacer es cambiar el nombre de Identificación de la máquina en la red, por lo que haremos clic con el botón secundario sobre Mi PC y elegiremos *Propiedades*. Una vez allí seleccionamos la pestaña *Nombre de Equipo*.

En esta ventana veremos la identificación de red del equipo. Nuestra tarea será cambiar el nombre del equipo para lo cual presionamos el botón *Cambiar*.





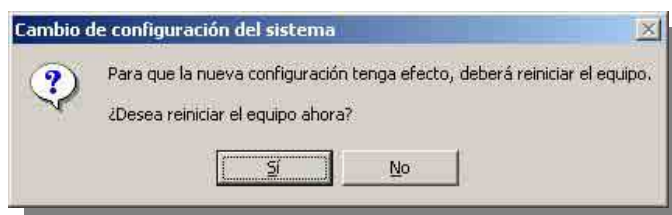
En esta nueva ventana ingresamos el nuevo nombre que le asignaremos al equipo (en nuestro caso: *ServerTSR*) y dejamos el nombre del *grupo de trabajo* (workgroup) sin cambios. Una vez hecho esto presionamos *Aceptar*.



En este momento el asistente nos informa que los cambios se producirán una vez reiniciado el equipo, presionamos *Aceptar*.



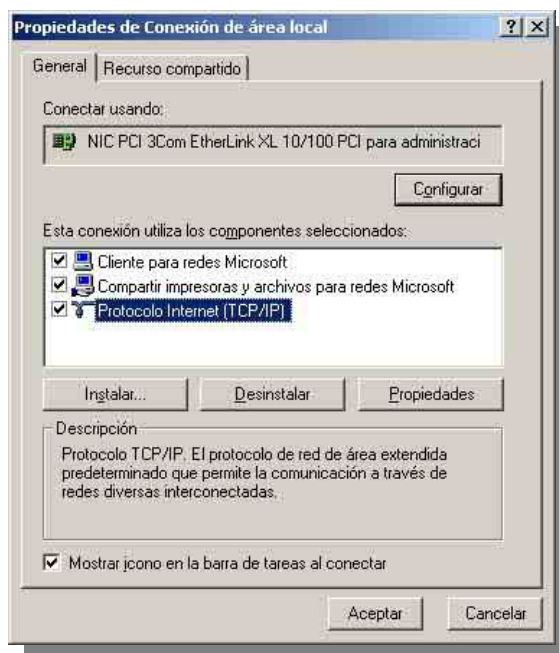
Luego de cerrar la ventana de propiedades de sistema, un mensaje nos informa ahora que deberá reiniciarse el equipo para que la configuración pueda actualizarse, por lo que presionamos el botón *Si* para permitir tal tarea.





Luego de producido el reinicio llegó el momento de configurar la dirección IP que tendrá el equipo, por lo tanto iremos al *Panel de Control*, Conexiones de red y de *Acceso telefónico*, una vez allí haremos botón derecho sobre *Conexión de área local* y elegimos *Propiedades*.

Al abrirse la nueva ventana, seleccionamos la opción Protocolo Internet (TCP/IP) y presionamos el botón *Propiedades*.



En esta ventana debemos asignaremos al servidor una dirección IP de tipo estática, (para lo cual 10.0.0.2 estará bien), luego escribimos la máscara de subred y confirmamos con *Aceptar*.





Instituto Tecnológico Argentino Técnico en Redes Informáticas

Plan TRI2A05A

Reservados los Derechos de Propiedad Intelectual

Archivo: CAP2A05ATRI0120

ROG: VCG

RCE: RPB

RDC: VCG

Tema: Instalación de Active Directory

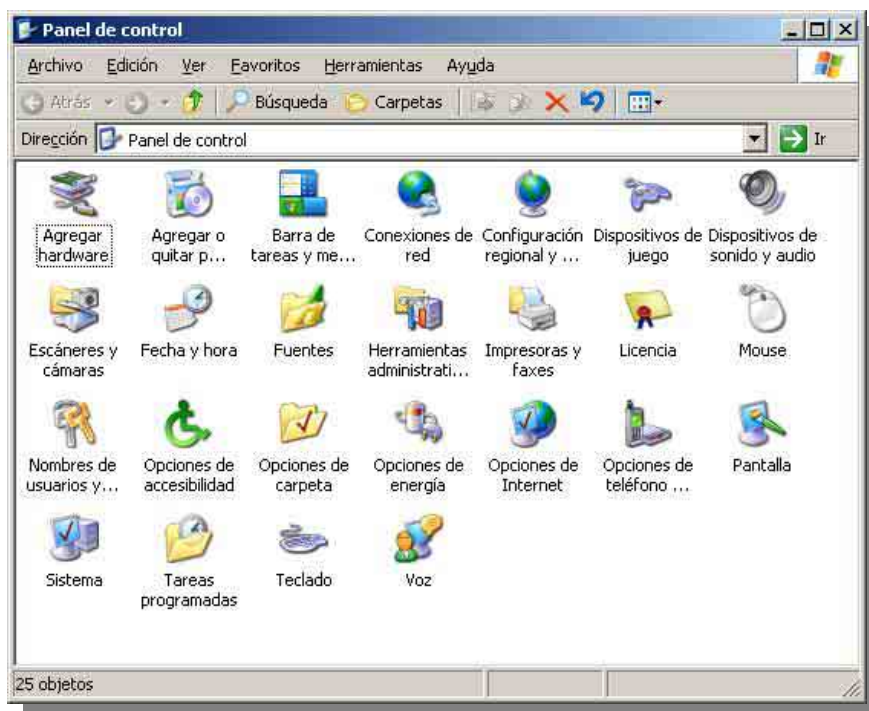
Clase Nº: 20

Versión: 1.2

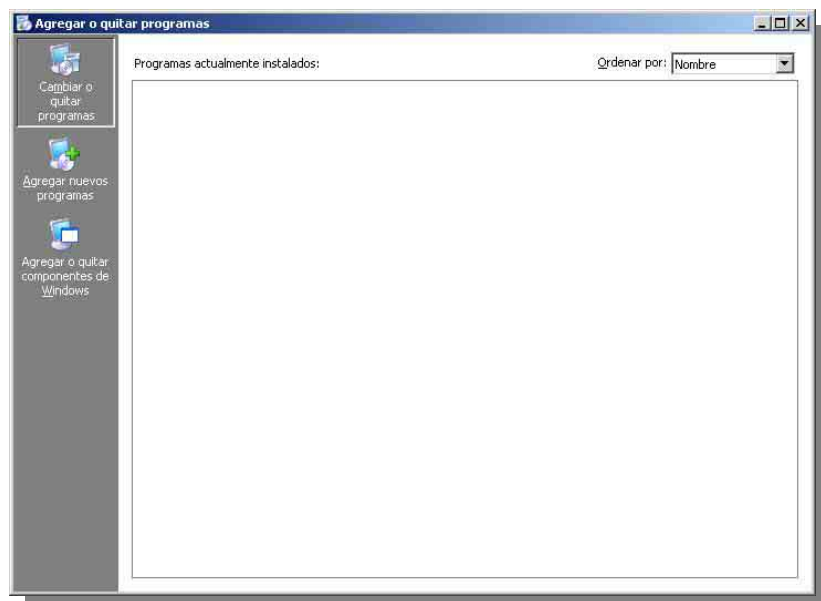
Fecha: 21/6/05

ESTUDIO

Una vez realizadas estas acciones, es hora de instalar el servicio DHCP para lo que iremos nuevamente al panel de control e ingresamos al ítem *Agregar y quitar programas*.

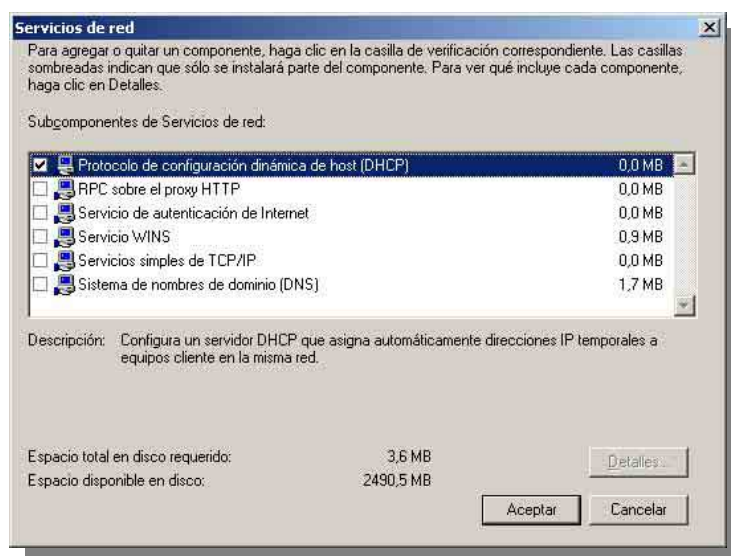


Luego de procesada la lista de los programas que ya están instalados en el equipo, presionamos el botón *Agregar o quitar componentes de Windows*.





Una vez abierta la nueva ventana seleccionamos *Servicios de red* y presionamos *Siguiente*. En la nueva ventana tildamos en la Opción *Protocolo de configuración dinámica de Host (DHCP)* y confirmamos con *Aceptar*.



Luego de realizada esta tarea, podremos observar que figura tildada en la lista la opción seleccionada por nosotros como así también el tamaño de los archivos que se copiarán, por lo que simplemente resta presionar el botón *Siguiente* para que comience la copia.





Instituto Tecnológico Argentino Técnico en Redes Informáticas

Plan TRI2A05A

Reservados los Derechos de Propiedad Intelectual

Archivo: CAP2A05ATRI0120

ROG: VCG

RCE: RPB

RDC: VCG

Tema: Instalación de Active Directory

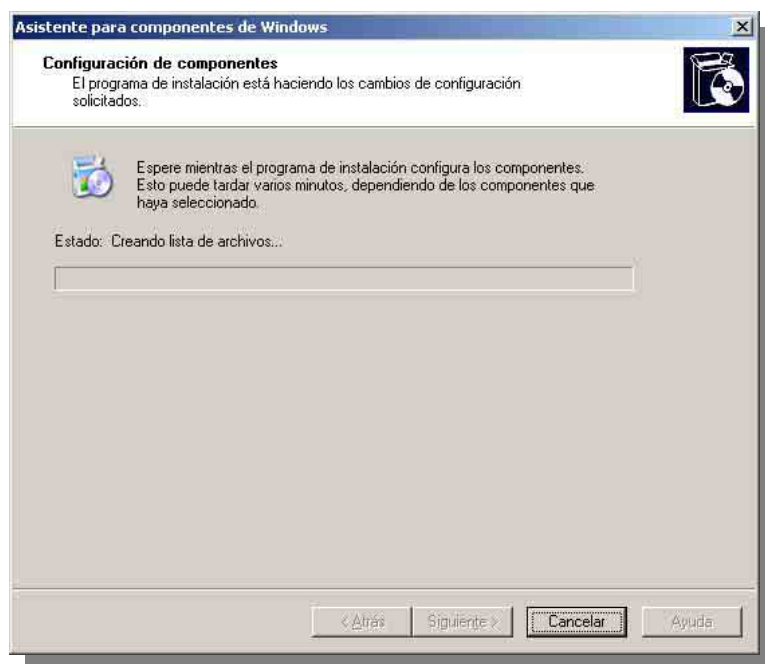
Clase Nº: 20

Versión: 1.2

Fecha: 21/6/05

ESTUDIO

Mediante un indicador de progreso el asistente mostrará el estado de la copia de los archivos necesarios para la instalación del servicio



Una vez concluida la copia de archivos el mismo asistente nos informa de la finalización del proceso, por lo que cerramos la ventana con el botón *Finalizar*.

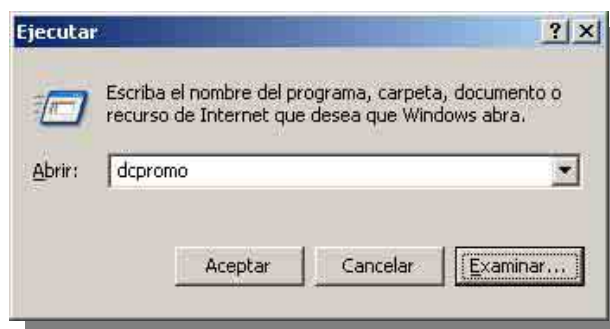




Es necesario una vez finalizado este proceso reiniciar el equipo, para que el servicio DHCP pueda ser levantado por el sistema y, nos permita luego realizar sin problemas las configuraciones que aun faltan. Por lo tanto reiniciaremos el equipo antes de continuar.

2.4 INSTALACIÓN DE ACTIVE DIRECTORY

Ahora nos abocaremos a la tarea de Instalar y configurar Active Directory propiamente dicho, para lo cual nos valdremos de la herramienta llamada dcpromo. Para ejecutarla abrimos *Inicio -> ejecutar* y una vez allí escribimos **dcpromo** y presionamos *enter*.



De inmediato se abrirá el asistente de instalación de Active Directory y su correspondiente pantalla de bienvenida, para continuar hacemos clic en *Siguiente*.





Instituto Tecnológico Argentino Técnico en Redes Informáticas

Plan TRI2A05A

Reservados los Derechos de Propiedad Intelectual

Archivo: CAP2A05ATRI0120

ROG: VCG

RCE: RPB

RDC: VCG

Tema: Instalación de Active Directory

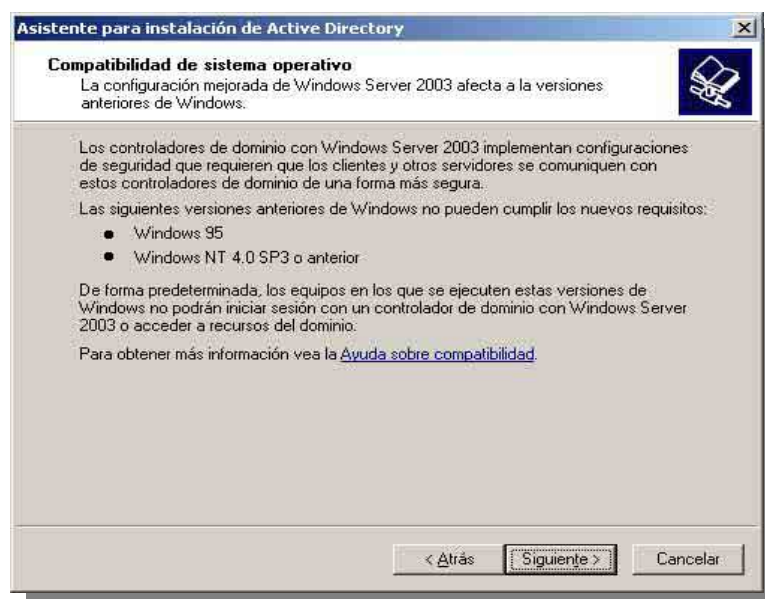
Clase Nº: 20

Versión: 1.2

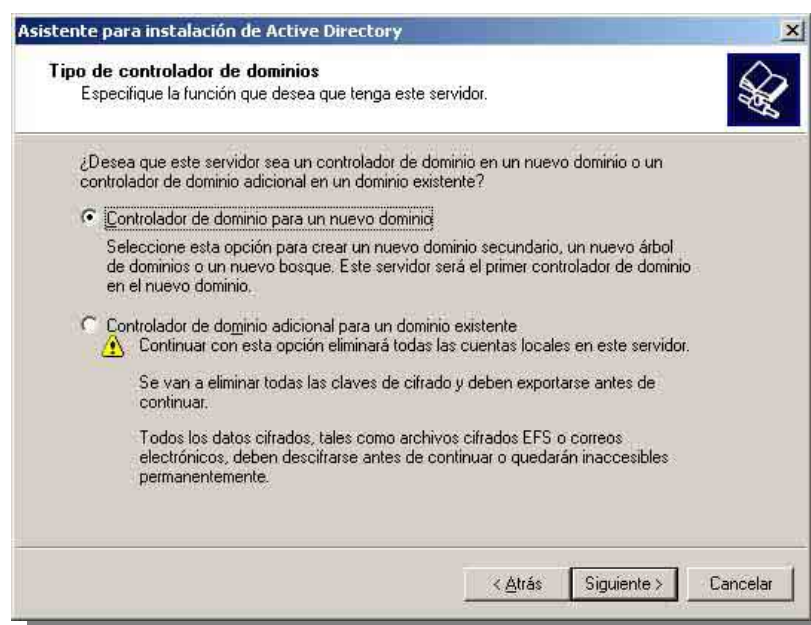
Fecha: 21/6/05

ESTUDIO

Una nueva ventana, nos informa sobre problemas de compatibilidad entre servidores 2003 y sistemas operativos como Windows NT 4 o Windows 95. En esos casos, puestos de trabajo con estos sistemas Operativos no podrán iniciar sesión en el Servidor ni acceder a recursos del mismo, debido a la baja seguridad que manejaban estos sistemas.

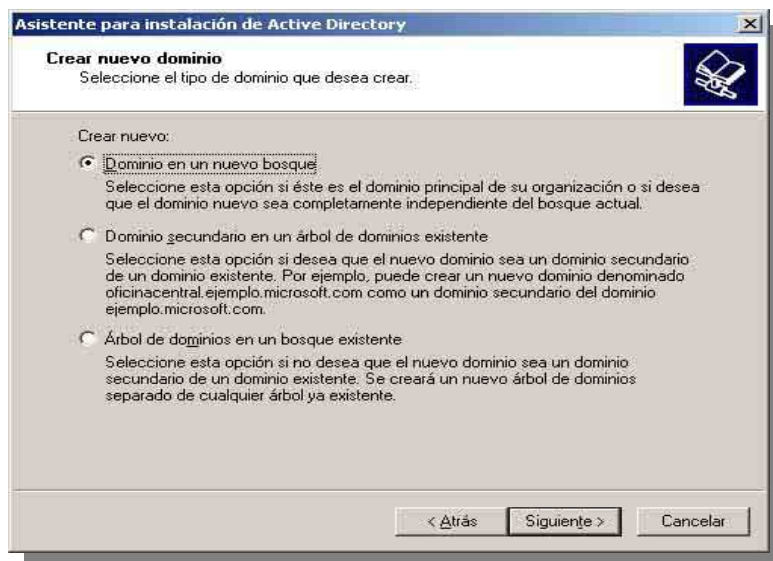


En este momento debemos informarle a Windows si este es el primer dominio de la red o si nos uniremos a un dominio ya existente. En nuestro caso seleccionamos *Controlador de dominio para un nuevo dominio*.





Seguidamente debemos seleccionar si este nuevo dominio será la base para un nuevo bosque, si será un dominio secundario en un árbol existente, o si será un dominio de un nuevo árbol. Seleccionamos *Dominio en un nuevo bosque* y hacemos clic en *Siguiente*.



La nueva ventana permite ingresar el estado del servicio DNS. Si existe un servidor DNS ya funcionando en la red, optaremos por la opción primera. En cambio, y como se da en nuestro caso, elegiremos No de modo que el asistente instale el Servidor DNS en el equipo, y lo deje configurado.





Instituto Tecnológico Argentino Técnico en Redes Informáticas

Plan TRI2A05A

Reservados los Derechos de Propiedad Intelectual

Archivo: CAP2A05ATRI0120

ROG: VCG

RCE: RPB

RDC: VCG

Tema: Instalación de Active Directory

Clase Nº: 20

Versión: 1.2

Fecha: 21/6/05

ESTUDIO

En este momento es hora de darle un nombre DNS a nuestro nuevo dominio, por lo que en esta ventana escribiremos *ita.com.ar* y presionamos *Siguiente*.

Asistente para instalación de Active Directory

Nuevo nombre de dominio
Especifique un nombre para el nuevo dominio.

Escriba el nombre DNS completo para el dominio nuevo
(por ejemplo, *oficinacentral.ejemplo.microsoft.com*).

Nombre DNS completo del nuevo dominio:

< Atrás Siguiente > Cancelar

Ahora debemos asignarle un nombre NetBIOS al servidor, el cual permitirá que estaciones de trabajo “legacy” (léase Win 9x) que no manejan la resolución de nombres vía DNS, puedan identificar dentro de la red al servidor. Nosotros simplemente ingresamos como nombre *ITA* y damos *Siguiente*.

Asistente para instalación de Active Directory

Nombre de dominio NetBIOS
Especifique un nombre NetBIOS para el nuevo dominio.

Éste es el nombre que los usuarios de versiones anteriores de Windows utilizarán para identificar el nuevo dominio. Si desea aceptar el nombre mostrado, haga clic en *Siguiente* o, de lo contrario, escriba un nombre nuevo.

Nombre NetBIOS del dominio:

< Atrás Siguiente > Cancelar



Instituto Tecnológico Argentino Técnico en Redes Informáticas

Plan TRI2A05A

Reservados los Derechos de Propiedad Intelectual

Archivo: CAP2A05ATRI0120

ROG: VCG

RCE: RPB

RDC: VCG

Tema: Instalación de Active Directory

Clase Nº: 20

Versión: 1.2

Fecha: 21/6/05

ESTUDIO

A continuación el asistente requiere la ruta donde se ubicara la base de datos y el registro de Active Directory, dejamos todo tal cual esta y apretamos *Siguiente*.

Asistente para instalación de Active Directory

Carpetas de la base de datos y del registro
Especifique las carpetas que contengan la base de datos y registro de Active Directory.

Para obtener un rendimiento y capacidad de recuperación óptimos, almacene la base de datos y el registro en discos duros separados.

¿Dónde desea almacenar la base de datos de Active Directory?

Carpeta de la base de datos:

¿Dónde desea almacenar el registro de Active Directory?

Carpeta de registro:

< Atrás Siguiente > Cancelar

El próximo paso es configurar la ruta en donde se ubicará la carpeta **SYSVOL**, que será la que contendrá los archivos públicos del servidor. Aceptamos la ruta que nos propone en forma predeterminada y damos *Siguiente*.

Asistente para instalación de Active Directory

Volumen del sistema compartido
Especifique la carpeta que debe compartirse como volumen del sistema.

La carpeta SYSVOL almacena la copia para el servidor de los archivos públicos del dominio. El contenido de la carpeta SYSVOL se replica en todos los controladores de dominio dentro del dominio.

La carpeta SYSVOL debe estar ubicada en un volumen NTFS.

Escriba una ubicación para la carpeta SYSVOL.

Ubicación de la carpeta:

< Atrás Siguiente > Cancelar



Instituto Tecnológico Argentino Técnico en Redes Informáticas

Plan TRI2A05A

Reservados los Derechos de Propiedad Intelectual

Archivo: CAP2A05ATRI0120

ROG: VCG

RCE: RPB

RDC: VCG

Tema: Instalación de Active Directory

Clase Nº: 20

Versión: 1.2

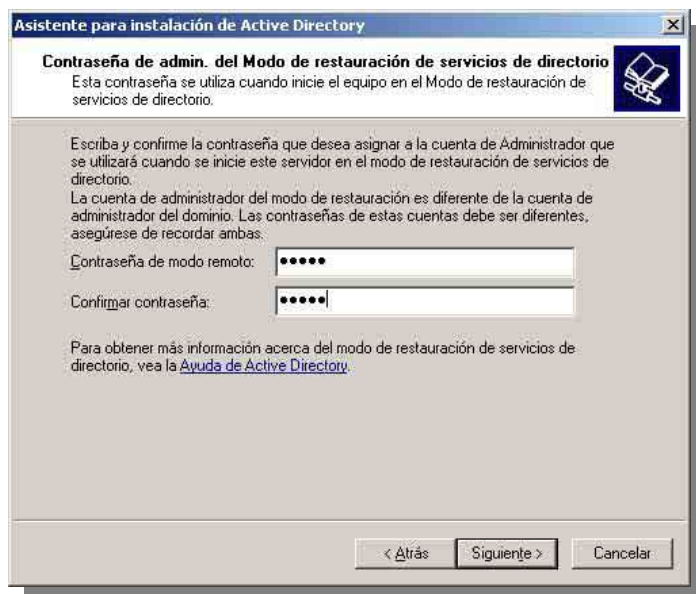
Fecha: 21/6/05

ESTUDIO

Una vez aceptado lo anterior, el asistente nos interroga acerca de la forma en que los programas accederán a la información que se almacena en el controlador de dominio, precisamente si deseamos tener compatibilidad con aplicaciones en servidores PRE-Windows 2000 (por Ej. si existieran servidores Windows NT 4 en la red) o no. En este caso usaremos la opción de *compatibilidad solo con Windows 2000 o 2003 Server*.



En la nueva ventana debemos ingresar la contraseña del administrador y confirmarla, la cual es solicitada para el modo de restauración de Active Directory. Una vez realizado esto presionamos *siguiente*.





Instituto Tecnológico Argentino Técnico en Redes Informáticas

Plan TRI2A05A

Reservados los Derechos de Propiedad Intelectual

Archivo: CAP2A05ATRI0120

ROG: VCG

RCE: RPB

RDC: VCG

Tema: Instalación de Active Directory

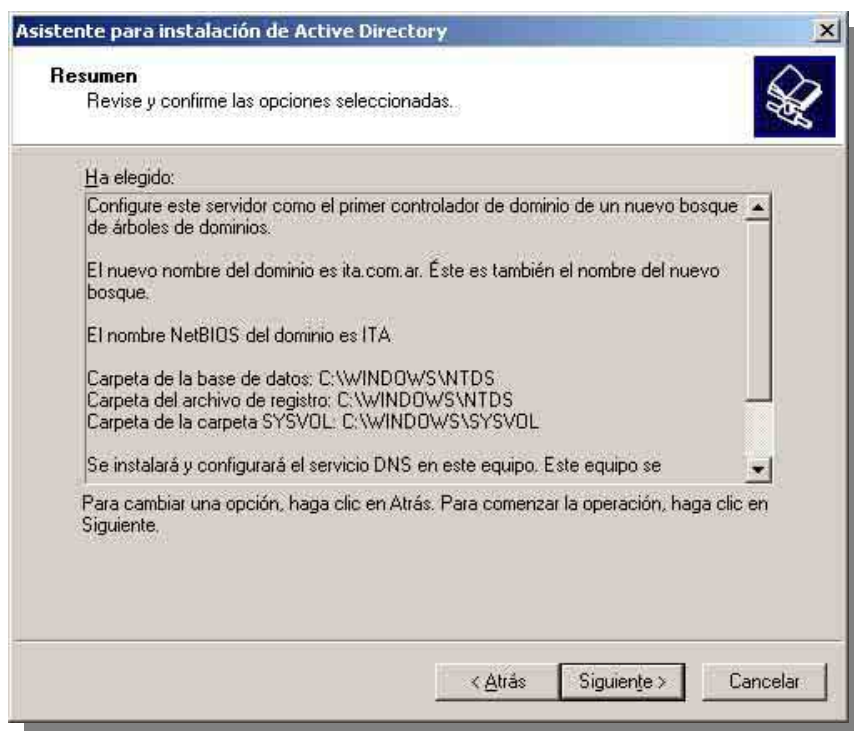
Clase Nº: 20

Versión: 1.2

Fecha: 21/6/05

ESTUDIO

Paso seguido, el asistente nos mostrará un resumen de las opciones elegidas, debiendo presionar *Siguiente* para iniciar la copia de archivos.



En cierto momento, el asistente nos puede solicitar el CD del producto Windows 2003 Server, en ese caso insertamos el CD y presionamos *Aceptar*. También durante el mismo proceso, se copiarán los archivos necesarios y se configurará el servidor DNS por lo tanto, será posible ver la pantalla de copia de archivos correspondiente.



Una vez concluido el proceso el asistente nos informa sobre la finalización de la instalación de Active Directory, por lo tanto cerraremos la ventana presionando *Finalizar*.



Una vez cerrado el asistente, el sistema nos informa sobre la necesidad de reiniciar el equipo, para que los cambios tengan efecto, por lo que permitiremos este procedimiento presionando *Reiniciar ahora*.



Una vez finalizado el reinicio, el servicio Active Directory ha quedado instalado en nuestro servidor. Por lo que solo nos restarán algunas configuraciones adicionales, para poder dejarlo totalmente operativo y funcional.



NOTAS

[illegible]



CUESTIONARIO CAPITULO 20

1.- ¿Cuáles son las principales funciones del servicio de directorio de Windows Server 2003?

2.- ¿Qué es un dominio? ¿Quien lo administra?

3.- En Active Directory ¿Qué es un Árbol? ¿Que un Bosque?

4.- ¿Cómo serían las relaciones de confianza entre Dominios de distinto Bosque?

5.- ¿Cuál es el resultado de elegir la opción “Dominio secundario en un Árbol de Dominios Existente”?
