

Redes en Windows 98/2000

Autor: Luis Uceda
07 de Octubre, 2002

Windows 98/2000

- ☞ Un PC con una de las siguientes funciones:
 - existe jerarquía de ordenadores
 - Servidor:
 - proporciona servicios de fichero, impresión, web, etc... a los clientes
 - Cliente:
 - realiza peticiones al servidor para acceder a los recursos de red
 - se identifica una vez por medio de nombre/contraseña
 - El control de los recursos es responsabilidad del servidor

(Cliente/Servidor)

Distribución lógica de redes

Repaso
3

Cliente/Servidor

- ☞ Concepto de dominio
 - Grupo de PC's que disponen de un conjunto de recursos que comparten y cuyo mecanismo de control esta centralizado en uno ó más servidores (Controladores de dominio)
- Inicio de sesión:
 - Es el primer paso que tiene que realizar un cliente para acceder a los recursos de red
 - DOS tipos de sesiones:
 - INICIO DE SESIÓN LOCAL
 - INICIO DE SESIÓN EN EL DOMINIO

Repaso

- ☞ Tipos de redes según su distribución lógica:
 - Un equipo que funciona tanto como cliente (*accediendo a recursos compartidos*) como servidor (*ofreciendo recursos*)
 - No existe jerarquía de ordenadores
- (RED de IGUALES)
- Cada Usr. comparte los recursos propios de su ordenador
 - La responsabilidad del acceso es del PC que los comparte

Cliente/Servidor

- ☞ Inicio de sesión LOCAL:
 - Un usuario se valida en el sistema de seguridad del propio equipo
- ☞ Inicio de sesión en el Dominio:
 - Un Usr se valida para acceder a todos los recursos del dominio.
 - Esta validación se realiza en uno de los controladores de dominio

Windows 98/2000

- ☞ Sistema Operativo Windows 2000
 - S.O. De funciones específicas, contemplando arquitectura cliente/servidor con software específico para ellos.
 - Tres tipos de S.O.
 - Windows 2000 Server
 - Windows 2000 Advanced Server
 - Windows 2000 Professional

Windows 98/2000

- ☞ Otros servidores Windows 2000
 - Windows 2000 Advanced Server
 - Extiende las funciones de Windows 2000 Server para incluir equilibrio de carga y agrupamientos.
 - Hasta 4 CPU's
 - Windows 2000 Datacenter Server
 - Sistema de agrupamiento más avanzado que el anterior.
 - Admite hasta 16 CPU's

Windows 98/2000

- ☞ Windows 2000 Professional
 - diseñado para trabajar como cliente,
 - va dirigido a Usr's finales
 - limitado conjunto de servicios

Redes en Windows 98/2000

Protocolo Netbios
3.1

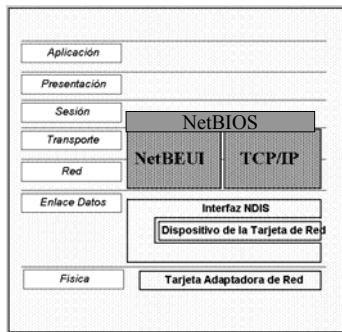
Windows 98/2000

- ☞ Windows 2000 Server
 - diseñado para ofrecer servicios y recursos a otros sistemas de la red.
 - Sustituye a Windows NT 4.0 Server
 - Admite hasta 2 CPU's

NetBIOS

- ☞ Network Basic Input/Output System:
 - Protocolo de resolución de nombres entorno windows
 - Funciona en N5 (nivel de aplicación)
 - Se puede encapsular (transportar)
 - TCP/IP (se conoce como NBT –NetBIOS sobre TCP/IP)
 - NetBEUI
 - Proporciona una apariencia uniforme a todas las redes Windows independientemente de los protocolos anteriores

Arquitectura NetBIOS



Activación NetBIOS

- ☞ Solo cuando se desea formar parte de un grupo de trabajo en red
- ☞ Cuando se configura el PC:
 - como un servidor de usuarios
 - Como un servidor de archivos

NetBIOS

- ☞ Proporciona un conjunto de API's (Access Point interface)
 - Permite acceder a los recursos o aplicaciones del sistema
 - Servicios de la capa de sesión usados por:
 - Resolución de nombres WINS
 - Transferencia de información entre equipos windows

Como activar NetBIOS/TCP

- ☞ Averiguarlo a través del menú
 - Funciona con W98 y con W2000 (para proporcionar servicios WINS) donde se guarda la BBDD de Netbios.
 - Red → propiedades tcp/ip ↔ netbeui
 - Verificar que esta habilitado
 - Para deshabilitar:
 - Red → cliente para redes microsoft (permiso de acceso a recursos compartidos de red)
 - Red → Inicio de sesión en microsoft family
 - "BORRARLOS" <QUITAR>
 - Verificar que ya se puede "habilitar/Deshabilitar"

Puertos NetBIOS/TCP

- ☞ Utiliza los puertos 137, 138, 139 de TCP-UDP
- ☞ Protocolo exclusivo de windows
- ☞ Se puede averiguar si esta activado por medio del comando *netstat -an*
- ☞ Este comando nos informa del estado de los puertos tanto TCP como UDP.
 - Activos -> "LISTENING"

Como activar NetBIOS

- Volver a restaurar la situación anterior
 - Red → cliente para redes microsoft (permiso de acceso a recursos compartidos de red)
 - Red → Inicio de sesión en microsoft family

Ej: Cuando Activar NetBIOS

- ☞ Dados los siguientes supuestos, indicar en cada uno de ellos como debería estar el protocolo NetBIOS (activado/desactivado)
 - Un servidor web
 - Una estación windows conectada a Internet mediante un modem
 - Una estación windows que forma parte de una de las subredes de una organización
 - Un servidor de usuarios y archivos

Funciones de W 2000 Server en una red

- ☞ Tres funciones
 - Servidor de dominio
 - Actua como Controlador de dominio
 - Servidor miembro
 - Actua como servidor de aplicaciones, impresión, etc...
 - Servidor Independiente
 - cuando se incorpora a un grupo de trabajo

Redes en Windows 98/2000

WINDOWS 2000 Server
Creación de un servidor de
Usuarios y Archivos
3.2

Redes en Windows 98/2000

Controlador de DOMINIO
"Active Directory"
3.2

Servicios de W 2000 Server

- ACTIVE DIRECTORY (Controlador de dominios)
- SERVIDOR DE ARCHIVOS (a otros sistemas de la red)
- SERVIDOR DE IMPRESIÓN
- SERVIDOR WEB (incluye FTP, correo y Web)
- SERVIDOR DE FUNCIONES DE RED (DNS, DHCP, RAS)
- SERVIDOR DE APLICACIONES (terminal server, BBDD)
- AVANCED SERVER (colas de mensajes, autoridad de certificación, instalación remota)

Active Directory

- Definición:
 - SERVICIO de directorio
 - Extensible
 - Escalable
- !!Es el corazón de Microsoft 2000!!
- Permite administrar eficientemente los recursos de red actuando como un centro de información de red para que los clientes busquen los recursos
 - Cualquier tarea administrativa se ve afectada por el Active Directory.
 - Permite controlar la seguridad de la red

Active Directory

- Conceptos manejados
 - Clases
 - Todos los Objetos se organizan en clases
 - Objeto
 - Es cualquier elemento ó recurso que se puede encontrar en la red
 - EJ: USUARIO, IMPRESORA, GRUPO, CARPETA...
 - Propiedades del objeto
 - Son los atributos del objeto
 - EJ: De USUARIO:
Nombre, Apellidos, Ciudad....
 - EJ: De Impresora:
Velocidad de impresión, características de color...

Modos de dominio

- ☞ Nativo
- ☞ Mixto

Active Directory

- Conceptos manejados
 - Diferencia entre clase y objeto
 - CLASES:
 - Representan la idea que tenemos de los objetos
 - OBJETOS:
 - Son casos concretos de clases

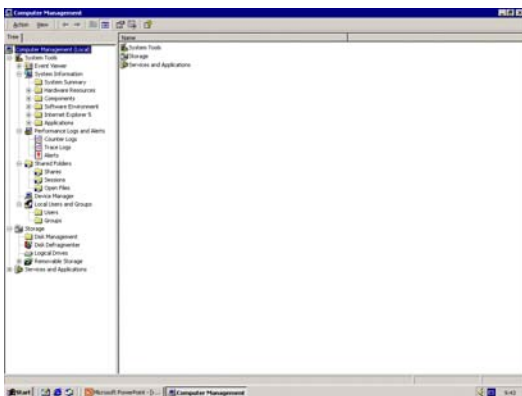
EJ: CLASE USUARIOS

OBJETO: Antonio Gomez Perez, Madrid

ATRIBUTOS:
Nombre Apellidos Ciudad

Modos de dominio

- ☞ Nativo:
 - Todos los controladores ejecutan W 2000 server
 - no hay controladores Windows NT Server
- ☞ Mixto:
 - Permite trabajar con controladores de dominio distintos de W 2000 server
 - W NT server



Clientes de Active Dir.

- ☞ Cualquier estación cliente
 - W 95, W 98 y W 2000 que tengan instalado el software cliente de Active Directory
 - W NT y los anteriores sin el software Active Directory
 - acceden a la red como si estuviesen en un dominio de W NT (Se debe configurar en el A.D.)

Tecnología de Active Dir.

- Utiliza los servicios de DNS
 - Por ello:
 - Organización JERARQUICA
 - Igual que con DNS se pueden definir dominios
 - Públicos
 - Privados
 - Mismo formato de estructura organizativa
 - Dominio principal
 - Subdominios (dominios secundarios)

Estructura Física

- Para que se utiliza la estructura física "Sitio"
 - Se utilizan para obtener la estructura física de la red
 - Son mapas independientes de las estructuras lógicas de dominio
 - No necesitan relación
 - Puede crear varios sitios dentro de un mismo Dominio
 - Un host está asignados a un sitio y debe pertenecer a una subred de ese sitio
- Los sitios y las subredes son accesibles a través de "Sitios y Servicios de Active Directory"

Estructura Active Directory

- Estructuras físicas
 - Subredes
 - Sitios
 - Estructuras lógicas
 - Dominios
 - Arboles de dominio
 - Bosques de dominio
 - Unidades organizativas
- !! MISMA ESTRUCTURA QUE DNS !!

Estructuras lógicas

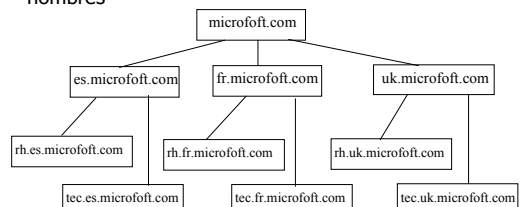
- Dominios
 - Nombres Unicos
 - No deben entrar en conflicto con otros dominios en el mismo entorno
 - Si son Públicos:
 - Deben registrarse en el InterNIC ó a través de las empresas de registro autorizadas
 - Un dominio se puede expandir a través de más de una localización física.
 - Cada dominio tiene un nombre de DNS

Estructura Archive Dir.

- Estructuras físicas
 - Subredes
 - Un grupo de red con un rango específico de direcciones IP y una máscara común
 - Sitios
 - Una ó más subredes que se utilizan para configurar el acceso al directorio y la replicación.

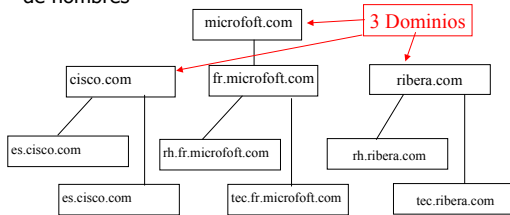
Estructuras lógicas

- Arbol de Dominios: Estructura continua de nombres



Estructuras lógicas

- ☛ Bosques de Dominios: Estructura discontinua de nombres

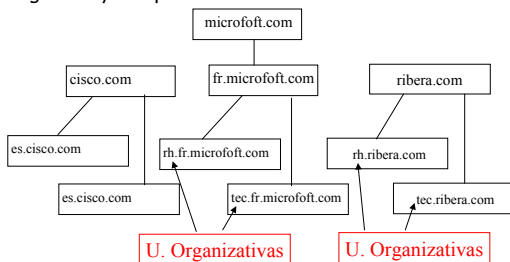


Servidor de Usuarios y Archivos

Gestión de Usuarios
"Grupos locales y Globales"

Estructuras lógicas

- ☛ Unidades organizativas: Subgrupos dentro de un dominio que comparten la misma política de gestión y participación de recursos.



Servidor de usuarios (Cuentas)

- ☛ Dos tipos de cuentas:
 - De Usuarios
 - De Grupo

Unidades Organizativas

- ☛ Se crean para reflejar la estructura de la empresa, organización ó negocio

Cuentas de Usuario

- ☛ De Usuario
 - Permite a estos iniciar la sesión en la red y acceder a los recursos de la misma
 - Dos tipos de cuentas de Usuario:
 - Cuentas USUARIOS DE DOMINIO:
 - Son las definidas en el Active Directory (guardadas en él)
 - pueden acceder a los recursos del Dominio
 - Cuentas USUARIOS LOCALES
 - Son las definidas en el equipo local.
 - Solo acceden a recursos locales.
 - Debe autenticarse a si misma para acceder a los recursos de red
 - Solo se guarda en el equipo al que se desea acceder

Cuentas Predeterminadas de Usuario (Built-in)

- Administrador
- Invitado
- Son cuentas locales para los sistemas individuales, estaciones de trabajo y servidores miembro donde están instaladas
- Tienen su reflejo en Active Directory.
 - Tienen acceso completo al dominio

Cuentas de Grupo

- ☞ De Grupo
 - Sirven para administrar las cuentas de varios usuarios (Con ellas **NO SE PUEDE** iniciar una sesión)
 - tres tipos de grupos:
 - GRUPOS LOCALES:
 - Definidos en un equipo local
 - Se utilizan solo en el equipo local
 - GRUPOS DE SEGURIDAD:
 - Los grupos pueden tener descriptores de seguridad asociados a ellos
 - GRUPOS DE DISTRIBUCIÓN:
 - Grupos usados para listas de correos (no tienen descriptores de seguridad)

Cuenta de Administrador

- Proporciona acceso completo a los archivos, directorios, servicios y otras facilidades.
- Es una cuenta que **NO SE PUEDE ELIMINAR** ó deshabilitar
- Tiene acceso solamente al sistema local
- Si está en Active Directory, tiene acceso completo al dominio y sus privilegios

Ambito de los Grupos

- Los grupos pueden tener **DIFERENTES AMBITOS** ó áreas en los que son validos:
 - **AMBITO DE DOMINIO LOCAL**
 - **AMBITO DE DOMINIO LOCAL INTEGRADOS**
 - **AMBITO DE DOMINIO GLOBAL**
 - **AMBITO DE DOMINIO UNIVERSAL**

Cuenta de Invitado

- ☞ Diseñada para usuarios que necesitan acceder de forma esporádica al sistema.
 - Inicialmente esta deshabilitada por seguridad

Ambito de los Grupos

- ☞ Grupos de **AMBITO DE DOMINIO LOCAL**
 - Grupos que se utilizan para garantizar permisos dentro de un único dominio
 - Pueden incluir solo cuentas (Usr, Grupo) y del dominio en el que se definen
 - Se utilizan para administrar el acceso a los recursos tales como impresoras y carpetas
 - Incluyen objetos de recursos

Ambito de los Grupos

- ☞ Grupos de *AMBITO de DOMINIO LOCAL INTEGRADOS* (Ya existentes)
 - Tienen ambito especial de grupo y tienen permisos de Dominio Local.
 - No se pueden crear ni eliminar, solo modificar
 - Se utilizan para GARANTIZAR a un USUARIO permisos y privilegios de grupo.

Ambito de los Grupos

- ☞ Ambito de los Grupos a crear si se tiene UN DOMINIO
 - Estructuras de grupo de
 - Grupos de *AMBITO DE DOMINIO LOCAL*
 - Grupos de *AMBITO DE DOMINIO GLOBAL*

Ambito de los Grupos

- ☞ Grupos de *AMBITO de DOMINIO GLOBAL*
 - Son grupos que se utilizan para dar permisos a objetos en cualquier dominio
 - Solo pueden incluir cuentas y grupos de dominio en el que estan definidos
 - Se utilizan para administrar cuentas de usuario y grupo en un dominio particular (otorgando permisos de acceso a un recurso haciendo al grupo con ambito global como miembro del grupo con ambito de dominio local)

Grupo de cuentas de Usuario

Clase de grupo de usuario	Entrono de red	Ambito de grupo	Miembro
Usuarios	<ul style="list-style-type: none"> ☞ Dominio Act. Dir ☞ Servidor miembro de Dominio ☞ Estación de trabajo 	<ul style="list-style-type: none"> ☞ Local Integrado ☞ Local 	<ul style="list-style-type: none"> ☞ Usuarios autenticados ☞ Usuarios de Dominio
Usuarios	<ul style="list-style-type: none"> ☞ Estación de trabajo independiente ☞ Servidor 	<ul style="list-style-type: none"> ☞ Local 	<ul style="list-style-type: none"> ☞ Cuenta de Usuario seleccionada durante la instalación del S.O.
Usuarios de Dominio	<ul style="list-style-type: none"> ☞ Dominio de Active Directory 	<ul style="list-style-type: none"> ☞ Global 	<ul style="list-style-type: none"> ☞ Administradores ☞ Invitados

Ambito de los Grupos

- ☞ Grupos de *AMBITO de DOMINIO UNIVERSALES*
 - Utilizados para dar permisos a gran escala en el arbol de dominio o bosque (distintos dominios con los mismos permisos)
 - NO SE necesita utilizar GRUPOS UNIVERSALES si SOLO se tiene UN DOMINIO

Grupos de Equipo

Clase de grupo de Equipos	Entrono de red	Ambito de grupo	Miembro
Equipos de Dominio	<ul style="list-style-type: none"> ☞ Dominios de Active Directory 	<ul style="list-style-type: none"> ☞ Global 	<ul style="list-style-type: none"> ☞ Todos los Servidores miembro ☞ Estaciones de trabajo del Dominio
Controladores de Dominio	<ul style="list-style-type: none"> ☞ Dominios de Active Directory 	<ul style="list-style-type: none"> ☞ Global 	<ul style="list-style-type: none"> ☞ Todos los Controladores de Dominio

Se utilizan para identificar y configurar los permisos predeterminados

Creación de cuentas USUARIO

- Usuarios de dominio
 - Crear un objeto en Active Directory
 - Permisos de administrador
 - Se pueden crear
 - en la carpeta USERS
 - En otra carpeta específica
 - Ej: Unidad organizativa MARKETING

Contraseñas y Directivas de las Cuentas

- Sirven para autenticar el acceso a los recursos
 - Las cuentas en W2000 utilizan
 - certificados públicos
 - Contraseñas
 - Conjunto de hasta 104 caracteres
 - Letras,
 - Números
 - Símbolos
 - Son directivas de Seguridad a aplicar en las cuentas

Creación de cuentas USUARIO

- Para crear una Cuenta tiene que considerar los aspectos de organización y configuración con DIRECTIVAS apropiadas.
- Esquema de nombres para las cuentas
 - Nombre para mostrar (maximo 64 caracteres)
 - Nombre completo que se muestra a los usuarios y que se referencia en las sesiones de usuarios
 - Nombre de inicio de sesión (recomendado menos de 64)
 - Nombre utilizado para el inicio de la sesión.

Directivas de Cuentas

- De contraseñas
- De Bloqueo de cuentas
- Kerberos

Creación de cuentas USUARIO

- Contraseñas
 - Vigencia, Historial de contraseñas, longitud mínima, etc
- Derecho de los usuarios
 - Privilegios, permisos de acceso e inicio de sesión
- Opciones de cuentas
 - Detalles adicionales con información que completa la ficha de la cuenta

Directivas de Contraseñas

- Con estas directivas, se puede:
 - Forzar el historial de contraseñas
 - Vigencia máxima de la contraseña
 - Vigencia mínima de la contraseña
 - Longitud mínima de la contraseña
 - Otras directivas

Directivas de Bloqueo de Cuenta

- ☞ Controla como y cuando se bloquean las cuentas en el dominio y en el sistema local:
 - Umbral de bloqueo de cuenta
 - Numero de intentos...
 - Duración del bloqueo de cuenta
 - Restablecer umbral del bloqueo de cuenta despues de.
 - Cada vez que un intento de inicio de sesión falla, se eleva el umbral

Variables de entorno

- ☞ %SystemRoot%
 - Directorio principal para el S.O.
- ☞ %UserName%
 - Nombre de cuenta del usuario
- ☞ %HomeDrive%
 - Letra del disco de directorio principal del Usr
- ☞ %HomePath%
 - Ruta completa del directorio principal en el disco base
- ☞ %Processor Architecture%
 - La arquitectura del procesador (Ej: x86)

Creación de cuentas GRUPO

- Cuentas de Grupo
 - Se utilizan las mismas herramientas que para usuarios
- Organización de los grupos:
 - Se pueden estructurar de muchas formas:
 - Para departamentos dentro de la organización
 - Grupo de usuarios de aplicaciones específicas
 - Cargos dentro de la organización

Parámetros del entorno de usuario

- ☞ Perfiles
 - Proporcionan las configuraciones de entorno para los usuarios
 - Cada vez que un Usr. Inicia la sesión en el equipo, se utiliza para personalizar el escritorio, panel de control, etc
 - Estos perfiles pueden residir
 - en el Equipo Local
 - en el Servidor de Dominio (PERFILES MOVILES)

Parámetros del entorno de usuario

- ☞ Las cuentas de Usuario pueden tener:
 - Perfiles
 - Archivos de comandos de inicio de sesión
 - Directorios Base asociados

HACEN USO DE LAS VARIABLES DE ENTORNO DEL SISTEMA

Parámetros del entorno de usuario

- ☞ Archivo de Comandos de inicio de sesión
 - Archivo tipo xxxx.bat
 - Archivos por lotes que se ejecutan cada vez que el usuario inicia una sesión
 - Se suelen utilizar para incluir conexión a unidades de red
 - Ejemplo: net use u:\servidor\ruta\carpeta usuario

Parámetros del entorno de usuario

- ☞ Ruta de acceso local (DIRECTORIO BASE)
 - Directorio que debería utilizar el Usr. para guardar sus archivos.
 - Puede estar:
 - En el EQUIPO LOCAL
 - En un SERVIDOR DE LA RED

Grupo Global "Procedimiento de creación"

- *USUARIOS Y EQUIPOS* boton derecho *Nuevo grupo*
 - *Escriba el nombre*
- Seleccione el ambito *GLOBAL*
- Seleccione el tipo de grupo *SEGURIDAD*

Cuentas de Usuario de dominio "Procedimiento de creación"

- ☞ Con la herramienta: *USUARIOS Y EQUIPOS* de ACTIVE DIRECTORY
 - Se deben crear en un dominio ó dentro de una unidad organizativa
 - Hay que crear objetos USUARIO

Grupo Local "Procedimiento de creación"

- Con la herramienta: *COMPUTER MANAGER* → Computer manager (local) y boton derecho → Conectar a otro equipo
 - Puede seleccionar el sistema cuyas cuentas que quiere administrar
 - Expanda el nodo *HERRAMIENTAS de Sistema (+)* y escoja *Usuarios locales y grupos* → *Grupos* → *Nuevo grupo* (Rellene los campos que se pide)

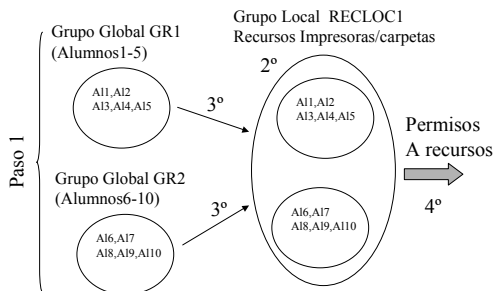
Cuentas de Usuario locales "Procedimiento de creación"

- Con la herramienta: *COMPUTER MANAGER* → Computer manager (local) y boton derecho → Conectar a otro equipo
 - Puede seleccionar el sistema cuyas cuentas quiere administrar
 - Expanda el nodo *HERRAMIENTAS de Sistema (+)* y escoja *Usuarios locales y grupos* → *Usuarios* → *Nuevo usuario* (Rellene los campos que se pide)

Asociar Usr's a Grupos "Procedimiento de creación"

- Se pueden agregar usuarios a grupos Globales ó Locales
- Se sigue el mismo procedimiento:
 - Seleccionar Usuarios y grupos y <Agregar>
 - Seleccionar los usuarios que se agregarán al grupo

Resumen creación de cuentas



Instalar Active Dir. en Serv.

- Formar grupos de trabajo para la realización de las practicas
- 4 grupos --> 4 dominios
 - grupo1.redes
 - grupo2.redes
 - grupo3.redes
 - grupo4.redes

Practica 1

Instalar Active Dir. en Serv.

Crear Unidades Organizativas

- Como se crearía una unidad organizativa
- Herramienta *USUARIOS y EQUIPOS*
 - Expanda el nodo de Dominio (+)
 - Click con boton derecho y seleccione *NUEVA UNIDAD ORGANIZATIVA*
 - Escriba el nombre y <ACCEPT>

Instalar Active Dir. en Serv.

- Debe tener instalados previamente los servicios de DNS
- Instalar Act. Dir:
 - Se ejecuta desde INICIO→ejecutar→cmd:"dcpromo" <aceptar>
 - Dos situaciones:
 - Existe un dominio
 - Se instala sobre el dominio
 - NO Existe un dominio
 - El asistente le ayuda a crear un dominio y también subdominios
 - se convierte en el CONTROLADOR DEL DOMINIO

Instalar Clientes de A.D.

- En estaciones cliente W9x
- Inserte el CD de W 2000 server
 - Con explorar busque en la unidad CD el fichero Dsclient.exe en la carpeta del CD "Clients\Win9x"
 - <Accept>
 - Aparecera el asistente y se deben seguir los pasos que indica hasta conseguir la instalación

Practica 2

Crear Cuentas de Usuario y Grupos

Verificación de equipos dentro del dominio

- ☞ Se puede saber los equipos que estan dados de alta en el dominio
 - COMPUTER MANAGER →

Integración de clientes

- ☞ Hay que darse de alta en el dominio
 - Solo puede hacerlo un usuario autorizado
 - Permisos de Administrador
 - Debe registrarse
 - el quipo
 - el usuario (administrador)
 - Datos necesarios:
 - Nombre del equipo. Ya especificado en el equipo
 - Usuario: "administrador" passw "dustin"
 - Nombre del dominio: Nombre SIN EXTENSION"

Verificación de usuarios dentro del dominio

- ☞ Se puede saber los usuarios que estan accediendo al dominio
 - COMPUTER MANAGER →session

Integración de clientes

- ☞ Hay que darse de alta en el dominio
 - con esto el controlador registra el equipo y lo da de alta en el dominio
 - Pedirá que se resetee el equipo para coger la nueva configuración

Verificación de estar dentro del dominio

- ☞ La forma más sencilla de verificar si realmente se esta dentro del dominio deseado:
 - Mi PC --> Propiedades --> Identificación de red
 - resultado:
 - Nombre completo del equipo
 - NETOPENxxxxx.dominio
 - Dominio:
 - Nombre del dominio creado por cada grupo

Redes en Windows 98/2000

Servidor de Ficheros 3.3

Servidor de Archivos

- ☞ Estructura de las unidades de almacenamiento de un equipo
 - Computer Manager (local) → Almacenamiento → Administración de discos
- Pueden ser tanto NTFS como FAT 32

Creación de un servidor de archivos

Creación de Carpetas

Carpetas compartidas

- ☞ Tipos de carpetas
 - Publicas para los usuarios locales del equipo
 - Privadas para los usuarios del equipo
 - Publicas para usuarios remotos

Servidor de Archivos

- ☞ Estructura de archivos de Windows 2000
 - Los volúmenes pueden ser:
 - FAT 16 (llamado volumen FAT)
 - Admite tabla de asignación de archivos de 16 bits
 - Volúmenes menores de 2 GB
 - Nombre de archivos menores de 8 caracteres
 - FAT 32
 - Admite tabla de asignación de archivos de 32 bits
 - Volúmenes de hasta 32 GB
 - NTFS 4.0
 - Permite controles de acceso locales y remotos pero no admite la mayoría de las características de Windows 2000
 - NTFS 5.0
 - Igual que 4.0 y admite todas las características de Act. Directory
 - Admite cuota de disco, cifrado y almacenamiento remoto

Carpetas compartidas

- ☞ Tipos de carpetas compartidas para usuarios remotos
 - Dedicadas Para grupos de trabajo
 - Personales Para usuarios de grupo
 - Publicas para todos los accesos remotos

Seguridad en Carpetas compartidas

Los recursos compartidos deben ser controlados con

- Permisos específicos
- 2 Tipos de permisos para acceder a carpetas y archivos
 - Permisos de ARCHIVOS Y CARPETAS
 - Llamados permisos de *SEGURIDAD*
 - Permisos de RECURSOS COMPARTIDOS
 - Llamados permisos de *COMPARTIR (Shared)*

Acceso a Carpetas Compartidas

Permisos de *COMPARTIR*

- Sin acceso
 - No se otorga ningún permiso sobre el recurso
- Leer
 - Se puede ver los nombres de archivos y carpetas
 - Tener acceso a recursos, leer los datos y atributos y ejecutar
- Cambiar
 - Lo mismo que Leer
 - Cambiar atributos, Crear, Eliminar y modificar carpetas y archivos
- Control total
 - Permisos de Leer y Cambiar. Además cambiar permisos

Seguridad en Carpetas compartidas

En volúmenes NTFS

- Permisos de *SEGURIDAD* (ARCHIVOS Y CARPETAS)
- Permisos de *COMPARTIR* (RECURSOS COMPARTIDOS)

En volúmenes FAT.

- Solo admite los permisos de *COMPARTIR* (RECURSOS COMPARTIDOS)

Seguridad en Carpetas compartidas

Permisos de *SEGURIDAD*

- Solo en Volúmenes NTFS
- Garantizan el acceso a los Recursos Compartidos
 - Hay permisos de Seguridad asociados a
 - *CARPETAS*
 - *FICHEROS*

Seguridad en Carpetas compartidas

Diferencia entre *COMPARTIR* y *SEGURIDAD*

- *COMPARTIR*:
 - Afecta a los usuarios remotos pero no a los usuarios que inician sesión local
- *SEGURIDAD*:
 - Afectan a todo el sistema incluidos los usuarios locales

Seguridad en Carpetas compartidas

ARCHIVOS:

- Control Total
- Modificar
- Lectura y Ejecución
- Leer
- Escribir

CARPETAS:

- Control Total
- Modificar
- Lectura y Ejecución
- Listar el contenido de la carpeta
- Leer
- Escribir

Seguridad en Carpetas compartidas

• Permisos NTFS de *CARPETAS*

- Control Total
 - Permite cambiar permisos
 - Tomarla en propiedad
 - Eliminar ficheros y subcarpetas
 - Además de los siguientes permisos
- Modificar
 - Permite eliminar carpetas y ficheros
 - Modificar carpetas y ficheros
 - Además de los siguientes permisos
- Lectura y Ejecución
 - Moverse a través de las carpetas y ficheros
 - Ejecutar aplicaciones
 - Además de los siguientes permisos

Permisos NTFS sobre Archivos

ARCHIVOS:

- Control Total
 - Cambiar permisos sobre el fichero
 - Tomar posesión del mismo
 - Además de los siguientes permisos
- Modificar
 - Modificar y eliminar ficheros
 - Además de permisos de Lectura/Ejecución y Escribir
- Lectura y Ejecución
 - Ejecutar aplicaciones y permisos de Leer
- Leer
 - Leer el fichero y sus atributos
- Escribir
 - Escribir en el fichero
 - Cambiar sus atributos y ver permisos

Seguridad en Carpetas compartidas

Permisos NTFS de *CARPETAS*

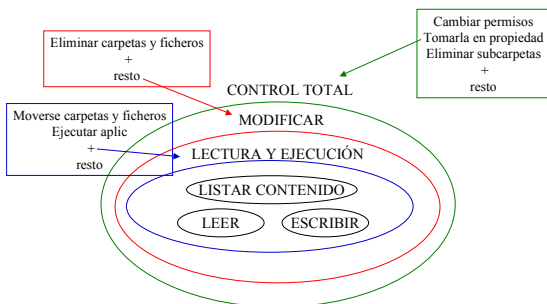
- Listar el contenido de la carpeta
 - Ver el nombre de los ficheros y subcarpetas
- Leer
 - Ver ficheros y carpetas
 - Sus atributos: oculto, sistema, etc
- Escribir
 - Crear nuevos ficheros
 - Nuevas subcarpetas
 - Cambiar los atributos de las carpetas
 - Ver los permisos aplicados

Seguridad en Carpetas compartidas

Aspectos a tener en cuenta con estos permisos:

- Leer
 - Es el único necesario para ejecutar Scripts
 - Es necesario para crear acceso directo
- Escribir
 - Puede borrar el contenido del archivo aunque no puede borrar el archivo
- Control total
 - Puede eliminar los archivos independientemente de los permisos que tuviesen

Permisos NTFS de *CARPETAS*



Donde se pueden crear Carpetas compartidas

Hay dos formas de compartir carpetas

- Carpetas locales
 - Equipo local (Estación de trabajo)
- Carpetas remotas
 - Equipo remoto
 - Generalmente un servidor de ficheros

Quien puede crear Carpetas compartidas

Carpetas de un servidor

- Se debe pertenecer a uno de los siguientes grupos:

- Administradores
- Operadores de servidores

Carpetas en una estación de trabajo

- Se debe pertenecer a uno de los siguientes grupos:

- Administradores
- Usuarios avanzados

Propiedades de cada tipo de permiso

- Opción 2. Admin. tienen control total. Usuarios solo LECTURA
 - Estos solo pueden ver los archivos y leer los datos
 - No pueden
 - Crear, Eliminar ni Modificar archivos ni carpetas

A quien se debe dar permisos en las Carpetas compartidas

Windows 2000 proporciona 4 opciones:

1. Todos los usuarios tienen control total
2. Administradores: Control total, otros Usuarios acceso de solo lectura
3. Administradores: Control total, otros Usuarios NO tienen acceso
4. Personalizar permisos

Propiedades de cada tipo de permiso

- Opción 3. Admin. tienen control total. Usuarios NO tienen acceso
 - Estos no tienen acceso
 - Se utiliza si se desea dar permisos más tarde
 - O para crear recursos compartidos por los administradores

Propiedades de cada tipo de permiso

- Opción 1. Todos los usuarios tienen control total
 - Todos los usuarios pueden realizar cualquier tarea
 - Crear
 - Modificar
 - Eliminar carpetas y ficheros
 - En NTFS además:
 - Derecho a cambiar los permisos

Propiedades de cada tipo de permiso

- Opción 4. Personalizar permisos
 - Por defecto todos tienen permiso de control total
 - Administradores
 - Usuarios
 - Resto de Usuarios (EVERYBODY)
 - Estos permisos se pueden personalizar
 - Distintos niveles desde MAS restrictivo a MENOS restrictivo

Propiedades de cada tipo de permiso

- Opción 4. Personalizar permisos
 - SIN ACCESO
 - No se otorga ningún permiso

Propiedades de cada tipo de permiso

- Opción 4. Personalizar permisos
 - CONTROL TOTAL
 - Todos los permisos de LEER y CAMBIAR
 - En NTFS:
 - Cambiar permisos de archivos y carpetas
 - Tomar posesión de archivos y carpetas

Propiedades de cada tipo de permiso

- Opción 4. Personalizar permisos
 - LEER
 - Ver los nombres de archivos y carpetas
 - Tener acceso a subcarpetas
 - Leer datos y atributos de archivos
 - Ejecutar archivos de programas

A quien se debe dar permisos en las Carpetas compartidas

- ☞ Carpetas personales (USUARIO):
 - Permiso de CONTROL TOTAL a usuario propietario del recurso
 - El resto de controles son a criterios del propietario del recurso
 - pero al menos debería proporcionar control de LECTURA
 - Para el grupo ADMINISTRADORES

Propiedades de cada tipo de permiso

- Opción 4. Personalizar permisos
 - CAMBIAR
 - Todos los permisos de LEER y:
 - Crear archivos y subcarpetas
 - Modificar archivos
 - Eliminar archivos y subcarpetas

A quien se debe dar permisos en las Carpetas compartidas

- ☞ Carpetas dedicadas (GRUPO):
 - Permiso de CONTROL TOTAL a los usuarios del grupo
 - El resto de controles son a criterios de los propietarios del recurso
 - pero al menos debería proporcionar control de LECTURA
 - Para el grupo ADMINISTRADORES

A quien se debe dar permisos en las Carpetas compartidas

- ☞ Carpetas Publicas (Abiertas a los usuarios del dominio):
 - Permiso de CONTROL TOTAL a todos los usuarios del dominio incluidos los ADMINISTRADORES

Conexión a unidades de red

- ☞ Se utilizan para ver un recurso compartido como si estuviese en el propio sistema
 - Windows Explorer (Mi PC) → Herramientas → Conectar a unidad de red
 - Con explorer localizar el recurso que se desea asociar (FOLDER) a la unidad de red que aparece en la ventana Driver

Creación de Carpetas compartidas

- ☞ Se utilizan las herramientas
 - *EXPLORADOR DE WINDOWS*
 - *ADMINISTRACIÓN DE EQUIPOS*
 - *Es necesario conectar con el equipo del que se desea compartir las carpetas*
 - *ADMIN. EQUIPOS → CONEX CON OTRO EQUIPO → SELECCIONAR EQUIPO*
 - *Expandir Herramientas del sistema → CARPETAS COMPARTIDAS*
 - *Seleccione NUEVO RECURSO*
 - *Rellenar los datos de carpeta*
 - *Especifique el tipo de cliente que accederá:*
 - *Microsoft, Netware, Apple*

Practica 3

Crear Carpetas compartidas en un volumen NTFS

Redes en Windows 98/2000

Unidades de red

Practica 3

- ☞ Estructura de los recursos compartidos NTFS
 - Al menos debe haber una carpeta para los distintos Grupos dentro del dominio y Usuarios además debe haber una pública con subcarpetas para que la puedan usar los invitados
 - Una carpeta con aplicaciones ejecutables
 - Cada alumno debe crear su estructura y asignar los permisos que crea convenientes de acuerdo con las necesidades de cada uno de los grupos

Practica 4

Crear Carpetas compartidas en un volumen FAT 32

Conexión a unidades de red

- ☞ Asociar, en las estaciones cliente, los recursos compartidos en el dominio a unidades de red

Practica 4

- ☞ Estructura de los recursos compartidos FAT
 - Al menos debe haber una carpeta para los distintos Grupos dentro del dominio y Usuarios además debe haber una pública con subcarpetas para que la puedan usar los invitados
 - Una carpeta con aplicaciones ejecutables
 - Cada alumno debe crear su estructura y asignar los permisos que crea convenientes de acuerdo con las necesidades de cada uno de los grupos

Practica 5

Describir las diferencias entre practica 3 y 4

Practica 4

- ☞ Posibles criterios
 - Los Adm. Control total
 - La carpeta de Aplicación
 - ☞ Ejecutar programas pero no modificar los archivos
 - Solo los miembros de un grupo tendran acceso total al grupo
 - Solo el usuario tendra acceso al recurso de su propiedad
 - Todos los usuarios tendran acceso a la carpeta publica pero no a las subcarpetas de los otros usuarios

Verificación de recursos usados en el dominio

- ☞ El administrador puede saber y controlar los recursos que los usuarios estan usando en un momento determinado
 - Averiguando las conexiones actuales
 - Computer Manager → Carpetas Compartidas → Sesiones

Verificación de recursos usados en el dominio

- ☞ Obtiene la siguiente información
 - Equipo ó Usuario:
 - Los nombres de equipos tienen el sufijo \$ para diferenciarlos de usuario
 - Equipo
 - Dirección IP del equipo
 - Tipo
 - Tipo de equipo utilizado
 - Conectado (Time)
 - Invitado
 - Si ha entrado como invitado u otra cuenta de usuario

Utilización de impresoras

- ☞ En una red hay dos tipos de dispositivos de impresión
 - De impresión local
 - Conectado físicamente a un equipo
 - Utilizado solo por los usuarios de ese equipo
 - De impresión en red
 - Configurado par acceso remoto
 - Conectado a:
 - Un SERVIDOR DE IMPRESIÓN
 - RED directamente con tarjeta adaptadora de red

Desinstalar Active Dir. en Serv.

- ☞ Desinstalar Act. Dir:
 - Se ejecuta el mismo comando que para instalar:
 - desde INICIO→ejecutar→cmd:"dcpromo" <aceptar>
 - Dos situaciones:
 - Existe más de un controlador de dominio
 - El servidor pasa a ser un servidor miembro del dominio pero sin ser controlador
 - NO Existen más controladores de dominio
 - La red se queda sin controladores de dominio por lo que se pierde la facultad de Active Directory → *no hay nadie que valide el acceso de usuarios.*

Servidor de impresoras

- ☞ Es un equipo que controla una o varias impresoras conectadas a red
 - Impresión en Red
 - Objetivos
 - Compartir el dispositivo
 - Manejar la cola de impresión

Redes en Windows 98/2000

Servidor de Impresión
3.4

Servidor de impresoras

- ☞ Como instalar una impresora en red
 - Inicio --> printers → añadir impresora

Configuración de propiedades

☞ Seleccionar Impresora → Propiedades

- Dar nombre a la impresora
- Compartir y asociar un nombre con el que verán la impresora
- Asociar mecanismos de seguridad como a las carpetas
- Seleccionar el puerto usado
- Disponibilidad
- Configurar características de impresión

Permisos sobre impresoras

☞ Tres permisos

- Imprimir
 - Permiso de conexión y envío de documentos
- Administrar impresoras
 - Imprimir y control de tareas administrativas
 - Parar, eliminar impresora, compartir, ajustar los permisos...
- Administración de documentos
 - Detener la impresión de un documento, reanudarla, reiniciarla y cancelar documentos enviados por otros usuarios
 - NO puede enviar documentos ni controlar su estado

Configuración de propiedades

☞ Incluir otros controladores para clientes

- Disponibilidad de otros controladores de impresora
 - Permite imprimir desde otro S.O. Distinto al que posee el servidor de impresoras
 - Permite a los usuarios descargar el controlador que necesita en función de su S.O.
- Seleccionar Impresora → Propiedades
 - Compartir (Add Drivers)